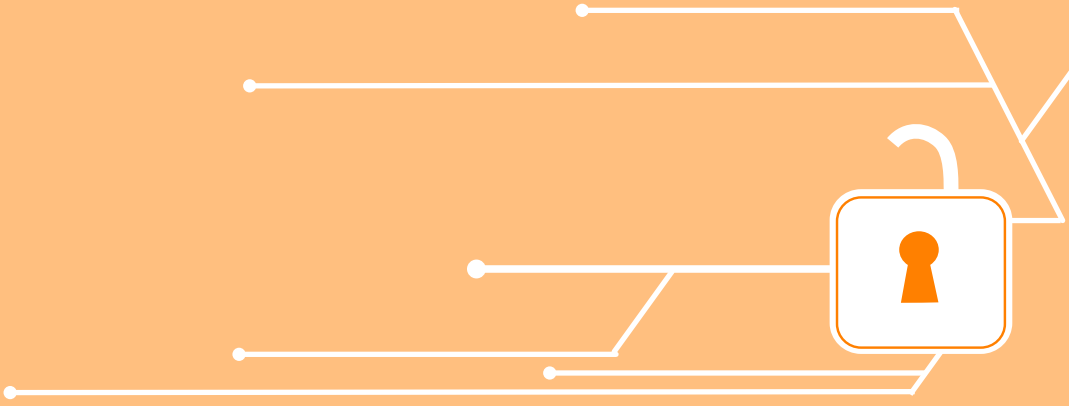
# Central American Observatory for Digital Security

- Annual Report 2016 -

# El Salvador



HlqVRomqgghOAC
j86Z/sIDhll vy5Wvr

# Central American Observatory for Digital Security

- Informe anual 2016 -

# El Salvador

# Central American Observatory for Digital Security

### -Annual Report 2016-

# El Salvador[1]

# INTRODUCTION

The Central American Observatory for Digital Security (OSD) emerged as an initiative of Fundación Acceso in 2016.

The OSD's main objective is to document and analyze digital security incidents that happen to human rights defenders working in El Salvador, Guatemala, Honduras and/or Nicaragua.

To achieve this goal, Fundación Acceso visits and follows up with people or organizations who work to defend human rights and who have reported a digital security incident, compiles a registry of reported incidents, and publishes an annual report with that compiled information.

The aim of this work is to strengthen security mechanisms for human rights defenders, to position the issue of digital security as a key component of integral security, to strengthen analysis of integral security for human rights defenders in Central America, and to support potential strategic litigation with information based on legal and technical computer analysis.

## a) What is a digital security incident?

The Central American Observatory for Digital Security will register those incidents that happen to human rights defenders in Central America and are related to their digital information and/or communications either stored, in movement or as part of various services.

For human rights defenders, we use the broad concept defined by the United Nations,[2] Declaration, including individuals, groups and institutions that are known to work in the defense of human rights in their villages and for the people of El Salvador, Guatemala, Honduras and/or Nicaragua, irrespective of gender, age, place of origin, professional background or any other characteristic.

We define incident as any adverse event (verified or suspected) related to information (including data and metadata) and/or digital communications.

1. The El Salvador chapter was compiled by in-country legal adviser Hernández Anzora with support from technicians David Oliva and Arturo Chub and Director of Organizational Development Luciana Peri.

2. United Nations, *Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms.* Available at: http://www.ohchr.org/EN/ProfessionalInterest/Pages/RightAndResponsibility.aspx

In order to be considered digital, this information and/or these communications must have been created, processed and communicated by current electronic computational devices (systems devices), and can be stored, in the process of being transmitted, part of an online service, or among any of the applications that we use to access them (including email, social media, blogs and independent online media, among others).

When an incident is identified that does not meet the criteria for the Observatory's registry, Fundación Acceso will provide the necessary technical assistance to protect the digital information that may have been compromised, and when it involves an incident of another security variable, whether physical, legal or psychosocial, the case will be referred to local and regional partner organizations that work on that specific issue.

## b) Incident typology

Registered incidents are catalogued according to the following typology:

- **Malware[3] or malicious software:** Any type of software[4] that is installed on devices to interrupt operations and collect sensitive information without the consent of the administrator (user). These also can be installed via a hidden method such as complementary programs that appear to be legitimate, legal, in good faith or without third parties or nefarious intentions. One of the most dangerous pieces of malware is known as spyware[5] which collects information stored on a device and transmits it to an external entity without the consent of the administrator. Programs installed on cellphones that eavesdrop on telephone calls or activate video and audio also are considered malware.

- **Loss of hardware:** Theft, robbery, destruction or extraction of equipment.

- **Retention of hardware:** Equipment seized, confiscated and/or retained by agents of the State, with or without a legal warrant, and with or without legitimate justification.

- **Remote attacks:** Taking remote control of equipment or remote extraction of information, obtaining access via an Internet connection or a network. Remote attacks exploit vulnerabilities of the Modem[6] or operating system.

- **LAN[7] attacks:** Blockage of data traffic that circulates on the local network, interruption of connections between the computers on a network, denial of service and generation of traffic on the network. One example is the reconfiguration of routers or modems to block specific pages.

- **Web attacks:** Any attack on Internet services that we use and the monitoring of the same. These can be blog or news services, our websites, blocking our YouTube channel or others,

3. Techterms, *Malware.* Available at: http://techterms.com/definition/malware.

4. We define software as any non-tangible component through which specific instructions or routines are carried out that allow for the use of a device.

5. Federal Trade Commission, *Staff Report. Monitoring Software on Your PC: Spyware, Adware, and Other Software*, (2005). Available at http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

6. A modem is a device provided by an Internet Service Provider. It converts digital information generated by computers into sound frequencies that are transmitted by a Telephone Network. In other words, the device through which our computers connect to the Internet.

7. The local area network (LAN) refers to a group of computers located in a determined space (such as an organization's office) that can share files between them and share Internet access.

as well as monitoring our behavior based on the sites we visit.

One of the primary techniques for this type of attack is Distributed Denial of Service (DDoS), an attack on the network that causes a service or resource to become inaccessible.

Also included in this category is censorship of specific websites by the Internet Service Provider, the monitoring of traffic, identity theft on the web, hijacking of the website, appearance of non-authorized publications on the website, changes to the Domain Name System (DNS), and inadequate updating and backup of the website.

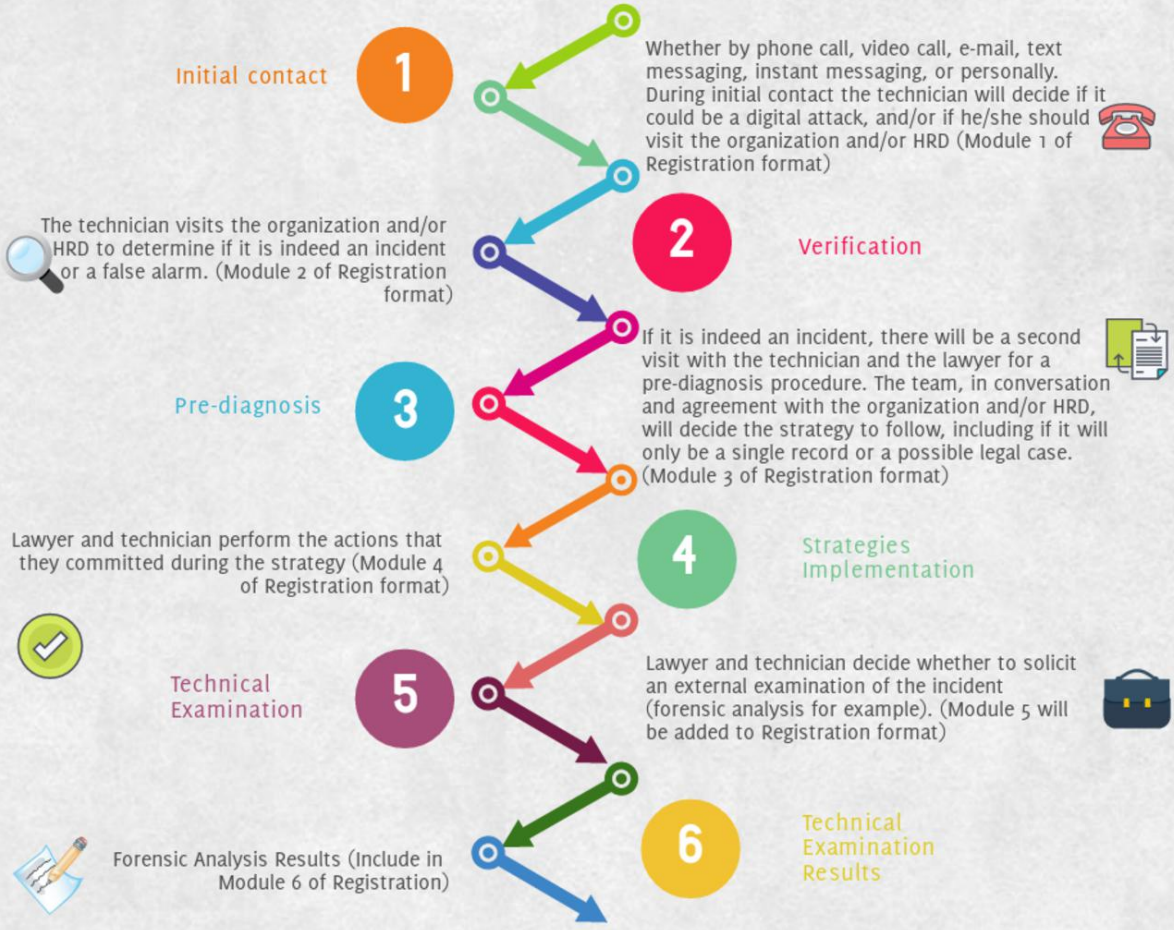
•**Compromised accounts:** This is a special category that should be included in "Web attacks," but that specifically involves hacking our credentials to access the services we use. We decided to separate this category due to the number of these types of incidents that frequently occur[8].

One of the primary techniques for this type of attack is **phishing**[9] or **identity theft**, characterized by an attempt to acquire confidential information in a fraudulent manner, particularly passwords of any email account, Internet subscriptions, social media, hosting administration and websites, bank accounts, credit cards, etc.

8. Recommendation of the Access Now team based on experience with Help Desk.
9. Ed Skoudis, *Phone phishing: The role of VoIP in phishing attacks.*

# Central American Observatory in Digital Security

## Intervention Moments:




FUNDACIÓN Acceso

## c) National context[10]

### Access to the digital world

While part of Salvadoran society is able to access first-world technology services, another important percentage of the population still lives in a situation of digital illiteracy, and access to cellphones likely is the only thing that both worlds share in terms of access to the digital world. In 2014, only 30% of Salvadorans used the Internet.[11]

Nevertheless, in 2014 an estimated 1.8 million active smartphones were in use in the country, of a total of 9 million registered mobile phones, a number that is greater than the country's total population of about 6 million people, according to statistics from the United Nations' specialized IT and communications organization, the ITU[12] and the country director at the company Telefónica[13] Despite the fact that possession of a computer and access to residential Internet service is still considerably low, smartphones have made it possible for many people in the country to access the digital world from their mobile devices.

Without a doubt, the new dynamics generated by information technologies have made rights such as access to information, freedom of expression, freedom of the press, the right to protect personal information and privacy, and others, increasingly important for public discourse in El Salvador[14].

In that sense, and given that registered testimony already has occurred in 2015 by defenders in El Salvador who faced situations that could be characterized as attacks on digital security due to their activism[15], it is particularly important for this project to delve into the nature of those actions and the entities that would be interested in affecting the digital realm of people dedicated to the defense of human rights, as well as understanding the legal-institutional and technological mechanisms that can be used by human rights defenders to protect themselves.

10. This section is based on the *El Salvador chapter in the Fundación Acceso investigation, Digital Privacy for human rights defenders? A study on how the legal structures in El Salvador, Guatemala, Honduras and Nicaragua can be used for protection, criminalization and/or digital surveillance for human rights defenders* (San José, Costa Rica: 2015). Available at: http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf

11. General Directorate for Statistics and Censuses (2013). Multipurpose home survey results for 2013 (slides). El Salvador: DIGESTYC. Recovered from: http://www.digestyc.gob.sv/index.php/servicios/descarga-de-documentos/category/47-presentaciones-estadisticas-sociales.html

12. United Nations International Telecommunication Union – UIT. (2014). *Report on statistics from individuals who use the Internet in El Salvador*. Recovered from: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

13. [El Diario de Hoy. 2014. 1.8 million smartphones circulate in the country. El Diario de Hoy, Nov. 4, Business section. http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=47861&idArt=9218924 (Date consulted: April 8, 2015).

14. Rafael Ibarra, "Internet governance," La Prensa Gráfica, http://blogs.laprensagrafica.com/litoibarra/?p=1205 (Date consulted: March 10, 2015).

15. Fundación Acceso (2015), Digital privacy for human rights defenders?

## Current situation of human rights advocates

The rise of the FMLN party in 2009 to the presidency was a point of inflection for people and organizations that work to defend human rights, given that several of its members accepted public positions and responsibilities within the FMLN government, but also because many of their important agenda points for the defense of human rights faced the dilemma of the agenda and priorities of a party that had been allied with the opposition, but that now had agendas and priorities defined by conducting the business of governing.

The actions by a second FMLN administration, which began in 2014, in the area of public security have placed in jeopardy some of the important agenda points of organizations and people who defend human rights, as those actions in many ways follow the iron-fisted approach by the administrations of the ARENA party.

In this sense, human rights defenders act in a context marked by criminal violence, but also one that is increasingly contradictory in terms of human rights and the state of law enforced by state security agencies and following a discourse of anti-terrorism toward gangs that was adopted by the government of El Salvador in recent years. In this context, the physical security of any person is fragile, but even more so when it entails those dedicated to the defense of human rights.

In this sense, many defenders with whom Fundación Acceso has maintained relations know how to identify those moments and actions that could be considered digital security attacks or vulnerabilities, identifying a basic sense about their digital security, as well as an initial conscientiousness about the need to protect aspects related to the computer and digital world, but without the capacity or the mystic to effectively defend themselves from possible digital attacks.

Nevertheless, an opening exists for them to become informed about these details and to adopt institutional/organizational practices and policies geared toward improving security in the digital environment. The primary goal now involves the formation, disposition and prioritization of resources to begin down the path toward creating and maintaining more secure digital environments.

# 1. MAIN FINDINGS IN EL SALVADOR

Following are the primary findings of the Central American Observatory for Digital Security in the case of El Salvador. These were registered between the months of June and November 2016. For this registry, a series of technical and legal tools was created to define criteria for the registry of digital incidents.

## 1.1) Procedure for the registration of incidents

In El Salvador's case, the team was composed of an in-country resident legal adviser and two resident technicians in Guatemala. This is because previously Fundación Acceso did not provide technical assistance in El Salvador (unlike Guatemala, Honduras and Nicaragua, where it did). Faced with this situation, the decision was made that assistance would be temporarily provided by technicians from Guatemala, who traveled to El Salvador three times for a total of 12 days.

During these visits, activities consisted of visiting organizations that defend human rights to be present with them and inform them of the current initiative, to introduce the working team, to offer technical assistance for digital security, to establish joint action plans, and later, to carry out agreed upon follow-up actions on the reported incidents. At the same time, this was an opportunity to begin to identify people residing in El Salvador who in the future could provide technical assistance in the country on behalf of Fundación Acceso.

Following the meetings with human rights organizations, in which a range of possible attacks or doubts about suspicious incidents related to digital security were identified, Fundación Acceso's technical-legal team provided follow-up both online and on the phone. That follow-up consisted primarily of reminding the defending organizations to send their reports of possible incidents to the IT systems managers and reminding the technical team to follow-up.

In some cases, calls or emails reporting incidents were directed to the legal adviser. In these cases the legal adviser forwarded the information to IT specialists via email and followed up via instant messenger with Signal.

In this context, the following intervention points can be highlighted:

| Incident report | Receipt of incident | Incident follow-up | | Technical resolution |
|---|---|---|---|---|
| | | Information technology investigation | Consultation and legal accompaniment | |

It is important to keep in mind that various factors prevented any of the reported cases from passing to final stages of technical investigation, making it impossible to identify possible perpetrators. Nor was the possibility discussed of presenting the cases to court proceedings or preparing litigation.

## 1.2) Registered cases

In El Salvador's case, it is important to remember that Fundación Acceso only very recently began fieldwork in the country (an important precursor was the investigation of digital privacy conducted in 2015) to strengthen trusting relationships with human rights defenders. Added to this is the fact that the technical team still doesn't have a permanent presence in the country, and the difficulty of many of the entities to have a permanent or stable IT systems engineer (only one of them has one person working full-time), the cases that were followed up on and more consistently registered were relatively few.

Four entities, primarily dedicated to defending women's rights, LGBTQ rights, youth at risk and the functioning of public security agencies, among other human rights areas, reported incidents. All of them have their headquarters and work in the Department of San Salvador, but a couple have developed projects and maintain a presence outside of this department.

In some cases, entities reported more than one type of attack, but given that consultations and technical expertise were conducted from a distance, those cases that were more manageable remotely were selected.

### a) Profile of people/organizations that reported incidents

The organizations and people who defend human rights were primarily working in areas related to public security. Three of the entities that reported incidents (two organizations and one person defending human rights) are involved in issues related to public security and work with youth at risk of violence and in conflict with the law, or because they register and/or provide some type of accompaniment to victims of human rights violations by agents linked to defense services and public state security. It's also important to mention that according to human rights defense entities, in three of the cases the reported attacks occurred in the context of visible actions to defend human rights (campaigns, reports, legal cases).

### b) Types of attacks

Following is a brief description (not technical) of registered attacks.

Attack 1

The website of one of the human rights defense organizations was breached, and users were automatically redirected to a pornographic website making it impossible to access the institution's official information.

Attack 2

The cellphone of an entity that defends human rights was corrupted and later damaged only a few hours after a person who defends human rights who uses the phone participated in protests against a public institution.

Attack 3

During a campaign initiated by an entity that defends human rights, the campaign's website was attacked and rendered inaccessible for users.

Attack 4

Only a few days after launching its recently created website, an entity that defends human rights was the object of attacks that managed to disable it.

## c) Possible perpetrators

The identification of possible perpetrators of the attacks is a task that interests the Digital Security Observatory, but we should make it clear that it's not always possible because an attacker regularly tries to remain anonymous and will use technical resources and methodologies that are convenient for the type of attack. In that sense, this task requires, for more complex cases, technical resources and access to services that are out of our reach. Nevertheless, based on the characteristics of the attacks we can create a possible cyber-profile of the attacker and their objectives.

Due to various factors, from technical limitations to limited resources or due to decisions by the entities, in none of these cases did cyber-experts reach the stage of searching for possible perpetrators.

It's important to understand that all websites hosted on the Internet are exposed to permanent attacks, and these are conducted by cyber-pirates who seek to increase their popularity on the Internet. In these cases, the websites that have little or no maintenance are usually victims of these attacks. We can observe this type of behavior in the cases described above.

# 2. PROTECTION MECHANISMS

In this section we present the legal framework that might have been violated in the cases that were registered in the chapter on El Salvador by the Central American Observatory for Digital Security. Likewise, we analyze possible strategies to move forward these cases in terms of promoting digital rights of people who defend human rights.

In El Salvador, on March 6, 2016, the Special Law Against Cybercrimes and Related Crimes (LEDI) entered into force. Based on that, we will primarily review the evaluations and recommendations for protective legal mechanisms. Before this law was adopted, anything related to cybercrimes was only sparsely existent in laws whose primary objective was not to prosecute cybercrime, such as the penal code or a consumer protection law. In this sense, LEDI strengthened and clarified issues related to cybercrimes, for which – given its peculiarity as a special law according to the Salvadoran legal structure – it should become the legislation that takes precedence in cases of legal disputes related to digital or cybersecurity.

## 2.1) Rights violations

### a) Possible fundamental/human rights violated

Given the nature of registered attacks, the primary human rights of people and organizations that defend human rights that were violated included the right to identity, privacy, image and property, according to Article 2 of LEDI and Article 2 of the Constitution of the Republic, which recognize the right to honor, personal and family privacy and one's own image (identity). The same article of the constitution also recognizes the right to property and possession.

Also, the right to freedom of expression could be interpreted as one of the possible rights violated, because taking into account the context of some of the registered attacks, the probability exists that the intent was to affect the capacity and possibility of expressing the position and proposals of the entities that defend human rights.

### b) Possible penal classifications

It's important to keep in mind that legal assessments of the criminal aspects contained in LEDI, in case of arriving at litigation, should come with the respective corroboration and IT support, as the awarding of an ideal type of crimes to a certain activity or conduct will be obstructed by the information technology assessment/interpretation that is given during the legal or pre-legal

16. Injunction Sentence 934-2007 issued by the Constitutional Chamber of the Supreme Court of Justice, San Salvador, March 4, 2011. Part III 1. B. a.

process (prosecutor). In other words, the awarding of the ideal types of criminal designations will depend, more than any other type of cases, on a highly specialized reading of the events, for which, in addition, it is complex or difficult for people who don't have training in these areas (such as prosecutors, defense counsels or judges).

Taking into account this initial limitation, one of the crimes that could be put together based on registered attacks to the websites of organizations that defend human rights is identity theft (Art. 22 LEDI). According to that, whoever impersonates or takes control of individuals or legal entities by means of Information and Communications Technologies will be sentenced to three to five years in prison.

Further, in the case of the attack on an institution's website that was redirected to a pornographic website, crimes of pornography could be lodged as outlined in the Penal Code (Arts. 172, 173, 173A and 173B), especially if it is confirmed that minors either were used in the making of the pornography or that minors were exposed to pornographic material.

## c) Possible civil infractions

Article 2 of the Constitution establishes that all persons have the right to moral integrity, and compensation is recognized for damages to moral character. In that sense, in addition to criminal litigation, the possibility remains open for civil damages if harm is proven to image (identity), privacy or property. LEDI also contemplates this possibility, although it doesn't specifically mention civil offenses, but rather legislation:

> The penalties outlined in the present Law will be applicable without prejudice to other penal, civil or administrative responsibilities incurred. For the determining of civil liability the applicable norms will apply (Art. 35).

However, because it dates to 1859, the Salvadoran Civil Code does not take into account many of the circumstances that could arise in the area of digital security, in addition to not contemplating many of the issues that the Constitution or secondary laws in force do contemplate regarding respect for the right to privacy, freedom of expression or one's image (identity).

Due to this, significant efforts are required for legal interpretation and integration by judges and prosecutors. For example, Article 2082 of the Civil Code, which states, "offensive accusations against a person's honor or reputation do not give the right to demand a pecuniary indemnification unless emerging damage or lost profit is proven, which can be visible via money," could be

17. Resolution 128-UAIP-FGR-2015 on Information Acces request presented by the investigator on July 24, 2015.

18. Fundación Acceso, 2015. *Digital Privacy for human rights defenders? A study on how the legal structures in El Salvador, Guatemala, Honduras and Nicaragua can be used for protection, criminalization and/or digital surveillance for human rights defenders.* San José, Costa Rica.

interpreted as if offensive accusations against one's honor or reputation are equivalent to the right to privacy, honor and one's image, contemplated by the Constitution of the Republic and LEDI.

## 2.2) Response strategies

### a) Legal

•In criminal matters

Criminal complaints are an important legal option following approval of LEDI in March 2016. In El Salvador's case, the monopoly of Penal Action falls on the Attorney General's Office of the Republic (FGR), where complaints should be lodged before the State body. However, despite the legal faculties conferred upon it by the law and the Constitution, the FGR's technical capabilities both in legality and in computing systems very probably are not yet compatible with the constant changes and technological advances of the digital and information systems world.

In addition, it should be taken into consideration that according to Fundación Acceso's investigation on privacy and surveillance of human rights defenders (2015), people who work to defend human rights said they do not have great trust in the FGR, and on the contrary, consider it a public entity that generates little trust and great resentment.

•In constitutional matters

The lawsuit for a constitutionality injunction has been empowered as a stopgap of Habeas Data according to Salvadoran constitutional jurisprudence, which established that while no ad hoc secondary legislation exists, it could be used to protect personal information[16]. Nevertheless, of the cases registered by the Observatory, a direct affectation to the information of human rights advocates can't be clearly distinguished. However, this could be a possibility if the technical expertise could demonstrate evidence of possible interference in personal information of some human rights organizations.

In the case of the Salvadoran legal framework, the unconstitutionality injunction lawsuit is filed at the Constitutional Chamber of the Supreme Court of Justice, the highest court for constitutional matters. Sadly, constitutional injunctions require a high level of legal training and are not accessible to just anyone.

•Administrative routes and others

Office for the Defense of Human Rights (PPDH)

Despite the fact that none of the registered incidents reached the stage of identifying possible perpetrators, it is important to outline some legal strategies that generally could be useful in hypothetical incidents involving digital security. In the case of the incident where a telephone's operating system was damaged after its user participated in a protest against a public agency, in addition to the complaint filed at the FGR based on LEDI, it would be important to file a complaint at the Office for the Defense of Human Rights (PDDH), as this agency has the legal ability to solicit reports about the Telecommunications Wiretapping Center, overseen by the FGR, in case of a possible misuse of abilities to intervene in the telecommunications of people presumed to be part of organized crime. Because it involves a possible incident that implies damage to the software of a mobile phone, the possibility should be covered that it doesn't involve an unwarranted or illegal intervention, for which it is important to utilize the PDDH.

Institute for Access to Public Information (IAIP)

Likewise, according to Article 31 of the Special Law for Telecommunications Eavesdropping (LEIT), the functioning and security of the Telecommunications Wiretapping Center, as well as the selection and permanent monitoring of the director, employees, staff and members of the National Civil Police (PNC) who work there, will be governed by regulations that shall be created by the Attorney General. However, these regulations are not public, as according to criteria of the Prosecutor's Office Access to Public Information Unit (UAIP), these regulations are classified as Protected Information[17]. However, both internal regulations and international principles establish that laws, regulations, decrees and other orders of a general nature shall only apply by virtue of their promulgation and publication.[18]

For this reason and generally speaking, it is initially suggested that a strategy be formulated for administrative channels, by means of filing a new request for access to information at the Attorney General's Office of the Republic (FGR), so that in case it is denied, it can be appealed at the Institute for Access to Public Information (IAIP). Subsequently, in case the administrative route was unsuccessful, the judicial route could be pursued by filing a constitutionality injunction lawsuit at the Constitutional Chamber.

## b) Non-legal

•Other response strategies of a political nature could include measures of persuasion, influence or pressure for the FGR to make public unofficial information regarding the Telecommunications Wiretapping Center. In other words, that which can, should be revealed, such as the number of interventions conducted in a year, those that continue, and those that have ended, the types of crimes for which these interceptions are occurring, among other information that is relevant and that does not affect the respective investigative penal process.

•Equally, influential actions are suggested, but also technical training so that the PDDH can undertake functions of oversight over the Center for Interventions that the Special Law for Telecommunications Eavesdropping (LEIT) authorizes it to do, as currently that institution is not complying with its function of verifying the respect for legality and human rights in telecommunications interception procedures. This is particularly true because it is a procedure that having not been efficiently controlled could become a grave and massive situation of surveillance and harassment of human rights defenders and political opponents, according to the interests or criteria of the acting attorney general.

# CONCLUSIONS AND RECOMMENDATIONS

## Conclusions

From technical-digital work it can be asserted that attacks on websites did take place, based on the results that were noted in the descriptions. In the cellphone case, due to the fact that we did not have access to the device, it can't be stated that it was the object of an attack. In any case, the only thing we can state is that it was a suspected attack, because it took place in the context of strong activism on the part of the device's user.

In respect to the identification of the objectives and identity of the perpetrators of the attacks, the Digital Security Observatory ideally should provide verifiable information to support any claim. In none of the four cases do we have conclusive proof that allows us to determine the objectives and the attackers, but that doesn't mean that the attacks didn't occur. We verified in one of the cases the existence of serious vulnerabilities in the Hosting service and in programs used to manage the site, which were exploited by the attackers. We were unable to identify the attackers, but the evidence points toward external intervention by persons not authorized to alter the analyzed websites. In other words, the attack can't be denied.

Although in one of the cases one of the sites was used to promote pornographic content, we do not have the elements that allow us to irrefutably claim that the purpose of the attack was precisely the facilitation of said content, and in the same manner, we also cannot affirm that the objective of the attack was to delegitimize or discredit the organization, but we also cannot rule that out.

After reviewing the websites of the organizations that reported incidents, in addition to other organizations' sites with whom we have worked, it is clear that the websites lack basic security standards, which permits sites to be cleaned, placing organizations and their digital content in a very delicate situation.

## Recommendations

Among the lessons learned for the case of El Salvador is the necessity that organizations and human rights defenders have for constant access to technical assistance, and that the person who fills this role be trained and up to date regarding digital security standards. With the exception of one of the entities, the rest do not have a stable technician or sufficient training in digital security. This is an important aspect for strengthening organizations and people who defend human rights in El Salvador, of which Fundación Acceso could make an even greater difference.

Until now, the level of sensitivity to digital security at the level of decision makers in organizations

that defend human rights is very good, improving significantly compared to 2015, when Fundación Acceso conducted an investigation of digital privacy and surveillance. An opening exists, along with interest and in some cases, some already have begun to implement initial decisions regarding digital security. It is important to point out that the only entity with which we worked that has a more stable IT specialist is the one that managed to take greater advantage of the training and capability of the Access team, but also with whom we could go the furthest in the process of the Observatory's registry.

For the case of El Salvador, it is vitally important to look for and train IT specialists connected to human rights, and if possible, create a network with them so that the entities and people who defend human rights can obtain better digital security.

Among the lessons learned we also can mention the need to have simple formats that are sufficiently understandable for people who are not information technology experts, so that they can make initial reports of what they consider to be potential attacks on their digital security. Also, generating bulletins or other types of information that illustrate and exemplify in a relatively simple manner some digital incidents, so that advocates can have better clarity when they potentially are facing one of these.

Likewise, in order for the Observatory's registry of incidents to be more effective it is highly recommended that a technician from Fundación Acceso be solely available for the registration of incidents in El Salvador, and if possible, based in the country or with the ability to frequently travel there. This is due to the fact that not being physically available makes it more difficult to register certain cases in which it is necessary to intervene or physically protect some devices. This is, for example, the case for a cellphone or computer, which can't wait weeks or months without being touched until a technician arrives to check it after the incident occurs.

# BIBLIOGRAPHY


## National Legislation

•CC. Civil Code. 1859. El Salvador: Legislative Assembly.

•CN. See Constitution of the Republic of El Salvador. 1983. El Salvador: Legislative Assembly.

•CP. See Penal Code. 1997. El Salvador: Legislative Assembly.

•CPP. See Penal Process Code. 2009. El Salvador: Legislative Assembly.

•LAIP. See Access to Public Information Law. 2012. El Salvador: Legislative Assembly.

•LEIT. See Special Law for Telecommunications Eavesdropping. 2010. El Salvador: Legislative Assembly.

LEDI. See Special Law against Cybercrimes and Related Crimes. 2016. El Salvador: Legislative Assembly.

## Jurisprudence

•Injunction Sentence 934-2007 of the Constitutional Chamber of the Supreme Court of Justice, San Salvador, March 4, 2011. Part III, 1 A.

•Injunction Sentence 934-2007 of the Constitutional Chamber of the Supreme Court of Justice, San Salvador, March 4, 2011. Part III 1. B. a.

## Other documents

•Fundación Acceso, 2015. Digital privacy for human rights advocates? A study on how legal structures in El Salvador, Guatemala, Honduras and Nicaragua can be used for protection, criminalization and/or digital surveillance for human rights advocates. San José, Costa Rica.

•General Office of Statistics and Censuses (2013). Multipurpose home survey results 2013 (slides). El Salvador: DIGESTYC. Taken from http://www.digestyc.gob.sv/index.php/servicios/descarga-de-documentos/category/47-presentaciones-estadisticas-sociales.html

•El Diario de Hoy (2014). There are 1.8 million smartphones in the country. El Diario de Hoy, Nov. 4, Business section.

•http://www.elsalvador.com/mwedh/nota/nota_completa.aspidCat=47861&idArt=9218924 Date consulted: April 8, 2015.

•United Nations International Telecommunication Union – ITU. (2014). Report on statistics of individuals who use the Internet in El Salvador. Taken from: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

•United Nations International Telecommunication Union – ITU. (2014). Report on statistics of individuals who use the Internet in El Salvador. Taken from: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

•Rafael Ibarra (2015), “Internet Governance” La Prensa Gráfica, http://blogs.laprensagrafica.com/litoibarra/?p=1205 (Date consulted: March 10).

HlqVRomqggh

j86Z/sIDhll vy5

j86Z/sIDhll vy5Wvrrsk

FUNDACIÓN Acceso