CYBER DISOBEDIENCE AS A NEW FORM OF CIVIL DISOBEDIENCE

JUDr. Rudolf Kasinec, PhD. [1] **& Mgr. Ján Šurkala**[2]

The civil disobedience is a traditional method of political protest emerged within civil society.[3] In general, the basic features of the notion are violation of law, nonviolent nature of action,[4] publicity and acceptance of a legal sanction.[5] In the last two decades, there emerged a new form of civil disobedience, which has rather different specific signs, namely anonymity, realisation in cyberspace and avoidance of legal punishment. We may label this form of modern protest as cyber disobedience.

In this short paper we aim to compare these two concepts in order to draw a basic outline of a future development with specific focus on globalisation and emergence of postmodern tendencies to subvert sovereign states and their legal orders.

[1] Assisstant Professor, Comenius University in Bratislava, Faculty of Law, Department of Theory of Law and Social Sciences. Postal Address: Šafárikovo nám. 6, P.O.BOX 313, 810 00 Bratislava 1, Slovakia, EU. e-mail: rudolf.kasinec@flaw.uniba.sk

[2] PhD. student, Comenius University in Bratislava, Faculty of Law, Department of Roman law, Cannon and Ecclesiastical Law. Postal Address: Šafárikovo nám. 6, P.O.BOX 313, 810 00 Bratislava 1, Slovakia, EU. e-mail: jan.surkala@flaw.uniba@gmail.com

[3] It is generally believed that the notion of civil disobedience has firstly occurred in famous classical piece of political writhing of Henry David Thoreau. Compare: Thoreau, H. D.: Resistance to Civil Government: A Lecture delivered in 1847. In: Peabody, E. P. (ed.): Aesthetic Papers, Boston & New York: The Editor & G. P. Putnam, 1849, pp. 189-211.

[4] Non-violent feature of the civil disobedience is contested by some authors. Cf. Moraro, P.: Violent Civil Disobedience and Willingness to Accept Punishment. In: Essays in Philosophy - A Biannual Journal, 2007, Vol. 8, Issue 2, Article 6; Morreall, J.: The justifiability of violent civil disobedience. In: Canadian Journal of Philosophy, 1976, Vol. 6, No. 1, pp. 35–47. Others consider violent civil disobedience as possible but unjustifiable. Cf: Bayles, M.: The Justifiability of Civil Disobedience. In: Review of Metaphysics, 1970, Vol. 24, No. 1, pp. 17-18; Brown, S. M.: Civil Disobedience. In: The Journal of Philosophy, 1961, Vol. 57, Issue 22, p. 678; Martin, R.: Civil Disobedience. In: Ethics, 1970, Vol. 80, No. 2, pp. 135-137.

[5] Compare: Bedau, H. A.: On civil disobedience In: The Journal of Philosophy, 1961, Vol. 58, No. 21, p. 656.

1. The New Situation in Cyber Space

"The rules of cultural and political resistance have dramatically changed. The revolution in technology brought about by the rapid development of the computer and video has created a new geography of power relations in the first world that could only be imagined as little as twenty years ago: people are reduced to data, surveillance occurs on a global scale, minds are melded to screenal reality, and an authoritarian power emerges that thrives on absence. The new geography is a virtual geography, and the core of political and cultural resistance must assert itself in this electronic space."[1]

The cyber space is a strange territory in which a small group of people may influence a public opinion in large scale expending relatively little of time and money. This natural ability of virtual space brings enormous potential of positive civil actions, enable such needed social networking between various individuals and groups and finally yet importantly cultivate public discussion and promotion of democracy as an open system of government.

On the other hand, it is frequently misused for manipulation with public opinion, dissemination of pure lies, which are manifestly disapproved only with high costs, or for direct subversion of democratic societies by non-democratic foreign or domestic structures.

In addition to that, social networks are perfect tools for organization various forms of civil disobedience and for realization of cyber disobedience. Large groups of people may disable internet sites of state authorities, business companies, political parties and many other important institutions with the aim of expressing their political or ideological believes and personal convictions.

The cyber space is also a platform for performance of traditional forms of the civil disobedience. In this way it may operate as a starter or catalyser of the traditional forms of civil disobedience. For example, it may enable easier mobilisation of conventional protests or sitdown strikes, better coordination and protests management or significantly swifter and more effective networking of already mobilised actors.

The cyberspace is one of the most free and unregulated areas in the world, even though it is only virtual space. Its virtual character, however, does not lower its importance in the lives of post-modern people, who spent a huge portion of their daytime there. Therefore it is essential that states and other public authorities have to

[1] See: Critical Art Ensemble, [http://www.critical-art.net/books/ted/ted1.pdf] 3.3.2017.

perform positive actions[1] in order to ensure that cyber space will not metamorphose to an area of lawlessness and unrestricted criminal and amoral practices.

The main object of our current research – the hacktivism – operates in so-called grey zone, while its compliance with law as well as their legitimacy may occur dubious. Hacktivists fight for freedom or for other "higher values", but they break "smaller rules", which, however, may result in serious consequences and unwanted side-effects. In the case of hackers' attack it is malfunction of important websites of public authorities, banks, bourse or other corporations etc., which targets not only directly attacked institutions but have serious negative impacts on ordinary users of attacked websites. And here the true problem with hacktivism lies – where is a borderline between hacktivism and cyber terrorism? Alternatively, are these two concepts identical?

2. Traditional Forms of Civil Disobedience

Civil disobedience was important symbol of human rights movement in the 20th century. By the words of John Rawls the civil disobedience is an act essentially political. Firstly, it is addressed to majority which holds political power, and secondly its legitimisation is secured by reference to principles of justice – which he considers to be dominantly political value. Personal believes of a "disobedient" certainly plays some role in it, but one cannot speak about civil disobedience when there is involved only self-interest of certain group or individual.[2] However, particular interests of social and political players – such as workers, races, gender etc. – are very often main causes of civil disobedience. On the other hand, they are always to change some public policy.

Actions committed under the civil disobedience are always violating law, but they are usually nonviolent.[3] As noted by Lawrence Quill, the civil disobedience has started to be widely accepted as a tool for reaching progress in liberal democracies as early as in 60s.[4]

John Rawls defined conditions of civil disobedience as follows:

1) Intentional breaching of a law;
2) Nonviolent nature of the action;

[1] For more about this see: Daňko, M.: The internet in reflection of human rights and fundamental freedoms. In: Communication as a measure of protection and limitation of human rights. Information in relation to human rights, Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2013, pp. 658.
[2] Cf. Rawls, J.: Theory of justice. Revised Edition. Cambridge: Harvard University Press, 1999, p. 321.
[3] For concurring opinions see note 4 above.
[4] Cf. Quill, L.: Civil Disobedience: (Un)Common Sense in Mass Democracies. Hampshire: Palgrave Macmillan, 2009, p. 2.

3) Public action with fair notice given;
4) Willingness to accept a legal consequences (punishment);
5) Aimed to change a law or policy of a government;
6) Addressed to the majority's sense of justice;
7) Addressed to a sense of justice that is mainly incorporated in the law and social institutions.[1]

The civil disobedience – likewise the most of the social and legal institutions – is also subject of change and dynamic. "In a sense there simply is no single agreed-upon concept of civil disobedience that has proven stable over the course of time. There is no undisputed and undisputable account of what civil disobedience can and cannot involve."[2] In last few decades, there occurred significant transformation of traditional (modern) concept of civil disobedience. The cyber disobedience is one of these current tendencies, which cannot be overlooked.

3. The Concept of Hacktivism as a Form of Cyber Disobedience

Cyber disobedience is usually identified with a term hacktivism. "Hacktivism is the convergence of hacking with activism, where 'hacking' is used here to refer to operations that exploit computers in ways that are unusual and often illegal, typically with the help of special software ('hacking tools'). Hacktivism includes electronic civil disobedience, which brings methods of civil disobedience to cyber-space. (…) Because hacking incidents are often reported in the media, operations in this category can generate considerable publicity for both the activists and their causes."[3]

As we has already mentioned above, there is growing importance of the cyber space in the contemporary world. Governments and global organizations (as well as private International Corporations) aim to control this area both by legal and extra-legal means. This "interference" of the public authorities and by them protected corporations is in striking contrast with the free character of the internet as is inborn in its very nature.

The cyber disobedience and hacktivism have firstly occurred at the end of 20th century. The Critical Arts Ensemble (CAE)[4] issued in 1996 a call for bringing a direct political action and civil disobedience to virtual space whereas it has become new

[1] Cf. Rawls, J.: Theory of justice, pp. 320-323.
[2] Cf. Milligan, T.: Civil Disobedience Protest, Justification, and the Law. London: Bloomsbury Academic, 2013, p. 13.
[3] Cf. Denning, D. E.: Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In: Arquilla, J. & Ronfeldt, D. F.: Networks and Netwars: The Future of Terror, Crime, and Militancy, Pittsburgh: RAND. 2001, p. 263.
[4] For more about this organisation see: [http://critical-art.net] 23.3.2017

space for elites to shift power. The means of this action shall be tactical blockades focused on flow of cyber-spatial information.[1]

However, in practice we can distinguish various activities aimed to reaching this goal. For example, it is online sabotage, which may range from distributed-denial-of-services (DDoS attracts) to harsher attacks on servers causing their overloading by directing overwhelming amount of information to particular websites and infiltration of computer system. Finally, hackers may also take control over the websites in order to reach their political targets.[2]

Specific feature of hacktivism is pubic demonstration of ability to disrupt proper function of targeted objects. Thus the publicity of the act is not only to intimidate those "who are in power", but it is also to create an approval of wide masses of internet users who may be part of broader "anti-systemic" identity. Paradoxically, this common identity is accompanied by anonymity.[3] Thus the group is well aware is its aims, tools for their reaching and actual power, but in same time the true identity of its members is not revealed.

The important role in advertisement of this kind of actions is played by current pop-culture. The movie V for Vendetta[4] was created in 2005 and two years before hackers group the Anonymous, who directly described themselves as hacktivists, had started their activities. Members of this "secret" cyber community choose their main symbol – the mask of Guy Fawkes[5] in style portrayed in graphic novel and later movie V for Vendetta. Main character in this movie fights against state regime in the dystopian Great Britain, but he uses violence as his main weapon (terrorist attacks, killing main state officials and exposure of state secrets). His action has fundamental influence to citizens and a large group of dissenting people choose a way of nonviolent civil disobedience (final scene of the movie).

[1] Jordan, T.: Activism! direct action, hacktivism and the future of society. London: Reaction Books, 2002, p. 120.

[2] Cf. Shantz, J., Tomblin, J.: Cyber Disobedience: Re://Presenting Online Anarchy, Washington: Zero Books. 2014, p. 10.

[3] Cf. Milligan, T.: Civil Disobedience Protest, Justification, and the Law, p. 4.

[4] For more about this interesting piece of cinematography see: [http://www.imdb.com/title/tt0434409/] 23.3.2017

[5] Guy Fawkes is a real historical figure of the Catholic terrorist who prepared failed attempted to blow-up English Houses of Parliament in 1605 in so-called Gunpowder Plot. For more about this person and the plot see: Fraser, A. The Gunpowder Plot: Terror And Faith In 1605. London: Hachette, 2010; Kenneth, A.: The Story of Gunpowder. London: Wayland, 1973.

4. Real Implications of Cyber Disobedience in the Contemporary World

Members of the Anonymous,[1] with 'V' mask on their faces, fight against state policies, international monopolies, security agencies and others corporations, individuals, businesses etc. Nevertheless, it is difficult to decide which form of protest is conducted by the Anonymous through these activities. It is either some form of the cyber disobedience – i.e. legally doubtful but more or less legitimate action – or it is criminal activity performed as the cyber terrorism and in that case it is clearly illegal, immoral and illegitimate.

Actions of the Anonymous – as well as of other cyber hacktivist groups – may appear to be rather hectic, disorganized, or even random from the point of view of an outside observer. However, they actually apply a wide range of organizing practices with their own internally functional methods of organizing, which are invisible for "outsiders".[2] That is caused by the absence of any firm hierarchical and command structures, which has to have every mainstream political or corporal body. Similarly, there is a lack of ordinary leadership positions or roles, schemes of authority, subordination, etc. Frequently, the decisions are made with participation of a whole body of members with wide range of autonomy of individuals or small units within the community, if they want to take responsibility for their own actions. That opens a space for trust and cooperation within these smaller operative unites.[3]

There is also not clear borderline between the cyber disobedience and extremism (including various forms of intolerance). The fresh case from Slovakia: a young woman expressed her political opinion about Islamism in very radical manner. She pissed on the Quran – the holiest symbol of Muslim faith – then she tore it to pieces, floated it with gasoline and flamed it at the end. She, of course, created video record of the whole procedure and published it on the internet.[4]

The Slovak law enforcement authorities commenced the criminal prosecution against her, while the Penal Code defines this sort of activity as a criminal act of manufacturing of extremist materials (výroba extrémistických materiálov) [5] in connection with a violence against a group of inhabitants (násilie proti skupine obyvateľov)[6] as well as defamation of nation, race and belief (hanobenie národa, rasy

[1] See Anonymous official site: [http://anonofficial.com/] 23.3.2017. The motto of this group is: "We are legion. We do not forgive. We do not forget. Expect us."
[2] Squire, J.: Anonymous and the future of hacktivism. In: Socialist Alternative Magazine [http://sa.org.au/node/1177] 5.3.2017.
[3] Shantz, J., Tomblin, J.: Cyber Disobedience, p. 14.
[4] For basic information of this case see: [http://metro.co.uk/2017/02/16/woman-films-herself-urinating-on-koran-before-setting-it-on-fire-6451744/] 23.3.2017
[5] Cf. § 422a of the Slovak Penal Code (Act No. 300/2005 Coll.).
[6] Cf. § 359 TZ thereof.

a presvedčenia)[1] and incitement of national, racial and ethnic hatred (podnecovanie k národnostnej, rasovej a etnickej nenávisti).[2] The potential punishment for this criminal conduct is imprisonment from 3 to 6 years.

This case is a clear example of the misuse cyberspace with the ill-aim to draw a public attention to message of somebody, who can spread the ideas of hate and discrimination.

5. The Features and Definition of Cyber Disobedience

The cyber disobedience and hacktivism are brand new concepts, which were built on basis of traditional civil disobedience. It is important to find differences between old and new meaning of disobedience. Both concepts exist side by side, but cyber disobedience and its importance rapidly growing in last few years. Specific features of cyber disobedience are:

a) **Anonymity.** Indeed, the public audience do not know true identity of people who stands behind the concerned activities. We can see only people in masks with symbols of hacktivist groups. Jordan and Taylor say that "hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaches out of cyberspace utilising virtual powers to mould offline life."[3]
b) **Activities violating law.** Almost all activities, which fall into the scope of cyber disobedience contradicting the law in some way. However, two important notes are relevant here. Firstly, the illegality of cyber disobedience is mostly caused by attempts of government to erase public disobedience from the virtual space. The existing rights to protest and resist against ill-acts of public authorities and by them protected big corporations are not sufficiently secured.[4] Secondly, the illegality is, however, balanced by practical inability to prosecute this "crimes". We have strong suspicion that this two fact correlates – by the other words, the global civil society does not feel pressing need to secure the legalisation of cyber disobedience while it is almost unpunishable.
c) **Large scale of interests.** There may be various interests – form politics, ecology, economy, corporation policy, labour conditions, local politics and many others – which may be targeted by the cyber disobedience. We may label the hacktivism as "anti-globalisation movement, whose methods can easily be

[1] Cf. § 423 TZ thereof.
[2] Cf. § 424 TZ thereof.
[3] Jordan, T., Taylor, P.: Hacktivism and Cyberwars Rebels with a cause? New York: Routledge. 2004, p. 1.
[4] Shantz, J., Tomblin, J.: Cyber Disobedience, p. 22.

described as viral and whose targets are often the immateriality, the virus-like nature, of millennial socio-economies."[1]

d) Specific forms of nonviolence actions:

1. **Virtual Sit-Ins and Blockades.** Its Purpose is analogical to occupational strikes – i.e. to call public attention to the protestor´s causes by disrupting a normal operation and blocking access to facilities.[2]
2. **E-mail Bombs.** It is a sort of blockade aimed to disrupt the ordinary operation of e-mail of a targeted institution. This serious restriction of rights of ordinary citizens or customers is excused by hacktivists saying that their legitimate e-mails would be glossed over, if they send only one regular e-mail even each day.[3]
3. **Web Hacks and Computer Break-Ins.** By this type of hacking activity it is possible to change the content of targeted website or redirect its users to alternative websites.[4] The main goal of this is to provide the users with some message important for protesters.
4. **Computer Viruses and Worms.** It is probably the most invasive tool of hacktivists. The aim is to cause some serious damage to targeted computer systems and websites by which they want to spread the message of the protest.[5]

e) **Realisation in virtual area – with all its specifics.**[6]

f) **Non-acceptance of any kind of punishment.** This goes hand in hand with anonymity. Main leaders of the traditional civil disobedience – such as Ghandi, M. L. King, D. Thoreau, Aung San Suu Kyi[7] – suffered in prison for days, weeks, months or years. The anonymity guaranteed for members of hacktivist group secures absentio of any kind of punishment. We can say that they are protected through internet anonymity. In reality, they hold no responsibility for their actions against any target regardless that the law declares their activities as illegal and criminal and impose serious punishment on them.

---

[1] Jordan, T., Taylor, P.: Hacktivism and Cyberwars Rebels with a cause? p. 39.
[2] Denning, D. E.: Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy, p. 264.
[3] Ibidem, p. 268.
[4] Ibidem, p. 272 - 273.
[5] Ibidem, p. 278.
[6] Bryant, R.: What Kind of Space is Cyberspace? In: An Internet Journal of Philosophy, Vol. 5, 2001, pp. 138–155. [http://www.minerva.mic.ul.ie/vol5/cyberspace.pdf] 3.3.2017.
[7] Political activist in Burma, who remained under house arrest for almost 15 of the 21 years from 1989 to 2010, become one of the world's most prominent political prisoners. More information about these remarkable woman you can find in Luc Besson's 2011 film The Lady, or from her books: Freedom from Fear: And Other Writings (2010), Letters from Burma (2010), Aung San Suu Kyi, Voice of Hope: Conversations with Alan Clements (2008).

6. Purposes of Cyber Disobedience

There is indeed thin borderline between a cyber terrorism, a cyber-criminal activity and a cyber disobedience. The participants of cyber disobedience have honourable purposes. They want to draw attention of the other people, citizens, civil society members, chosen groups of society to various problems in the contemporary world.

In our opinion, cyber disobedience is the new form of civil disobedience. A civil society and her actors are changed and political and legal processes have to change respectively. Society and its normative orders have to be adapted to different attitudes of particular social groups which have very effective tools provided due to enormous technological progress of recent years. As we have already pointed out above, repression and attempts to supress these tendencies by means of national criminal law are vastly infective. Moreover, the legitimacy of this state policies are more that dubious.

Therefore we prognose that this disparity will be reversed either by more effective cooperation between national states and international organisations with aim to create effective countermeasures against "cyber criminality" as defined nowadays, or that the definition of illegal cyber activities will be narrowed and most of deeds currently falling into the concept of cyber disobedience will be fully legalised and regulated by law.

The better prognose we give to the second scenario. This is partially confirmed by J. Squire – the former member of the hacker group LulzSec – who said in 2013: "Online activism and hacktivism will, undoubtedly, increase in the future. Partly, this is because of the ongoing attempts by governments and corporations to clear the online commons and the response that will be required to assert the rights of internet users against these encroachments. Partly, it is because the online space is becoming increasingly important as an organising forum for protest movements. Partly, it is because governments and corporations – the very targets of the left and protest movements – operate more and more online and, thus, are vulnerable to online activism."[1]

We can hear about hacktivists' activities permanently, but their actions are on the edge of public interest nowadays. A fight for political interests has changed territory, where it is primarily conduct – from streets and squares, front pages of newspapers, political declaration, and civil protest banners to the brand new area of the cyber space. It is space without strictly conventions, physical forms of violence and mostly without rules, but with new opportunities, mass population and voluntary

[1] SSquire, J.: Anonymous and the future of hacktivism.

publicity. In the current state of affairs, information have great value and therefore the cyberspace is one of the most important territories on the globe.

Bibliography :

1. Arquilla, J., Ronfeldt, D. F.: Networks and Netwars: The Future of Terror, Crime, and Militancy. Pittsburgh: RAND. 2001, ISBN-13: 978-0833030306.

2. Bayles, M.: The Justifiability of Civil Disobedience. In: Review of Metaphysics, 1970, Vol. 24, No. 1, pp. 3-20.

3. Bedau, H. A.: On civil disobedience In: The Journal of Philosophy, 1961, Vol. 58, No. 21, pp. 653-665.

4. Brown, S. M.: Civil Disobedience. In: The Journal of Philosophy, 1961, Vol. 57, Issue 22, pp. 669-681.

5. Bryant, R.: What Kind of Space is Cyberspace?. In: An Internet Journal of Philosophy, Vol. 5, 2001, pp. 138–155. [http://www.minerva.mic.ul.ie/vol5/cyberspace.pdf] 3.3.2017.

6. Critical Art Ensemble. [http://www.critical-art.net/books/ted/ted1.pdf] 3.3.2017.

7. Daňko, M.: The internet in reflection of human rights and fundamental freedoms. In: Communication as a measure of protection and limitation of human rights. Information in relation to human rights. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2013, pp. 657-660. ISBN 978-80-7160-345-0.

8. Denning, D. E.: Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. In: Arquilla, J. & Ronfeldt, D. F.: Networks and Netwars: The Future of Terror, Crime, and Militancy, Pittsburgh: RAND, 2001, ISBN-13: 978-0833030306.

9. Fraser, A. The Gunpowder Plot: Terror And Faith In 1605. London: Hachette, 2010. ISBN 9780297857938

10. Jordan, T.: Activism! direct action, hack tivism and the future of society. London: Reaktion Books, 2002, ISBN 1 86189 122 9.

11. Jordan, T., Taylor, P.: Hacktivism and Cyberwars Rebels with a cause?. New York: Routledge, 2004. ISBN 0-203-56995-4.

12. Kenneth, A.: The Story of Gunpowder. London: Wayland, 1973. ISBN 0853401888

13. Martin, R.: Civil Disobedience. In: Ethics, 1970, Vol. 80, No. 2, pp. 123-139.

14. Milligan, T.: Civil Disobedience Protest, Justification, and the Law. London: Bloomsbury Academic, 2013. ISBN-13: 978-1441132093.

15. Moraro, P.: Violent Civil Disobedience and Willingness to Accept Punishment. In: Essays in Philosophy – A Biannual Journal, 2007, Vol. 8, Issue 2, Article 6. [http://commons.pacificu.edu/cgi/viewcontent.cgi?article=1277&context=eip] 23.3.2017

16. Morreall, J.: The justifiability of violent civil disobedience. In: Canadian Journal of Philosophy, 1976, Vol. 6, No. 1, pp. 35–47.

17. Quill, L.: Civil Disobedience: (Un)Common Sense in Mass Democracies. Hampshire: Palgrave Macmillan, 2009. ISBN-10: 0–230–55505–5.

18. Rawls, J.: A Theory of justice. Revised Edition. Cambridge: Harvard University Press, 1999. ISBN 0-674-00078-1.

19. Shantz, J., Tomblin, J.: Cyber Disobedience: Re://Presenting Online Anarchy. Washington: Zero Books, 2014. ISBN 978 1 78279 556 8 [e-book].

20. Squire, J.: Anonymous and the future of hacktivism. In: Socialist Alternative Magazine [http://sa.org.au/node/1177] 5.3.2017.

21. Thoreau, H. D.: Resistance to Civil Government: A Lecture delivered in 1847. In: Peabody, E. P. (ed.): Aesthetic Papers, Boston & New York: The Editor & G. P. Putnam, 1849, pp. 189-211. [https://archive.org/stream/aestheticpapers00peabrich#page/n220/mode/1up] 23.3.2017

The authors address the problem of cyber disobedience and hacktivism in contemporary world. Firstly, they try to distinguish cyber disobedience from the traditional forms of civil disobedience. The main differences they see in avoidance of punishment for illegal conduct, exercising these activities in the cyber space and specific nature of "non-violence", which is at least disputable. They put to the correlation the anonymity of the actions and avoidance to accept the punishment for criminal deeds. They argue that the status quo – where virtually all acts of hacktivism are considered to be illegal and in the same time very little of such acts are punished – conserved the strange equilibrium. However, they prognose that the importance of cyber disobedience will grow in the near future and this movement should be followed by proper changes of the law in action.

Key words: *protests, civil society, cyber space, anonymity, hacktivism, cyber disobedience, cyber terrorism, the Anonymous, pop-culture.*