GUIDE

ONLINE MEDIA AUTONOMY: SECURITY RISKS AND PROTECTION MECHANISMS

WALKING ON THE DIGITAL EDGE

SHARE FOUNDATION - 2015

Guide

" GUIDE ONLINE MEDIA AUTONOMY: SECURITY RISKS AND PROTECTION MECHANISMS",
WALKING ON THE DIGITAL EDGE
SHARE FOUNDATION
OCTOBER 2015
EDITORS: ĐORĐE KRIVOKAPIĆ, VLADAN JOLER
TEXTS: NEVENA KRIVOKAPIĆ, BOJAN PERKOV, MILICA JOVANOVIĆ
PROOFREADING:MILICA JOVANOVIC
DESIGN AND LAYOUT: OLIVIA SOLIS VILLAVERDE
PRINTING: NS PRESS DOO NOVI SAD
CIRCULATION: 200

SUPPORT FOR THE PROJECT:

FONDACIJA ZA OTVORENO DRUŠTVO, SRBIJA
OPEN SOCIETY FOUNDATION, SERBIA

Kingdom of the Netherlands

CIVIL
RIGHTS
DEFENDERS

ABSTRACT

Cyber attacks on online media and journalists in Serbia have recently become more frequent. Websites were targets of DDoS attacks which hindered traffic, but also by attacks that harmed the integrity of databases. The authorities have not yet solved any of the cases SHARE Foundation was involved in reporting. Journalists faced challenges of social engineering, online identity theft and impersonation and unauthorised access to private communication. Citizen journalists and active participants in public debates were struck by manipulations of public opinion, anonymous threats and intimidation, and also by authorities using double standards in processing cases of alleged abuse of freedom of speech.

In order to offer a better view on those issues we will asses the position of online media and journalists in the digital environment, particularly considering the fact that they carry confidential and sensitive information not only on their physical devices but all over the Web. This paper will therefore take a special focus on digital risks, like data loss or leakage, on tools for mitigating and avoiding these risks and accountable agents, as well as on relations between conflicting values, like that of privacy and security.

Finally, analysing the risks threatening basic human rights, and the weaknesses of the current system, we will suggest series of measures that the state should take in order to regain public trust in its capabilities to ensure protection.

KEY WORDS online media, journalists, digital security, cyber attacks, risks

INTRO-DUCTION

In the past two years, we have witnessed a sharp rise of human rights violations in the Serbian online environment. There were articles and videos that criticise the government mysteriously vanishing, blogs and news portals suddenly becoming unavailable while private email correspondence was exposed to the public, and citizens being brought in for questioning by the police for expressing their opinion on the Internet.

Particular cases of breach of online rights and freedoms that Share Foundation has been monitoring:

- Arbitrary blocking or content filtering ;
- Cyber-attacks on independent online and civic media;
- Arrests and judicial proceedings against social network users and bloggers;
- Public opinion manipulation through the use of technology;
- Surveillance of electronic communication, violation of rights to privacy and protection of personal data;
- Pressure, threats and diminishing safety of online and civic media, journalists and individuals.

KEY FINDINGS

Share Foundation has been monitoring digital rights and freedoms on Internet since May 2014. In this report we shall focus on the period between September 2014 and September 2015, after a brief overview of the key findings from the said period.

- Some 20 different online media websites came under DDoS attacks that interrupted or suspended their services. Some of them (like Peščanik and Teleprompter) were targeted more frequently and for longer periods of time
- During the state of emergency declared because of the floods in May 2014, at least 13 articles and blogs were taken down. This was a one-time incident
- By the end of summer of 2015, nearly 30 people were questioned, taken into custody or brought to court for views they shared on social networks or blogs.
- We have detected a variety of different malware and SQL injection attacks that compromised online media databases and computers.
- Journalists and individuals were victims of unauthorised access to their private correspondence
- Stories were published about leaked software and manuals allegedly produced for the ruling party on how to manipulate the perception of public opinion by overflooding news sites with positive or negative comments, votes and likes, depending on the topic.

- In April 2015 the most intrusive attack against a news site took place, when a hosting server, 4 email and 2 main social network accounts were taken over by an attacker. Although the site had solid security procedures (different random passwords, two step verification, etc.) the takeover was quite efficient. The attack aimed at destroying all available content and dissuading the site editor from doing any future work (which eventually did not happen).

- The Legal team of Share Foundation represents online media and CSOs that were targeted by cyber attacks, initiating about 10 legal procedures (mainly criminal). All procedures that are to be taken by the authorities are still pending. Additional legal aid services were provided for online media, activists and citizens in dozens of other cases.

TOP 5 CASES

1. TELEPROMPTER – FIRST CASE

Although notorious for its political incorrectness with occasional nationalistic outbursts, private blog Teleprompter grew into a typical citizen online media outlet, which is seldom seen in Serbia. One of the most visited websites of that kind, in the past couple of years Teleprompter is steadily focused on criticising the political party in power as well as its coalition partners.

Since it operates outside the circle of conventional media, the prevalent public discourse designates Teleprompter as irrelevant, untrustworthy and with dubious intentions and questionable sources. Yet, government representatives including top officials often engage in public arguments against various reports published on this website, rebuking some of the allegations even during formal public addresses.

Meanwhile, Teleprompter was acclaimed as a significant source most recently apparent when the web portal published a letter written by five U.S. Congress members to Vice-President Joseph Biden, which was later picked up by other news sites such as The Balkan Insight.

Teleprompter was the target of various sorts of cyber attacks over the past years, but two cases that took place in January and April of 2015 stand out as atypical and reveal some of the procedures attackers rely on in preparation of a main attack.

In early 2015, the publisher and editor of Teleprompter noticed strange activities on his website. Some 300 emails of unusual content came through the contact form available to website readers. As it turned out, it was an SQL injection, attempted malicious code injection into the database.

From the available evidence, the cyber security analyst at Share Foundation concluded that the attack was launched by a tool (Acunetix Web Vulnerability Scanner) of low efficiency, legal software used for website vulnerability scanning. Applied in this manner, the software utilises cross-site scripting (XSS) flaws of the system to bypass security measures and insert malicious code.

The simplest prevention of this kind of attack is to use reCAPTCHA validation for the user-dialogue system, as well as to include the 'escapeshellcmd()' function with the code that enables the system to block executable commands when so called meta-characters are written in a comment box.

Teleprompter filed a criminal complaint with the public prosecutor's office requesting investigation of this attack and criminal proceedings.

2. TELEPROMPTER – SECOND CASE

The attack targeting Teleprompter in April of 2015 so far represents the most complicated technical assault recorded in the online media community in Serbia.

The attackers took control over four email accounts owned by the editor of Teleprompter, that were protected with 2-Step-Verification, which means a code was sent to the owner's phone via text message at each login attempt. From the available evidence, and considering the two-step login procedure, Share's cyber analyst was not able to determine how the attackers obtained the access codes for the email accounts. In the ensuing criminal complaint, the legal representative of Teleprompter's editor suggested that the attackers may have intercepted the text messages containing the verification codes, which is undetectable to forensic tools and permissions available to citizens.

After the email accounts were taken over, their entire content was deleted and passwords and other security settings, such as the recovery phone number, were altered. Using those email accounts, the attackers accessed Teleprompter's public and the editor's private social network accounts.

One of the four email accounts had permissions to access the hosting server's control panel, which was used to delete articles and other content available on the website at that moment. Finally, by changing the port settings of the system, the incoming traffic was redirected to a Government website of Kosovo.

With technical assistance, Teleprompter's editor was able to take back the control of his website, and restore the content from the backup. Access to the four email accounts was also regained eventually, while the deleted messages were restored from the trash folder in all but one account that was thoroughly emptied.

From the server logs it was possible to locate at least that segment of the attack, while the question of obtaining passwords and especially possible interception of verification codes – remains open.

The Special Prosecutor for cyber crime initiated proceedings ex officio, while on May 12 2015 the publisher and editor of Teleprompter filed additional complaint with the legal assistance of Share Foundation. Legal proceedings are underway.

3. DRAGANA PEĆO

The Center for Investigative Reporting in Serbia (CINS), a non-profit NGO, was founded by the Independent Journalist Association of Serbia as an autonomous platform free from commercial pressures. The Center mostly focuses on topics related to higher level political corruption, financial and industrial crime.

CINS raised its profile as a modern team, aware of the essentially different environment it works in, using various technical solutions for protection of content, including encrypted communication.

After series of reports on the criminal background of the gambling industry and the Balkan narco cartel leader, as well as on poor crisis management during the floods in 2014 and non-transparent procedures for rebuilding in the aftermath, CINS became frequent target of public denouncements.

In mid-January, Dragana Pećo, at the time a CINS journalist, was called by a public relation representative of a state-run company that received a FOI request that was allegedly signed and submitted by the journalist. In the following days, it would turn out that the identical request signed by the same journalist was sent to several public institutions, state and private companies. The requests were sent from an email account registered at Gmail that the journalist had never used, nor created.

Furthermore, the only authentic document these emails contained was a standard electronic form of FOI request with a signature of the journalist.

False impersonation thus gained plausibility, so about twenty of the recipients of FOI requests sent from the fake email account actually replied. The electronic signature form was probably acquired from actual correspondence with the journalist.

The deception of the FOI request recipients speaks of undeniable case of false impersonation that damages the reputation of the journalist and the media organization she works with. Further, there are elements of gathering personal information with the intention of distributing them to unauthorised persons.

With the legal aid of Share Foundation, by the end of January a criminal complaint was filed with the public prosecutor's office against unknown person(s) on suspicion of damaging reputation, unauthorised disclosure of information, committing computer fraud, or of other criminal offense prosecuted ex officio.

4. PEŠČANIK

Launched as an online magazine of the citizens association Peščanik, the website succeeds a years long tradition of radio programme of the same name that the website editors used to make as an independent production for Radio B92. The format was expanded with texts and video podcast, while keeping its anti-nationalistic platform that brought them troubles with the authorities and the mainstream public opinion.

Earlier incidents of systematic radio jamming during broadcast, threats and assaults from Peščanik's 'analog' stage remained in past, without resolution. Since transferring to the digital environment, this media outlet has been exposed to constant attacks that became more intense and technically advanced since the floods in May of 2014, and particularly after the website published the analyses of plagiarised doctoral theses of several top state officials in June of 2014. A month later, during the malicious code attack, entire front page content was deleted and replaced with the message "Stop the lies" that was posted instead of original articles, headlines and section names. In November of 2014 three articles relating to plagiarised PhDs and their English versions, were deleted.

In April this year, unknown person(s) managed to upload two texts on the website, one of which was also placed on the website of the

"Danas" daily followed by a remark that it was retrieved from the Peščanik website. Due to this incident, Peščanik filed a criminal complaint against unknown person(s) for unauthorised access to the server, falsifying content and false impersonation.

In June of 2015 the website suffered the most severe DDoS attack in its history. According to data gathered by its technical/web administrator, the attack was launched by a 'brute force' search of SSH protocols – i.e. automatised attempts of breaking the system encryption used for securing channels between the server and the website. Analysing the server logs, the administrator established that SSH service suffered continuous attack coming from some 2000 IP addresses. Website editors pointed out that, by comparison, during the previous large attack two months earlier there were 280 IP addresses involved.

On this occasion, during the attack on SSH, several hundreds IP addresses were involved in simultaneous attack on other services like FTP, Postfix, and mySQL (system protocols and programs required for server maintenance and operation).

According to the criminal complaint filed by the legal team of Peščanik, due to several layers of protection (firewall) each IP address involved in the attack was blocked after its third attempt. The entire website traffic passes through a mitigation center that filters all malicious attempts it recognises. That is why this time the functions of the website was not slowed down, there weren't any breaks into the server, deleting, neither changing its content, as it happened on three previous occasions.

The editors concluded that the significantly multiplied requests overloading the server couldn't result from an increased visit through the regular site traffic, but with the single aim to prevent its normal use.

Meanwhile, the legal team received the first formal response to one of its three criminal complaints filed against unknown person(s) for cyber attacks launched after publishing texts about plagiarised PhD theses and floods.

The office of the Higher public prosecutor in Belgrade notified legal representatives of Peščanik that it made "5 formal requests for gathering information to the Department for cyber crime at the Ministry of Interior; 2 motions for issuing a warrant to locate the place of communication". It is also said that "based on the prosecutor's motion and upon the order of the Higher court in Belgrade, search of premises on two locations in Belgrade was done and tenants' electronic equipment was seized and collected for forensic examination at the Department for special investigative methods at the Ministry of Internal Affairs". The Prosecutor's office also pointed out that "no order for investigation was issued".

5. MILJANA RADIVOJEVIĆ

Archaeologist and postdoctoral researcher in Cambridge leading the international team studying ancient metallurgy at the archaeological sites of Vinča culture, became known to the wider public in Serbia last summer when she analysed the doctoral thesis of the then Rector of Megatrend University, a private academy at the center of the scandal of issuing doctoral degrees for plagiarised theses to several government officials.

The analysis actually showed that the then Rector of the University had no doctoral thesis, while the details of this unsuccessful research were published on the website of Peščanik where the affair of Megatrend and other universities plagiarised PhDs was first revealed.

In his defense, the then Rector accused the scientist of conspiracy against him and his institution, as well as against the officials whose theses were analysed, with the purpose of "discrediting the government". Appearing in talk shows on two national broadcast stations, he publicly read parts of private email correspondence between the scientist and her colleagues, presenting that as evidence to his claims.

As it turned out, unknown person(s) accessed the scientist's email account, gathered parts of correspondence and used her account to send them to several media outlets. The Rector claimed that he obtained her emails from the Serbian chapter of the international hacktivist network "Anonymous". Several days later, the group "Anonymous Srbija" publicly denied any involvement with hacking into that particular email account.

Reviewing the activity logs on the account, the location of unauthorised access was established as well as that the access was made on three occasions.

With Share Foundation's legal aid, a criminal complaint was filed to the prosecutor against the then Rector of Megatrend and against unknown person(s) for unauthorised access to a protected computer, a computer network, and to electronic data processing, and also for breach of mail privacy, or other criminal offenses prosecuted ex officio.

RISKS

JOURNALIST SECURITY AND "THE DIGITAL SHADOW"

JOURNALIST SECURITY AND "THE DIGITAL SHADOW"

Journalists and citizen media activists, for instance bloggers, are faced with a variety of pressures while participating in the public sphere, varying from threats, intimidation and other kinds of harassment, to violence and even murders. While these issues are relatively common in the physical world, especially in less democratic countries, they are increasingly influencing the work environment on the Internet as well. The Council of Europe Resolution on the Safety of Journalists, adopted in Belgrade in November 2013, strongly condemns "... physical attacks and violence, intimidation, misuses of the power of the State, including unlawful monitoring of communications, and other forms of harassment of journalists as well as others who contribute to shaping public debate and public opinion by exercising their right to freedom of expression and information".[1]

Endangering both physical and digital integrity of journalists presents a great challenge, but it is important to note that physical protection might look fairly easy compared to the protection of one's digital assets. Namely, whether a journalist, a blogger, a human rights activist, a lawyer or just an "ordinary" citizen, you are a data-producing machine. This human-produced data is scattered throughout the Internet, mobile phone networks, private IT or video surveillance systems and so on, as "digital footprints"[2], which can provide a lot of detail about someone's professional and personal life if combined in a right way. Therefore, it can be said that individuals possess a dual identity, consisting of two "personalities", offline and online, even though there is just one physical person. This online personality is not under the full control of the person it rep-

[1] Council of Europe Resolution on safety of journalists, adopted at the Conference of Ministers responsible for Media and Information Society, Belgrade, Serbia, 7-8 November 2013, para. 11 (b): https://www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted _ en.pdf

[2] For more details, visit Me & My Shadow website: https://myshadow.org/

resents, since anyone can interact with it without one's permission or even knowledge. The digital identity and its safety are harder to protect, for there are not just many security challenges in the real world, but also a "Pandora's Box" full of potential threats in the cyberspace.

The essence of digital security lies in protecting the same assets you would usually protect - for journalists, these are confidential information which might concern the identity of their sources, leaked classified materials, research plans, and so on. Therefore, one should be aware of the most common risks in the digital environment, not just for professional journalists but for everyone dealing with sensitive information (bloggers, human rights activists, government officials, diplomats, etc.):

- PERMANENT LOSS OF ACCESS. When your hard drive dies, your phone gets smashed, or you lose your camera's memory card. This can also refer to incidents of losing access to various online accounts due to hacking, unauthorised change of passwords and deletion of data.
- SENSITIVE DATA DISCLOSURE. Someone learns something that you would prefer to keep confidential or private.
- COMMUNICATION INTERRUPTION. Access to data is impeded by a break of network connection, or phone losing signal.

In the following sections, we will further outline issues and possible solutions for improving digital security. Please note that there are many aspects in regard with this topic, and we will focus on the most important ones for the purposes of this report.

PERSONAL V. ORGANIZATIONAL SECURITY

PERSONAL V. ORGANIZATIONAL SECURITY

When it comes to the digital security of journalists, it is rarely viewed from the perspective of their network of people, i.e. others that are communicating with them, most importantly sources and their colleagues. When there is at least one weak link in the communication chain, the consequences for privacy and security can be serious and that is why organisational security must also be a priority for media outlets. For instance, it takes just one email account breach to compromise many different people, so always remember that it's not just about you.

Here are the most common issues with digital security practices:

- Technical intrusion of private communication and access to data
- Stealing and seizure of equipment
- State surveillance
- Social engineering
- Blocking access to content
- Online security risks

TECHNICAL INTRUSION OF PRIVATE COMMUNICATION AND ACCESS TO DATA

General security risks are associated with hacking, malware injection, use of surveillance technology by private actors or data leaks from the website or database due to an inadequate protection.

Primary targets of attacks are email servers, personal computers and other devices such as smartphones and tablets, online accounts (social networks, collaborative tools, chat applications, etc), storage space (hard drives, USB flash drives, cloud storage – Dropbox, Google Drive).

The aim of these attacks is to disclose information and data that a journalist, blogger, activist or a media organisation would certainly want to protect. This can include the following:

- WHAT ARE YOU WORKING ON: plans and drafts of investigative stories or campaigns, documents, recordings, notes etc.
- DATA YOU ALREADY HAVE: sensitive information received from sources, potential evidence of wrongdoings by state officials or

private actors (companies, criminals...)

- WHO ARE YOUR COLLABORATORS: information about your network of colleagues, sources, editors…
- WHERE ARE YOU GOING: information about your movement, daily routines, plans for a trip abroad...
- IS THERE ANYTHING YOU HIDE: deeply personal information that could be used for an ill purpose.

CONFLICT: Privacy and secrecy of communication v. technical attacks v. digital security of companies storing your data

MEANS OF PROTECTION: Digital literacy, legal safety through national law and instruments of the Budapest Convention on Cybercrime, reliable and quality service providers, content encryption

WHO IS RESPONSIBLE: Internet and telecommunication companies, information society service providers, internet governance organisations, states, media organisation and IT support, individuals for their own content

STEALING AND SEIZURE OF EQUIPMENT

One of the possible scenarios could be theft or a warrant for seizure of equipment (by the police, a prosecutor, or court). Although police raids of media premises may not be that common in Serbia, it shouldn't be ruled out. The incident in late last year involving news site Klix.ba from neighboring Bosnia and Herzegovina, after the site published an audio recording of Srpska PM Željka Cvijanović, speaks for itself. The police searched the newsroom, seized and destroyed some of the equipment.[3] Speaking of stealing devices like laptops, tablets, phones or cameras, if a perpetrator has a sufficient degree of technical knowledge, it would be easy to access information protected with a simple code, like the one on your logon screen. Encryption of hard disks could be of great importance to prevent any unauthorised access, even if the computer is stolen.

MEANS OF PROTECTION: advanced encryption techniques, data backup copies

WHO IS RESPONSIBLE: Corporations, IT support, individuals for their own devices and data

STATE SURVEILLANCE

A risk all should be aware of in handling sensitive information is possible interception of communication by state authorities (police and security services). In Serbia, privacy of communication is guaranteed by Constitution, and can be breached only in cases of criminal proceedings or protection of national security, in line with the law and by a court order. Video surveillance in physical space may also constitute a breach of privacy, particularly given that this matter is not regulated by the Personal Data Protection Law.

Proper control over the surveillance market (equipment and services) has not been established. Individuals and private entities can easily and with little legal provisions acquire needed equipment and embark into the business of surveillance, which is formally restricted to the authorities, secret services and police, within the clear boundaries of law and only by a court order. This puts the matter of citizens privacy on even lower level.

However, data concerning communication that could reveal far more information than its actual content are so-called metadata. Taken from a simple phone call, they reveal the number you called, or from which you received a call, at what time, how long the call had lasted, and so on. Electronic Communication Law provides that operator store those data for up to 12 months. By carefully combining large quantities of such data, a complete digital profile of a certain person can be constructed: location, daily routines, one's network of people, sources of information, personal interests. Access to these data makes quite an intrusive measure, violating the guarantees of communication secrecy, which is why parties in public and private sectors must follow procedures prescribed by the Personal Data Protection Law. Nevertheless, The Commissioner for Information of Public Importance and Personal Data Protection, an autonomous public authority, after conducting inspection supervision in phone network operators in 2012 revealed a disturbing fact that state authorities have been breaking the law on regular basis, accessing personal data without proper legal grounds. Describing an example, the Commissioner pointed out to at least at least 270.000 registered cases of direct access to communication data that the Ministry of Interior made in 12 months, at one of the four phone companies.[4]

[3] You can read about the Klix.ba case here: http://www.klix.ba/vijesti/bih/ko-su-glavni-akteri-koji-su-naredili-i-odobrili-pretres-portala-klix-ba/141230118

[4] Research available at: http://labs.rs/en/invisible-infrastructures-surveillance-achitecture/

CONFLICT: Privacy v. security

MEANS OF PROTECTION: International standards of human rights, watchdog initiatives[5]

WHO IS RESPONSIBLE: States, police, secret services, judiciary, phone and Internet network operators

SOCIAL ENGINEERIG

A tactics that can also be used for gathering sensitive information from journalists or their sources, is social engineering or use of tricks and manipulation to retrieve information or gain access to the computer or the network. Usually it's one of many steps within a complex scheme. For example, a journalist can receive an email from a seemingly credible contact that has a "sensitive document" attached which in fact contains virus; or an email from a false source wishing to retrieve information about journalist's work. Anonymity or unverified contact details may also serve to false impersonation as a particular journalist[6] with a malicious intention. Due to all kinds of reasons, breaches of trust occur (as in "leaking" information by a former disgruntled colleague), and that can cause severe problems.

CONFLICT: Trust v. anonymity

MEANS OF PROTECTION: National criminal law, identity verification (encryption of emails, electronic signature)

WHO IS RESPONSIBLE: States, corporations, IT support, individuals

BLOCKING ACCESS TO CONTENT

In most cases, security of content is related to safety measures used for online platform where this content is published. Most common threat is overloading servers through DDoS attacks, that is clogging the server hosting a particular web site of an online media outlet, by sending multiple synchronised requests for access.[7] The integrity of contents could also be damaged by changing or deleting it in attacks aimed at a database, using malicious code injections for compromising its content (SQL injection).[8]

Other, legal means of making targeted parts of content difficult to access, is related to the so-called right to be forgotten, or notice-and-takedown procedures. The right to be forgotten that is now in effect in EU member states, is based on rulings of the European Court of Justice (the Costeja case).[9] This enables EU citizens to request removal of information relating to them that is "inadequate, irrelevant, or no longer relevant" from search engine's results (for example, Google Search). The request pertains only to search results and not to actual websites where these information remain published.

As for notice and takedown process, content is removed by the host as a response to court orders or legal allegations (for instance, copyright infringement).

CONFLICT: Open data access v. web architecture

MEANS OF PROTECTION: Budapest Convention on Cybercrime, national legal frame

WHO IS RESPONSIBLE: Internet governance organisations, states, corporations, hosting & IT support

ONLINE SECURITY RISKS

Threats to the safety of journalists is rapidly spreading from the offline world to the Internet, particularly on social networks, where the abuse is less noticeable due to a degree of retained anonymity. It is estimated[10] that over a quarter of threats aimed at journalists are made online, while female journalists experience roughly three times as many abusive comments as their male counterparts on Twitter. OSCE Representative on Freedom of the Media Dunja Mijatović called upon participating states[11] to take all necessary steps to ensure saf-

[5] One example are the 12 international principles for applying human rights standards on communications surveillance, which received support from more than 400 organizations worldwide, with Share Foundation among them: https://en.necessaryandproportionate.org/

[6] As in the case of journalist Dragana Pećo, in whose name unknown person(s) had sent FOI requests from a false email address: http://www.cins.rs/srpski/news/article/saopstenje-za-javnost-783

[7] For more information about DDoS attacks see: http://www.digitalattackmap.com/understanding-ddos/

[8] For more information about SQL injection attacks see: https://www.acunetix.com/websitesecurity/sql-injection/

[9] Text of the ruling available here: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

[10] IWMF, Violence and Harassment against Women in the News Media: A Global Picture / Intimidation, Threats, and Abuse: http://www.iwmf.org/intimidation-threats-and-abuse/

[11] See the communique of the OSCE Representative on Freedom of the Media on the growing safety threat to female journalists online: http://www.osce.org/fom/139186?download=true

er working environment for female journalists online.

The main goals of this sort of attacks are intimidation, to hinder journalists from reporting about certain issues, public humiliation and abetting or vindicating physical assaults against media professionals. Commonly used methods are open threats, publishing private information such as home address, names or photos of family members, hate speech, insults inciting violence, online stalking and so on. Somewhat more 'subtle' tactics involve damaging reputation and hiring hackers.

CONFLICT: Freedom of speech and anonymity v. rights of a person and information quality

MEANS OF PROTECTION: International standards of human rights, national legal frame, self-regulation

WHO IS RESPONSIBLE: Internet community, states, corporations, individuals

WHO SHOULD BE PROTECTED? WHO PLAYS THE ROLE OF INFORMING THE PUBLIC?

Not so long ago there was little consideration that apart from professional journalists, other persons actively involved in public discourse should also enjoy special legal protection. Recent events[12] point to the necessity of considering this question seriously.

There is no special legal definition of a journalist in Serbia, which makes it harder to take a definitive stance on who should be protected. We believe that alongside professional journalists, there are other entities and social positions related to channels of general communication and information that should also enjoy protective legal provisions – such as online and citizen media, bloggers, watchdog and civil society organisations, and in some instances netizens recognised for their work by online community.

The Committee of CoE Ministers confirmed this concept, stating that some privileges which are usually recognised for journalists, may extend to other actors who may not fully qualify as media but can be considered part of the media ecosystem contributing to the functions and role of media in a democratic society.[13]

[12] There is an impression that there is a kind of "selective protection" of individuals in Serbia when it comes to threats made on the internet: http://www.shareconference.net/sh/blog/selektivna-zastita

[13] Council of Europe Resolution on safety of journalists, adopted at the Conference of Ministers responsible for Media and Information Society, Belgrade, Serbia, 7-8 November 2013, para. 9: https://www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted _ en.pdf

AFTERMATH

AFTERMATH

INSECURITY AND FEAR

Given the incidents described so far and risks posing in the digital environment, we should now address the issue of consequences which cyber attacks have on online media and journalists in Serbia. Most of the cases of DDoS attacks or disappeared articles, had little or no lasting impact on media contents. Some other consequences are still present, though. As one of the founders of EFF John Gilmore famously stated: "The Net interprets censorship as damage and routes around it". Contents taken off the network usually get multiplied on different places, republished by other blogs or online media websites, while its label of a censored or otherwise threatened item attracts even more readers.

We shall further outline consequences of the described attacks and their impact on autonomy and safety of online and citizen media.

The main consequence of these attacks lies in the raise of insecurity and fear, that result in a chilling effect[14] on freedom of expression online. The fact that publishing contents that criticise the structures of power (government, criminal groups or any other power) can cause destruction, blocking or temporary disappearance of a website, followed by lots of stress and expensive work hours to restore the system – which can affect the will to express freely. In cyberspace, the defense costs are always higher than the cost of the attack and in most cases there is probably no foreseeable effective and reliable way of protection against these attacks. This can be highly discouraging for small and independent online and citizen media that cannot afford expensive cyber security experts nor technical solutions to protect themselves.

[14] "Chilling effect" in legal context can be explained as discouraging the legitimate and allowed enjoyment of a certain right with a threat or a legal sanction. It originated in the US legal theory and it is mostly used in relation to endangering freedom of expression: http://www.shareconference.net/sh/blog/ciling-efekat-presude-protiv-dva-foruma-sa-u-slucaju-malagurski-da-li-je-sloboda-izrazavanja-na

CHILLING EFFECT ON THE GENERAL PUBLIC

Arresting individuals because of what they publish on their blogs, or for commenting news, or any other form of online expression, have a chilling effect not just on the journalists and online media organizations, but on the general population of online users in Serbia (up to 60% of citizens). Citizens feel their freedoms lessened, their safety in the digital environment endangered, and that causes derogation of freedom of expression. This perception is further encouraged by conventional media assuming a perspective of a state force and not civil liberties while focusing on incidents of police interrogations, arrests and legal proceedings against citizens for comments given on political issues online.

PRIVACY VIOLATION AND SURVEILLANCE

Targeted attacks on personal and professional communication and working tools such as emails, online documents and databases can endanger the sources anonymity, reveal investigative plans or they can be used to discredit the victim by publishing private information, as well as for identity theft. Reaching the necessary level of digital security often implies complex procedures, change of usual habits related to the use of technology, that could unfortunately diminish the efficiency of a journalist and the entire media organisation.

PUBLIC OPINION MANIPULATION THROUGH THE USE OF TECHNOLOGY

Technical tools used for manipulation of public opinion in the digital environment are getting more sophisticated. Application software is being used for covert goals of political parties, corporations, and other self serving circles. Occasional floods of comments, statuses and likes on news sites and social networks, change the space open for dialogue and freedom of expression, creating a false perception of public opinion. This induced noise silences authentic voices of citizens, discouraging important debates within the society.

In The Declaration on the Respect for Internet Freedoms in Political Communication[15], Share Foundation and 200 notable organisations and experts pointed out that cases of internet censorship, attacks against websites and private accounts represent violation of human rights and basic provisions of the Constitution and laws of Serbia.

[15] Text of the Declaration is available here: http://deklaracija.net/

CONCLUSION

ROLE OF THE STATE

Addressing the role of the authorities concerning these cases starts with questions on the correlation between targeted contents, overall political context and the attacks themselves. The primary target of the attacks have been web sites, critical of the government, publishing articles that expose corruption and assert the government's inefficiency.

It should be pointed out that there is no substantial evidence to claim that any governmental body, or any political party stand behind the cyber attacks on online media. The nature of those attacks and the network structure make it almost impossible for independent researchers to track the attacks, while the attackers usually stay well hidden behind anonymity and multiple bot networks from abroad. Even if there were traces pointing to an individual, a "black hat"[16] hacker or an organisation, it would be almost impossible to establish who ordered the attacks. Furthermore, those attacks do not constitute a policy of Internet censorship, such as Internet filtering or blocking of content that is endorsed by the governments in Turkey or China.

Based on experience from the past two years, we can certainly argue that the government has failed to establish trust in its abilities to successfully protect the online media and citizen journalists in Serbia. We are aware that certain state agencies have limited technical and organisational capacities for a more efficient reaction in such situations. However, the real danger lies in discretion of the authorities (prosecution, police and judiciary) to discriminate between cases of online violation of rights.

Most cases of cyber attacks on online media, investigative journalists and citizens' media, critical of the government, have been processed very slowly or not at all. Over the past year, Share Foundation took an active role in monitoring and conducting cyber forensic analysis of the attacks on online media, submitting results to the authorities and publishing them whenever it wasn't against the interest of the investigation.

[16] Hackers seeking security vulnerabilities in information systems in order to use them for personal financial gain or other malicious purposes: https://www.techopedia.com/definition/26342/black-hat-hacker

However, none of the major cases led to identifying and arrest of suspects, while expected reactions were reduced to occasional formal statements. Such practice further degrades public trust in protection the state is obliged to provide.

Nevertheless, the authorities proved to be quite efficient when it comes to arresting and instituting legal proceedings against social media users and bloggers (the Malagurski case and cases of inducing panic during the floods in 2014). Immediate consequences reflect in lack of legal certainty in this area and unsatisfactory level of rule of law.

WHAT SHOULD BE DONE?

Threats to freedom of expression and privacy in the digital environment, as well as the safety of journalists and individuals, must be dealt with as a matter of priority. Serbia has a duty to develop instruments for protection of journalists and media, while building capacities for online media to protect themselves from the cyber attacks, as much as possible.

Formal and informal education on cyber security, privacy and freedom of expression in the digital environment for the general public and specific target groups is necessary in order to ensure safety and consistent protection of human rights on the Internet.

Judicial training, harmonisation of laws and regulatory reform are required for a wider recognition of new sorts of human rights violation (freedom of expression, right to access and exchange information, right to privacy) and of new ways to exert pressure on individuals and media organizations.

The needs of the state and security services to respond to new types of threats in the cyberspace should not be used as an excuse to disproportionate surveillance measures, Internet censorship or any other form of cyber policing.

SUGGESTED STEPS

In order to improve and respect standards of freedom of expression in the digital spheres of Serbia, each of the actors in charge should take appropriate steps to reduce risks and impacts to a minimum level. Some of these steps require cooperation between a variety of agents, while others call for personal engagement of every individual and organisation within the scope of their resources. The Republic of Serbia should institute a series of measures to improve the present state and upgrade our digital future.

HARMONISATION AND IMPLEMENTATION OF LAWS AND REGULATORY REFORM

- Passing a law on information security and implementing the Budapest Convention on Cybercrime in line with international standards of human rights, and particularly with the European Convention on human rights and decisions of the European court of justice;
- Improvement of the regulatory framework for control over surveillance equipment and software trade;
- Instituting instruments of control over deploying electronic surveillance measures solely on a court order;
- Effectuate the below stated measures through the Action plans for chapters 23 and 24 [of the negotiation process with the EU].

CAPACITY BUILDING AND CHANGE OF PRIORITIES

- Judicial trainings for implementing the international standards of human rights in cyberspace;
- Improving human and organisational capacities of the police and prosecution for cyber crime;
- Instituting a functional national center of Computer Emergency Response Teams (CERT);
- Support for establishing a functional network of CERTs and organizations in charge of immediate response and assistance to various groups;
- Prioritising cases of endangering freedom of expression, data privacy and digital security of citizen journalists and online media;
- Cooperation between cyber crime units and other police departments, using common investigative techniques alongside gathering digital evidence.

INTERNATIONAL COOPERATION AND PARTICIPATION IN PROCESSES OF SELF-REGULATION AND REGULATION

- Improving cooperation on international level in resolving cases of cyber crime;
- Building good relations and cooperation with the international regulatory agencies, Internet governance organisations and large Internet companies;
- Improving instruments of coregulation and further support for self-regulation in content and network management;
- Recognition and respect for Internet culture and social norms of Internet community in the course of legal processes.

DIGITAL LITERACY

- Enabling individuals and organisations to actively use technology and system of protection of basic human rights in the digital environment, in order to secure freedom of expression, assembly and association, protect data privacy and improve digital safety;
- Encouraging use of technological innovations based on active participation and collaboration for empowering creative and innovative media and information production.

MONITORING RESULTS AND ANALYSES

Detailed reports and analyses can be found at the following sites:

- www.sharedefense.org
- www.shareconference.net
- www.labs.rs

SHARE FOUNDATION - 2015