Asian Social Science; Vol. 10, No. 18; 2014
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

Subculture of Hackers in Russia

Roman Dremliuga[1]

[1] School of law, Far Eastern Federal University, Vladivostok, Russia

Correspondence: Roman Dremliuga, School of law, Far Eastern Federal University, Vladivostok, Russia. Tel: 79-1-4707-1474. E-mail: dremliuga.ri@dvfu.ru

Received: June 12, 2014 Accepted: August 4, 2014 Online Published: August 22, 2014

doi:10.5539/ass.v10n18p158 URL: http://dx.doi.org/10.5539/ass.v10n18p158

Abstract

This article observes the situation with hacker subculture in Russia. The author is analyzing the reasons why this subculture doesn't need a lot of time to conquer Russian net society. He is proving that tremendous growth of popularity of hacker subculture in Russia is caused by easy acceptance of hacker's ideology. Also, the author is studying modern functions of hacker subculture and researching why Russian society does not regard hackers as criminals.

Keywords: hacker, hacker subculture, cyber society, hacker ideology

1. Introduction

Nowadays the Internet is not just a means of mass communication but the phenomenon that spread in all spheres of a human life. Many processes are transferred from the real world to the virtual space. The Global net provides conditions to forming of new net societies, generates kinds of slang unknown before, erases the borders between states and, finally, causes new forms of culture.

It seems that in addition to the positive effect of the Internet; it contains a number of negative sides, brings some harm and leads to negative consequences. Some features of this technology, which helped it to spread throughout the world, at the same time provide opportunities for many types of criminal activity. The novelty of the social relations that have arisen as a result of the Internet, and the lack of appropriate legal framework relating to this technology, have led to a variety of issues affecting relations on development of global computer network. Probably the most famous problem of the modern Internet is hackers.

It raises concerns that the tremendous technical strength and limitless power of the Internet is increasingly in modern conditions can be used for criminal purposes. In this case, the Internet, on the one hand, led to more efficient and with impunity pre-existing traditional crime, on the other hand, it has generated new and unknown to the world community until recently kinds of socially dangerous attacks. Global network in recent years began to be used not only for ordinary crimes, but also for extremely dangerous acts of international importance-such as "Internet war", "Internet terrorism", "Internet strike" that threaten security of entire nations and the world community.

The possibility of committing a socially dangerous act directly through the Internet itself has changed its quality: due to the global network the crime has become anonymous, remote in space, cross-border, global. Internet isolated location of the criminal acts and the place of the consequences, and also made detection, suppression and prosecution of crime are extremely difficult, and in some cases impossible.

Some researchers mention that the community of the Internet users represents a special subculture that is grounded on information liberalism (Smirnova, 2000). And hackers are just a radical group of this subculture that can commit a crime to achieve information freedom. We describe a subculture as an integral formation inside the mainstream culture that differs in a value system, customs and accepted standards (Denisov, 2002). Also a subculture is a system of standards, traditions, maxims, traditions, customs and outward attributes that are provided by some social group of people united by common interests and supported by all members of this social group. In our opinion, the concept of subculture is relative because every subculture can be researched only as a part of wider subculture.

2. Discussion

If we survey outward side of hackers, we will conclude that hackers are not united subculture, because they have different specializations (for example, virus writers, phreakers, crackers etc.) with different slang, appearance and methods of hacking. It seems there are many subcultures, not only one, but if we pay attention to value system, norms, behavioral models, main ideas and conceptions, it will apparently be one subculture.

The first basis of hacker subculture, as it was mentioned above, is the liberalization of information access. Like famous hacker Mentor said, that hackers are not criminals but researchers. They just want to provide free access to information and believe that every data will be opened for all humanity. He claims that world of free computer information is much better than ours. (Mentor, 1986). This idea is supported among most people of the net community; even in China where liberalization concept is not widely spread, there is a new tendency of free covering the main state events by the Internet (Qiang, 2003).

The second thesis of hacker subculture is their rejection of consumer culture. This is evidenced by the extract from «Let's crack the slave-masters» (very spread in the Internet), written under the pseudonym of hacker «Orc +», which is filled with hatred for the existing social order. Call to combat consumer society repeats the ideology of other youth subcultures, which makes this even more popular subculture. Thus, similar lines can be found in many lyrics of rock groups, and rock music is popular among young people. Denial of consumer culture and opposition to the existing society is a part of many other youth subcultures such as hippies, punks, rockers, etc., all of which support the so-called anti-consumerism movement against the culture of consumption.

The third important aspect of ideology is the belief in the ability of the computer to make a difference; rejection of any authority and denial of racial, religious and social differences. All hacker's life: work and leisure, music, books and movies, is somehow connected to the computer. As famous hacker Mentor + said, that hackers don't judge somebody by appearance, color of skin, cultural distinctions or political view. According his opinion people, who create nuclear weapon, unleash wars, put innocents in prisons, lie to society, unreasonably try to blame hackers (Mentor, 1986).

Subculture of hackers has some similar characteristics with common criminal subculture, but mostly has a lot of differences. Resembling features principally concern all subcultures. For example, all subcultures have own slang ("argo" in case of criminal subculture), have tradition to give nicknames for participants, have special signs (tattoo, dress code), own system of rules etc. Differences are expressed in a greater openness of subculture of hackers. According to our study nicknames in Russian criminal subculture mostly humiliate or degrade people, on the contrary hackers choose nicknames from books, movies and computer terminology. Probably, the main distinction is that criminals recognize their crimes as "crimes" (Tulegenov, 2003) but not like something good, as hackers do.

It is a fact that hacker subculture was the product of Western culture, and in Soviet Union there were no destructive subcultures which were widely-spread. When the Internet began to conquer Russian Federation in 90-s, on the one hand, some its values were extremely accessible for the reforming society, but, on other hand, were adapted with some difficulties. As some Russian authors claimed, any domestic youth subculture presents a more organic phenomenon than yielded by or borrowed one. Western models of subculture styles, rituals, and values in many cases were completely recycled and reanalyzed in accordance with peculiarities of Russian civilization and Russian mentality (Aliphapova, 2009).

The first impression is that in Russian society liberalization of information access was not perceivable idea but people were tied by long term communism propaganda and censorship. In 90-s authorities and society took up suggestion that freedom of information is the main value of any modern country (Bezborodov, 2010). And this ideological basis was in trend of soviet institute and ideology reformation. It was forbidden fruit of communistic era that generated great interest to this issue.

The idea of free sharing of information had other basis in Russian society. Before 90-s USSR had no institute of intellectual property like it was in Western Europe and USA, inventors could not sold the inventions to everybody, and they just got some modest compensation from the state. Even in 2000s Russian society didn't recognize value of intellectual property at all its aspects. For instance, according our studies of this issue in 2006, unlicensed software was used not only by individuals, but by entire organizations and institutions, including the state structures. All respondents from Russian courts, prosecutor office and police confessed that they cracked soft on their computers. Conversely, according to our questionnaire people who used licensed are perceived as "silly" persons.

It should be noted that the rejection of consumer culture has already existed in social ideology of the Soviet

Union because implied that wealth was not the main value for USSR nationals. Even more, to be rich meant to be unfair and marginal. Anti-consumerism was easily accepted by new Russian hackers.

Time when western culture became very popular was also in the 90-s, people liked to use western words, wear western clothes, and listen to western songs etc. (Grigorieva, 2012). Subculture of hackers provided all of it. Because hackers slang has mostly English words as basis, it became very popular in Russian computer society. Even now when we analyzed 112 Internet sites that host materials for hackers, we found that the "nicknames" of hackers wrote primarily in Latin alphabet; in 1000 identified "nicknames" only four were written by Russian alphabet (Dremliuga, 2007). In our opinion, this is due to several reasons. On the one hand, the Russian alphabet is not supported in all computer systems, on the other hand, Latin alphabet is used in the most programming languages and system file names of the most common computer operating systems (Windows, UNIX, etc.).

Usually every criminal subculture is a closed system; it has its own hidden, often dangerous values that are contrary to the mainstream system of values. Subculture of hackers is also a closed system, but the hacker values have a well-developed ideological basis, and it gives some legitimacy to hacker ideas, especially in Russia, where ideas of socialistic communities and common property are extremely natural for all society. For example, according to our studies 14,29 % of people who do not use the Internet, associate the hacker with «fighter for Internet freedom». The term «hacker» in Russia is not only used to show criminal propensity of personality, but also to emphasize its exceptional ability in the field of computer technology. Under our research, more than 90 % of professionals in the field of information technology and more than 50% of Internet users without computer education are considered primarily a hacker as high skilled programmer (Dremliuga, 2008). It should be noted that even some legal researchers supported and spread opinion that hackers are not dangerous (Baturin, 1991).

Some studies show us that Russian hackers have their own characteristics which are differ from hackers of other states. Russian hackers have due to the type of the common features of the cultural development of our country: the uncertainty of identity and the search for cultural identity; binary nature of existence and development of culture; collectivism consciousness that denies hierarchy; perception rule of law as an external, alien element; perception of the head of state as the protector of the people and the opposition of his bureaucratic structures (Vershinin, 2004).

Characteristic of the ambiguous attitude to the hackers-on the one hand, the identification of criminals, on the other-the desire to see a beginner hacker's creative impulse, requiring state and public support.

Even authorities didn't take them seriously. Imagine that in Russia magazine «Hacker» has been printed since 1999. Everybody can find a lot of hacker advice, descriptions of intrusions, and even promotion of hacker's soft in November 2013 issue of this magazine. Also magazine is provided with hacker soft DVD with computer programs for password cracking, video guidance of hacking etc. It would be difficult to imagine a "Pickpocket" magazine to go out regularly in Russia where there would be recommendations on how to avoid criminal liability, effectively commit crimes and where in the annex to the magazine would be blades for cutting purses. In fact, hackers are also criminals because in Russian Criminal code we have articles establishing criminal liability for illegal access (Article 272), spreading of malicious software (Article 273) etc., but nobody thinks that they are. The price of the above mentioning magazine in Russia is more than the price of other popular magazines such as «Cosmopolitan» or «Forbes»; it can be regarded as the evidence of extreme popularity of mentioned issue.

Moscow court of Tushino district sentenced one hacker just to two and a half years in prison; he committed hacker attack on the portal of "Aeroflot", held in 2010. Damage from the attack, which resulted in the sale of tickets has been blocked for several days, was more than 150 million rubles (it is near 4 million US dollars) (Ermakov & Voronetsky, 2013). Russian Criminal code permit to impose more severe punishment for such actions, but judge choose soft penalty. It sustains idea, that Russian courts also don't recognize hacker as dangerous criminals.

Subculture of hackers would not be so important for the cybercrime society if it did not perform many functions. The most significant for cybercrimes, in our opinion, are the following.

The first is the function of integration. The fact that hackers around the world have similar ideological attitudes, outlook to life and ways to make money, use the same books and slang terms, is a powerful unifying factor. Hackers can easily join international groups to commit socially dangerous acts, share professional information and tools.

The second is the function of legitimacy. Justification of Internet crimes in the eyes of others, and compliance with its moral and ethical guidelines provides an additional incentive to select a criminal way to achieve the objective. Absence of clear public condemnation for such wrongful conduct leads to a paradoxical situation where computer criminals do not hide, but show off their illegal achievements, are not afraid of responsibility, leave logos or slogans of hacking groups in the location of crime. In addition, as it was already said above, hackers do not call themselves criminals creating a romantic image of them.

The third is the function of sharing information. Ideological and instrumental information is distributed as a part of the subculture. In the hacker environment new ways and means of modern computer hacking are transferred. Through subculture of hackers learn how to evade law enforcement and how to destroy the evidence, methods of obtaining money by criminal means and what the safest tools are. Environment of hacker information distribution creates technical advantage over the private security services and public services fighting cybercrime.

The last is the criminogenic function. Accumulation, preservation and transfer of criminal traditions help hackers to resist social institutions and maintain reproduction and dissemination of cybercrime.

Forecast on the ability to fight against the subculture of hackers rather pessimistic, today it is developed subcultural association that covers the broad masses of people around the world. Reasonableness of ideology, which formed moral system, makes the subculture of hackers easily disseminated and spread not only by people prone to crime. In turn, all the anti-social and antisocial youth subcultures form a stable, adaptable to the current set of social conditions structures, so that the response to these informal organizations only by the law is useless.

3. Conclusion

Three main theses of hacker subculture ideology are extremely acceptable in Russian society. Due to long the history of living with communistic values hackers' subculture got advantages to conquer Russia. Some ideas were controversial to communism ideology, but complied with new ideas of Russian Federation society reformation.

Hacker environment is one of the main criminogenic factors for Internet crime, because it performs the functions of combining, information and legitimizing. It seems that neutralization of the negative effects of hackers' subculture is one of the priorities in combating Internet crime.

Idealization in the mass opinion illegal activities of hackers interferes with the fight against Internet crime; and it creates additional incentives for conducting a criminal lifestyle in the Global Network. First of all it is necessary to restrict the flow of information, popularizing subculture of hackers and stop to promote the necessary conditions for committing Internet crimes; provide alternative information about the true portrait of the hacker, the negative consequences of its activities in order to demystify the hackers as "freedom fighters", and provoke to doubt that intentions of computer criminals are pretty transparent.

References

Aliphapova, F. N. (2009). Factors forming youth subculture. *Siberian Pedagogical Journal, 7*.

Baturin, J. M., & Zhodzishky, A. M. (1991). *Computer crime and computer security*. Juridical Literature Publishing House. Moscow (USSR).

Bezborodov, A., Eliseeva, N., & Shestakov, V. (2010). *Reforming and destroying of USSR (1985-1993)*. Saint Petersburg (Russia). Norma.

Denisov, N. L. (2002). (In Russian language) *An Influence of the criminal subculture on the formation of an underage personality*. Dissertation of PhD (Law). Moscow (Russia).

Dremliuga, R. I. (2007). Criminological value of hacker. Scientific notes Faculty of Law. In A. A. Liverovskii, & A. A. St. Petersburg (Eds.), *University of economic and Finance 2007* (Vol. 7, Issue 17, pp. 11-15).

Dremliuga, R. I. (2008). Hacker's subculture and other factors of computer crime. *Journal of Criminology Baikal State University of Economics and Law*. Irkutsk (Russia): Izd BSUEL.

Ermakov, D., & Voronetsky, I. (2013). Customer hacker attack on the portal of "Aeroflot" received two and a half years. *Administrative Law, 4*, 104-106.

Grigorieva, M. R. (2012). "Perestroika" of Russian state policy in the sphere of culture in the 1990s. *Bulletin of Udmurt University, 5*(3), 150-154.

Mentor. (1986). *Hacker Manifesto*. Retrieved March 14, 2014, from http://project.cyberpunk.ru/idb/hacker_manifesto.html

Qiang, X. (2003). *China's Virtual Revolution/Project Syndicate*. Retrieved March 14, 2014, from http://www.project-syndicate.org/commentary/china-s-virtual-revolution

Smirnova, I. A. (2000). (In Russian language) Virtual space of the culture. *Materials of the science conference*, 11-13. Saint Petersburg (Russia), Saint-Petersburg philosophical society. Retrieved March 14, 2014, from http://anthropology.ru/ru/texts/smirnova_ia/virtual_53.html

Tulegenov, V. V. (2003). *Criminal subculture and its criminological value: Thesis of PhD (Law)*. Rostov on Don river (Russia), 2003.

Vershinin, M. (2004). Modern youth subcultures: Hackers. Retrieved from http://psyfactor.org/lib/vershinin4.htm

Copyrights