HOW THE SOCIAL MEDIA MAY BE USED TO PARALYSE THE CRITICAL INFRASTRUCTURE?[1]

Péter Bányász

Abstract: *The social media plays increasing role in our present life. I would like to demonstrate in this article how the new media platform may threaten critical infrastructure systems. I have identified three priorities in this regard; those are all parts of the same structure. The first priority area is open source intelligence. Social media is often used for this purpose. As my second point, I will assess the role of the individual responsibility. Finally, I would raise the attention to the importance of critical infrastructure vulnerability analyses with the involvement of IT experts. To bring "white hat hackers" for the favour with the topic of critical infrastructure protection I consider strong relevance in the promotion of the aims of the defence agencies such as the armed forces, security services, and law enforcement. In the same time highlight certain risks and also some opportunities social media concerns. I propose more public attention for promoting these intentions and, in general for the topic itself, that may lead to get more support from IT specialists, researchers and even from the wide spheres of the public.*

Keywords: critical infrastructure, social media, cyberspace, OSINT, social engineering

1. Introduction

A new era began on 19 July 2012. Barack Obama, the President of the United States submitted the Cyber security Act to the Senate[2] that clearly indicates that in our changed world the concept and the methods of warfare have been fundamentally transformed by information operations. This is an important date because it indicates that the increasing demand to give the appropriate answer to one of today's greatest challenges, cyber warfare, is now handled as a priority at the highest level. After all, cyberspace is inherently a kind of space where you cannot apply the kind of warfare that was common practice in the past few millenniums. This kind of development greatly facilitates asymmetric warfare, which can provide extra benefits to terrorists.[3]

Threats of cyber attacks are no novelty to the people working in the field of security and defence policy. However, the general public (whose ignorance, as we shall see, comes

[1] This article was elaborated with the support of the Critical Infrastructure Research Project TÁMOP-4.2.1.B-11/2/KMR/001

[2] GROSSE, Grant: Obama Administration Supports New Cybersecurity Bill, PC World, 26. Jul, 2012. ISSN: 0737-8939 . See at http://www.pcworld.com/article/259906/obama_administration_supports_new_cybersecurity_bill.html, (Downloaded: 6 October 2012.)

[3] Horváth, Attila: Terrorfenyegetettség, célpontok, nagyvárosok közlekedése, Nemzetvédelmi Egyetemi Közlemények. A Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Lapja. 10. évfolyam 3. (tematikus) szám. Budapest, 2006.

in handy for the cybercriminals in many cases) and the decision makers do not have sufficient knowledge in this matter.
Several studies have drawn attention to the shortcomings in handling the threats coming from cyberspace. These include the study of Attila Horvath from 2010 called „How to explain the necessity of the complex interpretation of critical infrastructure and the importance of its protection" and that of Csaba Krasznay and Laszlo Kovacs from 2010 called "Digital Mohacs – the scenario of a cyber attack against Hungary". As the authors demonstrate there are currently a lot of shortcomings in these areas. Reflecting these documents, the present study aims to draw the attention of decision makers to the urgency of the development of our weak cyber protection skills. However, this requires a strategic concept applying to several areas:

- appropriate legislation;
- education should be extended to raise the user awareness of the citizens as well as to prepare the public for a possible crisis;
- close collaboration with research units.

Failures and damages of critical infrastructure may result from circumstances independent of human activities, such as natural disasters, but also from intentional damage (terrorism[4], military attack). We shall only cover this latter herein, more specifically computer attacks against the elements of a critical infrastructure, or more precisely a special area within the scope of cyber protection, namely the hazards generated by social media, the tools of which can be used for attacks against critical infrastructure.

2. Social Media

Social media is „a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content"[5] That said, social media tools are the ones used by the users for creating and sharing content, the platform of which is provided by a specific service provider. Such contents may be written, image, video and music formats. Social media tools are thus social networking, image and video sharing sites as well as blogs and micro-blogs.
Today, the use of various devices has become so widespread that their role in military science cannot be underestimated. All the more so since some social media tools can be used for military promotion, crisis communication management, communication of the soldiers with their family members, the interpretation of military events to form public opinion[6], but it is also great for open-source intelligence, or in extreme cases for influencing the internal political affairs[7] of certain nations in our favour[8] or for preparing attacks against critical infrastructure, which we are discussing.

[4] Nowadays terrorist organisations use computers regularly for online communication, for propaganda and for preparing cyber attacks. As Attila Horváth pointed out *„In the organisation of al-Qaeda we can find the most up to date organising principles, for their working they use all the tools and methods of modern communication in a wide range. Because of the international act and pursuit angainst the network and illegal activity, groups separated from each other, unfortunately can efficiently organise and accomplish acts of terror in separate parts of the world."* In. HORVÁTH, Attila: Az élelmiszerellátási lánc kritikus infrastruktúrái, terrorfenyegetésének jellemzői, Hadmérnök, 2009.

[5] KAPLAN, Andreas- HAENLEIN, Michael, Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons,2010.

[6] See e.g. the shocking video which was made by the syrian rebels, it was uploaded to youtube, and preceded the electric media which took the recordings from the video sharing sites

[7] See events of Arabic Spring

[8] It might be not accidental that the Iran government/leadership decided to disconnect the country from the internet and develop an own network. Its last step was to prohibit Google services. (According to

In the following we will examine how critical infrastructure may be paralyzed by the use of social media.
There are four areas with relevance to our topic that I want to address: open-source intelligence, personal liability, building a positive perception of the army, one of the aims of which is the involvement of hackers in the protection of critical information infrastructure, and finally a brief note on the role of crisis communication and education.

3. Open Source Intelligence

Open Source Intelligence refers to intelligence collected exclusively from publicly available sources and analysed thereafter. Such open sources include traditional and electronic media, the Internet, libraries, studies by experts etc. Since the information is freely available it is obviously no substitute for knowledge derived from classified information, but information obtained from these sources can help you navigate through classified information. Analysis of social media plays a significant role in providing internal security of the United States. FBI uses advanced software to analyse social media in real time and combine the obtained information with information from other sources[9]. The great advantage of OSINT is that it allows free and real-time access to information for everyone at a relatively low cost. The disadvantages are the large number of available data, and the inaccuracies or intentional misinformation contained in some materials.
Let's take a closer look at what kind of data you can access by applying open-source intelligence to the elements of social media. First we will select our target, the seat and sites of which can be found on its official website. Whether this target is public utilities, public transport or other institution serving as critical infrastructure is irrelevant. Afterwards a number of free services are available enabling us to download a satellite image or even 3D map images of the site to be attacked.
In many cases video sharing sites can also help attackers in exploring the target since a lot of videos made by amateurs are uploaded to these sites which may provide us with some missing information when searched for purposefully. However, it is important to point out another aspect as well. With a slightly larger than average aptitude for conspiracy, that may reasonably be expected from a group planning to attack critical infrastructure, these may easily be used for sharing information between individual members of the group without arousing any suspicion. Just think about it, by using a smartphone, allowing us to record HD-quality images, we can make important recordings in the vicinity of the target and then disguise them with a legend. After that it only takes a few minutes to upload them to a video-sharing site so that the insiders could watch and find what they need while visitors checking it accidentally shall find just another uninteresting video.
Another source for open-source intelligence are the different social networking sites and mobile platforms, which we shall examine from the perspective of personal liability.

---

official account because of the mocking video of Mohamed), but the truth might be that they're affraid of a similiar events like the Arabic Spring, In. DIAZ, Jesus: Iran Shuts Down Google, Will Completely Cut Citizens Off the Internet, In Gizmodo, 24. September, 2012., See at http://gizmodo.com/5945862/iran-shuts-down-google-will-completely-cut-citizens-from-internet, (Downloaded: 25 September 2012).

[9] WITECKA, Magdalena: Social media for National Security, 7th PhD Conference - New trends in National Security, University of Defence, Brno, 2012.

4. The Individual Responsibility

In general, a vast majority of users do not bother with the protection of their personal data or complying with the security guarantees required by the applied IT tools. This is exactly the kind of ignorance taken advantage of by cybercriminals. However, it might be a good idea to split the issue into two parts.

Continuing the train of thought of the previous section, a lot of open-source intelligence may be gathered with the unconscious help of careless users[10]. Although in material terms the use of social media is free of charge in many cases, there is a huge price to pay for the quasi-free usage: we provide these firms with our personal information, our own social network, almost every little detail of our lives, and afterwards the collected information is sold to different companies for advertising purposes.

A conference recently published on the Internet examines the statutory data collection of mobile service providers. The lecture of Malte Spitz called "Your phone company is watching" paints a gruesome picture[11]. Mobile and internet service providers are required by EU and national legislation to store the subscriber-related data such as the duration of conversations, the name of callers and called parties, the date, content and receiving party of text messages sent, the locations where the phone was used and the actual location of the owner for a minimum of six months up to two years. Malte Spitz has made a shocking video from the data stored by the service providers, mapping how often the phone was used and for what purposes, where the owner went and what means of transport he used etc.[12]. While service providers are required by law to collect these data, we provide access to our data for social media sites voluntarily. Take the example of Facebook that, in response to the European Data Protection complaints has temporarily turned off its facial recognition software in Europe until it can be redesigned to dispel these concerns[13]. The facial recognition software was introduced last summer by the social networking site. It is capable of automatically recognizing the users registered on the site on the uploaded photos.

Today, an increasing amount of social media tools are moving to mobile platforms[14]. The practical use of smartphones and tablets is provided by different applications. Some applications, whether used on social networking sites, news sites, video sharing sites or maps require different authorizations. The most popular social networking tools require access to the following data, to mention the most important ones: contact details of all our partners, how often and for how long we communicate with these partners, reading our text messages and e-mails, our location using GPS. The vast majority of users have no idea that they actually provide access to these data. Mobile applications obviously carry other risks beyond the above listed security hazards. There may be viruses hidden

---

[10] It was a sensation in 2009 when new chief's wife of the British Secret Intelligence Service (a.k.a. MI6) posted unguardedly in her facebook profile their contacts and some moments of their private life. WALKER, Kirsty: Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net, In. Daily Mail, 6. June, 2009. ISSN: 0307-7578, See at http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html , (Downloaded: 28. September, 2012.)

[11] SPITZ, Malte: Your phone company is watching, In. TED, June, 2012, See at http://www.ted.com/talks/lang/en/malte_spitz_your_phone_company_is_watching.html , (Downloaded: 25. September, 2012.)

[12] Tell-all telephone, In. Zeit Online, ISSN: 0044-2070, See at http://www.zeit.de/datenschutz/malte-spitz-data-retention, (Downloaded: 7. October, 2012.)

[13] SENGUPTA, Somini - O'BRIEN, Kevin J.: Facebook Can ID Faces, but Using Them Grows Tricky, In. The New York Times, 21. September, 2012., ISSN: 0362-4331, See at http://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html?_r=0, (Downloaded: 22. September, 2012.)

[14] Smart phones, tablets

in popular applications enabling hackers to take control of the phone's camera and transfer the obtained information to the desired location[15].

The latest results of the Norton Cybercrime Report, one of the world's largest researches on cybercrimes have recently been published by Symantec[16]. The report published annually aims to provide a comprehensive picture of the impact of cybercrimes on consumers as well as the security requirements of the development and application of new technologies. For the 2012 survey more than 13,000 adults in 24 countries were interviewed. The conclusion is startling: every second 18 people fall victim of cybercrime that means one and a half million people per day internationally. When breaking down the financial loss to the individual level, the average direct financial loss per user resulting from online crime amounts to $197 which equals to the monthly food consumption of a typical Hungarian family of four. In the past 12 months 556 million adults fell victim of online crime worldwide, which is more than the entire population of the European Union. This figure means that 46 per cent of adults using the Internet fell victim of cybercriminals last year, similarly to the figures of 2011 (45 per cent). The study highlights the changing trend in cybercrime directed more and more against social networking sites and mobile applications:

- 15 per cent of the users of social networking sites reported that someone broke into their profiles and used the site on their behalf;
- one in ten users admits to have fallen for scams or false links spread on social networking sites;
- while 75 per cent are aware that cybercriminals have turned their attention toward social networks, less than half of them (44 per cent) use a security solution protecting them from the threats of social networking sites and only 49 per cent use the privacy settings to choose who they share the information with;
- almost one third of mobile phone users (31 per cent) received text messages from unknown numbers asking them to follow a link or dial an unknown number to access a voicemail message.

Almost every attacked IT system is equipped with a complex protection preventing or significantly restraining access to information through computer intrusion. To bypass this, attackers have recourse to Social Engineering by means of which the desired information is accessed by gaining the users' trust, fraud, or even violence and blackmail. By using the above tools we can easily gain the trust of users ignoring privacy considerations or use the obtained information against them.

Another aspect of personal liability is the possibility of using social media tools to create zombie networks. Zombie machines are tools that take control of the computer through a malware without the user's knowledge. In many cases the user does not detect anything because the infected software fulfils an otherwise useful function on the computer, but in the meantime such program elements are installed that may perform undesired operations. The length of this study does not permit me to go into more details on the technical background of cyber attacks so we will only attempt to briefly outline how IT devices can be switched into a zombie network by using social media tools. As mentioned above, the vast majority of users do not use anti-virus software and

[15] Kémkedhet utánunk a kamerás telefon [Our own cell phone may spy on us], In. Index, 1. October, 2012., ISSN: 1585-3241, See at http://index.hu/tech/2012/10/01/kemkedhet_utanunk_a_kameras_telefon/, (Downloaded: 1. October, 2012.)

[16] Symantec: Norton Cybercrime Report-2012, See at http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf , (Downloaded: 4. October, 2012.)

neglects the importance of protecting IT devices. It is a general trend on social networking sites that various entertaining applications are used for fun.

These applications often take advantage of the inauspiciousness, naivety or ignorance of people[17], whereby in the "mildest" case access is requested or viruses are downloaded to the user's computer[18]. The threats of phishing and machines infected with viruses have been discussed previously so I will not cover them again.
However, it is essential at this point to emphasize the importance of raising the user awareness of the citizens. The U.S. Army provides an excellent example thereof since they published a handbook[19] on social media in February 2011 with several recommendations including those on the presentation of the required security settings[20].
This type of education is not merely intended to avoid the undesired - and in many cases illegal - use of personal data or to protect IT devices from being used for unconscious participation in the above mentioned scenarios. We think it is equally important to prepare the citizens for an eventual attack against or failure in critical infrastructure.

5. Marketing

Now that we have discussed the threats and risks of social media, let's talk about the positive opportunities provided by this tool. In chapter "Protection Options" of the previously mentioned study "Digital Mohacs"[21] the authors declare that it is essential for defence planning purposes to involve the hackers in the protection of critical infrastructure. However, this requires strategic thinking creating the possibility of building a positive perception of the army. This can be achieved by using the social media.
Don't forget that the famous Anonymous[22] group was formed by the members of a forum called „4chan" which launched several attacks over the years in order to influence the internal decision making process of different nations and in many cases they did succeed. In order to reach these hackers a new strategy is required that includes

[17] An excellent example the "what's your indian name?" application, which was used by over 8000 users. Aftwerwards it turned out that application was developed by a jewelry shop, and they used all of the datas of the users for their ad campaigns, In. BERÉNYI, Konrád: Pukkadjatok meg, In. Onlinemarketing blog, 12. December, 2011., See at http://onlinemarketing.blog.hu/2011/12/11/pukkadjatok_meg, (Downloaded: 7. October, 2012.)

[18] In this case the hackers usually made fake news about the celebrities (e.g. see somebody drunked or naked) to exploit the credulousness, naivety, curiousity of the users to infect the computers by clicking on the link.

[19] Online and social media division, Office of The Chief of Public Affairs: U.S. Army Social Media Handbook, 1500 Pentagon, Washington DC, January, 2011., See at http://fbmonitor.com/social_media_handbook.pdf, (Downloaded: 29. September, 2012.)

[20] The risks of such an incident to be illustrated from 2007: New helicopters arrived to an Iraqi base, which were photographed and uploaded to the community sites by using mobile phones of the soldiers from the base. They did not expect that the mobile phone recorded the geolocational data that were fallen into hands of the insurgents, who destroyed 4 AH-64 Apache helicopters by indirect mortar fire. See in: MARTON, Péter.: Hírszerzési trükkök: iraki gerillák vs. Apache helikopterek [Intelligence tricks: Irqi guerillas vs Apach helicopters] In. Kprax blog, 16 March 2012 See at http://kprax.blog.hu/2012/03/16/hirszerzesi_trukkok_iraki_gerillak_vs_apache_helikopterek, (Downloaded: 28. September, 2012.).

[21] The expression of „Digital Mohács" reflects to the historical event, the battle of Mohács (29 August 1526 A.D.) when Turks defeated the army of Louis II king of Hungary and Bohemia. At this moment not only the battle was lost, but the king and the country as well. KOVÁCS, László-KRASZNAY, Csaba: Digital Mohács, Nemzet és Biztonság, Budapest, 2010.

[22] ANDERSON, Nate: Who Was That Masked Man? In. Foreign Policy, 31. January, 2012. ISSN: 0015-7228, See at http://www.foreignpolicy.com/articles/2012/01/31/who_was_that_masked_man, (Downloaded: 29. September, 2012.)

the popularization of the army with the help of web 2.0 tools since these are the areas that offer a real chance of addressing hackers and "digital natives"[23].

6. Crisis Communication

Finally I would like to talk about the role of social media in crisis communication. Nowadays news are consumed primarily through social media, thus it is a perfect platform to broadcast information in an emergency situation besides the standard media. Its great advantage is that the information is displayed in real time. Remember when the Americans assassinated Osama Bin Laden in Pakistan: a nearby resident, without knowing what the actual event was, broadcasted it live on Twitter.
The hazards and risks are known. Are we ready?

References

[1] ANDERSON, Nate: Who Was That Masked Man? In. Foreign Policy, 31. January, 2012. ISSN: 0015-7228, See at http://www.foreignpolicy.com/articles/2012/01/31/who_was_that_masked_man. (Downloaded: 29. September, 2012).

[2] BERÉNYI, Konrad: Pukkadjatok meg, In Onlinemarketing blog, 12. December, 2011. See at http://onlinemarketing.blog.hu/2011/12/11/pukkadjatok_meg. (Downloaded: 7. October, 2012).

[3] DIAZ, Jesus: Iran Shuts Down Google, Will Completely Cut Citizens Off the Internet, In. Gizmodo, 24. September, 2012. See at http://gizmodo.com/5945862/iran-shuts-down-google-will-completely-cut-citizens-from-internet. (Downloaded: 25. September, 2012).

[4] GROSSE, Grant: Obama Administration Supports New Cybersecurity Bill, In. PC World, 26. Jule, 2012. ISSN: 0737-8939, See at http://www.pcworld.com/article/259906/obama_administration_supports_new_cybersecurity_bill.html. (Downloaded: 6. October, 2012).

[5] HORVÁTH, Attila: Az élelmiszerellátási lánc kritikus infrastruktúrái, terrorfenyegetésének jellemzői, Hadmérnök, 2009. ISSN: 1788-1919, p.441.

[6] HORVÁTH, Attila: How to explain the necessity of the complex interpretation of critical infrastructure and the importance of its protection, Hadmérnök, 2010. ISSN: 1788-1919.

[7] HORVÁTH, Attila: Terrorfenyegetettség, célpontok, nagyvárosok közlekedése, Nemzetvédelmi Egyetemi Közlemények. A Zrínyi Miklós Nemzetvédelmi Egyetem Tudományos Lapja. 10. évfolyam 3. (tematikus) szám. Budapest, 2006. ISSN: 1417-7323, p.16.

[8] KAPLAN, Andreas. HAENLEIN, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010. ISSN: 0007-6813.

[9] Kémkedhet utánunk a kamerás telefon, [Our own cell phone may spy on us], In. Index, 1. October, 2012. ISSN: 1585-3241, See at: http://index.hu/tech/2012/10/01/kemkedhet_utanunk_a_kameras_telefon/. (Downloaded: 1. October, 2012.).

[10] KOVÁCS, László, KRASZNAY, Csaba. Digital Mohacs – the scenario of a cyber attack against Hungary, Nemzet és Biztonság, 2010. ISSN: 1789-5286.

[23] PRESNSKY, Marc: Digital Natives, Digital Immigrants, On the Horizon. MCB University Press, Vol. 9 Iss: 5, pp.1 – 6 No. 5, 2001.

[11] KOVÁCS, László: Informatikai hadviselés kínai módra, Nemzet és Biztonság, 2009. szeptember ISSN: 1789-5286.
[12] MARTON, Péter: Hírszerzési trükkök: iraki gerillák vs. Apache helikopterek, [Intelligence tricks: Irqi guerillas vs Apach helicopters]. In Kprax blog, 16. March, 2012. See at http://kprax.blog.hu/2012/03/16/hirszerzesi_trukkok_iraki_gerillak_vs_apache_helikopterek. (Downloaded: 28. September, 2012)
[13] Online and social media division, Office of The Chief of Public Affairs: U.S. Army Social Media Handbook, 1500 Pentagon, Washington DC, January, 2011. See at http://fbmonitor.com/social_media_handbook.pdf , (Downloaded: 29. September, 2012).
[14] PRENSKY, Marc. Digital Natives, Digital Immigrants, On the Horizon. MCB University Press, Vol. 9 Iss: 5, pp.1 – 6 No. 5, October 2001. ISSN: 1074-8121
[15] RÁCZ, Lajos: Informatikai hadviselés nem csak kínai módra, Nemzet és Biztonság, 2010. február ISSN: 1789-5286.
[16] SENGUPTA, Somini- O'BRIEN, Kevin J. Facebook Can ID Faces, but Using Them Grows Tricky, In. The New York Times, 21. September, 2012. ISSN: 0362-4331, See at http://www.nytimes.com/2012/09/22/technology/facebook-backs-down-on-face-recognition-in-europe.html?_r=0 , (Downloaded: 22. September, 2012.).
[17] SPITZ, Malte: Your phone company is watching, In. TED, June, 2012. See at http://www.ted.com/talks/lang/en/malte_spitz_your_phone_company_is_watchin.html , (Downloaded: 25. September, 2012.).
[18] Symantec: Norton Cybercrime Report-2012, See at http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf. (Downloaded: 4. October, 2012.).
[19] Tell-all telephone, In. Zeit Online, ISSN: 0044-2070, See at http://www.zeit.de/datenschutz/malte-spitz-data-retention. (Downloaded: 7. October, 2012.).
[20] WALKER, Kirsty: Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net, In. Daily Mail, 6. June, 2009. ISSN: 0307-7578, See at http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html. (Downloaded: 28. September, 2012.).
[21] WITECKA, Magdalena: Social media for National Security, 7th PhD Conference - New trends in National Security, University of Defence, Brno, 2012. ISBN: 978-80-7231-876-6.