Co-joint Convention of the
Central and East European International Studies Association (CEEISA) and
the International Studies Association (ISA)
23rd-25th June 2016 – Ljubljana, Slovenia

The Politics of International Relations

The Influence of Cyberspace Communication on Social and Political Life (paper in progress)

Mariya Granovskaya,

Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Moscow, Russia
mariyagranovskaya@yandex.ru

Cyberspace in XXI century is one of the most important spaces of human communication. It should be noted the growing importance of the effects of communication in cyberspace. The networks have become the models of development in such phenomena as international terrorism or global hacker organizations as widely known organization Anonymous. The organization has become an influential force in modern communication sphere and their activities aimed at the struggle of justice. Their main enemy today is a terroristic organization IS.

In this case we are faced with phenomenon of cyber warfare, which is defined as informational confrontation in cyberspace.

The paper researches such phenomenon as communication in cyberspace and its influence the on global public opinion. The methods of the modern cyber warfare are being analyzed in this paper.

Key words: cyberspace, communication, Anonymous, IS, cyber warfare

Author`s name:	Mariya Granovskaya
Author`s Address:	36, 218, Frunzenskaya nab., Moscow, Russia
Author`s Affiliation:	Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation
Author`s e-mail:	mariyagranovskaya@yandex.ru

Introduction

The research presented seems rather crucial today as communication in the cyberspace manifests, primarily, political boom (growing social protest and civil defiance, social networks used to stir riots and recruit terrorists) and affects the current global policy in (WikiLeaks activity, Edward Snowden's case, actions of Anonymous hackers). Ubiquitous cyberspace has amplified the capacities of terrorism and facilitated the transformation and improvement of terroristic operations.

The world today can't be drawn without such notions as a **cyber-warfare, cyber-terrorism, hacktivism**. Each category listed has its own features; however we have to admit that no blatant lines between cyber-terrorism and hacktivism exist, as an individual knowledgeable in information technologies can become a hacktivist as well as a cyber-terrorist, despite the fact that the damage rendered by hacktivists doesn't infer human losses.

The methodology of the research is based on the method of comparative analyses and the method of content-analyses. A large number of works devoted to the study various activities in cyberspace (Dorothy E.Denning 2001; Heickerö 2014; Singh 2014, Clarke 2010, Kabernik 2012)

"Cyber-warfare – efforts of a nation-state to infiltrate into computers or networks of another nation-state in order to inflict damage or destruction." (Clarke 2010) "The Economist" magazine describes a cyber-warfare as "the fifth field of war alongside with land, sea, air and space." Generally speaking, a cyber-warfare is a type of information war, a computer standoff in the Internet including.

The interpretations of this notion are numerous, however, by and large a cyber-warfare can be characterized as "a revolution in a war conduct", retreat from traditional methods of warfare conduct. We would like to touch upon an important aspect of a cyber-war – cyber-terrorism; our aim is to assess future consequences of cyber-war and hacktivism. In this regard particularly vital is a problem of cyber-security in the modern world. Kim Taipale, a founder and executive director of the Stilwell Center for Advanced Studies in Science and Technology Policy, believes that "cyber-terrorism, whatever it is, is a useless term,

because terrorists will use any strategic tool they can." After cyber-threats were made to Slobodan Milosevic`s bank accounts during the 1999 Kosovo crisis, for example, the cyber-terrorism discussions were raised in the U.N.. Russia also expressed interest in the problem. The U.S stalled the discussion. As Mr. Taipale said: "Now there are no rules; now we are reaping the problems because these separate entities are incompatible and inconsistent, making us more vulnerable to terrorism."

Kosovo conflict is the first Internet warfare. Officials and non-officials alike strived to employ the Internet for information dissemination, propaganda management, and attraction of new supporters. Hackers used the websites to condemn both Yugoslavia's and NATO's hostilities via the disruption of governmental computers and gaining the control over the websites. According to D. Denning, people all over the world shared war information and photos, that ultimately could shape indirectly political and military decision-making.

In the course of NATO military action the Chinese hackers broke several US governmental websites after China's embassy in Belgrade was bombed. The website of American embassy in Beijing posted a slogan which named Americans "barbarians"; the photos of three journalists – victims of the bombardment – were placed on the website of Department of Internal Affairs.

Cyber-terrorism and Hecktivism

Cyber-terrorism – a universal term describing various activities in the cyber-space; it unites numerous organizations, groups, and people. Professor Dorothy Denning, one of the most prominent researchers in the field of cyber-terrorism, suggests cyber-terrorism be assessed as an illegitimate, socially or politically bent attack or as a threat of attack on computers, websites, and stored data. Cyber-terror as a cyber-warfare tool is focused on grave economic and human losses and constitutes a new threat for security of many states. A great number of computer networks remains highly vulnerable to attacks, however it is worth mentioning that today's cyber-attacks rarely inflict physical damage to be followed by lengthy repair and recovery. Predominantly, the academic discussions focus on two antagonistic opinions on cyber-terrorism. According to

Roland Heickerö (Heickerö, 2014) the first approach states that the threat of cyber-terrorism is absolutely clear-cut and massive, as the number of computer-controlled interconnections. Mostly national officialdom and private security companies support such point of view.

The opposite approach rejects the threat per se. Scholars and researchers sticking to it think that cyber-terrorism is far more expensive than traditional terrorism; moreover the mass media repercussions are more powerful than the ones of traditional terrorist attacks of suicide-bombers. In all cases cyber-attacks are less effective and destructive than physical violence. Their only advantage is that they are easier to execute than physical attacks.

Meanwhile we can't but mention that presently cyber-attacks are launched every day. In the early 2000-s various types of viruses such as Nimda, Code Red, Love Bug, Melissa were used. The Malaysian Airlines plane which disappeared in March 2014, is likely to have fallen victim to cyber-terrorism. Recently virus Stuxnet, which messed up the atomic power plant in Bushehr, has come to light. V.V.Kabernik draws our attention to the fact that this virus targeted the particular system with its vulnerabilities. No doubt, Stuxnet is a custom software development for intelligence community; this cyber-weapon has never been designed for mass use. It has heavily damaged the plant control system as well as Iranian nuclear program as a whole. This operation can be called an episode of a cyber-war.

Hacktivism and Phenomenon of Anonymous (computer-hacker federation)

Hacktivism combines hacking and activism. It intergrades the moves based on hackers' techniques to disrupt the routine functioning of networking sections not to render substantial harm (email bombing, web-hacking and computer cracking and viruses). To that end, hackers' group Anonymous which has declared cyber-war on the Islamic State, arouses interest. The capacities of the group to standoff against the IS insurgents must be assessed. Anonymous is a virtual association of individuals communicating through computer network. Ideologically,

Anonymous confronts the IS might and impunity. In a way, they are successors of WikiLeaks mission.

There is no denying that Anonymous has turned into a global phenomenon. It testifies for the fact that many politically active people concurrently come to a conclusion that the established methods of policy-making through elections, traditional mass media, generally accepted ways of bringing different opinions to the authorities fail to deliver. Radical means proposed by Anonymous anarchists are in many aspects a response to the global crisis of civil identity, growing inequality, and violence. Such types of protesting have gained popularity. WikiLeaks phenomenon proves this tendency. Anonymous group won general recognition after "Chanology" project against Church of Scientology in 2008. They also launched several attacks (including computer cracks) on the websites of organizations and individuals who promote the bills constraining Internet freedoms.

Anonymous group has devised and implemented operation Payback, which was retaliation to the arrest of Julian Assange, a founder of WikiLeaks. The payment systems – PayPal, Mastercard, Visa which have frozen the Assange accounts, - were brought down. The first governmental website of Senator Joe Lieberman, who lobbied the bill permitting to hold Assange accountable for espionage, was hacked as well as Sarah Palin's website and personal email. She had previously called for physical disposal of Julian Assange. The websites of Swedish government and prosecution office, on whose request Assange had been arrested, was attacked as well

Anonymous group launched an attack on Egyptian governmental websites in 2011. The international hacker group Anonymous declared war against Turkey accusing it of the IS support. Experts name Anonymous a forerunner of future cyber-troops. At present the Anonymous warriors are a powerful force in the cyber-space. Nearly 30 states have by now been attacked by them. Since 2015 the activities of the group have noticeably intensified. The reason – Paris terrorist attacks in November 2015. Anonymous has declared war against the IS which can ipso facto be named "the dawn" of a new era of hacktivism and cyber-warfare. Anonymous said

"enough is enough" as the world grieved for Paris, declaring assaults on the IS via all available mass media. An Anonymous member posted a video on behalf of the group, stating "this is only the beginning for ISIS. We will hunt you, take down your sites, accounts, emails and expose you…You will be treated like a virus and we are the cure. We are Anonymous. We are legion…" Anonymous backed up the threats with some action, shutting about 20.000 Twitter accounts associated with ISIS recruitment. ISIS has been taking the attacks seriously and issued warnings for their members. We can't but agree with Tim O`Neil who says that both Anonymous and the IS are showing that warfare has a new dimension in the cyber theater – in particular, social media.

Currently Anonymous is decentralized, however if they get controlled by a state organization aiming at waging a real war, it will turn into a genuine threat.

Conclusion

Cyber-terrorism and hacktivism are manifestations of a cyber-war. At the moment no grounds exist for an urgent threat of a cyber-war. Meanwhile certain spots of its developments can be seen. Information confrontation between Anonymous group and IS insurgents serves to rather attract public opinion. All acts of Anonymous hacktivists are highlighted by mass media around the world. How influential cyber-terrorism and hacktivism are on the foreign policy of individual states and global politics in general, is difficult to assess, however their activity being covered by global mass media definitely renders an impact on the society. They are decentralized, structurally non-united, uncoordinated at different levels. Daesh militants, on the other hand, neither use the Internet far and wide nor developed industry and infrastructure. Consequently, hacktivists will hardly inflict tangible damage to the Islamic State.

References

Dorothy E. Denning. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Available from: http://journal.georgetown.edu/the-rise-of-hacktivism/ [Accessed 15 May 2016]

Roland Heickerö. Cyber Terrorism: Electronic Jihad. Available from: http://www.idsa.in/strategicanalysis/38_4/CyberTerrorism [Accessed 10 March 2016]

Patricia L.Schouker. The Energy Sector: A Prime Target for Cyber Attacks. Available from: http://beforeitsnews.com/media/2016/06/the-energy-sector-a-prime-target-for-cyber-attacks-2-2498926.html [Accessed 16 June 2016]

Swaran Singh & Jayanna Krupakar Indo-US Cooperation in Countering Cyber Terrorism: Challenges and Limitations Available from: http://www.idsa.in/taxonomy/term/1512 [Accessed 16 June 2016]

Clint Watts. Did Anonymous just save world from ISIL? Available from: http://warontherocks.com/2015/11/did-anonymous-just-save-the-world-from-isil/ [Accesses November 2015]

ANONYMOUS kak provozvestniki ery kibervojn Available from: http://gpolitika.com/politika/anonymous-kak-provozvestniki-ery-kibervojn.html [Accessed April 2016]

Kiberorujije stanovitsya opasnee yadernogo. Available from: http://izvestia.ru/news/611996 [Accessed 15 May 2016]

Kibervojna i kiberorujije. Available from: http://eurasian-defence.ru/?q=node/3115 [Accessed April 2016]

Tim O`Neil. Anonymous vs. ISIS – A New Dimension of Cyber Warfare. Available from: https://www.garlandtechnology.com/blog/anonymous-vs.-isis-a-new-dimension-of-cyber-warfare [Accessed 12 June 2016]