OPERATIONAL SECURITY AND PERSONAL RESILIENCE: AN OVERVIEW OF THE EASTERN NEIGHBORHOOD

OPERATIONAL SECURITY AND PERSONAL RESILIENCE: AN OVERVIEW OF THE EASTERN NEIGHBORHOOD

Handbook on Cyber, Information, Intelligence and Personal Security Threats from Foreign Authoritarian Regimes, Domestic Oppression, and Harassment

Author

Georgia: Media Development Foundation – Mariam Pataridze, Sopho Gelava, Tinatin Gogoladze

Moldova: IPIS - Institute for Strategic Initiatives – Victoria Olari

Ukraine: Ukraine Crisis Media Center – Liubov Tsybulska, Oleksandra Tsekhanovska

Operational Security Recommendations: European Values Center for Security Policy team

Editor

Andrea Michalcová, European Values Center for Security Policy

1. INTRODUCTION

This report follows a year of cooperation between civil society organizations (CSO) and think-tanks from Central Europe and the Eastern Neighborhood (EN). It is one part of the *Project on Enhancing and Sharing Lessons Learnt in Resilience and Self-Protection*, which evaluates the capability of civil society in Georgia, Ukraine, and Moldova to use guidance from the European Values Center for Security Policy (EVC) in operational security and exposing illegitimate methods of influence. Here, we adapt their approach and apply it to the political realities in the EN.

The authors conducted thorough desk research of relevant open source information, public surveys, and investigative reports. The desk research was conducted by structured interviews with relevant experts and local officials. Media representatives as well as foreign policy and security experts from civil society organizations provided most of the information. Due to the sensitivity of the topic, we decided not to publish the list of names of the interviewees, which can be obtained from the editorial team of the European Values Center for Security Policy.

Our researchers focused on the media situations in Georgia, Ukraine, and Moldova:

In Georgia, some case studies of foreign malign influence are available, but there is a paucity of detailed and comparable assessments on the full scale of foreign malign influence, and consequently few specific policy recommendations for civil society-driven advocacy campaigns. A handful of states operating outside the EU-NATO framework are projecting malign influence in Georgia by means of diplomatic activities, leveraging energy and economic policy, deploying information warfare, and backing domestic fringe or mainstream groups with subversive potential. Post-Soviet countries like Georgia are especially vulnerable to the mischief precipitated by these groups, which are not only well-documented by US and EU reports, but are palpable to the public; the so-called "borderization process" brought a spate of power cuts to Georgians. Hostile acts in Georgia through certain CSOs, media outlets, and agents of influence and political forces is aimed at discrediting the country's Euro-Atlantic process and fueling skepticism about democratic development. The recent presidential elections held on October 28, 2018 obviated just how closely several campaigns were linked to corruption and disinformation, all of which stand in the way of civil society organizations' activities[1].

Ukraine is also rife with challenges to agents who seek accountability of the government. Even after CSOs won a right for open and free work on public policy issues following the Revolution of Dignity, they have more recently (especially in late 2018, a year before both presidential and parliamentary elections) come across more pressure from the state. To discredit civic activists, the government initiated a new law requiring those who are working to counter corruption to declare their his or her income and assets publicly2. After heavy foreign criticism plus e massive resistance of the activists themselves, this proposal was abandoned. Several CSOs and civic activists have encountered direct physical and verbal assaults. The eastern regions of Ukraine are especially difficult terrain, where the corrupt, pro-Russian local

---

1   Crosby, Alan. "Sex, Lies, And Audiotape: Just Another Election Campaign In Georgia." *RadioFreeEurope/RadioLiberty*. Accessed on October 24,2018. https://www.rferl.org/a/sex-lies-and-audiotape-presidential-election-campaign/29561804.html

2   "Ukrainian Civil Society Unites to Counter Mounting Threats." *Freedom House*. Accessed on April 18, 2018. https://freedomhouse.org/article/ukrainian-civil-society-unites-counter-mounting-threats

authorities and police are unsympathetic to physical attacks on journalists. The most striking example is the story of anti-corruption activist Kateryna Handziuk from Kherson, who was attacked with sulfuric acid. Handziuk was a critic of the police and security authorities and condemned corruption in the regional department of the Ministry of Internal Affairs. She had publicized the involvement of the police in several cases of corruption. She died from her wounds 3 months later.

Civil society actors have lost ground in Moldova as well[3], particularly after 2016, when the government changed hands and is under the full control of the Democratic Party of Moldova. In 2017, the Ministry of Justice attempted to introduce legislation that would prohibit political activities and legislative advocacy[4] by CSOs that receive foreign funds. The controversial provisions were included in the draft law at the end of March 2018 but were later dropped. After opposing the controversial amendment of the electoral system, Moldovan CSOs are under constant attacks from public officials, and other entities affiliated with the ruling party[5], including mass media, bloggers, and online trolls. Several Moldovan CSOs reported assaults between 2016 and 2018. These include libelous allegations of involvement with individuals accused of the 2014 1bn euro banking fraud or in the "Laundromat" scandal. A recent notable case involves a parliamentary inquiry into a trip to the European Parliament[6] undertaken by several Moldovan activists, journalists, and two notable opposition figures, which was sponsored by the Polish CSO the Open Dialog Foundation. Parliamentary officials alleged that the Foundation was a pro-Russian stooge aiming at the destabilization of the political situation in Moldova and some of them opined that the participants in the trip should be investigated on charges of treason. Often, such character assassination operations are accompanied by the publication of private email exchanges of said activists or their conversations via various messenger apps, which shows that vocal critics of the government are vulnerable to cyberattacks.

The overall situation of the CSOs in these three targeted countries was critical. Very little is being done to support them. Therefore, EVC decided to raise the awareness of these environments and share best practices from the operational and personal security based on the consultations with several security experts.

Based on the categorization of the threats, we identified the main hurdles to their continued operation and issued the following recommendations.

3   Macrinici, Sorina."Shrinking space for Civil Society in Moldova." *The Soros Foundation Moldova*. Accessed on April, 2018. https://www.soros.md/files/publications/documents/Civil%20 Society%20Macrinici.pdf

4   RFE/RL's Moldovan Service. "Moldovan NGOs Reject Proposed Ban On Foreign Funding" *RadioFreeEurope/RadioLiberty*. Accessed on July 12, 2017. https://www.rferl.org/a/moldova-ngos-reject-foreign-funding-ban/28612337.html

5   Macrinici, Sorina."Shrinking space for Civil Society in Moldova." *The Soros Foundation Moldova*. Accessed on April, 2018. https://www.soros.md/files/publications/documents/Civil%20 Society%20Macrinici.pdf

6   Dulgher, Maria."An outline of the 'Open Dialog' scandal. PAS and DTPP in the gunsight of the Moldovan Parliament." *Moldova.org*. Accessed on November 13, 2018. https://www.moldova. org/en/outline-open-dialog-scandal-pas-dtpp-gunsight-moldovan-parliament/

2. METHODOLOGY: CATEGORIZATION OF THE THREATS AND SUGGESTED RESPONSES TO THEM

CATEGORY	THREAT	WHAT TO DO	DESCRIPTION	EXAMPLE OF VERBAL OR WRITTEN THREAT
1	General unaddressed hate mail, or with a hint of a threat	Write an email to a contact at your organization[7] the same day[8]	Unaddressed message rudely and negatively assessing the institution, without further specification of the threat, or an implicit threat	"You lay about, paid by God knows who. Learn how to work with your hands. Jews and faggots like you will end badly. We will sort you out."
2	Addressed message with a hint of threat	Write an email to a contact at your organization during the same day, personally report to your superior/ security manager of your organization	Addressed message with a hint of threat directly sent to a person or specifying that person, without further specification of the threat/ the threat is only implicit; anonymous phone calls without explicit threats.	"How dare you insult the President like that, you primitive. You've got it coming. I'm looking forward to seeing your US-paid offices on fire. I know where you have them, morons."
3	Addressed threatening message, or an urgent threat	Immediately call your superior/security manager of your organization	Message specifically addressed to someone containing a specific threat against that person or their loved ones. Contains a non-public information (address, name) and an urgent threat.	"A warning wasn't enough for you, huh? Guess I'll have to use different 'arguments,' you pig. Just wait. I know where you live – Nováková 3."
4	Physical incident	If necessary, call 911. Immediately call your superior/security manager of your organization.	A particularly targeted person has a legitimate impression of being followed, intimidated, or there is an attempted assault or direct physical confrontation.	Feeling that you are being followed on the street. Any, even implicit, attempts to intimidate (a stranger saying, "Stop it, or else…", and leaving).

---

7   It's good to have a specific email set-up for these cases, which is then forwarded to the security manager automatically.

8   We catalogue for the future, in case the person escalates their behavior.

3. FRAMEWORK OF SOURCES OF THE MOST COMMON SECURITY THREATS IN TARGET COUNTRIES

	MOLDOVA	GEORGIA	UKRAINE
CYBERSECURITY	• Direct denial of service (DDoS) (unavailable websites) • Phishing (fake emails and website links received)	• DDoS (unavailable websites) • Phishing (fake emails and website links received) • Ransomware (data encrypted) • Loss of data (documents, correspondence)	• DDoS attack (Short to mid-term paralysis of operations) • Phishing • Loss of data (documents)
INFORMATION SECURITY	• A leak of passwords (Yahoo, Facebook) • Hacking emails (disclosure of communication, stealing data) • Online discrediting (gossips, lies, insults, etc.) • Online identity theft (impersonation)	• A leak of personal data (address, telephone number, etc.) • A leak of passwords (Yahoo, Facebook) • Hacking emails (disclosure of communication, stealing data) • Online discrediting (gossips, lies, insults, etc.) • Online identity theft (impersonation) • Penetration of the memory of a smart device and stealing personal items to blackmail with these materials (esp. photos of minors or underage photos and videos)	• Hacking emails (leak of correspondence, stealing data) • Online discrediting (internet bullying) • Creating fake social media and experts accounts • Attacks from disinformation campaigns and operations • Harassment and discrediting by foreign entities (frequently suffered by targets of Russian malign operations) • Harassment by local authorities (using the organization for political gain; harassment by ruling political party)
BASIC COUNTER-INTELLIGENCE SECURITY	• Suspicious activities in a close circuit (spying, snooping, curiosity, etc.) • Recruitment by hostile intelligence service (direct offers, promotion, etc.) • Invitation to (fake) interview • Eavesdropping/surveillance through special equipment inside a TV company		
PERSONAL (PHYSICAL) SECURITY	• Intimidation (threats, persecution) • Blackmailing • Vandalism	• Intimidation (threats, abuse) • Blackmailing • Slight injuries (bruises, cuts, grazes)	• Bullying during international travels (detention in Russia, Belarus, Moldova, Armenia) • Vandalism (robbery into office)

UKRAINE

4. UKRAINE

Background

We solicited 10 CSOs in Ukraine over a four month period to conduct a survey on current cybersecurity challenges and possible threats as well as institutional capacity to face and overcome them. Against the backdrop of a flourishing third sector, a relatively small number of respondents and the general unwillingness of many CSO-representatives and/or activists to take part in the survey is itself indicative. We surmise that an essential number of them refused to take part in the polling precisely for one of the reasons the survey aims at exploring-–they feel concerned about the safety of their personal data as well as the degree of integrity with which it would have been handled.

Should the hypothesis be true, more awareness-raising and then trust-building is required in the field when informing respondents of research objectives, especially when wading into unfamiliar cybersecurity waters. Moreover, possible respondents have to demonstrate the awareness and knowledge of these security challenges and share trust, not only in the integrity of the partners for whom they provide, but also in their security capabilities, as there were known cases of hacking and leaking sensitive information that harmed not only the target but also those with whom they had been in close contact.

Among the 10 surveyed organizations, all have the same background: working in the CSO sector with a heavy focus on countering disinformation and propaganda, or to a lesser extent, human rights protection. But simply because these organizations are highly aware of cyber and information threats, it is unacceptable to assume that the Ukrainian third sector as a whole knows how to navigate these threats, where they may lack the same skill in recognizing threats. Taking that into consideration, the data reveals the following tendencies:

Training on operational security

The majority of respondents stated that security training was unavailable or insufficient. Those who received any educational assistance on the matter often got it in the form of protocols and/or instructions, which is not as effective as practical learning in the form of workshops, even if understood and applied completely. One of the organizations involved stated that it usually on the providing end on such operational security trainings, while it would also desire to strengthen its own resilience capabilities. This indicates a two-level problem, where one of the few providers of relevant information might not have access to the best and latest tools to counter the threats, sharing limited expertise with others and remaining vulnerable at the same time.

Presence of operational security guidelines

Only 2 of the respondents have standard operational security protocol. One attempts to use a guideline provided by the third party, but even when properly adopted, the abovementioned lack of practical skills to implement it correctly still leaves the organization at risk. Others have no specific guidelines or refer to their own resources.

Crisis management during security incidents

Only one of the respondents asserted that they would turn to their IT department, which shows the lack of technical specialists capable of negotiating possible cyberattacks. The majority claims that they would turn either to colleagues or international partners. Without knowledgeable allies, these organizations are wide open for digital raiders. Foreign assistance is scarce as well and is frequently unaccustomed to the weaponry deployed in the Ukrainian media landscape. Interestingly, the CSO's trust in law enforcement is so low that only 2 respondents mentioned them as a recourse. Regardless of their partners, all the survey participants pointed out the need for additional security trainings, mostly in work-related information and cyber fields, but also for enhancing personal security. Also, they lack respective human resources (IT specialists, etc.) whom they could address with various security issues.

Security challenges

Cybersecurity

Most respondents expressed concern over the possibility of data leak, loss of personal information, DDoS, phishing, and other types of cyber-attacks. Preserving and securing data is of key importance given the bullying that some of the organizations have either directly or by proxy experienced. With the little Internet warfare readiness limited financial resources they possess, it is unsurprising that the CSOs stated that cybersecurity challenges remain the most common liability.

Information security

Targeted discrediting and reputational damage are among chief concerns in the area. The issue of personal data safety and its potential loss via communication disclosure is also of high relevance.

Personal security

Several organizations have expressed concern that their members could be arrested in countries (like in Belarus – which actually happened to some other CSOs representatives from Ukraine) that have close ties to Russian Federation. They quite understandably recalled the bullying, direct personal threats (including also those anonymous ones), theft, assault, and property damage suffered by their colleagues, whether or not the incidents of the latter two were clearly politically motivated.

Future threats

Most of the respondents anticipate information threats directed at discrediting their respective organizations and inflicting reputational damage. While the disruptive and violent power of the government of the Russian Federation is very familiar in a country under attack, they fear that their own state will seek revenge if not portrayed in a positive light. They are wary of the newly-elected (in 2019) administration's authority to impose new communication policies that would severely limit CSOs' activities and involve secret security services or issuing to cyber threats such as personal data leaking and bullying.

Sources of threats

As elaborated above, some of the respondents harbor fears that the government of Ukraine, and specifically representatives of the *Sluha Narodu* presidential party, presidential envoys, and pro-Russian politicians, will obstruct their work. External threats, namely those stemming from the Russian Federation, are another concern, which explains their predominant specialization on Russian malign influence among the respondents. Local criminal groups, involving also public officials, who misuse their power, often exhort pressure on representatives of local civil society, who are trying to disclose such facts (of existence of local criminal groups).

USI MODERNE DE INTERIOR

Magazinul "MARITA" etajul 2

Centrul comercial "DOMUS" Pavilionul Nr. 114

62-75-16
62-75-17

MOLDOVA

5. MOLDOVA

The Institute for Strategic Initiatives (IPIS) has conducted a survey on cyberbullying and cybersecurity challenges faced by journalists, CSOs, activists and media representatives from the Republic of Moldova, working on the issues of Russian influence, propaganda, disinformation, corruption, etc. Ten respondents were selected to complete the questionnaire. Having analyzed the questionnaires, the following points can be highlighted:

Training on operational security

Almost all the respondents stated they did not receive help with operational security from any national or international organization. Some mentioned that they are self-taught, whilst other respondents said they prefer keep it within their organization.

Presence of operational security guidelines

We can conclude that the practice of using manuals, guidelines or procedures on operational security is not widespread among CSOs, activists and media representatives from the Republic of Moldova. But still we can mention some positive aspects. Most organizations are trying to protect themselves by using standard operational security solutions offered by Google and Facebook, such as 2-step authentication, Antivirus software, firewalls, etc.

Crisis management during security incidents

In situations of security crisis, most respondents mentioned that they do not trust state institutions such as the Police or Prosecutor's Office and largely avoid contacting them. Some even stated that they feel hostility from state institutions and experience cynical behavior from the Police and Prosecutor's Office. Interestingly, in situations when they've been attacked, persecuted or blackmailed, organizations decided that the best way to protect themselves was to inform the public about such incidents in an attempt to make sure they wouldn't happen again.

Security challenges

<u>Cybersecurity</u>

The majority of respondents named trolling and cyberbullying by government actors as their key security challenge. The organizations carry out investigations and report on corruption, conflicts of interest and abuse of power committed by government representatives. The respondents mentioned that there were attacks on their websites and found suspicious devices near their offices.

Information security

Almost all interviewees have experienced leaks of Facebook passwords and email hacking. Also, the purposeful discrediting of journalists, CSO's activist, etc. raises concern among our respondents. This is done by duplicating or creating fake accounts - online theft of personality. The practice intensified during the electoral campaign for the February 2019 Parliamentary elections when many journalists and civic activists found impersonators commenting in their names on different public pages. In this case, there was an unprecedented decision by the Facebook to close 168 Facebook accounts, 28 pages and eight Instagram accounts in Moldova, some belonging to government officials, because it was suspected they were spreading fake news, political propaganda and misinformation ahead of elections. Facebook newsroom stated that although the people behind this activity attempted to conceal their identities, their manual review found that some of this activity was linked to employees of the Moldovan government.

Personal security

A number of respondents reported attacks, threats, physical intimidation and car damage during their activity on the field. Some of these actions were carried out by unidentified persons, while others were by law enforcement personnel. It was the case of the Occupy Guguta protest when police officers forced activists to release their place of protest. Banners and other materials were also seized. Furthermore, government-related television channels tried to spread fake news about the protest movement by infiltrating dubious, alcoholics in the area where they were protesting. Thus, causing personal security problems to the protesters.

Future threats (within the next 1-3 years)

Most of the respondents have already been blackmailed, bullied, sued, harassed and physically attacked. The also drew attention to some changes in the law that might affect their day by day activity: CSO law, Media Freedom law, Grants from abroad law, Access to information law. Given the subjects they emphasize (financial crimes, corruption, abuse of power), the possible threats may refer to blackmail, harassment or even illegal detention of the relatives. Other possible threats may refer to harassment from fiscal authorities or even from the legislative body (during the reporting period, the Parliament had an initiative to forbid the external financing for Moldovan CSOs).

Sources of threats

All respondents indicated that the biggest sources of risk come from internal actors, namely the government, which acts through the law enforcement institutions or through people linked to the Moldovan government, that have led fraudulent Facebook campaigns using the tactics of Russia's notorious "troll farm". This also causes a possible danger of external intervention, because Kremlin agents know how to exploit the weak in such situations.

GEORGIA

6. GEORGIA

The Media Development Foundation (MDF) has conducted a survey on cyberbullying and cybersecurity challenges faced by CSOs, activists and media representatives working on the issues of Russian propaganda, corruption and human rights. 24 respondents were selected for the survey, which was conducted using a mixed questionnaire method. Analysis of the collected data has revealed the following tendencies:

Training on operational security

The majority of respondents have not been offered training or other procedural help in operational security. Several respondents have participated in training on digital security, which did not fully cover the threat avoidance mechanisms necessary for this person/organization.

Presence of operational security guidelines

The majority of respondents do not use operational security guidelines during their organizational activities. Only a small number have developed internal rules.

Crisis management during security incidents

The majority of respondents noted that during cybersecurity incidents apply to the organization's IT service, as well as the Defense Ministry's Cybersecurity Bureau and the Interior Ministry's cyber unit. Once they disclose the cases with elements of crime, they report to the police.

In cases of information security incidents (personal data infringement), respondents report to the Personal Data Protection Inspector and in rare cases, to the Public Defender.

Some respondents have no information about who to apply to in cases of various incidents for problem solution and taking relevant action.

Almost all respondents need training in digital (password, internal network security, ransomware detection) and information (personal data protection) security. The majority of respondents noted the importance of developing skills that will help them effectively solve problems during various crises. Several respondents noted that they need help in business continuity planning.

Security challenges

Cybersecurity

The majority of respondents named trolling and cyberbullying by ultranationalist groups and government actors as their key security challenge. The so-called government trolling caused by critical material about government activity is especially noteworthy.

15

Phishing and hacker attacks on the organizations' official websites in an attempt to obtain information are also named by respondents as significant problems. The website (www.eurocommunicator.ge) of MDF's Myth Detector was twice hacked by Luxas Hacker in 2015. During the first attack, it was impossible to track down the hacker, but during the second attack it was determined that the attack occurred from IP address registered in Turkey. The videos uploaded on YouTube clearly show the address of a website "Dark Mirror" http://dark-mirror.org. The hacker was using the link when attacking the website.

Georgia became the target of massive cyberattack on October 28, 2019. The hackers targeted the websites of the Georgian government and private agencies, as well as media outlets (TV Pirveli, Imedi, Maestro, Trialeti and Sakinform) and non-governmental organizations (Media Development Foundation).

The homepages of the hacked websites were replaced with an image of Georgia's ex-President Mikheil Saakashvili with the caption "I'll Be Back."

The hacked websites were uploaded on the servers of Pro-Service, a local web hosting provider. According to the company, about 15,000 pages were affected as a result of the cyberattack. The Interior Ministry announced that it launched investigation under Articles 284 and 286 of the Criminal Code of Georgia, involving unauthorized access to computer system, as well as unauthorized handling of computer data and/or computer systems.

The Interior Ministry said that "the cyberattack could have been carried out from either inside or outside the country." "The investigative measures have revealed that the cyberattack was carried out, causing the so called website defacement - changes to the visual appearance of homepages."

"Georgian private companies provide hosting services to the majority of targeted companies. The style of cyberattack on each website is identical," reads the statement.

All the websites uploaded on the servers of the company Pro-Service resumed operations on October 29.

Information security

Purposeful discrediting of respondents by radical groups and government trolls to ensure that the information spread by them loses legitimacy was named by the surveyed respondents as a widespread problem. In respect of information security, the majority of respondents stressed the issue of disclosing personal data (hacking into accounts, information leaks, disclosure of communication, online theft of personality).

Personal security

A number of organizations have become the targets of attacks, threats (of physical reprisal, raping) and aggression from ultranationalist groups, which have become stronger over the past years. The surveyed journalists noted cases of physical and property damage (broken apparatus and cars). Several respondents became the targets of physical assaults simply because they were performing their journalistic activities.

Rustavi 2 TV journalist, Davit Eradze, became the target of physical reprisal by members of the ultranationalist movement Georgian March (2018); moreover, his house was shot at and cartridges were found on his balcony simply because he prepared a TV story during his journalistic activities (2019);

Journalists from Tabula were attacked in a restaurant with assailants citing insults to their church by Tabula as the reason (2016).

In addition, 39 representatives of various media outlets sustained physical injuries whilst performing their professional duties during the dispersal of the June 21 anti-occupation rally.

Future threats (within the next 1-3 years)

The majority of respondents believe the cases of trolling and cyberbullying by ultranationalist groups and government actors, as well as online discrediting, personal data disclosure and threats will continue throughout the next 1-3 years. According to them, some organizations/representatives may even become the targets of physical assaults and arrests.

Sources of threats

Among the main sources of threats, respondents named insiders – state structures, hate groups hired and encouraged by them, and marginalized actors, including trolls. As for the main source of outsider threats, respondents named Kremlin actors and their satellites (private persons and organizations), because some of the surveyed respondents have been working on issues related to Russian influences.

Respondents said that they have not received help from international donors/governments to address these threats.

7. WHAT CAN BE DONE? RECOMMENDATIONS FOR CSO & CIVIC ACTIVISTS

CSOs should follow the basic security manual involving areas of Cyber, Information, Intelligence and Personal Security.

Levels of information sensitivity

Generally, we distinguish three levels of information sensitivity. The primary criterion is the level of political, personal, and security importance for the organization, individuals, and the security.

The reason for the classification is to ensure compliance with the time-proven "need to know" principle – sensitive information is given only to those who need to know it for a specific reason.

LEVEL OF SENSITIVITY	IMPORTANCE CRITERION	WHERE CAN WE DISCUSS THE INFORMATION IN PERSON	WHERE CAN WE DISCUSS THE INFORMATION ELECTRONICALLY
0	Common operational information, which is not sensitive politically or security-wise, a de-facto public information	Anywhere	Anywhere: e-mail, Facebook, etc.
1	**Internal information** (non-public political information that doesn't present a threat to national security, or to involved people)	Only in a designated meeting or bilaterally with a responsible person, without the presence of electronic devices	Signal only (message or call) or ProtonMail, not e-mail, SMS, or phone call
2	**Very sensitive information** (concerning national security, identity of sensitive sources, politically bombshell information)	Only at the designated meeting, bilaterally with the involved person, without the presence of electronic devices	**Nowhere, only in person without electronics**

Every member of the organization must set up and follow security arrangements in five areas:

- Basic cybernetic security of devices and profiles
- Social media security
- Communications security
- Data security
- Personal security

Basic cybernetic security of devices and profiles

a. Basic security rules

We assume that you are using only the widely used operating systems. In the case of "classic" computers, that means Windows and macOS, in the case of portable computers (i.e. tablets and mobile phones) iOS and Android. Apple products (although significantly more expensive) are considered the most secure devices, followed by Android. We strongly recommend not to use any Lenovo products.

i.   Password setting

Rule #1: We use different passwords for different accounts (different numerals, special characters etc.). There is a brief manual on how to do it on the webpage of Mozilla.

Rule #2: Password must have at least 22 characters consisting of letters, numerals, and special characters.

Rule #3: Passwords should be changed ideally every 3 months. It is convenient to put a reminder in your calendar.

Rule #4: We write passwords down only on paper (stored in a location that only we know of, not in our place of employment, and each password must always be missing at least one character, so they are unusable in case of a loss of the paper) never in computer-stored text documents. There is an exception in the form of password managers, such as LastPass or KeePas2. Another tool for having safe passwords can be a so-called electronic keychain (iOS – iCloud Keychain, Windows – Smart Lock, alt. 1Password), which we recommend using for a two-factor authentication or disc encryption (see below).

ii.   Two-factor authentication = a generated code must be entered together with a password

Rule #5: Two-factor authentication must be turned on for every service that enables it. The code may be delivered via text message or a mobile application. We recommend not using text message authentication and setting up Google Authenticator. At the very least, it is essential for Facebook, Twitter, Google, and internet banking. We recommend not to use face-recognition technology.

- The web page displays a QR code which we scan using a mobile application. The account in question is then added to it. Every 30 seconds, the application displays a new unique code, which must be used within its validity. You do not need to have an Internet connection or even mobile phone signal in order to use the application; your device and the server are synced forever after you set them up for the first time. Universal tools: Google Authenticator (iOS, Android), Authy.

Rule #6: Always sign out of the device after finishing work so anyone else after you must sign in again. We recommend using another password and finger print for opening important applications (Signal, Wickr Me, ProtonMail).

Rule #7: Never log in to your main profiles (Google, Facebook, internet banking) on other people's devices unless it is absolutely necessary. If you do, change your passwords afterwards. In Facebook's privacy settings, turn on the notifications about logins on unrecognized devices, ideally via e-mail. Set up a firmware password on your Mac device.

Rule #8: If you receive a suspicious e-mail or private message, forward it to your colleagues with a strong warning (in the subject and the body of the message) not to open it and send it to cert.incident@nukib.cz. The specialists from NUKIB will help you with following steps if needed (e. g. in case of ransomware etc.).

b. Antivirus

Rule #9: Operating systems such as Windows 10 already have a built-in antivirus (Windows 10). In general, there is no need to install a paid third-party protection. If you do use such protection, avoid products from Kaspersky Lab (as there is a reasonable suspicion that it is connected to the Russian intelligence services), Huawei or ZTE (as there is a reasonable suspicion that they collaborate with Chinese intelligence services). We recommend the Avast Antivirus or Eset. We strongly recommend not using Chinese antivirus software (e. g. Qihoo 360, Tencent PC Manager). We recommend using 2 antivirus programs at the same time. Download the VirusScanner program.

Rule #10: Big majority of cyberattacks are via email – phishing. The basis of a functional protection against viruses is to avoid opening e-mail attachments coming from unknown senders. Be especially aware when the file attached has extension such as .exe, .pkg, .dmg, or .app. Moreover, do not forget to check the authenticity of the sender before opening the attachment. Remember that even files in formats like .pdf or .doc. may contain harmful background processes. If prompted, always refuse to "enable macros" in Excel. If somebody sends you a link, it is a good idea to copy it into virustotal.com first, as it will provide you with at least some idea whether it is trustworthy. Apply rule #8 afterwards.

If you are certain that you have been infected with malware, the safest and best course of action is to wipe the media with a disk wiping tool, re- install the operating system and applications and copy your data from a backup (having checked that the backup is not infected).

If you suspect devices are infected, run a malware scan immediately. Even if the scan comes up negative, continue to be proactive by following these steps. If you are still suspicious, use a second AV product.

The actions should include:

i. WINDOWS

Step 1: Disconnect the computer from the network. Run anti-malware scan (preferably run from an external USS stick with updated AV on it).

Step 2: Enter Safe Mode. Do this by turning your computer off and on again. Then, as soon as you see anything on the screen, press the FS button repeatedly. This will normally bring up the Advanced Boot Options menu. From there, choose Safe Mode and press Enter.

Step 3: Delete Temporary Files. While you are in Safe Mode, you should delete your Temporary Files using the Disk Cleanup tool. To do this:

- Go to the Start menu;
- All Programs or just Programs);
- Accessories-System Tools, Windows Administrative Tools (depending on the version)
- Disk Cleanup;

- Scroll through the Files to Delete list, and choose Temporary Files.

  Deleting these files could remove malware if it was programmed to start when your computer boots

Step 4: Download and run a Virus Scanner. If you have been infected, then your anti-malware did not intercept it. You should download (on a different computer) and then transfer it to the computer in question and install (or run):

- A real-time scanner, such as AVG Antivirus free or Avast Free Antivirus, which scan for malware in the background while you're using your computer;
- An on-demand operating system scanner, like Microsoft Safety Scanner, but this needs to be run manually each time you want to scan.

  It may be necessary to use both types of scanner to remove the malware. Depending on the type of anti-malware, it may be necessary to reconnect to the internet and download an additional product.

  It may be necessary to remove a virus manually. You should only attempt this if you are experienced at using the Windows Registry and know how to view and delete system and program files.

Step 5: Once you have removed the malware, you will need to recover (from your backups) or reinstall any damaged files or software.

c. Software updates

Rule #11: Software updates are absolutely essential. Make sure that you have automatic updates turned on both at your computer and your cell phone.

- If you have an older version of Windows (such as 7 or 8), it is necessary to keep the update settings as default (i.e. have automatic updates turned on). If the system wants to install an update, you must let it do so. In Windows 10, there is no easy way to turn updates off (you can delay them only in the Pro version, which we do not recommend).
- Mac: By default, the system automatically checks for updates via the Mac App Store application. Apple always provides the best support only for the newest version of macOS. Turn on automatic updates in Mac/About this Mac/Updates/Advanced.
- Mobile OS: regularly check for updates in the system settings and always have the most up-to-date version. For iPhones, we recommend the iVerify app, which guides you in several steps through all necessary security measures.
- Default browsers (Safari, Internet Explorer, Edge, or Chrome in Android devices) are usually updated together with the OS itself. Third-party browsers, such as Chrome or Firefox, are updated separately, usually automatically. If the browser offers you an update, you must immediately install it! Having an up-to-date web browser is truly the alpha and omega of Internet security. We recommentd installing the app "HTTPS Everywhere", which controls the security of visited websites for you.

d. How to properly lock and track mobile devices

Rule #12: It is essential to use a numerical or other code for unlocking the device (password with at least 22 characters). If the device has a fingerprint scanner, have it activated.

- It is also essential to set up lock on your laptop, so it locks and demands password every time you close it and re-open it. Lock your PC every time

you leave it even for a while (press Windows button + L).

- Buy a screen foil that allows you to look at the screen only from a straight angle and prevents strangers to see what you write or do from other angles. When working with sensitive data, pay attention to your position towards windows. The best way to obtain passwords and other data is by looking through windows.

Rule #13: There is usually an option in the device's settings to erase all data if a certain number of unsuccessful attempts to unlock it was made. We recommend having this option turned on. Moreover, it is also good to have your SIM-card password-protected so that it is not possible to simply put it in a different phone.

Rule #14: It is imperative that you have phone tracking activated. In iOS, turn on the function Find My iPhone (here you can find further instructions, Apple also describes what you should do in case your iPhone gets lost or stolen). If you use Android, you need to have installed and activated the Android Device Manager.

- Loss or theft of a device: you must immediately open the application on another device or web (Android Device Manager / iCloud), log in to your account and try to locate your device. Using these tools, you can also securely erase all data stored on the device, even if it is not possible to locate it at the moment – data will be erased the moment the device is connected to the Internet.

Rule #15: Apple devices also have a function called Activation Lock. If you have the Find My iPhone function turned on and erase the device through it, it will still be paired with your account which means that the thief will not be able to use it or activate it, which will prevent them from being able to sell it on the black market. The device will be paired with your account forever unless you physically type in the password or the new owner finds it out – which is in combination with two-factor authentication practically impossible.

- Android: if you have the Android Device Manager turned on, you should have access to all the security functions your phone offers.
- Services such as Find My iPhone or Android Lost also enable you to access your device remotely and erase all data stored in it in case of loss or theft.

Rule #16: It is also important to be cautious when using Wi-Fi or Bluetooth on mobile devices. These services should always be turned off if not being used. Furthermore, limit the number of applications which have access to your location data to a minimum. Usually it can be set up in folder Settings/Applications/Accesses. Go through all the accesses and consider if they are reasonable, then disable all of the others. We caution against using hands-free Bluetooth devices (printers, headphones), as they present further security risk. We recommend acquiring the so called "charger condom" which makes sure there is only electricity flowing to your device. This type of device penetration is very simple if not accounted for.

Rule #17: The camera and microphone on your mobile device might be remotely activated. Never carry your smartphone in places where it might be used by an adversary to gather sensitive information. During sensitive meetings, put the phone away or, if technically possible, remove its battery. The ideal solution is to put all electronics into a bag which you then move at least 7-10 meters away from you. This way, you will be able to keep an eye on it but the devices will be incapable of "hearing" your conversation. Apart from camera cover, we recommend disabling the camera in your computer altogether and installing the "Oversight" app, which guides foreign usage of your camera and microphone.

Rule #18: It is convenient to cover the web camera on your laptop and take down the cover only when needed. The same goes for your cell phone – cover the

camera with a case and only take it out when needed.

e. Backup and emergency protocol (in case of loss/theft of device)

Rule #19: We recommend backing up your personal and work documents on an encrypted external hard-drive that you have safely stored at home and off-line. iStorage company sells cheap and well encrypted external hard-drive devices. It is recommended to keep very sensitive data on an isolated clean computer which never connects to the Internet. We recommend backing-up your personal calendar (ideally on Google), which can come in handy if you need to check events from years ago.

Rule #20: There are a lot of disk-encrypting apps, both free and paid. VeraCrypt is often recommended.

Rule #21: You only need to backup unique and irreplaceable documents. In the vast majority of cases, this will not be more than few hundred megabytes. Make sure that you back up at least once a month.

f. In case of loss or theft of device

Step 1: check the location of the device using the tracking service of your choice. If you left your phone or tablet in school, work, or café, contact the personnel and pick up your device as soon as possible. Such scenario does not possess significant risk.

Step 2: if you locate the device in places that you did not visit or you see that it is moving, we suggest that you immediately contact the police and hand over the information about the device's location. Acting swiftly is important, as you will be able to see the device's location only until its battery dies or it is disconnected from the Internet.

Step 3: if you are aware that you have extremely sensitive information stored on the device and for some reason you did not act according to the recommendations from previous chapters, we advise to remotely erase the device at once.

Step 4: immediately change your passwords for all your accounts.

Rule #22: In the event of loss or theft of your device, always remember that it is better to lose, for example, 14 days of finished work than to jeopardize the security of all data stored on your device. Moreover, by ignoring this you might endanger the data stored on the cloud servers of your employer as well. If you are unable to have your phone on your person (if storage in a locker is required), use single use sealing bags to make sure it was not manipulated with. They are called Security envelopes and can be purchased at EuroSeal.cz for example.

Social media security

Rule #23: Be strict in setting up your privacy settings on Facebook – make your posts visible only to your friends, eventually you can create various groups for specific content within your friends. Make sure that you have to approve posts in which you are tagged. Below you can find a detailed manual. Disregard these rules if your Facebook profile is a deliberately public presentation.

About Facebook Apps

Do not login to or link third-party sites (e.g. Twitter, Bing, LinkedIn) using your Facebook account. "Facebook Connect" shares your information, and your friends' information, with third party sites that may aggregate and misuse personal information.

Also, use as few apps as possible. Apps such as Farmville access and share your personal data.

Edit your profile by changing all the options to Only Me (most secure) or Friends Only.

Editing Your Privacy Settings

1) **Control Your Default Privacy** – Change to Friends Only

2) **How You Connect**

   a. Who can look up using your e-mail or phone number? - Friends

   b. Who can look you up using the email address or phone number you provided? - Friends

   c. Who can send you friend requests? - Friends of Friends

   d. Who can send you Facebook messages? - Friends

3) **Timeline and Tagging**

   a. Who can post on your Timeline? - Friends

b. Who can see what others post on your timeline? - Friends

c. Review posts friends tag you in before they appear on your timeline - On

d. Who can see posts you've been tagged in on your timeline? - Friends

e. Review tags friends add to your own posts on Facebook - On

f. Who sees tag suggestions when photos that look like you are uploaded? – Friends

4) **Ads, Apps and Websites**

   a. Apps you use – Limit use of Apps

   b. How people bring your info to apps they use – Uncheck all boxes

   c. Instant personalization – Disable Personalization

   d. Public Search – Disable Public Search

   e. Ads >subpages>Ads shown by third parties – No one

   f. Ads >subpages>Ads and friends – No one

5) **Limit the Audience for Past Posts** – Limit the Old Posts to Friends Only

6) **Blocked People and Apps** – Here you can block certain people, events and game invites.

General
Security and login

Privacy
Timeline and Tagging
Blocking
Language

Notifications
Mobile
Public Posts

Apps
Adverts
Payments
Support Inbox
Videos

Timeline and Tagging Settings

Who can add things to my Timeline?	Who can post on your Timeline?	Only me	Edit
	Review posts that friends tag you in before they appear on your Timeline?	On	Edit
Who can see things on my Timeline?	Review what other people see on your Timeline		View As
	Who can see posts you've been tagged in on your Timeline?	Only me	Edit
	Who can see what others post on your Timeline?	Only me	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Only me	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

Public Post Filters and Tools

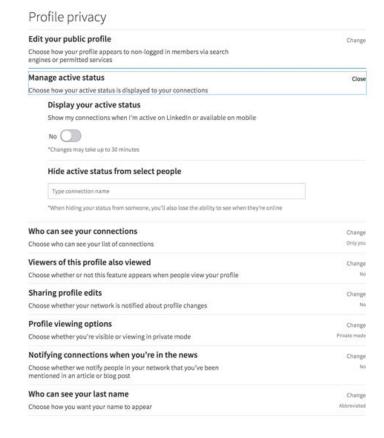| Who Can Follow Me | Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you. Each time you post, you choose which audience you want to share with. Learn more. | 👥 Friends ▼ |
Public Post Comments	Who can comment on your public posts? **Friends**	Edit
Public Post Notifications	Get notifications from **Nobody**	Edit
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? **Friends**	Edit
Comment Ranking	Comment ranking is **Off**	Edit
Username	You have not set a username.	Edit
Twitter	Connect a Twitter account	Edit

Rule #24: It is wise to hide your home address, phone number, e-mail, and other data (or never enter them in the first place, Facebook often sells them to third parties). Go to the "About" tab on Facebook – erase your address and set your e-mail and phone number to "only me" so that it is not visible to anyone else. Take a look at how your profile looks from a friend's or stranger's perspective using the "view as" function. To be sure, Google your e-mail, home address, and phone number to see where this information is accessible and where it can be erased from. You should also repeat this procedure for your family members.

Rule #25: Limit the possibility to look up your profile to <u>friends only</u>. Each month erase the content of all your Facebook conversations. If somebody steals your profile, they will not gain sensitive data from your personal conversations.

Rule #26: Do not permit other search engines than Facebook to <u>access your profile</u>.

Rule #27: Turn off <u>personalized ads</u>.

Profile privacy

Blocking and hiding

| Job seeking

Data privacy and advertising

Security

Job seeking

Sharing your profile when you click apply Change

Choose if you want to share your full profile with the job poster when you're taken off LinkedIn after clicking apply No

Let recruiters know you're open to opportunities Close

Share that you're open and appear in recruiter searches matching your career interests

We take steps not to show your current company that you're open, but can't guarantee complete privacy. Learn more

No ⬤

Update career interests

Data privacy and advertising

Manage who can discover your profile from your email address Change

Choose who can discover your profile if they have your email address Nobody

Manage who can discover your profile from your phone number Change

Choose who can discover your profile if they have your phone number Nobody

Representing your organization Change

Choose if we can show your profile information on your employer's pages No

Profile visibility off LinkedIn Change

Choose how your profile appears via partners' and other permitted services No

Advertising preferences Change

Choose whether LinkedIn can serve interest-based advertising through our platform for services No

Security

Two-step verification Change

Activate this feature for enhanced account security On

Profile privacy

Edit your public profile Change

Choose how your profile appears to non-logged in members via search engines or permitted services

Manage active status Close

Choose how your active status is displayed to your connections

Display your active status

Show my connections when I'm active on LinkedIn or available on mobile

No ⬤

*Changes may take up to 30 minutes

Hide active status from select people

Type connection name

*When hiding your status from someone, you'll also lose the ability to see when they're online

Who can see your connections Change

Choose who can see your list of connections Only you

Viewers of this profile also viewed Change

Choose whether or not this feature appears when people view your profile No

Sharing profile edits Change

Choose whether your network is notified about profile changes No

Profile viewing options Change

Choose whether you're visible or viewing in private mode Private mode

Notifying connections when you're in the news Change

Choose whether we notify people in your network that you've been mentioned in an article or blog post No

Who can see your last name Change

Choose how you want your name to appear Abbreviated

Rule #28: When using Facebook on your phone, <u>limit or disable the app's access to your location.</u>

Rule #29: Photos taken on a smartphone contain a lot of sensitive data about the time and location they were taken at. If possible, do not share them directly on social media or turn off the location for photos. Furthermore, reduce the size of the photo and edit it (this will corrupt the photo's metadata). iVerify can also delete your metadata for you. Otherwise, you are risking information about your software and operational system to be exposed.

Rule #30: Do not log in to Facebook via other web pages – such login always shares your data.

Rule #31: Do not add people you do not know as your friends. If you were not strict in this matter in the past, go through your current friends and unfriend those that you do not actually know. This does not apply for those who have a public profile deliberately.

Rule #32: LinkedIn is often used for personal data gathering. If you need to use this network put only publicly known information there. Check what information you have already put on LinkedIn. Carefully look for any connection leading to your family or close friends (other than publicly known), because there is a risk of "approaching" (who will make contact and how it will be made to gain your trust).

a. Securing sensitive information about you and persons close to you

Rule #33: Decide what information you want to protect. The essentials are your home address, information about your relatives, and your personal affairs which could be abused by an adversary (e.g. that you have a relationship crisis). Divide the information into three groups:

- public (can be found online and you post them on social media)
- private (e.g. your home address, or the identity of your partner, which is only known to your friends)
- sensitive (accessible only to a limited number of people which you fully trust)

Rule #34: Be aware that whatever you post on social media will become a virtually inerasable information that might prove useful to your adversary years after you post it. Therefore, do not post photos of your home, your kids, and your close friends or relatives. We advise to go through <u>all</u> your photos on Facebook, Twitter, or Instagram and delete those which reveal the identity of places or people that you want to protect.

Rule #35: Devote a few hours to select the information about you that you consider to be private or sensitive and Google it to see if it has not appeared somewhere. By doing so, you will find out what information about you is publicly accessible through open sources. Go through the profile of your close friends or relatives and ask them to delete already posted photos with you and not to post any in the future. If you want to protect your relatives, you cannot have them in your friend list (identical surname makes them easy to look up), which calls for additional series of steps for retrospective protection of their identity – the authors of this manual will gladly provide you with another set of <u>more sensitive measures</u>.

Rule #36: Your permanent address is partly public information, which is available in state databases or commercial contracts. In case you do not want your residence to be easily found, change your permanent address to, for example, the house of your parents or other relatives. It is possible to set your permanent address commercially through your organization.

Rule #37: Set up a notification in Google Alerts that will send you an email if your name (or the combination of your name, your job title, or your employee) appears on any website. Do this for different combinations of your name, position or employer. The results will not include social media.

b. Internet anonymity

All your activity on the Internet shares some level of information about your identity. This information can be analyzed, compared and used for creating a profile of you that might uncover a lot of sensitive information about your behavior on-line. Even though there is no such thing as a complete Internet anonymity, we advise trying to at least minimalize the amount of information that you share about yourself, especially if you carry out sensitive activities. What may now seem banal can be in five or ten years used for psychological analysis of your profile:

Rule #38: Use DuckDuckGo (http://duckduckgo.com) as your primary search engine. This engine uses encoded connection and store neither IP addresses nor your search history. Delete automatic sign-in in all other browsers. Cookies: in commonly used browsers (Chrome, Firefox, Internet Explorer, Safari) you can make use of private/anonymous windows that do not save cookies. However, your IP address is still being identified and your Internet provider can track your on-line activity.

Rule #39: A good service for anonymous and confidential document sharing is Crabgrass (https://we.riseup.net/crabgrass), where you can register anonymously and use it for sharing documents in your team.

Rule #40: In order to cover your on-line identity, we suggest using a paid version of a VPN. Our recommendation would be VPNSecure.me, Proton VPN or Avast and not only on your laptop, but also on your phone or tablet. If you ever connect to unsecured Wi-Fi, it is very easy to track precisely your actions. Never deal with anything sensitive on unsecured Wi-Fi. Never update your software on unsecured Wi-Fi. Change your home Wi-Fi password every 3 months. We recommend using the VPN's "kill switch", which immediately disconnects you from the internet in case of a weak connection, making sure you are covered by VPN at all times.

Rule #41: There is only one way to achieve a high level of anonymity on the Internet and that is by using Tor, a special web browser. We do not recommend using it ordinarily – it is rather slow, besides other things - but only when you want to make sure that some of your on-line activities will not be linked to you (this does not imply only illegal activities; you might want to protect yourself because of politically sensitive statements, communication with people that you do not want to become public etc.). If you are using Tor, do not install plug-ins or download torrents at the same time. It is also recommended not to open documents via Tor (even .doc and .pdf files). If you need to work with documents, temporarily disconnect your computer from the Internet.

Communications security

a. Communications encryption

If you write sensitive information by hand into a notepad, we recommend destroying them every day (tear up into little pieces and flush into a toilet). This makes sure you won't forget a notepad with many days' worth of notes, making the information vulnerable.

The least secure ways of communication are:
- Phone calls, text messages: providers keep records of phone calls and text messages and are often able to provide them to a third party (under certain conditions). It is not difficult to monitor your calls and text messages using commercially available technology.
- E-mails are stored on the servers of your provider which makes them accessible to anyone who knows the password to your e-mail account or even to the provider itself. The same goes for Facebook and Twitter. Uncripted email is like sending a postcard via mail – anyone who wants to can read it.

Rule #41: The most secure civilian encrypted app for messages is Signal, through which you can call as well (not group calls). If you are using Signal, it is important that you have everything in the privacy setting turned on – including setting up a passphrase and regular deletion of messages (we recommend the interval of one day). We don't recommend using WhatsApp or Skype for sensitive information. For significantly sensitive data we recommend Wickr Me. Do not use Viber or Telegram. When making calls through an encrypted app, mind your surroundings. Never speak about sensitive information in public transport, in a car with a stranger, or in a room with other people. Best thing to do is to walk around outside.

Rule #42: The most secure app for encrypted e-mails is ProtonMail, provided that it is used by both sides. ProtonMail is available for iOS, Android, and on the web. It is recommended to download Proton Bridge in paid version, because it allows you to install Proton Mail to e-mail client in your computer. Do not forget to set up two-factor authentication. Erase ProtonMail every 3 months by erasing all delivered and sent e-mails. As we need a secondary backup email for ProtonMail, we recommend setting up a separate (can be unpaid) ProtonMail with a super strong password (40 characters), which will be used as a backup email for all your other profiles – Facebook, Twitter, LinkedIn, Instagram, bank accounts.

Data security

Every shared folder (e.g. on Dropbox) is only as secure as the least secure team member.

Recommended iPhone settings:
- Settings>Notifications> go through every app and ensure notifications cannot be accessed in locked screen
- Settings>privacy>location services>
  - >share my location – set to off
  - Go through each app and determine whether you need GPS on 'while using' or 'never'. Make sure nothing is on 'always'
  - Make sure 'never' is selected for: camera (or all your pictures are stamped with where they were taken); all social media apps (i.e. twitter, Facebook, Instagram)

- – >systems services – all off except 'Emergency SOS' and (optional) 'Find My iPhone'
- – >frequent locations – 'clear history' and turn to 'off'
- – Product improvement – all 'off'
- • Settings>privacy>
  - – Diagnostics & Usage – 'don't send'
  - – Advertising – 'Reset Advertising Identifier' and 'Limit Ad Tracking' – on

a. Disk encryption

Rule #43: Encrypt your disc:

- • macOS: contains a disk encryption program called FileVault – after you turn it on, it will generate a recovery key (which may be safely stored on Apple servers) and then encrypt the whole disk. The subsequent decryption is a background process, unnoticeable for the user, and does not slow the system down.
- • Windows: the encryption feature BitLocker is included only with the professional editions of Windows. Applications such as VeraCrypt or CipherShed represent a good alternative for owners of the editions without BitLocker.
- • Cell phones and tablets with Androids 5.0 (Lollipop) and newer usually support encryption, however, in many cases it degrades the device's performance and therefore decreases user comfort. Accordingly, we recommend keeping the encryption off in such cases provided that the user will adhere to the following tips.

b. Encryption and secure deletion of data stored on removable disks

Rule #44: USB flash drives: on Macs, it is sufficient to "right-click" on the disk icon in Finder and choose the option Encrypt. If you then insert it into another computer, you just type in the password. If you have a version of Windows with BitLocker, you can encrypt disks either in the BitLocker section of Control Panel or simply by right-clicking the removable disk icon. If your version of Windows does not contain BitLocker, you can use the above-mentioned app VeraCrypt, which has the same function. Never load an unfamiliar USB flash drive into your device, even it would your friend's – you don't know if he/she takes care of its safety. Install USB software Safeguard, which will open only verified flash drives. For unfamiliar files use Sandbox application.

Rule #45: Simply deleting data from a disk does not make them inaccessible – it is therefore necessary to carry out a safe erasure, which may take longer but you will be able to hand the disk over to anyone:

- • MacOS: you may use the system application Disk Utility (section Erase disk contains a button for secure erasure). Use Eraser application.
- • Windows: currently, Windows does not support secure erasure in its basic configuration. Nevertheless, even the free version of CCleaner, for instance, is able to securely erase data from removable discs.

<u>Personal security</u>

Rule #46: Do not have your name on the doorbell at the entrance to the building. If you must have it there, then you cannot have it on the doors to your flat.

Rule #47: If you are away from home for a longer period of time, do not announce it publicly and make sure that your posts on social media do not display your location. Alternately, post travel snapshots only after your return home. If you order taxi or Uber, it is recommended not to do it exactly at the location of your stay, but at least 50 meters away, and similarly for leaving the vehicles. Location data is stored in your profile and can be obtained relatively easily.

Rule #48: Arrange a password with people close to you so that they can text or call you when they feel endangered, and you will immediately call the police and go search for them – make sure they also tell you their location. Do the same for your family. If you are unable to make a phone call, you can also send out a distress signal.

Rule #49: Never enter an enclosed space alone with an unknown individual. Instead slow down, fake a phone call or turn elsewhere and take a different way. If you are feeling uncomfortable in any place, immediately take out your phone and fake a phone call to a person close to you, say out loud where you are and, for example, that there is a weird person there whose appearance you describe aloud. That almost always works a successful deterrent. Alternately, start yelling, loudly and unwaveringly. A false alarm costs you nothing, which cannot be said about the alternative.

Rule #50: In order to be able to roughly recognize how urgent is a certain threat, memorize the table below. The basic rule in case of physical incident is: run, hide, fight.

8. KEY FINDINGS

- Lack of Cyber security manuals within the CSO.
- Lack of operational security routine/lack of willingness to follow the routine.
- Lack of respective human resources (specialists) within CSOs
- Operational security is taken too lightly.
- Usual operation security mistakes made by government officials, journalists and CSOs, resulting to them becoming easy targets:
  - "I am not that important."
  - "I am not doing anything illegal."
  - "This is not classified."
- Working in the field of countering Russian and Chinese influence leads to you becoming a target.
- Russia and China can survey thousands of individuals working in this area with ease.

9. SUMMARY

The Ten Security Habits everyone should follow

The rules we recommend following are listed above. Often these are steps that you need to apply just once. Beyond this initial adjustment of your security behavior, it is recommended you adopt these daily habits, and follow them in the same way you regularly brush your teeth or lock your door:

Habit # 1: For secure communication use only the Signal app (to message and to call), and ProtonMail for encrypted emails. Do not trust applications such as WhatsApp, Facebook Messenger, or Telegram for more sensitive conversations (Rules # 41 - # 42)

Habit # 2: Regularly delete data on your computer using the Permanent Eraser or Cleaner programs. (Rule # 45)

Habit # 3: The majority of cyber-attacks come through phishing. Therefore, open all email attachments in Sandbox and check all links received via virustotal.com. (Rule # 10)

Habit # 4: Do not trust any USB drives, as it isn't possible to verify their security. It is better to have the data sent to ProtonMail if possible. Alternatively, keep a separate computer without Internet connection where you can open the USB drive. (Rule # 44)

Habit # 5: Store mobile phones safely during sensitive meetings. Ideally, electronics should be placed in a bag about 7-10 meters away, so it is within your sight but without the risk of devices "hearing" your conversation. (Rule # 17)

Habit # 6: It is advisable not to use wirelessly connected devices (headphones, printers). Purchase "USB condoms" for your phone and computer chargers (Rule # 16).

Habit # 7: When adding information and photos to your social media accounts, only add the ones you'd allow your opponents to see. If you post anything about your family and relatives or your personal life, your opponents can create a psychological profile and social map and can exploit this information. (Rule # 33)

Habit # 8: Always use a VPN: VPN Secure Me, Proton VPN or Avast. Keep the kill-switch rule set. (Rule # 40)

Habit # 9: If you write sensitive notes by hand, we recommend processing them during the day, then shredding them (or tearing them into small pieces and discarding them into a bin away from your home or office).

Habit # 10: SET UP A CALENDAR REMINDER: We change passwords every three months. (Rule # 1 - # 4). We recommend that you back up your personal documents, electronic calendar contents, and your own work files to an encrypted external drive on a monthly basis. (Rule # 19)

A NON-ENCRYPTED EMAIL IS EQUIVALENT TO POSTING YOUR MESSAGES PUBLICLY IN REAL TIME

MAKE IT HARDER FOR THE ADVERSARY

1) Use a good VPN (Avast Secureline, ProtonVPN, NordVPN,...), .
2) Use a good anti-virus and anti-ransom software (Avast, Eset, McAfee...).
3) Encrypt your data (VeraCrypt).

DON'T PUT ALL YOUR EGGS INTO ONE BASKET

1) Secure all your accounts and profiles with two-level authorization.
2) Have several well protected emails for your accounts, so if one gets hacked, not everything can be taken.
3) Use strong passwords, do not use one password for all your accounts

ALWAYS DOUBLE-CHECK NEW PEOPLE YOU ARE MEETING

1) Always research (via Google) their background and ask for quick references from people who know them.
2) Don't let strangers into your offices.

KNOW WHICH IDENTITY INFORMATION YOU ARE PROTECTING

Is your Facebook profile full of information about your partner and your children?
Understand that public information is easily available to adversaries and can be used against you.