CENAA
Centrum pre európske a severoatlantické vzťahy

Policy Papers

CYBER SECURITY

CYBERSECURITY, CYBERTERRORISM AND ITS MORAL QUESTION

Viktória Sučáková

Over the past couple of years and decades, there has been a shift in the international sphere on how people portray security. The rapid evolvement of cyberspace and technology development led not only into complete change of preserving information but also change in thinking.

"As government agencies, private sector corporations, the military, and even retail shoppers shift their activities to the Internet, cybersecurity becomes increasingly important." (Harknett, 2011)

This paper will deal with the question of moral acceptance of cyber warfare and cyber attacks around the world by defining the cyber security, national security and cyber terrorism through the most recent and important case studies of Anonymous, WikiLeaks and current situation around Edward Snowden and the NSA leaks. Over the past five years the level of cyber attacks massively spread around the globe. More and more the role of cyber security is not only affecting the state to state conflicts, but role of individuals have become more important within the field. Pentagon concluded that a cyber attack on another state is considered as an act of war (Harknett and Stever). How does one then measure the act of individual or uninterested group?

Definitions

Before we understand how cyber warfare threatens the international community, we need to analyze several terms that come to our knowledge. Security is hard to define, mostly due to the variety of explanation given by scholars. To some of them, security is threatened when a foreign attack occurs (Levy, 1995). This mostly depicts that security is only at a stake when foreign action are implemented. Some might argue that this definition needs addition of domestic actors, which are especially vital in the role of cyberspace and cyber warfare. Cyber security therefore lies in the security of cyberspace, disregards on origin of the attackers. Terrorism is in international community considered as a misleading term. To public eye terrorists are promoted as a complete evil who strives to harm the innocent lives of citizens. FBI states that terrorism "is and acts dangerous to human life that violate federal or state law" or "Appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping;". Cyber terrorism is therefore acts of violence which put in danger civilians. Given the explanation, it is understandable for governments to perceive cyberwarfare as a terrorist attacks. However, it is not always sure, if objectivity comes first in dealing with the cyberattacks in the international sphere.

Anonymous, WikiLeaks and the beginnings of government leaks.

Julian Assange, the founder of WikiLeaks, was heard to believe that information wants to be free and should be free. However in the broader view, it is not always possible to allow all information to be free and for everyone. This was mainly stated as the opinion of governments. Governments seek many different ways to protect their confidential information, and it is widely believed that they have the right to hide all information that might harm the government or its people (Alford, 2011). With the recent events however, we learn a new side to given case, and that is the legacy of hiding information and objectivity of certain actions. These events have brought several questions to the surface and that is mainly: Where is the line between protecting information to safeguard people, and using the confidentiality to serve for non-objective/subjective purposes? If such a thing happens, is it morally acceptable for people leaking information to continue without prosecutions, or are they considered as cyberterrorist who harm the security of other citizens? they considered as cyberterrorist who harm the security of other citizens? Several groups and individuals became the main protagonist within the cyber security. Since 2008, self–called group "Anonymous", previously linked with hacking several websites for "fun" launched a series of attacks on the Church of Scientology. This movement led to unimaginable consequences. Group of young men sometimes even children, from all around the globe managed to take down and hack corporations such as Sony, Visa or MasterCard, succeeded in hacking the websites of governments of Israel, USA and Uganda. The most considerable attacks within the international community might be considered the attacks on databases in Tunisia and Egypt, which helped the revolutionaries gain access and power over their governments. . Within a leaked FBI documents, the group was categorized as a national security threat (Cadwalladr, 2013).

On the other hand supporters have called them "freedom fighters" or "digital Robin Hood" (Bailey, 2013). This however didn't end just with cyber attacks and intrusions. Massive outrage of protests has spread around the world, where people adapt the principles of "Anonymous". It is possible to suggest that the role of Anonymous is no longer only within the sphere of cyberspace, but also within the minds of people. In 2006, WikiLeaks, a non-profit international organization started to leak confidential documents from various anonymous sources. Julian Assange has been believed to be the founder and leader of the organization. In 2010 WikiLeaks started to publish several documentations concerning wars in Iraq and Afghanistan, which have not been previously published to the public. The "Iraq War Logs" and "Afghan War Diary" became the main reason in the prosecution started by U.S. Justice Department against the organization, and more importantly, the founder Assange (Roberts, 2011). There are no ground rules on how to bring Assange to justice, and the only prosecution that would be positive is on the grounds of the United States. WikiLeaks are publishing new documents till this day and no further actions have been successful in stopping leaks from happening.

Edward Snowden and the domestic resistance

The case of Edward Snowden is particularly interesting in the contrast of above stated cases. In the earlier mentions of cyber warfare it was usually foreign attackers who sought to act against the governments of the U.S. This year a new case came into surface, after Edward Snowden, US citizen employed by the intelligence, leaked many confidential documents and information from NSA (National Security Agency).

A domestic, inside job is somewhat different to the outside attacks. Whereas foreigners might be believed to act against US government to harm them, an US citizen, who pride himself as not a hero, nor a traitor, but an American can't be viewed in the same light as those who preceded him (Simpson, 2013). Even though Snowden is considered as a "whistleblower" or a "dissident", a further explanation needs to be sought. It is not completely understandable to why someone who is believed to protect the government decides to do the opposite and threaten the security of the state, unless there is a coherent injustice implemented by the institutions. If the confidentiality of information is primal to the security of citizens and institutions, why someone who is fully coherent of the fact decides to leak these information on purpose. In many of these cases, the individuals were described as cyber-terrorist. Given the above explanation of terrorist as someone who threatens the lives and well–being of citizens and individuals, it is easy to link these actions to terrorism. However, it is also important to state, that these actions were taken in no direct aim to harm people, it was usually described as providing the people with information they have the right to know. In this case terrorism doesn't explain the purpose. Acceptance and morality of cyber warfare is very questionable and opinions vary in a great scale. To some, these people are "heroes", who serve the justice and define the modern revolution against the hierarchy. On the other hand, they are portrayed, mostly by institutions and hierarchies as a penetrators of governments, thus dangerous individuals to the system. It is very hard to draw a line where the two meet, that's why it is not possible to fully categorize them under any terms.

Conclusion

This essay dealt with the basic explanation of cybersecurity, cyberwarfare and cyberterrorism. It tried to answer the moral question through the cases of various groups and individuals who have been accused of committing acts witing the cyberwarfare – especially Anonymous, WikiLeaks and Edward Snowden. It battled the relation between terrorism and rebellion and acknowledged the importance of furthering the study of cyber security in greater depth.

Author is a MA student in International Relations at the University of Aberdeen, currently focusing on International Security.

Reference:

Alford, R., P., Leaks in the Internet Age (Proceedings of the Annual meeting, American society of international law, vol. 105, march 23-26, 2011, pp. 147-150)

Bailey, K., Cybercrime – the acceptable face of modern warfare?, (Clearswift, September 6, 2013)

Cadwalladr, C., We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous and the Global Cyber Insurgency by Parmy Olson – review, (The observer, Sunday 18 August 2013, Accessed: 10. November 2013)

Definition of Terrorism in the U.S. code, 18 U.S.C. § 2331 defines "international terrorism" and "domestic terrorism" for purposes of Chapter 113B of the Code, entitled "Terrorism”:

Gorman, S., Barnes, J., E., Cyber Combat: Act of War: Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force, (The Wall Street Journal, Last modified: Updated May 31, 2011, Accesses: November, 21, 2013)

Harknett, R., J., Stever, J., A., The new policy World of cybersecurity, (Public Administration Review, Volume 71, Issue 3, pages 455–460, May/ June 2011)

Levy, M., A., Is the environment a national security issue? (The MIT Press, International Security, Vol. 20, No. 2 Autumn 1995, pp. 35-62)

Roberts, A., The WikiLeaks Illusion, (The Wilson Quarterly 1976-, Vol.35, No. 3 summer 2011, pp. 16-21)

Simpson, C., Snowden Speaks: 'I'm Neither Traitor Nor Hero. I'm an American, (The Wire, 12 June, 2013, Accessed: 20. November 2013)

The Policy Paper is part of the new CENAA`s long-term program Global Netizenship in Cyber World. It aims to analyse in-depth multispectral and cross-cutting issues of national and international cyber security. Through the establishment of the network of national and international partnerships, CENAA strives to ensure that cyber security will get into focal point of political, corporate and expert elites. Goal of the program is also to uncover the issue of cyber security to all.

CENAA Policy Papers

No. 1/2014, Vol. 3

Centre for European and North Atlantic Affairs

Tolstého 9, 811 06 Bratislava

www. cenaa.org/publikacie/policy-papers/