Magyar Rendészet Vol. XVI. 2016/2. 161–174.

Hacktivism and Its Status in Hungary

SIMON Béla[1]

In recent years the definition of Hacktivism has entered mainstream communication. Our everyday lives are defined by info-communication devices, almost like a house of cards in the wind. This statement is verified by several scientific sources. Nevertheless, according to other pieces of news, this house of cards might as well be destroyed by a secret movement – called hacktivists – at any time. In this study I try to examine whether the news on hacktivist movements in Hungary have sufficient grounds, or it is just the demonization of the phenomenon.

Keywords: *Hactivism, Hungary, Cyber defense, Anonymous, Governmental Computer Emergency Response Team*

What is Hacktivism?

Basically, we may compose quite a few definitions of the hacktivist movement. As one, we may describe it as a political expression of a public movement of hackers, second, a movement of hacking with political aims, or we may recognize such actions as hacker measures relativized to political mean.[2] We may find a common thread in all three definitions, and that is politics.

On a wider scale, trends in hacktivism go against religious and social activity, including the rejection of tyranny and other threats perceived as leading to submission, also stating that "hacktivism is fundamentally about refusing to be intimidated or cowed into submission by any technology and acquiring the power to repurpose it for our individual needs, and for the good of many."[3] Similarly, we may refer to the announcement of one of the leading hacktivist group, Anonymous, protesting against manipulations, fear, indifference and repression indicated by politics, whereas, at the same time, its members seem to consider themselves a hidden power of the people.

In the 21st century, we all live in the golden era of free speech. After all, it's no wonder that the ones eager to protest may feel that they are not able to realize their beliefs, so they decide to take their chances within the frame of networks and become hacktivists. Recently, the means of cultural and political protest have changed. Progressive

1 SIMON Béla dr., police major, assistant lecturer, National University of Public Service, Faculty of Law Enforcement, Institute of Criminalistics, Criminal Intelligence Department, PhD candidate, Faculty of Military Science and Officer Training, Doctoral School of Military Sciences
Dr. SIMON Béla tanársegéd, NKE RTK Kriminalisztikai Intézet, Bűnüldözési és Gazdaságvédelmi Tanszék.
simon.bela@uni-nke.hu

2 Tessa Jade Houghton: *Hacktivism and Habermas: Online Protest as Neo-Habermasian Counterpublicity*, PhD thesis, University of Canterbury, 2010, 91.

3 Peter Ludlow: *What Is a 'Hacktivist'?* 2013. Source: http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/?_r=0 (11.09.2015.)

sciences have dissolved boundaries and re-defined loyalties. Hacktivists seem to believe that people are nothing more than plain figures of databases these days. Human virtues together with fundamental human rights are simply being lost. Therefore, according to their opinion, grounds for combat against oppression must be transferred into cyberspace, hosting initiatives of liberation for the layers of society feeling repressed.[4]

The hacktivist movement is rather heterogeneous, and complies participants who perform in the movement through different initiatives (that is a broad scale from protesters against consumerism to those targeting to fight against the growing powers of multinational enterprises), essentially, this study shall aim to explore the political motives of those who try to influence governmental institutions.

There are several ways for those devoted to reaching their political objectives in this sense. Primarily, any acts of expressing political viewpoints in personal relationships are designated at the lowest stage beyond the measures of representative democracy. A higher level of engagement is required for a person willing to express political commitment, sharing his policy with others, taking time, resources and devotion, without any personal intercourse whatsoever. Participation at a demonstration, strike or slowing down traffic are common forms of expressing political sentiments. In such cases, when drawing the attention of decision makers and fellow citizens, participants sacrifice their own resources, namely, their spare-time for demonstrations, their wages for strikes, etc. The more resources invested, the greater attention is invoked by the political message. In itself, the number of participants seem to underline the given mass demonstration, therefore, anyone who has become aware of the notion, eventually appreciates the number of people investing their time in the movement.

We may state, that on a societal level, those protest events are recognized at which the harm suffered by and fought against the activists, or the assets invested during the protest, are greater than the offenses suffered by the addressee of the message in connection with the action.[5] Obviously, any terrorist attack is excluded from the above category, in these cases the addressees of the political message have to suffer much greater injuries.

However, in case of a hacktivist action such balance can be easily disturbed, as sometimes the actions of only one or two persons stand behind the destabilization of the governmental information system wrecked by botnet or malware. Consequently, hacktivist protest is essentially designed not to be approved by the addressees who suffer significant injunctions in relation with the action.

Public sentiments have been influenced by several controversial debates in the news, in connection with the movements subject to this survey. News and more or less scientifically-based opinions – or even movies – seemed to have shaped two major approaches. Principally, our lives are dependent on info-communication means that seem to function as a house of cards, as our existence is surrounded by a rather fragile

4 Tim Jordan, Paul Taylor: *Hacktivism and Cyberwars: Rebels with a Cause?* Routledge, 2004, 10–15.

5 For example, it is impossible to use vehicles in the city due to a mass demonstration taking over public roads, or public transportation is not available yet, demonstrators do not get their wages, etc.

and vulnerable environment. Nevertheless, another approach puts more emphasis on international groups independent from governmental influences and aware of the vulnerability of the system, whereas they are able to or soon might be able to shake or even capsize the system.

This survey does not aim to verify or detail the aspects mentioned first,[6] however, it is essential to point out that the present threats are likely to be aggravated alongside with the expansion of the system. If we only take into consideration the expansion of the sorts of devices available for direct internet access,[7] we may prognose, that the equipment, networks, platforms and applications that support the expansion of Internet of Things (IoT) multiply the dangers of exposure and threat of potential malicious attacks.[8]

The second part of the above assumption may seem to be a hypothetical speculation or somewhat of a conspiracy theory, nevertheless, by all means, it is advisory to examine, whether the independent but politically motivated group of hackers, the so called hacktivists represent a real and crucial threat for Hungary.

We must point out that in this study we do not investigate cases, whereas

- illicit activities have economic goals,
- IT systems are being compromised upon governmental instructions – this issue is subject to surveys on espionage and information technology warfare.

Nevertheless, the borderline between the above principal groups is rather flexible.

Both international trends and domestic experiences show that electronic administrative services are constant targets of organized crime, hackers and official boroughs of other countries.[9]

Certain parts of the governmental information technology system commonly suffer crypto-malware attacks aiming at financial benefits – acquiring bitcoins – through blackmail and extortion, moreover, such attacks may disturb the operation of the state and may be sufficient enough to create insecurity and capsize trust in the protective functions of the government in citizens. These goals may not be primary aims, yet, they are principal objectives of several terrorist groups. Therefore, the aims to achieve financial benefits can easily manifest in political results.

In case of any attacks against governmental IT systems we may only presume that such attacks are not being initiated by governmental institutions. If we detect that a malware has created a backdoor in the systems of an institution of significant importance, we may suspect that another state was interested in accessing such information, only upon demonstrably acquired data and proof of information. However, we may not be able to determine the source of attack above a certain level of information technology advancement, contrary to the trajectory of a missile, for example.[10] Seemingly, it

6 See more in: László Kovács – Csaba Krasznay: *Mohács Digital – Cyber attack script on Hungary,* http://krasznay.hu/digitalis-mohacs/, notwithstanding to the governmental aims specified for example in Act CLXVI of 2012 and Act L of 2013.

7 Especially devices formerly used without internet access, such as coffee machines, cars, heating equipment, traffic lights or medical laboratory and diagnostic imaging devices, etc.

8 Jon Howes: *IoT multiples risk of attack in Network Security*, Elsevier Ltd, Oxford, 2015, 20.

9 Krasznay Csaba: *A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai*, PhD thesis, Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola, 2011, 4.

10 There is still a debate over the Estonian – Russian cyber war of 2007, whereas the attacks - generating DdoS attacks with the speed of 100 Megabyte per second - were launched from 178 countries.

is rather difficult to separate compromising actions initiated by governmental forces from activities of an independent group or organisation.

Naturally, it is rather hard to define, what we call 'Hungarian' hacktivism. For crimes related to cutting-edge technology, and even more likely to hacktivist activities, detection of the actual crime scenes is more than difficult.

Evaluation of hacktivist groups upon scientific measures is extremely complicated, due to reasons other than latency. A significant part of the available information is from IT security enterprises or mainly from the media seeking noisy and glaring news (written and electronic media, news programs, etc.). We may state that these sources are basically biased against hacktivism, often to the extent to demonize the phenomenon. Consequently, it is their well-recognized financial interest to represent hacktivist activities way above their actual significance in public talk, whereas the news value is based on exposing negative forces.

Undoubtedly, the moving force of hacktivist actions is publicity. Hacktivists aim to gain the greatest publicity possible awarded their successful actions. If we take into consideration the eagerness of the press to broadcast news on such actions, and the fact that we did not hear of any hacktivists events lately, we may assume that there were no events of the sort recently.

In accordance with the above, I shall try to summarize the appropriate consequences on the state and prospective tendencies of hacktivism upon the available sources, principally statistics and former criminal procedures. Likely to the previous metaphor, we must detect former events in order to determine the trajectory of hacktivism.

Hacktivism in Hungary

The existence of the hacktivist movements is a rather new phenomenon in Hungary. Practically, it can be defined as the Hungarian wing of Anonymous. Hacktivists first appeared alongside with the attack of Anonymous in 2008. The number of their members was of course a lot smaller than their supporters' in Western-Europe or in the United States, nevertheless, similarly to other movements, they have gained grounds in the Eastern-European region. Activities of the Hungarian members grew between 2011 and 2012; however, we can find proof of their presence at earlier stages of the movement as well.

So far, their actions can be specified as hacking the website of Rózsa Hoffmann and the 'Hamisítás Elleni Nemzeti Testület' (National Board Against Counterfeiting), attacking kuruc.info, a portal of an extreme right-wing political party, nevertheless, their most far-reaching project was hacking into the home page of the Supreme Court, when they 'implemented' modifications in the text of the constitution available on the website. Above all, according to their statement, members of the Hungarian Anonymous group sympathized with the notions of WikiLeaks by joining the Anonymous project referred to as #opMayhem2012, aiming to collect and store classified governmental information and planning to 'leak it all' later on. According to their announcements, the

Hungarian group itself has collected such information as well. Like the foreign Anonymous groups, the issue raised by the phenomenon of the Hungarian group is that new members of any social groups or classes can align themselves with the movement easily and simply. Tasks are distributed loosely, in accordance with the interests of the hacker and cracker entities of the group.

Further DDos, SQl injection, deface attacks raised dust in 2011 and 2012, against the following sites: artisjus.hu, iksz.net, kormany.hu, nrszh.hu, parlament.hu, keh.hu, zsaru.hu, police.hu, nmhh.hu, koverlaszlo.hu, uj.katolikus.hu and brdsz.hu. Despite the results of the ambitious and successful investigations, judgements were anything but draconic. Even the most significant principal was given a suspended sentence.

Investigations exposed that the activists attempted to compromise several governmental, administrative and religious websites, besides corporate and business homepages (for example, felvi.hu, fidelitas.sopron.hu, gyongyospata.hu, jobbik.hu, kdnp.hu, koverlaszlo.hu, kulugyminiszterium.hu, magyargarda.hu, magyarorszag.hu, mnvh.hu, nat.hu, nemzetiforum.hu, nmhh.hu, szebjovo-ert.com, sztnh.gov.hu, tpf.hu or uj.katolikus.hu).

Their popularity grew together with the world-wide protest 'madness',[11] meaning that protest movements not only became trendy, but lately, they are often considered a programme or form of occupancy, these demonstrations and events are organized in cyberspace, and work provided that masses become familiar with the policies of the movements, amongst them Anonymous. For many, participating in such demonstrations it became a fashionable form of self-fulfilment.[12] It's not likely, that the means of subsistence of qualified IT experts ready to ally with hacktivists would be endangered.

They could further increase their popularity in connection with the political policy of Fidesz winning the elections in 2014. Due to several moves and instruments included – namely, the debates over educational reforms and taxing Internet usage - effecting college students, the main age group of the Hungarian Anonymous, this programme has definitely increased the interest of young people in joining the ideology. Protesting Anons appeared in the series of mass demonstrations against Fidesz's concept on taxing Internet usage. Consequently, we may assume that a significant part of the members of the Hungarian movement seem to show alliance with the ideology of the group just for joining the trend, and labelling themselves as members of Anonymous because it simply seems to be 'cool'.

On the other hand, members of the Hungarian movement do follow world-wide tendencies, and respond in accordance with the framework of the mainstream Anonymous beliefs. They too avoid extreme opinions, however, new members must comply with the ideology and be aware of the basic shared policy. Practically, we may state that the Hungarian wing has become full partner of the Anonymous group. However, due

11 Occupy movement. See more at http://hu.occupy.wikia.com/wiki/Occupy_mozgalom

12 Previously, most of the demonstrations targeted the lower motivation levels of the Maslow pyramid or hierarchy of needs (safety and protection: i.e. higher wages, job security or extensive employees' rights, etc.) However, in the past few years participants demonstrated for the recognition of their needs, esteem or self-realization on the streets.

to the time delay it cannot be as representative as other developed wings, furthermore, significant friction is expected due to the trend-like approach to hacktivism. Notwithstanding the above, even at this stage, they represent similar sources of danger as other existing departments that started their operations earlier.[13]

It is also specific to Hungary that people who consider themselves members of the hacktivist community believe that hacktivist activities and hacktivism are the frame of the general understanding to be followed. In accordance with the above-mentioned facts, principally, they represent the younger generations. Naturally, the majority of them do not have the knowledge or tools sufficient enough to pursue such activities. However, they may gain further skills, acquaintance, and finally, occupancy in accordance with their qualifications through various Internet portals.[14] Therefore, many newbies only become members of hacktivists groups upon their desire to join the hacker society. Most of them only have user skills, therefore, they do not understand the operational means of the programs received, so even if they eventually conduct any illicit actions related to a hacktivist group, they are likely to be the first ones caught, not having the appropriate technical skills to cover their moves and not being able to carry out their actions in a sophisticated sense.

Hacktivist actions do appear in every IT systems. Obviously, latency is still a significant factor, even if in accordance with provisions of the Information Security Act[15] the entities operating critical information technology infrastructures are obliged to report on security incidents and possible threats.[16]

Reports are handled by the Nemzeti Kibervédelmi Intézet ('National Cyber-security Institution'). Besides its other activities related to the reports, the institution is entitled to analyse and evaluate the reports, furthermore, it informs other bodies on the current trends, possible damages, however, it is not obliged to inform law enforcement bodies on specific cases.

The Information Security Act obliges the authority appointed by the Government – the 'Nemzeti Kibervédelmi Intézet' – to supervise the safety of the information technology system subject to the Act, and moreover, the initiation of the administrative procedures targeting the investigation of the reports received,[17] such provisions do not refer to the initiation of criminal procedures.

Amongst the duties of Kormányzati Eseménykezelő Központ (Governmental Computer Emergency Response Team, hereinafter referred to as GovCERT) the Information

13 Halász Áron: Ők az Anonymous – interjú a hackermozgalom magyar csoportjával. Source: www.mohaonline.hu/eszme/anonymous_hacker_mozgalom_magyar_interju (10.04.2015)

14 For example, Low Orbit Ion Cannon (LOIC)

15 According to point m) of subsection (1) of section 11 and subsection (1) of section 19 of Act l of 2013 on State- and Local Government-Owned Organisations' Electronical Information Security

16 Central governmental institutions except for the Government and governmental committees, the President's Office, Office of the Hungarian National Assembly, Office of the Supreme Court of Hungary, National Office of Courts, courts and attorney's offices, Office of the Commissioner for Fundamental Rights, State Audit Office of Hungary, Hungarian National Bank, metropolitan and county government offices, offices of the assemblies of the local and ethnical municipalities, authority administrative associations, Hungarian Defence Forces

17 Point e) of section 14 of Act l of 2013 on State- and Local Government-Owned Organizations' Electronical Information Security

Security Act stipulates the tasks of keeping contact with other organisations, receiving and coordinating the reported security events and taking the necessary actions, however, it does not specify the obligation to investigate the possibility of any eventual criminal acts, and does not mention the initiation of criminal procedures either. To sum it up, the 'Nemzeti Kibervédelmi Intézet' provides assistance in the localization of damages and turning off harms related to IT incidents, but it is not obliged to initiate criminal procedures. Such action shall be the discretional right of the organisation actually effected by the incident. Reports received by GovCERT are stipulated in the following charts.[18]

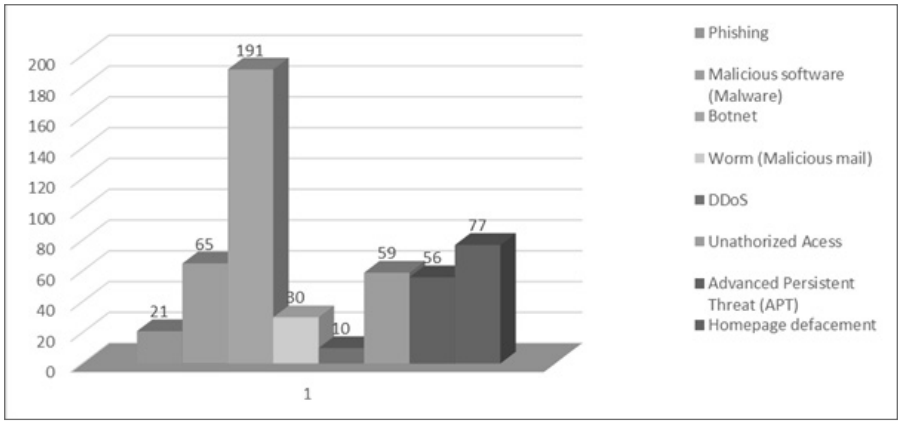

Figure 1. Reported incidents related to governmental and administrative institutions in 2014

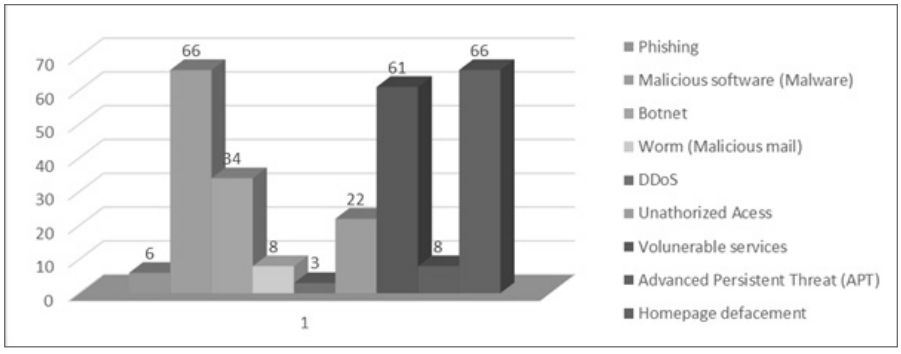

Figure 2. Reported incidents related to governmental and administrative institutions in the first half of 2015

18 GovCERT data

In the first half of 2015, 9 of the 66 state defacements (website destruction incidents) had political targets, whereas 5 of them were connected to ISIS, whilst the other 4 were related to illegal migration.

We may state that a great number of attacks target IT systems operated by the state and state administration, but we must underline that the proportion of such attacks is fragmental compared to other incidents targeting non-governmental institutions, as in 8.8% in 2014,[19] and 2.5% in the first half of 2015.

Between July 1st, 2013, and November, 2015, the officers of GovCERT gained information on two cases in which the effected institution initiated criminal procedure and turned to the police after examining the IT attack they suffered.

At present, hacktivism cannot be specifically examined upon the data of criminal statistics. Neither the long existing 'Egységes Nyomozóhatósági és Ügyészségi Bűnügyi Statisztika' (unified criminal statistics of law enforcement bodies and attorney's offices), nor the statistic module of the recently developed operational software 'Robotzsaru Neo' can allocate data related to the hacktivist phenomenon. The following chart stipulates the completed criminal offences specified in the previous Criminal Code.

Table 1. Completed criminal offences specified in the previous Criminal Code

	2009	**2010**	**2011**	**2012**
Number of criminal acts registered	394,034	447,186	451,371	422,920
Harassment	6,400	7,777	7,594	7,779
Violation of privacy	1	4	2	2
Misuse of personal data	164	552	677	201
Violation of the privacy of correspondence	7	28	16	40
Illicit possession of private information	13	18	20	15
Crimes against computer systems and computer data	321	623	570	671
Criminal conduct for breaching computer systems and computer data	33	21	15	34

19 Altogether 509 attacks effected governmental and administrative offices in 2014, whilst the number of incidents related to information systems of non-governmental institutions was 5,747. in the first half of 2015, this proportion was 275 to 11,116. Certainly, these numbers and proportions are conditioned by the measures of lawful conduct of the entities obliged to report the incidents.

The following chart stipulates the criminal acts specified in the new Criminal Code that took effect in 2013.[20]

Table 2. Criminal acts specified in the new Criminal Code

	2014	**January – October 2015**
Number of criminal acts registered	328,587	406,430
Harassment	7,862	5,388
Misuse of personal data	78	95
Violation of the privacy of correspondence	219	15
Fraud committed using information system or device	1,398	1,538
Crimes against information systems and data	347	345
Compromising the integrity of the information protection system or device	26	12
Unauthorized covert information gathering	27	16

The available statistics on the above mentioned criminal conduct does not allow us to allocate acts of political motives, likewise, we cannot stipulate whether the institutions abused or effected by the attack were state or administrative entities. Criminal acts underrepresented in numbers are insufficient in establishing well founded trends, since even a few criminal cases can influence the numbers, otherwise, only completed criminal conducts are being surveyed for statistics purposes. Also, the fact that some of the procedures are closed in only a few months, whilst others continue for years, causes severe deformities. Certainly, this principle applies for criminal actions represented by higher numbers as well, nevertheless, taking a much larger number of convicts into consideration, one or two individual cases shall not influence statistics.

The old Civil Code regulated fraud related to information technology systems in different sections, but this criminal conduct seemed to show a serious upward trend. The number of principals committing crimes against information systems and data show a significant shift in tendency, nevertheless, if we take into consideration that fraudulent activities committed by using information systems we penalized in accordance with the legal provisions on crimes against computer systems and computer data earlier, we have to admit that the number of cutting-edge technology based criminal acts of financial interest show a notable growth. Anyhow, these acts are only remotely related to hacktivism.

20 Lack of interpretation of 2013's data is due to differences in jurisdiction in the given year, and due to the fact that statistic data allocation was not quite effective either.

Past – future

In the past few years governments seemed to use hacktivism as a tool, provided to achieve their own social, political and geopolitical goals. Hacktivism has not become more politicised, but in fact state subsidized or enforcement conduct are being presented as if they were hacktivist actions. In fact, it is not hacktivism, but intelligence or information warfare.

According to Joe Gallop's[21] opinion 'in several cases we have observed groups pursuing publicly destructive hacktivist-like actions, – and sure enough, in some cases - these activities were supported by a nation state.[22] Attacks of the Al-Quassam Cyber Fighters, the Anti WMD Team, Parastoo, the Syrian electronic army and the Cyber Berkut are fine examples. Growing tendencies have left no hope for any possible decline in the past two years. However, some observers find that the nature of hacktivism might have changed after a few activists have been arrested.[23]

In the past few months, Anonymous pursued actions against ISIS and Vladimir Putyin, however, quite a few commentators noted that these operations could not bring such great results as the previous acts of the past. Basically, this originates in the fact that both targets are much more difficult to localize than any governmental institution or international financial service provider, for instance. For the latter, it was actually easy to gather a large a number of participants in order to reach the defined goal, but, for example, the Islamic State of Iraq and the Levant does not have an internet surface with central access where it would be able to communicate with numerous visitors of its own, so from the hacktivists' point of view such targets and enemies operate in a rather decentralised and diversified way.

Future hypothesises

Experts make two directions probable: according to the first one hacktivism shall grow stronger, while according to the other, it shall loose its significance.

International vice-president of ISACA and security strategist of Dell, Ramses Gallego claims that hackting is a new form of protest that shall not terminate, on the contrary, it has gained ground as the form of threat that corporations, organisations and governments should definitely be aware of and prepared for. Hacktivism is undoubtedly a global phenomenon that is now getting more and more attention, but it can be harmful as well. Some see it as way of protesting, nevertheless, they must be aware of the fact that when political and religious motivations drive a movement, such protests

21 Head of the Hacktivism Intelligence Practice at ISIGHT Partners

22 Joe Gallop: *Real worlds wars go online in Network Security*, Elsevier Ltd, Oxford, 2015.

23 Arrests of teenagers who introduced themselves as members of Anonymous, or the FBI striking on Hector Xavier Monsegur, a 28 year old Puerto Rican, who proved to be the head of the hacktivists group known as Sabu a LuzSee. He is accused of committing several computer attacks against American enterprises, amongst them against the New York Corporation, the intelligence consultant Stratfor, against British and American law enforcement bodies and against Irish political party Fine Gael.

might lead to far-reaching and unpredictable consequences. He further states that "I believe that we have to recognize that further threats and attacks may originate for any part of the globalised world."[24]

According to Joe Gallop's opinion on the bare results of the Anonymous offensive targeting ISIS and Vladimir Putyin, "surely Anonymous does not have the power it has possessed before, and chance of revival are rather meager."

Characteristics of hacktivism is likely to change, shifting from barefaced destruction – like a DDoS attack, for instance – towards covert intrusions requiring higher level of qualifications and skills, since the possible targets prepare for such eventual attacks both technologically and technically, furthermore, participants of the movement are willing to veil their identity due to their fear of retribution.

Notwithstanding the above, the hacktivist attacks threatening Hungary are often parallel to terrorist threat. Actually, neither of them have any specific reason to take Hungary into consideration as a target, however, if such attack would occur the country would have to face enormous hostile potential. Building up the resistance of the entire governmental information technological system against hostile cyber-warfare would be a rather costly development; the country cannot be expected to spend major sources for a purpose that is unlikely to occur.[25]

We cannot foresee the forms of protest in the near future, but we can assume that as we approach an information society even more online activities shall be more appreciated, and shall function as the possible foundation of further movements, as we experienced with the internet tax issue. Chances that protests of political means would be projected at online surfaces, and taking over public areas, demonstrations, blocking roads, performances and other 'offline' protest forms would fade into the background are rather minor.

Nevertheless, a new form of protest activities is being shaped, a special mixture of hacktivism and social engineering known as mediahack, whereas representatives of hacktivists familiar with the internal operational rules of the media – by making use of its deficiencies, but with the cooperation of the media – forward and share information with numerous addressees, that the media otherwise would not have broadcasted, if it had known the facts.

Today, there is no need for grand infrastructure under the control of the entity willing to share notions and ideas with others – there is no need for young revolutionaries to overtake a press using violence and share their pamphlets with the masses taking on serious risk. Some IT skills to secure anonymity and to start a spark to launch a process is quite enough. However, generating movements and shaping the minds of people for a political or social reason is much more difficult. Actually, even ISIS was able to fan-

24 Ramsés Gallego: *Origins of hacktivism in Network Security*, Elsevier Ltd, Oxford, 2015.

25 It is obvious that circumstances force national governments to take such actions. Hungary shall not oblige its citizens to build earthquake-proof properties. Due to series of attacks suffered, Israel has implemented its entire administrative and social structure to avoid and reduce terrorist threat. After the events that took in 2007, information security awareness has gained grounds amongst citizens and on governmental level as well, alongside with the support and dedication of sources to developments.

tasize people this way in several cases. Consequently, internet surfaces and especially hacktivism can easily become means of marketing and recruitment for numbers of radical groups.The following graphics shall demonstrate the presence and vulnerability of hacktivism.

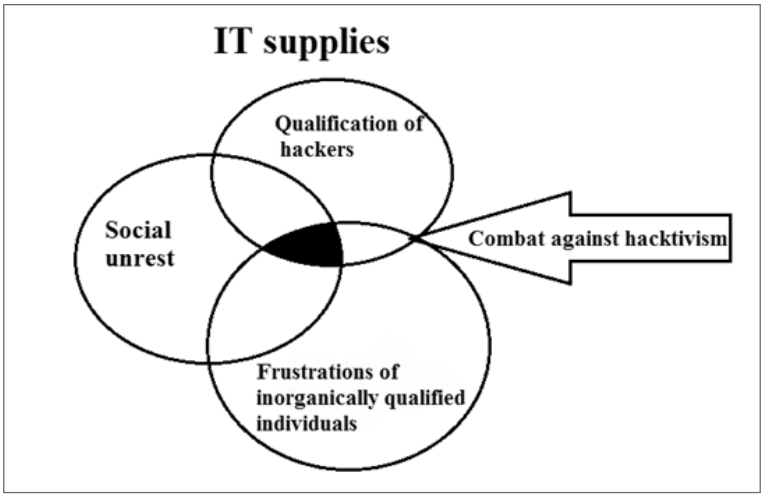

Figure 3. The presence and vulnerability of hacktivism

The entire system of relations may only be embedded into the IT environment of the given country. It is easy to admit, that hacktivism is unlikely to find soil in a settlement where citizens, enterprises or governmental institutions are not dependent on their IT systems.[26]

We may stipulate the following areas:

- The first one is the qualification necessary for the hacker activity. If the number of persons opposing social rules and able to carry out attacks against information systems is low, or their skills are not sufficient enough, this area shall be small.
- The second issue is the frustration and well-being of the qualified IT experts. Individuals with strong IT skills may only be radicalized if they are displeased with their circumstances. Changes in demand and supplies can lead to interesting alterations. In case of an eventual recession that is similar to a dotcom balloon IT experts would become bored, frustrated or unemployed, consequently, it would result in the extension of this section.
- The third set represents social unrest. In case of wide-spread social issues (for example, escalation of the migration crisis, mass unemployment, significant raise of living costs or taxes) the well trained individuals will identify with the unrest of the masses, even if they are much effected by the problem.
- Finally, we find hacktivism in the overleaping area of the sets.

26 For example, if an eventual compromise or termination of a customer site becomes public only days after the attack, we may assume that there are no serious problems.

Naturally, the field represented by the overleaping sets is also influenced by the intensity of the governmental combat against hacktivism. The measures of this combat: criminal regulations, criminal procedural rulings, data retention and data providing policies, personnel and professional conduct of the given law enforcement bodies.

These measures are represented by the arrow in the above graphics, demonstrating that any growth in these means would part and separate the sets from each other, simultaneously decreasing the power of hacktivism stipulated in the overleaping area.[27]

In connection with the authorities' activities we must take note, that if law enforcement bodies would initiate criminal procedure for every illicit action, it would be the same, as if we had reported an offence against anyone who illicitly picked some apples from the branch of our tree stretching out to a public road. Surely, actions should be taken against those who reach through the fence to steal the fruit. Obviously, it is much more efficient to narrow the space between the benches of the fence, but it also advisory to plant the apple tree further away from the fence. Consequently, it must be secured that protected data, information and processes are segregated and operate separately when establishing the information systems of the system parts of crucial importance, also, they must be protected by both technical and personal means. IT protection in itself is insufficient and would be rather expensive. Progressing the information security awareness of the personnel is just as important. The newly established 'Nemzeti Kibervédelmi Intézet' and the applicable legal provisions point in this direction.

A former study proved that the majority the hacker community in Hungary has patriotic sentiments and would be willing to give assistance to the execution of cyber-protection activities (for example to testing).[28] By these means, the hacker community does not only represent a source of danger, but also it embraces participants willing to cooperate in the protection of the systems of key importance.

According to my personal opinion, the trajectory of pure hacktivism – whereas some try to achieve political goals by using mainly IT means – shows an obvious decline.

Undoubtedly, movements consisting of different political activists have learnt from hacktivists. I find that hacktivist activities become more and more important measures of protesting, and cases when they are the form of protest are being excluded.

BIBLIOGRAPHY

Manuscript closed: 2015. October

Assange, Julian: *Cypherpunks: Freedom and the Future of the Internet*, New York, 2012.

Casserly, Martyn: *Who is Anonymous? A short history of hacktivism*. Source: www.pcadvisor.co.uk/features/internet/3414409/what-is-hacktivism-short-history-anonymous-lulzsec-arab-spring/ (10.04.2015)

Critical Art Ensemble, 1996. Electronic Civil Disobedience and Other Unpopular Ideas. Source: www.critical-art.net/books/ecd/index.html (06.04.2015)

27 We must take note that the actions of the authorities raising to dust might be contraproductive amongst the persons who stand for the idea of the freedom of information and those who use info-communication devices on a regular basis.

28 Krasznay: *op. cit.*, 98.

Denning, Dorothy: *History of Hacktivism.* Source: www.schneier.com/blog/archives/2015/09/history_of_hack.html (05.10.2015)
Gallego, Ramsés: *Origns of hacktivism,* Network Security, Elsevier Ltd, Oxford, England, May 2015, Source: www.journals.elsevier.com/network-security (05.10.2015)
Gallop, Joe: *Real worlds wars go online,* Network Security, Elsevier Ltd, Oxford, England, May 2015, Source: www.journals.elsevier.com/network-security (05.10.2015)
Guillermo Fernandez, Ampie: Wikileaks and Freedom of the Press, 2010, Source: www.havana-times.org/?p=31387 (14.09.2015)
Halász Áron: Ők az Anonymous – interjú a hackermozgalom magyar csoportjával Source: www.mohaonline.hu/eszme/anonymous_hacker_mozgalom_magyar_interju (10.04.2015)
Hao, Li: *Who is LulzSec, Hacker of PBS? Are they hacking Sony again?* International Business Times, 3 June 2011.
Hatamoto, Michael: *Anonymous vs. the ISIS Cyber Caliphate -- War in the Middle East Goes Digital* Source: www.dailytech.com/Anonymous+vs+the+ISIS+Cyber+Caliphate++War+in+the+Middle+East+Goes+Digital/article37154.htm (23.04.2015)
Houghton, Tessa Jade: *Hacktivism and Habermas: Online Protest as Neo-Habermasian Counterpublicity,* PhD thesis, University of Canterbury, 2010.
Howes, Jon: *IoT multiples risk of attack,* Network Security, Elsevier Ltd, Oxford, England, May 2015, Source: www.journals.elsevier.com/network-security (05.10.2015)
Jordan, Tim, Taylor, Paul: *Hacktivism and Cyberwars: Rebels with a Cause?* Routledge, 2004.
Krasznay Csaba: *A magyar elektronikus közigazgatási alkalmazások információbiztonsági megoldásai*, PhD thesis, Zrínyi Miklós Nemzetvédelmi Egyetem Katonai Műszaki Doktori Iskola, 2011.
Ludlow, Peter: *What Is a 'Hacktivist'?* Source: http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/?_r=0 (11.09.2015)
Mills, Elinor: *Old-time hacktivists: Anonymous, you've crossed the line*. Source: www.cnet.com/news/old-time-hacktivists-anonymous-youve-crossed-the-line/ (08.04.2015)
Olson, Parmy: *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*, Hachette Digital Inc., 2012.
Tsotsis, Alexia*: RIAA Goes Offline, Joins MPAA As Latest Victim Of Successful DDoS Attacks*. Source: http://techcrunch.com/2010/09/19/riaa-attack/. (15.08.2015)
Vörös András: *Kiberbűnözés, különös tekintettel a hacktivizmusra*, thesis, NKE RTK, 2015.
Weisenthal, Joe: *Notorious Hacker Group LulzSec Just Announced That It's Finished*, Business Insider. Source: www.businessinsider.com/lulzsec-finished-2011-6 (01.10.2015)

ABSZTRAKT

Hacktivizmus és helyzete Magyarországon

SIMON Béla

Az elmúlt évek során kialakult és a hétköznapi nyelvben is meghonosodott a hektivizmus fogalma. A médiából érkező hírek szerint a mindennapi életünk ki van szolgáltatva az infokommunikációs eszközöknek, mint egy kártyavár a szélben. Ezt az állítást több tudományos forrás igazolta. A hírek egy másik csoportja szerint ezt a kártyavárat egy titokzatos mozgalom – a hektivisták – bármikor összeboríthatják. Dolgozatomban megpróbálom megvizsgálni, hogy van-e valós alapja Magyarországon a hektivista mozgalmakról szóló híreknek, vagy csak egy jelenség démonizálásáról van szó.

Kulcsszavak: *hektivizmus, Magyarország, kibervédelem, Anonymous, Kormányzati Eseménykezelő Központ*