REPORT

LESSONS LEARNED FROM RESILIENCE AND SELF-PROTECTION CAPABILITY OF CIVIL SOCIETY ORGANISATIONS IN GEORGIA

2020
This Report follows a year of cooperation between non-governmental organizations and think-tanks from Central Europe and the Eastern Neighbourhood (EN) with the support of the European Commission. The aim of the project was to enhance the resilience and self-protection capabilities of civil society in Georgia, Ukraine, and Moldova. The project envisages empowering organizations and experts in target countries who counter the Kremlin disinformation, as well as media representatives and civil activists.

This report identifies the institutional and personal security challenges and needs of Georgian civil society organizations (CSOs), media, and activists draw from in-depth interviews with representatives of these sectors, all of whom faced different types of cyber, personal, counter-intelligence and information security issues.

The Media Development Foundation (MDF) conducted in-depth interviews with 24 respondents, out of which 12 represent CSOs, 8 come from media services, 3 are civil activists, and 1 hold office in a government institution.

Authors

Mariam Pataridze, Sopho Gelava, Tinatin Gogoladze, Media Development Foundation

Editor

Andrea Michalcová, Deputy Director for Projects, European Values Center for Security Policy
Most of the respondents do not use any manual or guideline of operational security.
KEY FINDINGS

Training in operational security

Only 10 respondents said that they attended training in operational security, while most of the respondents (14) do not have any training in this field. In 10 cases, respondents identified that the training concerning cybersecurity and only one training was on physical security. Out of the journalists, CSOs, and civil activists, the higher number of representatives of CSOs identified that they received some training (6) and, at the same time, did not (6). In addition, 24 respondents said that they needed training in cyber and digital security, and only 2 said that they need training in personal security. The respondents identified the following needs:

- Password security
- Information storage policy and back-ups
- Business continuity planning in crisis situations
- Information security and cyber hygiene
- Highly-protected websites
- Licensed programs
- Personal data protection
- Identification of fake news
- Identifying viruses, phishing
- Network security
- Secure use of new gadgets
- Countering online discreditation campaigns and troll attacks
- VPN

Operational security guidelines/manuals

Most of the respondents (14) do not use any manual or guideline for operational security. Media employees (5) and CSOs (4) are the most aware of operational security guidelines. Out of those respondents who use operational security manuals/guidelines, only 3 identified that their workplace has an IT specialist. Besides internal documents, respondents also named IREX Safe, ITU, and ICANN international guidelines. In most cases, the issues covered in the guidelines were traffic monitoring, login controls, MD5 generated passwords, multi-factor authentication, closed ports, antivirus policies, backup policies, and use of secure messengers. The representative from the NATO & EU Information Centre, which is a government institution, explained that the Centre acts according to the order issued by the Minister of Foreign Affairs on information security instructions.

Addressing authorities

Most of the respondents (22) clarified that they are aware of whom to address in case of operational, cyber, or personal security threats. Respondents identified that the authorities they would address differ according to the incidents, which is shown in the table below.

Some of the respondents expressed their mistrust towards state authorities and their investigations and preferred to go public in case of the incidents. Several respondents would alternatively address international organizations, other CSOs, diplomatic missions, and media.

<table>
<thead>
<tr>
<th>INCIDENT</th>
<th>AUTHORITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDoS attack</td>
<td>– IT specialist</td>
</tr>
<tr>
<td></td>
<td>– Investigation agencies</td>
</tr>
<tr>
<td></td>
<td>– Special Cybercrime Unit under the Ministry of Interior</td>
</tr>
<tr>
<td>A leak of personal data</td>
<td>– State Inspector Service</td>
</tr>
<tr>
<td></td>
<td>– Special Cybercrime Unit under the Ministry of Interior</td>
</tr>
<tr>
<td>Phishing</td>
<td>– IT specialist</td>
</tr>
<tr>
<td>Online discredits</td>
<td>– Charter of Journalistic Ethics</td>
</tr>
<tr>
<td></td>
<td>– Facebook</td>
</tr>
<tr>
<td></td>
<td>– Public Defender’s Office</td>
</tr>
<tr>
<td>Identity theft</td>
<td>– Ministry of Interior</td>
</tr>
<tr>
<td>Physical or verbal abuse</td>
<td>– Investigation agencies</td>
</tr>
<tr>
<td>Counter-intelligence security</td>
<td>– Investigation agencies</td>
</tr>
</tbody>
</table>
Future Threats

Respondents have also reported concerns and fears that could jeopardize their security over the next 1-3 years. Most of them (13) named an array of cyberattacks, including unauthorized access to accounts and servers or ransomware. Respondents anticipate the intensification of online discreditation and cyberbullying incidents from hate groups and government trolls.

Sources of the threats

In most cases (14), respondents traced the sources of these threats to inside actors. Two of them named outside actors, and 7 respondents identified both. 4 main groups were identified from the inside actors: government-backed hate groups (Georgian march was named several times), radical groups linked to the Orthodox Church, local Kremlin satellites, government trolls, and related pages. As for the outside actors, respondents concentrated on hybrid warfare challenges and threats originating from Russia.

Experienced threats

Respondents also recorded the threats they have experienced in the past. Most of them named cyber (21) and information security (21) threats, followed by personal security (16) and counterintelligence security (12) threats. In most cases, participants experienced phishing, distributed denials of service (DDoS), online discredits, email hacking, and intimidation.

| The cyberattack, including hacking, unauthorized access to accounts and servers, ransomware | 13 |
| Online discreditation, cyberbullying and harassment | 10 |
| Physical attack | 9 |
| Threat (including physical threats, rape, burn down the office) | 8 |
| Blackmail | 4 |
| Arrest | 2 |
| Problems with government agencies, including financial audit | 1 |
| Attempts of information extortion | 1 |

<table>
<thead>
<tr>
<th>CYBERSECURITY</th>
<th>INFORMATION SECURITY</th>
<th>COUNTERINTELLIGENCE SECURITY</th>
<th>PERSONAL SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing (fake emails and website links received)</td>
<td>15</td>
<td>Online discredit (gossips, lies, insults)</td>
<td>18</td>
</tr>
<tr>
<td>DDoS (websites unavailable)</td>
<td>12</td>
<td>Hacking emails (disclosure of communication, stealing data)</td>
<td>14</td>
</tr>
<tr>
<td>Ransomware (data encrypted)</td>
<td>9</td>
<td>Leak of personal data (address, telephone number)</td>
<td>9</td>
</tr>
<tr>
<td>Loss of data</td>
<td>8</td>
<td>Leak of passwords (Yahoo, Facebook)</td>
<td>9</td>
</tr>
<tr>
<td>Hacking</td>
<td>3</td>
<td>Online identity theft (impersonation)</td>
<td>7</td>
</tr>
<tr>
<td>Suspicious devices near office (USB sticks, DVDs on the ground)</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CASE STUDIES

Throughout the project, the MDF has identified 21 cases related to cyber security, personal security and information security.

<table>
<thead>
<tr>
<th>CATEGORY ACCORDING THE TOPIC</th>
<th>NUMBER OF CASES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online discrediting against NGOs and critical media</td>
<td>9</td>
</tr>
<tr>
<td>Threats by hate groups and pro-Kremlin groups</td>
<td>4</td>
</tr>
<tr>
<td>Violence by hate groups</td>
<td>2</td>
</tr>
<tr>
<td>Violence during the dispersal of anti-occupation demonstration</td>
<td>2</td>
</tr>
<tr>
<td>Detention of anti-occupation demonstrations’ activists</td>
<td>1</td>
</tr>
<tr>
<td>Corruption related violence</td>
<td>1</td>
</tr>
<tr>
<td>Violence on religious grounds</td>
<td>1</td>
</tr>
<tr>
<td>Obstruction of journalism</td>
<td>1</td>
</tr>
</tbody>
</table>
Acknowledged government trolls have published content that attacked media outlets critical of the government.
Government Trolls Harassing NGOs, Critical Media Outlets, and Activists

Throughout our research period, MDF identified government trolls (fake accounts) and related fake pages that were involved in discrediting NGOs, critical media outlets, and activists.

Against anti-occupation demonstrations: Pro-government fake pages, trolls, pro-Russian bodies, and hate groups who targeted anti-occupation demonstrations in front of the Parliament. All three sources employed identical messages and narratives that aimed at discrediting the activists. These actors linked the rallies to the pride and LGBT community as well as unlawful political opposition.

About Pankisi developments: With the blessing of the Interior Ministry, government trolls and fake pages attempted to discredit the Kist community. The Facebook page Inews released a video with the caption that Kists were shouting “Allah Akbar”, which is adapted as a battle cry by some terror groups. The video aimed at inciting strife on religious grounds. According to some comments made by government trolls on other posts, the Kists worship “another God.” Such actions aim at distancing and alienating the Kist citizens of Georgia from the Orthodox Christian community.

Against NGOs: A fabricated photo and story was spread by GD supporter Leila Tsinadze-Melikidze on the Facebook page “კახა კალაძე - თბილისის მერი” (Kakha Kaladze – Tbilisi Mayor), which calls out Eka Gigauri, Head of Transparency International Georgia (TI), as an opponent of a pension increase. The post features Gigauri’s photo and a caption reading, “If you increase pensions, pensioners will then demand something else.” GD lawmaker Karlo Kopaliani shared the post on his own Facebook page with the inflammatory caption that “This is the face of some non-governmental organizations that are taking care of the public welfare!” Kote Inashvili, journalist of Obieqtivi TV, spread the post in various Facebook groups, including “Bidzina Ivanishvili’s friends on Facebook”, and “Against the country’s enemies.” Facebook users wrote negative and insulting comments under each post and the image. On October 17, Transparency International Georgia released its assessments and recommendations about the 2020 draft state budget. According to one of its recommendations, the government should refrain from increasing pensions and salaries of public employees in the months prior to elections, because such actions would be perceived as the use of administrative resources in a pre-election period. MP Akaki Zoidze, who chairs the Parliament’s Healthcare and Social Issues Committee, misinterpreted TI Georgia’s recommendation, describing it as a prohibition.

Several discrediting posts published by well-known trolls against the Media Development Foundation (MDF) and Open Society Georgia Foundation (OSGF) discussed the March 15, 2019 study “Informing Ethnic Minorities on Georgia’s Euro-Atlantic Integration.” That work was followed by a handful of misleading stories aired by the Georgian

2 Public protest in Georgia’s mountainous Pankisi Gorge over the construction of Khadori 3 hydroelectric power plant grew into clashes between locals and the riot police on April 21. Police used tear gas and rubber bullets against the protesters. Locals threw stones back at them. Several dozen people, including police officers and locals, sustained injuries. Police cars were damaged, and the construction machinery burned down.
Public Broadcaster (GPB). The Georgian Public Broadcaster provided a manipulative interpretation of the results of the study, claiming that the study categorized its own broadcast content as the product of Russian disinformation. The public television for its part dedicated several one-sided and unbalanced stories about the March 15 study, while pro-governmental online editions released a number of one-sided publications that were followed by a troll mobilization campaign on social networks. Besides the posts published on personal walls, the mentioned trolls were also sharing discrediting posts in the groups thematically associated with the ruling Georgian Dream party.

Pro-governmental website Zetnews, which was created on February 10, 2019, sponsored critical discussion hosted by the Media Development Foundation that focused on the study. Additional coverage prepared by POST TV on the same topic had also received government financial sponsorship.

The second campaign of government trolls against Open Society Georgia Foundation targeted the CRRC-fielded survey, which included several questions about the trust towards the GPB. Results released on April 3, showed that 47% of respondents have never watched GPB. The public television evaluated the survey results as a campaign unleashed against it and then aired an unbalanced story and false facts suggesting that the Foundation was concealing the real survey results. Government trolls intensified their efforts in social networks, sharing GPB’s statement against OSGF and writing maligning comments. Some pages even sponsored this statement.

On November 13, 2019, Corridor of Shame, a pro-governmental Facebook page that specializes in disparaging content, published a post according to which Myth Detector labelled posts by Corridor of Shame as accurate information. Corridor of Shame pinned this post until November 15, ensuring that everyone who visited the pagewould see this fake post before everything else. In this way, Corridor of Shame aimed to discredit Myth Detector on the one hand, and increase the legitimacy of its own fake posts on the other. Myth Detector responded with an article that called on its readers not to be misled and to report the untruthful post on the grounds that it contained false news.

Against critical media: Acknowledged government trolls have published content that attacked media outlets critical of the government. For example, Rustavi 2 and TV Pirveli, as well as publications of the online edition Liberali were among the targets of attacks. Trolls criticized Rustavi 2 TV for its police blotter and quoted the pro-governmental expert Gia Abashidze, who said that the majority of news stories aired by Rustavi 2 TV were fake or misrepresented. Trolls shared Abashidze’s comments in various media. TV Pirveli’s anchors Vakho Sanaia and Inga Grigolia came under digital ambuscade after its program “Pirvelebi” hosted Interior Minister Giorgi Gakharia on March 22.

After the ruling of the European Court of Human Rights which changed the ownership of Rustavi 2, its former director and major journalists established the new Mtavari television company, which also fell under attack by pro-regime trolls and related fake pages. For instance, the anchors of its primetime news and talk shows were targeted by pro-governmental page “Giorgi Aghapishvili Blog”, portraying them not as journalists but as representatives of the United National Movement. Myth Detector revealed that the person pictured on Aghapishvili’s blog was actually AI-generated photo and did not exist. This was the first incident that identified the use of artificial intelligence from the governmental fake page.

Massive cyberattack on government, private agencies and media organizations

Georgia became the target of massive cyberattack on October 28, 2019. The hackers targeted the servers 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

---

9 Before ECHR ruling on July 18, which changed the ownership of Rustavi 2.
10 Before the changes in editorial policy of media outlet.
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.

According to the statement of the Georgian MFA from February 20, 2020, the results of the investigation of Georgia and UK and information received through cooperation with international partners, the cyber attack was planned and carried out by the military-intelligence agency of the General Staff of the Armed Forces of the Russian Federation (GRU).

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.

**Cyberattack on MDF’s Myth Detector website**

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.

**Cyberattack on TV Pirveli**

The hackers attacked the TV channel using a new generation virus - cryptovirus, which deletes all files and information on August 13, 2019. The virus destroyed the TV channel's video archive.

The opposition accuses the government of having a hand in the cyberattack on TV Pirveli, citing the legal proceedings against a family member of Vato Tsereteli, TV company's founder.

**Cyberattack on Transparency International Georgia**

Official Facebook page of Transparency International Georgia was hit by cyberattack. Hackers, apparently, targeted the page of one of its admins, paralyzing the TI Georgia’s official Facebook page for several hours.

On December 12, 2019, the Parliament Mandaturis (supervisors) interfered with the journalists’ professional activities during the session of the Parliament’s Legal Issues Committee and forced them to quit the chamber. The Mandaturis behaved especially rudely with Tabula journalist Tiko Eradze, who has scratches on her hand.

During the December 12 session, MPs were discussing the issue of appointment of the Supreme Court judges. The committee recommended 14 judicial candidates for the Supreme Court. The parliamentary opposition, independent lawmakers and non-judge members of the High Council of Justice were against this list. Tensions erupted after MP Eka Beselia came to the committee chair, urging him to promise something, otherwise threatening to thwart the session. Journalists tried to shoot their conversation, but the Mandaturis took them out of the room.

“‘They used violence against journalists, they beat us, we have bruises and scratches on our hands, probably others too, not only me; one Mandaturi acted especially violently; he said that he was Alexander Kavelashvili and told me that I would be the first to leave the room. I do not know why he decided this way,” says Tako Eradze.

After journalists unveiled the fact of violence by Mandaturis, media representatives were allowed to enter the room.
Threats against “Tbilisi Pride Week” Organizers

In February 2019, Tbilisi Pride, a non-governmental organization, announced its plans to hold Pride Week, a series of cultural and educational events, in addition to Pride March in June 2019. The announcement prompted ultranationalist groups to threaten thwarting the event and using violence against its participants.

On June 19, 2019, some organizers of Tbilisi Pride, among them Nino Bolkvadze, Giorgi Tabagari, Tamaz Sozashvili, and Mariam Kvaratskhelia received death threats on their mobile phones. Nino Bolkvadze, a lesbian activist, also received a message in which her children’s lives were threatened. The activists asked the police to protect their rights and they were granted the victim protection in October 2019. However, the authors of the threats have yet to be identified.

Besides personal threats, on June 19, the ultranationalist groups, along with some clerics, besieged the office of Equality Movement with the organizers of Tbilisi Pride trapped inside. They demanded the cancellation of the events. The police had to evacuate LGBT people from the office.

Threats against Khatia Akhalaia for releasing video on sex education

Sex education and gender activist Khatia Akhalaia became the target of threats and cyber bullying after she recorded and released a video on sex education based on UNESCO standards in February 2019. After the video became public, Akhalaia became a target of cyber bullying and hate speech and received numerous threats via Facebook Messenger. They warned that they would kill her and torture and rape her child. Akhalaia approached the prosecutor’s office with scathing attacks from 50 Facebook accounts, but nobody has been charged yet. She has also reported bribes from religious groups to make videos about religious subjects instead of sex education.

Threats against Georgian Public Broadcaster and Keti Tutberidze

In December 2018, members of an ultranationalist movement threatened Keti Tutberidze, a journalist affiliated with the Georgian Public Broadcaster, with physical reprisal after Tutberidze prepared a television report on Russian propaganda.

In the story aired on December 23, an anonymous respondent, who had renounced his months of work on one of the anti-Western Facebook pages for months, spoke about the strategy of spreading disinformation and propaganda by xenophobic groups.

Tornike Vashakidze, activist of an ultranationalist movement Georgian National Unity, wrote on his Facebook page that the public television deserved a Molotov cocktail for airing the story and recommended impalement for Tutberidze. The author of the TV story then took to a social network to documented how an alleged troll cascaded her with hate speech and wrote that she deserves gang rape by Arab men, then reported the disturbing content to law enforcement. According to the Interior Ministry, an investigation for threat has been launched under Article 151 of the Criminal Code of Georgia.

On May 2018, police arrested Tornike Vashakidze and other activists of the Georgian National Unity Party on charges of petty hooliganism and disobedience to police orders. Several xenophobic, homophobic appeals calling for violence are visible on the group’s Facebook page. Giorgi Chelidze, its chief plotter, makes no secret that he is a follower of Nazi ideology, and has been imprisoned on charges related to the illegal purchase, storage, and carrying of firearms.

---

12 “ჯურნალისტს ანტიდასავლურ ფაშისტურ ჯგუფებზე მომზადებული სიუჟეტისთვის ემუქრებიან.”

---

THREATS BY HATE GROUPS AND PRO-KREMLIN GROUPS

---

11
Threats from Ramzan Kadyrov and others against journalist Giorgi Gabunia for insulting Putin

On July 7, Giorgi Gabunia, host of Rustavi 2 TV, insulted Russian President Vladimir Putin during a live broadcast with vulgar verbiage. The faux pas triggered anxiety among the Georgian public and stimulated a demonstration outside the station. Rustavi 2 quickly apologized.

The Russian Foreign Ministry, as well as Chechen leader Ramzan Kadyrov, called on the Georgian government to condemn the journalist’s invective. The Georgian Foreign Ministry called on the international community and all international organizations promoting press freedom “to give proper appraisal” to Giorgi Gabunia’s actions. Lawmakers in Russia’s State Duma even suggested criminal charges against Giorgi Gabunia.

Ramzan Kadyrov threatened Gabunia for swearing at Putin and advised him to go into hiding. Some politicians echoed his sentiments. Ermile Nemsadze, a member of the group ensuring civilian control of the military, communicated his wish for Gabunia’s physical destruction to Russian President Vladimir Putin. Nemsadze is affiliated with an Georgian March, an ultranationalist movement, and the anti-Western Facebook page “Azimuti (Azimuth)”. Azimuti posts material from Russian propagandistic media outlets, has misrepresented an anti-occupation rally, and incites hatred towards the LGBT community and other groups.

In a YouTube address, he called on Vladimir Putin to bring special troops to Georgia to complete this task and eviscerate the network’s director.

Inciting hatred on ethnic and religious grounds

In summer of 2018 number of media outlets reported the news about rape case where the alleged perpetrator was from Iran and the victim was Georgian. One of media outlets Excent.ge asked the director of an NGO Tolerance and Diversity Institute Eka Chitanava to comment on the issue.

In her comment Eka pointed out the standard for ethical news coverage and explained that if the ethnicity of the perpetrator is not directly linked to the crime or motive, media organizations should not point it out.

After the media outlet published Eka’s quote the facebook group Anti- liberac club, affiliated with far-right Georgian March and known for spreading far right conspiracy theories, hate speech and misinformation, along with Beka Vardosanidze launched a facebook bullying campaign against Eka Chitanava. Campaign included spreading misinformation, offensive photo fabrications memes and hate speech directed towards TDI’s director.

Nika Gvaramia. The duo, along with Litvinenko, Berezovsky, and Bendukidze were categorized as “betrayers of Russia”. Gabunia was singled out as “sick” and a “pederast.”
VIOLENCE BY HATE GROUPS

Assault on activist Ana Subeliani to block the premiere of “And Then We Danced”

Radical violent groups held a protest rally near Amirani Cinema on November 8, where the premiere of “And Then We Danced,” a Georgian-Swedish film with gay protagonists, was underway. A couple of days before the premiere, leaders of various ultranationalist movements made violent statements that threatened to cut off access for moviegoers and disrupt the screening. The protestors hounded spectators including Ana Subeliani, a leader of the White Noise protest in May 2018. Beki Vardosanidze, one of the champions of Georgian March, verbally insulted and accosted her. Later, police officers took cordoned off Subeliani, but not before she was hit in the head near her eye. The police launched an investigation pursuant to involuntary bodily injury in Article 118 of the Criminal Code of Georgia, which would have carried a sentence of one to three years. The victim, however, demands to try Vardosanidze for a hate crime.

Georgian March assault on Rustavi 2 TV employees

On March 19, 2018, activists of Georgian March, an ultranationalist movement, gathered outside the Rustavi 2 TV building again and assaulted its journalists and employees. They gathered to protest controversial remarks made by TV host Giorgi Gabunia during the late-night program P.S. According to Gabunia, “Jesus Christ made a big mistake when he chose Israel for preaching; he should have come to Adjara in about two or three years and he would not have been crucified, because there would have been no trees there to make a cross. All the trees would have been replanted to (former Prime Minister) Bidzina’s yard.” The Georgian March claimed that the journalist insulted their religious feelings and demanded an apology from him but then blocked entry to the automobile carrying TV host Giorgi Gabunia and Rustavi 2 TV lawyer Tamta Muradashvil. Gabunia and Muradashvil were illegally deprived of liberty for half an hour. Activists attempted to break its windows and forcibly pried open the door to settle the score with the passengers trapped inside. The protestors assailed reporters who were trying to cover the incident, among them Davit Eradze, who was hospitalized with injuries. Activists tried to break into the yard of the station. Police officers arrested six protesters.

Violence on religious grounds

On November 17, 2017, Georgian citizen Gocha Maisuradze burst into the office of Tabula TV, demanding journalists to vacate the office, otherwise threatening to burn it. Later, Gocha Maisuradze explained that he lived in the same building and he paid attention to the organization after seeing Levan Sutidze, journalist, as well as author and host of the program “Talks about Religion” on the balcony of the office. Gocha Maisuradze threatened Levan Sutidze and other journalists of Tabula, trying to compel them to find a new location for their office. The Tabula staff asked police to help them. Later, on November 18, at 8:45pm, burning clothes and towels were thrown down into the broadcaster’s balcony from the upper floor, where Maisuradze lived. Investigation was launched under article 151 (Threat) of the criminal code of Georgia. On February 15, 2018, Gocha Maisuradze was released from courtroom after getting a conditional sentence.

This is not the first time Levan Sutidze and other journalists of Tabula, among them Irakli Kiknavelidze, Nino Macharashvili and former employee, Avto Koridze were attacked largely due to their liberal editorial policy on religious issues. In particular, on January 12, 2016, they were verbally and physically insulted at a restaurant “Chashnagiri” with the assailants citing their professional activities and swearing at the church by Tabula as the reason behind the attack.

Investigation was launched under article 156 of the criminal code of Georgia, involving persecution of persons because of their speech, opinion or activities using violence or threat of violence.
The Prosecutor’s Office of Georgia launched an investigation into alleged abuse of power by certain officials of the Ministry of Internal Affairs.
Activists Injured in Violent Dispersal of Anti-Occupation Rally

On June 20, Russian Communist Party MP Sergei Gavrilov, who recognizes the independence of Abkhazia and Tskhinvali Region, addressed the delegates of the Inter-parliamentary Assembly on Orthodoxy (IAO) during its 26th session in Russian from the Georgian Parliament Speaker’s seat. His speech that triggered robust public demonstrations. MPs of the opposition European Georgia Party bemoaned the address in the Parliament, demanding that Gavrilov leave the legislature. Protesters gathered inside and outside the Parliament, calling for the resignation of Parliament Speaker Irakli Kobakhidze. The Interior Ministry mobilized riot police outside the Parliament building.

Riot police started to disperse the rally using tear gas and rubber bullets overnight June 20-21 and unleashed fierce crowd control techniques. Georgian student Mako Gomuri, as well as Giorgi Sulashvili, Rustavi 2 TV’s security guard, both lost eyes after being hit by a rubber bullet. A total of 240 people, including journalists and police officers, sustained bodily injuries during the dispersal and required hospitalization. Of these, 25 worked for TV channels, 11 served online media, and 3 staffed international media outlets.

The Prosecutor’s Office of Georgia launched an investigation into alleged abuse of power by certain officials of the Ministry of Internal Affairs with regard to the use of force during the dispersal of the rally. Some of the investigatory work came up short. The Prosecutor’s Office, for example, refused to grant victim status to Gomuri, Sulashvili, and others who lost their eyes after being hit by rubber bullets. Rustavi 2 TV journalist Tamar Bagashvili was also denied victim status for a shot in her arm that required hospital treatment. Civil.ge photographer Guram Muradov, who was hit by at least ten rubber bullets, has not been granted a victim status either.

But The Georgian Young Lawyers Association (GYLA) filed a lawsuit in court on October 11, 2019, on behalf of 16 victims (including 8 journalists) after the Prosecutor’s Office unreasonably refused to grant these people protection. The Tbilisi City Court as well refused to grant victim status to 16 individuals. A month later, on November 11, the Prosecutor’s Office announced that Mako Gomuri, Omar Sekhniashvili, and Mirza Liparteliani were granted victim status. Three police officers have been charged with exceeding official powers during the dispersal of the rally. Other grave cases

The following diagram shows the professional affiliation of media representatives on the scene of the occupation of the Parliament buildings:

<table>
<thead>
<tr>
<th>#</th>
<th>TV CHANNELS</th>
<th>ONLINE MEDIA</th>
<th>INTERNATIONAL MEDIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Rustavi – 2</td>
<td>On.ge – 3</td>
<td>Radio Liberty – 2</td>
</tr>
<tr>
<td>2</td>
<td>TV Pirveli – 6</td>
<td>Netgazeti – 2</td>
<td>Reuters – 1</td>
</tr>
<tr>
<td>3</td>
<td>Georgian Public Broadcaster – 5</td>
<td>Interpressnews – 2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>TV Imedi – 4</td>
<td>Civil.ge – 1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Adjara Public Broadcaster – 2</td>
<td>Gurianews – 1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Maestro – 1</td>
<td>Kavkazski Uzel – 1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>OC-media – 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>25</strong></td>
<td><strong>11</strong></td>
<td><strong>3</strong></td>
</tr>
</tbody>
</table>


of causing bodily injuries remain uninvestigated. Even after the GYLA’s advocacy, only seven civilians have been recognized as victims. In parts of the investigation carried out by the Interior Ministry, charges were brought against 17 protesters while 67 police officers were granted the victim status.

DETENTION OF ANTI-OCCUPATION DEMONSTRATIONS’ ACTIVISTS

Giga Makarashvili, a civil activist and member of the სირცხვილია (Shame) movement, was arrested on November 18 alongside 37 other citizens during the protests on the grounds of the Parliament buildings surrounding the rejection of a fully proportional electoral system in 2020. The 37 detainees were charged with petty hooliganism and disobedience to police orders in a group trial. Judge Valerian Pilishvili sentenced 10 people to administrative detention for periods of 5 to 13 days. Giorgi Mshvenieradze, a human rights activist, said that the judge was “very strict” and that his ruling on the majority of cases was built on the testimony of only one police officer. “Unfortunately, the judge delivered his ruling with such weak and low standards,” Mshvenieradze said, adding that his employer will challenge the court ruling in the Tbilisi Court of Appeals.

A group of 16 civil society organizations, including Transparency International Georgia, Georgian Democracy Initiative, the Georgian Young Lawyers Associations, and the Human Rights and Monitoring Center, asserted in a joint statement on November 21 that Pilishvili “neglected legal requirements, was biased, and restricted the detainees’ rights.” The CSOs noted that the court hearing was “biased” and “politicized.” “Since the court rarely uses imprisonment as a type of administrative punishment, the rulings made against activists aim at weakening protests that may have a negative effect on freedom of assembly and expression in the future.”

<table>
<thead>
<tr>
<th>CSOs</th>
<th>MEDIA</th>
<th>ACTIVISTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlantic Council</td>
<td>International Society for Fair Elections And Democracy (ISFED)</td>
<td>Ana Charkhalashvili, Russia is Occupier</td>
</tr>
<tr>
<td>Media Development Foundation</td>
<td>Institute for Development of Freedom of Information (IDFI)</td>
<td>Khatia Akhalaia, Education and Labour Association</td>
</tr>
<tr>
<td>Journalistic Charter of Ethics</td>
<td>Rondeli Foundation, Georgian Foundation for Strategic and International Studies</td>
<td>Mako Gomuri, Activist</td>
</tr>
<tr>
<td>Georgia’s Reforms Associates (GRASS)</td>
<td>Georgian Institute for Strategic Studies (GISS)</td>
<td>Public Broadcaster</td>
</tr>
<tr>
<td>Tbilisi Pride</td>
<td>Soviet Research Laboratory (SOVLAB)</td>
<td>Nato &amp; EU Info Center</td>
</tr>
<tr>
<td>Tolerance and Diversity Institute</td>
<td>Transparency International Georgia</td>
<td>TV Pirveli (N of respondents: 2)</td>
</tr>
</tbody>
</table>
CORRUPTION RELATED VIOLENCE

Opening fire at the house of journalist Davit Eradze

On January 25, 2019, unidentified persons opened fire at the house of Davit Eradze, sports journalist at Rustavi 2 TV. The door of his house was damaged and a cartridge was found on the balcony. According to some doubts, the attack upon the journalist's house was allegedly linked to the TV story prepared by him.

 Shortly before the incident, Eradze prepared a TV story about the scandal around Georgian wrestlers. He obtained a video footage depicting a conflict between the Champion of Europe and the President of the Georgian Wrestling Federation. The footage showed the President of the Federation assaulting the champion. After the story was aired on Rustavi 2 TV, police arrested the President of the Georgian Wrestling Federation.

The Interior Ministry launched an investigation into the shooting incident under article 236 of the criminal code of Georgia, involving illegal purchase, storage, carrying, manufacturing, transportation, forwarding or sale of firearms, ammunition, explosives or explosive devices.

WHAT CAN BE DONE?
RECOMMENDATIONS FOR CSO & JOURNALISTS

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 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.

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

Every member of the organization must set up and follow security arrangements in five areas:
1. Basic cybernetic security of devices and profiles
2. Social media security
3. Communications security
4. Data security
5. Personal security

1. BASIC CYBERNETIC SECURITY OF DEVICES AND PROFILES

a. Basic security rules

We assume that you are only using 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: Use different passwords for different accounts (different numerals, special characters etc.). There is a brief manual on how to do this on the webpage of Mozilla.
- Rule #2: Passwords 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: 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 KeePass2. 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 using 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 Internet connection or even a mobile phone signal in order to use the application; your device and the server are synced forever after you set them up. 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 fingerprint technology 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 notifications for 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. 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: A large 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:

**WINDOWS**

**Step 1:** Disconnect the computer from the network. Run an anti-malware scan (preferably run from an external USB 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 F8 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 it 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, which needs to be run manually each time you want to scan.

It may be necessary to use both types of scanner to remove 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 for both your computer and 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 provides the best support for only 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 recommend 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 the password every time you close it and re-open it. Lock your PC every time you leave it, even momentarily (press Windows button + L).
  – Buy a screen foil that allows you to look at the screen from a direct angle only and prevents strangers seeing your work 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 is 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 that 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 practically impossible due to two-factor authentication.
  – Android: if you have 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 all that are necessary, then disable 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 them but the devices will be incapable of “hearing” your conversation. As well as a camera cover, we recommend disabling the camera in your computer altogether and installing the “Oversight” app, which monitors foreign usage of your camera and microphone.

• Rule #18: It is convenient to cover the web camera on your laptop and take off the
cover only when necessary. 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 offline. The iStorage company sells cheap and well encrypted external hard-drive devices. It is recommended that you keep 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 previous events.
- Rule #20: There are a lot of disk-encrypting apps, both free and paid. VeraCrypt is 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.

i. 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 a café, contact the personnel and pick up your device as soon as possible. Such a 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 only be able to see the device’s location 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 the 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 is not tampered with. They are called Security envelopes and can be purchased at EuroSeal.cz for example.
2. 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.

- 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 friends only. 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 access your profile.
- Rule #27: Turn off personalized ads.
- Rule #28: When using Facebook on your phone, limit or disable the app’s access to your location.
- Rule #29: Photos taken on a smartphone contain a lot of sensitive data about the time and location they were taken. 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 operating 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 you to go through all 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 more sensitive measures.

• Rule #36: Your permanent address is partly public information, which is available in state databases or commercial contracts.
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 stores 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 online 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 online 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 a 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 online 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.
3. 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. Encrypted 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. The 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 a 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.
4. 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 the locked screen
  - Settings>privacy>location services>
    o >share my location – set to off
    o Go through each app and determine whether you need GPS on 'while using' or 'never'. Make sure nothing is on 'always.'
    o 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)
    o >systems services – all off except ‘Emergency SOS’ and (optional) ‘Find My iPhone.’
    o >frequent locations – ‘clear history’ and turn to ‘off’
    o Product improvement – all ‘off’
  - Settings>privacy>
    o Diagnostics & Usage – ‘don’t send’
    o 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 if it would be 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 the 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 the 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.
5. PERSONAL SECURITY

- 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 a 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 a physical incident is: run, hide, fight.
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 advisable to 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 the 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 your 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)