Hacktivism: a new form of political activism

AydeliaGareeva,
School of Governance and Politics, MGIMO University

Kira Krylova,
School of Governance and Politics, MGIMO University

Olga Khovrina,
School of Governance and Politics, MGIMO University

Abstract

Nowadays activism has become a significant tool for affecting politics. We observe the revitalization of grassroots lobbying, particularly hundreds of social movements fighting actively for their ideas. At the same time we see the rise of such controversial modern phenomenon as hacktivism. In this article we determine the meaning of hacktivism, study its followers' goals and tactics by illustrating the examples of various international hacktivist groups activities and their impact on politics, national security and decision-making process.

Key words:

hactivism, activism, anonymous, hacking, cybersecurity

Main body

Nowadays activism has become a significant tool for affecting politics. We observe the revitalization of grassroots lobbying, particularly hundreds of social movements

fighting actively for their ideas, from Gillets Gaunes in France to #BlackLivesMatter and Never Again MSD movements in the U.S.

Activism has changed in the era of new technologies. The development and widespread of information technology have created new opportunities for activism. While there are hackers who covet money or do it 'just for fun', as well as nation-states and independent actors conduct cyber attacks, there are also online activists who use social media to spread the word and create a movement and, what is more important for this work, there are hacktivists who seek to reshape politics.

Hacktivism is a controversial phenomenon. While some skeptics believe that hacktivists are nothing but a bunch of teenagers who have fun online attacking governmental websites, others argue that they became a new political force which does indeed make changes. We aim to outline what hacktivism is basing on; various approaches to its definition, find out what motivates hacktivists and finally answer the question whether their actions do affect political and social spheres and, if so, in what way.

1. The definition of hacktivism

Due to the variety of meanings of the term, hacktivism might be difficult to define. It is often considered as a type of cyberterrorism or hacking. Moreover, it gets even more confusing when some nations-states "operate under the guise of hacktivism" in order to pursue their own objectives[1].

Some of the most spread definitions which help to understand the phenomenon are the following:

---

[1]Return to Normacy: False Flags and the Decline of International Hacktivism[Electronic resource] / Recorded Future – Electronic data – 2019 – Mode of access:https://www.recordedfuture.com/international-hacktivism-analysis/

1. “the non-violent use of illegal or legally ambiguous digital tools in pursuit of political ends”(Samuel, 2004)
2. “a combination of grassroots political protest with computer hacking” (Jordan and Taylor, 2004)
3. “a politically motivated single incident online action, or a campaign thereof, taken by a non-state actors in retaliation to express disapproval or to call attention to an issue” (Vegh, 2003)

Following on from that, we can define hacktivism as a politically motivated use of hacking skills undertaken by anonymous non-governmental actors in order to spread the word, draw attention to an issue and cause change. These are the key points which help to distinguish hacktivism from hacking, cyberterrorism and online activism. In order to provide a better understanding of what political influence can be exerted by hacktivists, we should first study the incentives that stand behind hacktivist activities.

2. The values of hacktivists

Anonymous as a “tip of the spear” of the modern hacktivist movement pursues in its actions basic political values that are expressed in “5 Principles: An Anonymous Manifesto” among which there are such as fight for an “open, fair, transparent, accountable and just society” where information is “unrestricted and uncensored” and defending human “rights and liberties”. All the actions aimed at spreading these values all over the world take place online (Fuchs, 2013).

At the same time hacktivism is not always committed to democratic values. But in contrast to cyberterrorism, hacktivists do not seek to cause significant damage, monetary loss, interruption of work of a governmental body or an organization, as well as to frighten authorities or civilians. Hacktivists tend to achieve their goals “in a

relatively peaceful manner"[2]. Each hacktivist has his own value system and his own set of goals which makes their actions unpredictable.

3. The goals of hacktivism

Nowadays there are lots of hacktivist groups with specified objectives and tactics. As there are many approaches to what hacktivism is, these objectives are varied, too.

Originally "For the lulz" was the primary objective of such world-famous hacktivist groups as Anonymous, LulzSec etc.This peaceful manner often makes people think that hacktivists are teenagers who act aimlessly, "just for lulz", and thus not to take them seriously. Indeed, this kind of tomfoolery was the primary objective of an international hacktivist group called Anonymous. But today "for the lulz" has paled into insignificance and hacktivist activity itself has turned into collective political action and hacktivists have turned into lobbyists promoting their own interests from social justice to cyber libertarianism (fight against governmental regulation of "free" internet) (Fuchs, 2013).

Even though it was initially focused on different information issues, such as freedom of information and human rights in this regard (free access to all kinds of information, freedom of the Internet, freedom of individuals to think for themselves, etc.), hacktivism is now mostly considered as an activity aimed at showing some kind of protest against any political or social issue that seems unfair to activists (Alexopoulou and Pavli, 2019). These issues range from corruption, poverty, adoption of a law limiting human rights and unauthorized whaling to "tyrannical" governments, such as those in Egypt, Libya or even China (Lim, 2012).

4. Hacktivists'tactics

---

[2]What is hacktivism?[Electronic resource] / Stanford Computer Science – Electronic data – 2019 – Mode of access:https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Hacktivism/what.html

Nowadays there are lots of hacktivist groups with specified objectives and tactics that they often use. Furthermore, social networks like Twitter and Facebook and Internet in general as a prominent platform of hacktivists' activity give them a lot of room to manoeuvre, especially in case of tactics.

A. DDoS attacks.

One of the tactics that hacktivists often use is DDoS (Distributed Denial-of-Service) attacks, which means a malicious attempt to disrupt normal traffic of an online service by overwhelming it with a flood of Internet traffic. In the past years the frequency of such attacks has increased, as they represent an efficient method for hacktivists to be seen and to be heard, especially by GO and NGO agents.

One of the largest DDoS attacks launched by Anonymous group was the one against the sites included the U.S. Department of Justice, the FBI, the U.S. Copyright Office and those associated with Warner Music and Universal Music in 2012.

In 2016 in Brazil there was a series of DDoS attacks on state and city websites. Several hours before the Olympic Games opening ceremony Anonymous Brazil released a statement complaining about the illusory happiness sold by the media which hided[3]. Anonymous blamed the government for hiding poverty, evictions and violence against local population behind the glitter of the Games[4].

B. Doxing

---

[3]Major Events and Hacktivism #opolympichacking[Electronic resource] / RSA - Electronic data – 2016 – Mode of access:https://www.rsa.com/en-us/blog/2016-08/major-events-and-hacktivism-opolympichacking

[4]With Anonymous' latest attacks in Rio, the digital games have begun[Electronic resource] / OpenDemocracy – 2018 – Mode of access:https://www.opendemocracy.net/en/with-anonymous-latest-attacks-in-rio-digital-games-have-begun/

Second most used hacktivists' tactic is doxing. It refers to the exposing and publishing one's identity and their personal information online including not only names, dates of birth, phone numbers, but also confidential photographs and documents[5]. This tactic is frequently used with reference to high profile individuals (actors, singers, politicians etc.) and major organizations in order to reveal something interesting, discouraging and even incriminating.

In the past 5 years such international non-profit organization as WikiLeaks has been the focus of the online community. It became famous in 2010 after leaking information and videos from Bradly Manning (later – Chelsea Manning), US Army Intelligence Analyst[6]. The most well-known doxing case is the one dealing with the candidate for the presidency in 2016. WikiLeaks published more than 30 thousand private compromising emails and emails attachments that had been sent to and from Hillary Clinton's email archive. This doxing activity gained worldwide visibility both positive and negative.

C. Webdefacement

Website defacement as a hacktivist tactic means visual or verbal changing of a site. It gained popularity in 2001 when there was a US-China mid-air collision after which Chinese hacktivists defaced about a thousand of American sites and in response to this action US hacktivists hit back in kind. Webdefacement still happens, nowadays there are many cases of hijacking individual's Twitter or Facebook pages. For

---

[5]A defender's playbook [Electronic resource] / Deloitte – Electronic data – 2016 – Mode of access:https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-hacktivism.pdf

[6]Bradley Manning given 35-year prison term for passing files to WikiLeaks[Electronic resource] /The Guardian– Electronic data – 2013 – Mode of access:https://www.theguardian.com/world/2013/aug/21/bradley-manning-35-years-prison-wikileaks-sentence

example, in 2014 Anonymous hacktivists hijacked Ku Klux Klan's Twitter account and left a warning message with the #OpKKK hashtag[7].

5. Impact on politics

Despite its decline since 2016, hacktivism has already changed political world. A proper analysis reveals that hacktivism practices have both positive and negative impact on national security and decision-making process (Karagiannopoulos, 2018).

A. Impact on national security

Hacktivists' case illustrates an increasing tendency of governments to portray electronic civil disobedience (ECD) as terrorist activity. For instance, the National Security Agency director has expressed his concern that Anonymous could soon have the ability to cause a limited power outage through cyberattacks. Nevertheless, it is not correct to claim that hacktivism is nothing else but a threat to national or corporate security. Hacktivists help states and corporations to find weak points in their informational systems to protect consumer privacy and online safety. There are several cases when hacktivists' attacks and tools helped to improve the protection of customer data and software (Cult of the Dead Cow's the BackOrifice tool for Windows 98, probable PlayStation Network outage by the Anonymous)[8].

B. Impact on the decision-making process

---

[7]Anonymous leaks identities of 350 alleged Ku Klux Klan members' [Electronic resource] /The Guardian – 2015 – Mode of access:https://www.theguardian.com/technology/2015/nov/06/anonymous-ku-klux-klan-name-leak

[8]We are Anonymous. We do not forgive. We do not forget [Electronic resource] / Dazed – Electronic data – 2013 – Mode of access:https://www.dazeddigital.com/artsandculture/article/16308/1/we-are-anonymous-we-do-not-forgive-we-do-not-forget

It is believed that ECD and hacktivism in particular can reinstate marginalized citizens as participants in legislative processes, from the formal democratic procedures from which they might feel excluded. The government bodies should accustom themselves to a new type of activism, anonymous and decentralized, so cash flow, threat of punishment or violence will not be any longer used as a state control mechanism. Thanks to new information technology and the emergence of hacktivism young people have received an opportunity not only to promote their own political views but also to perform some politically motivated actions. However, numerous arrests and criminal convictions of cyber protesters reveal the general official presumption is to consider hacktivism criminal, rather than an exercise of participation rights and free speech.

Hacktivists, generally adhering to cyber libertarian or anarchic values, contribute to decentralization of power and increased accountability, as well as a more informed, democratized and as a result more efficient decision-making process. However, it is doubtful that "everyday regulatory multi-stakeholderism" which denotes dynamic and more frequent interactions between governmental and non-governmental actors may be fully established (Karagiannopoulos, 2018).

Conclusion

Since we are entering an era of information society, many social spheres are undergoing profound changes and new threats to security ranging from individuals to states are emerging. Special attention is given to cyberspace which is rapidly becoming the main platform for international and intra-state communication, crimes and acts of war, political activism. Hacktivism movement occupies a unique place in the complex system of cyber interactions, although, it often uses the same tools and tactics that hackers and cyber terrorists do. A conclusion to be drawn is that hacktivist actions are neither a dangerously criminal nor a totally justifiable political practice. However, we should note that further marginalization of these protesters and the

generation of more intense internet censure policy could give rise to numerous even more severe online and offline acts of civil disobedience.

References

1. Alexopoulou S., Pavli A. (2019) BeneathThis Mask There is More Than Flesh, Beneath This Mask There is an Idea': Anonymous as the (Super)heroes of the Internet // International Journal for the Semiotics of Law. Vol. 32. No. 1. P. 1 – 28.
2. Fuchs C. (2013) Anonymous movement in the context of liberalism and socialism // Interface: a journal for and about social movements. Vol. 5. No. 2. P. 345 –376.
3. Jordan T., Taylor P. A. (2004) Hacktivism: informational politics for informational times. Abingdon:Routledge.
4. Karagiannopoulos V. (2018) Living With Hacktivism: From Conflict to Symbiosis. London: Palgrave Macmillan Ltd.
5. Lim M. (2012) Clicks, Cabs, and Coffee Houses: Social Media and Oppositional Movements in Egypt, 2004–2011 // Journal of Communication. Vol. 62. No. 2. P. 231–248.
6. Samuel A. W. (2004) Hacktivism and the Future of Political Participation. Cambridge, Massachusetts: Harvard University.
7. VeghS. (2003) Hacking for Democracy: A Study of the Internet as a Political Force and Its Representation in the Mainstream Media, American Studies. Maryland, College Park: University of Maryland, College Park.