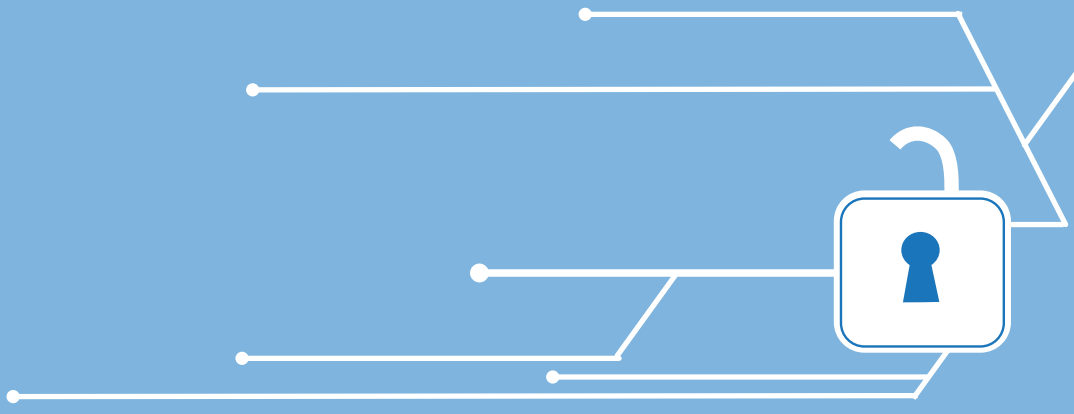
Central American Observatory for Digital Security

- Annual Report 2016 -

Honduras



Central American Observatory for Digital Security

- Annual Report 2016 -

Honduras

Central American Observatory for Digital Security

Annual Report 2016

Honduras[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.

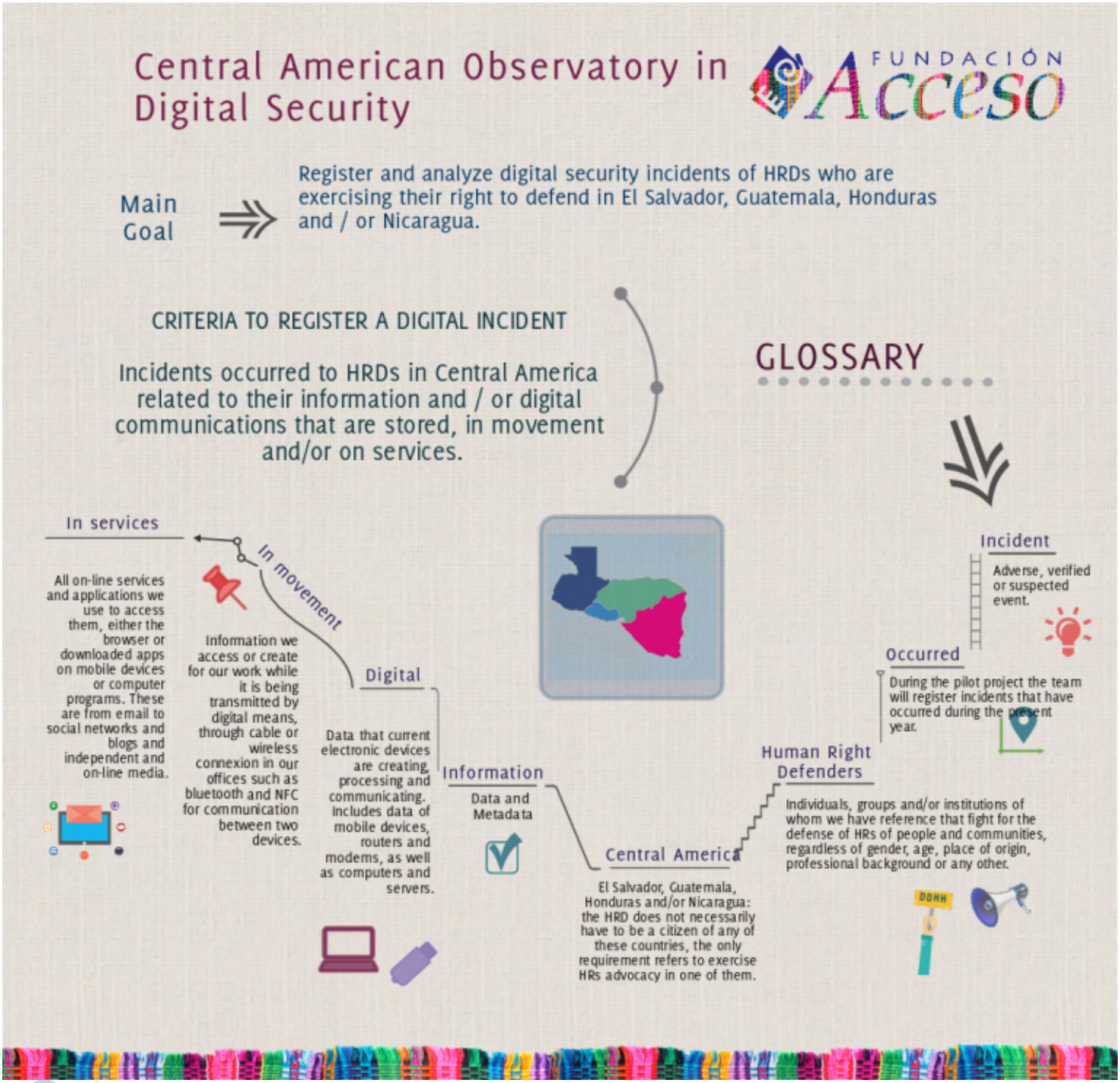
For human rights defenders, we use the broad concept defined by the United Nations[2] Declaration, including individuals, groups and institutions that are known to work in the defense of human rights in their villages and for the people of El Salvador, Guatemala, Honduras and/or Nicaragua, irrespective 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 Honduras chapter was compiled by in-country legal adviser Kenia Oliva with the support of technicians Mario Ávalos and Alejandro Durón 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.

c) National context

Fundación Acceso published an investigation in 2015 titled, "Digital privacy for human rights defenders?"[10] that discussed the applicable legal frameworks for the right to privacy in the region. This investigation corroborated that in January 2011 in Honduras, the Private Communications Surveillance Law went into effect, eliminating Penal Procedural Code rules governing communications surveillance. This new law aims to "establish the legal framework of procedural regulations for communications monitoring" and constitutes "an essential tool in the fight against traditional crime, and above all, against organized and non-conventional crime." That means the law now applies to investigations of any crime[11].

For example, in February 2013, the judicial branch ordered surveillance of the private communications of an Ombudswoman for Women's Rights over a complaint against her of supposed defamation on social media network Facebook[12]. That means the law that was conceived to aid investigations of organized crime and drug trafficking opened the door to surveillance and investigation of any type of crime, including private-action crimes.

It is important to point out that prior to approval of this Communications Surveillance Law, the Law Against Terrorism Financing also was approved. These two pieces of legislation have placed human rights defenders on high alert, and defenders have noted that since the 2009 coup d'état their communications could be intercepted with the goal of targeting and criminalizing their work.

The Comité por la Libertad de Expresión ("Committee for Freedom of Expression," or C-Libre) published an analysis of the Communications Surveillance Law that determined that it could open the door to violations of the constitutional guarantee to the right of privacy, an individual right that protects citizens from unwarranted government intrusion. This right is recognized both nationally and internationally. Article 100 of the Constitution of the Republic states that, "All individuals have the right to inviolability and secrecy in communications, especially regarding telegraphic and telephone communications, except when under judicial order." Considering this last order, we can say that the existence of a special law restricting this right is not unconstitutional, but that restriction should be proportional to the degree that the legal right that is said to be protected has been affected, as clearly a conflict of protected legal rights exists: On one side is privacy, and on the other any type that could harm by the illegal activity of one person or group of people against others.

10. Fundación Acceso, 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. Fundación Acceso, Digital Privacy for human rights defenders? 316-317.

12. Lesbia Pacheco Case, Tegucigalpa Sentencing Tribunal in Honduras, File 68-2013.

The petition to approve this type of law should be subject to the establishment of adequate control mechanisms, as it will result in a powerful weapon to violate this right guaranteed by the constitution and other international treaties, such as those outlined in Art. 11, point 2 of the Pact of San José, Costa Rica, 17.1 of the International Covenant on Civil and Political Rights, 12 of the Universal Declaration of Human Rights, and 5 of the American Declaration of the Rights and Duties of Man.[13]

In the last months of 2016, human rights organizations denounced the hacking of their websites, blaming state officials for the crimes. The complaints were directed to the appropriate authorities for investigation, but the Public Prosecutor's Office in resolution 347-2016, dated Nov. 16, 2016, responded with a request for information about the complaints filed for intervention of digital communications. The Public Prosecutor's Office, on the date of that resolution, stated that the Special Prosecutor's Office for Protection of Intellectual Property and Cybersecurity had no complaint registered in 2015-2016. This should give us pause to reflect.

Attack on human rights advocates

In Honduras during 2015-2016, at least two human rights organizations denounced public attacks on their websites[14] and at least four people who defend human rights denounced attacks on their social media networks and email.

The attacks denounced by organizations like the Asociación para una Ciudadanía Participativa ("Association for Participative Citizenship," or ACI Participa), refer to the hacking of the institution's account. This organization denounced that it was attacked "on Sept. 22, 2015, using, among others, the technique of Fishing to obtain the information contained on said account. In their cybercrime, the criminal(s) managed to obtain and later delete all of the organization's contacts as well as all of its archives, carpets and emails sent and received, enormously jeopardizing the communication of both national and international bodies and institutions such as the beneficiaries of our work to defend."[15].

The registered attacks correspond to the possible crime of identity theft and intervention of private communications. As of this writing, in Honduras, people who are dedicated to the defense of human rights constantly denounce on social media or in news media these types of attacks.

13. http://conexihon.hn/site/opiniones/palabra-libre/an%C3%A1lisis-sobre-la-ley-especial-de-intervenci%C3%B3n-de-las-comunicaciones

14. C-Libre, "ACI Participa victim of cyberattack," Alerta 162-15, Sept. 24, 2015. Available at: http://www.clibrehonduras.com/alerta/aci-participa-sufre-ciberataque and Criterio, "COFADEH denounces hacking of its website and construction of false-positives," Dec. 16, 2016. Available at: http://criterio.hn/2016/12/16/cofadeh-denuncia-hackeo-pagina-construccion-falsos-positivos/

15. C-Libre, "ACI Participa victim of cyberattack," Alerta 162-15.

1. MAIN FINDINGS IN HONDURAS

Next we present the primary findings of the Central American Observatory for Digital Security for the case of Honduras. These have been registered between the months of June and November, 2016. In order to create the registry, a series of technical and legal tools were designed to define the criteria for the registration of digital incidents.

1.1) Procedure for the registration of incidents

The moment Fundación Acceso learns of a possible digital security incident, in addition to providing the necessary technical assistance to protect the information of a person or organization, incident registration begins.

First, informed consent is obtained to ensure that the affected person is informed of the intervention that will be conducted on his or her equipment. Later, authorization is obtained from the person to conduct a technical inspection (depending on the type of incident, this could take hours or even weeks).

During the duration of the inspection, the lead technician should fill out a log that registers all actions carried out on the equipment in order to demonstrate that the intervention included only actions directed at determining the origin of the problem with the equipment. Finally, the finalization of the inspection is registered and the equipment is returned, along with the inspection's conclusions and possible follow-up actions.

1.2) Registered cases

The start of the Observatory was marked by a stage of defining processes both in the technical realm and the legal realm. In a first phase, Fundación Acceso, together with a technical team in Honduras, visited several human rights organizations in the country, and later, a meeting was held to report advances with the organizations visited in the first stage, and new organizations were invited along with Cooperation Agencies in the country.

It was not possible for the Observatory to register all cases, in light of the fact that those who publicly denounced incidents do not believe that upon identifying the person or persons who carried out the attacks on their social media or emails will be punished by law enforcement, which helps to understand why the Special Prosecutor's Office for the Protection of Intellectual Property and Cybersecurity reported that they have no record of any case regarding hacks to email and social media accounts.[16]

16. Resolution DGF-347-2016, Nov. 15, 2016.

In 2016, the Observatory registered three cases in Honduras. Two other cases were not registered due to the inability to conduct visits with the complainants. However, some were approached to inform them of the possibility of registering their cases.

The cases effectively registered are related to people who work as human rights defenders. One of them was assassinated in March 2016; another is a defender who is known to have publicly denounced corruption among the National Police, naming high-ranking officials as suspects; the third organization works to defend the land and food security of rural residents.

a) Profile of people/organizations that reported incidents

Human Rights Defender: This is the first case that came to our attention and that initially met the criteria to be registered by the Observatory. It involved the daughter of Bertha Cáceres, a prominent human rights defender assassinated in March 2016 in retaliation for her work defending indigenous territories and the environment. After her murder, her daughters denounced and publicly named those who possibly were responsible.

Human Rights Defender: The second case involved a Police Commissioner, who for several years repeatedly denounced acts of corruption and abuse within the institution, and who was fired for speaking out. This person also has been harassed and threatened in various manners.

Organization that Defends Land: This organization works for the defense and promotion of the rights of rural residents who are fighting to reclaim land access rights. Honduras faces grave complaints for human rights violations related to land access. In this context, Vía Campesina is an organization that constantly has accompanied victims and denounced and identified those possibly responsible for violations.

b) Types of attacks

Bertha Zúñiga Cáceres contacted Fundación Acceso because the personal email of her mother was being used after she was assassinated. The request was made for technical assistance to help determine more information about the nature of the unauthorized use of this Gmail account.

María Luisa Borjas: A human rights defender who filed a complaint with the Comité por la Libertad de Expresión (C-Libre) regarding the hacking of her Twitter account, the changing of her profile photograph and the issuing of a threat at the same time.

Her Twitter account was manipulated, placing as a profile photo the image of a bloodied woman with her mouth gagged and with a threatening message on her profile. This occurred directly after she gave statements to news media about those possibly involved in the death of a police official.

Fundación Acceso visited her, took her statement to understand the context in which the events occurred, and she signed the informed consent form regarding the use of her name and information by Fundación Acceso.

The technician communicated with an allied organization in Costa Rica that also works in digital security, and this organization reported that due to the passage of time and Twitter's security policy it was difficult to determine where the attack originated.

Vía Campesina Honduras: They reported a site denial on their institutional website starting in March, for which technical tests were conducted, along with a visit in which we were informed that the organization had cancelled the website's hosting and no longer used it. Nevertheless, they also reported a possible hack of their Facebook page.

A technical analysis was conducted where it was verified that there was bad use of the page, with many channels open, which allowed other people to publish from their page.

In addition, their router did not have a password, which means that any person could access their Internet network.

2. PROTECTION MECHANISMS

In this section we present the legal frameworks that could have been violated in the cases registered in the Honduras chapter by the Central American Observatory for Digital Security. Equally, we analyze the possible strategies these cases suggest in further promoting the digital rights of human rights defenders.

2.1) Rights violations

Next we present an analysis of the legal framework in relation to each of the violations that could have occurred after analyzing the cases described in the previous section.

a) Possible fundamental/human rights violated

The case of the two defenders could include the crime of violation to the right to privacy outlined in Article 76 of the Constitution of the Republic, which guarantees the right to personal and family privacy, and one's own image (identity).

The crime committed in the case of the use of Berta Cáceres' email after her assassination could be considered, in addition to the crime of violating personal privacy, as a crime of identity theft.

b) Possible penal classifications

In Honduras legislation does not exist to duly regulate the issue of digital privacy. Currently, the only sanctions for identity theft or intervention of communications are contemplated as crimes of fraud or financial fraud, but there is no law that regulates and sanctions the illegal intervention of communications, among them the intervention of digital communications.

2.2) Response strategies

In this section we present the different response strategies that can be implemented to address the cases that have been registered by the Observatory, as well as prevent future incidents from affecting the digital security of human rights defenders.

a) Legal

These are some of the legal mechanisms that could be implemented to respond to incidents registered by the Observatory:

- Constitutional actions (Habeas Data, Constitutionality Injunction, Habeas Corpus, etc.)

  In Honduras, a lawsuit seeking an injunction could be filed according to the Law of Constitutional Justice, which establishes the procedure for these injunctions and seeks to

protect the rights guaranteed by the Constitution. Because the privacy of communications is a constitutional right, a lawsuit seeking an injunction could be attempted to protect this right. Also, a habeas data action could be carried out, as the Constitution establishes the right to safeguard personal information.

This recourse could only be used if it is determined that the intervention of communications was ordered by an authority, and it was done in a manner that violated due process.

•Complaints

In the cases registered in Honduras, they should be denounced to the National Mechanism for Protection of Human Rights Defenders, as this Mechanism has the responsibility to investigate these acts and protect the integrity of defenders, as well as prevent, in some form, that they be blocked from doing their jobs as defenders.

•Inter-American Human Rights System

Regarding the Inter-American Human Rights System, these and other cases should be documented to identify patterns of behavior on the part of actors who could be conducting surveillance on human rights defenders. This information should be passed on to respective court reporters so that they can be included in periodical reports in order to raise awareness about the digital security situation on a regional level.

•Others that are considered relevant (National System for the Protection of Human Rights Defenders, Journalists, Social Communicators and Justice Officials)

One of the Observatory's strategies in Honduras should be to ensure that the National Mechanism for the Protection of Human Rights Defenders assumes the legal responsibility for carrying out all actions aimed at providing security to human rights defenders, promoting public policy that allows the open defense of human rights and to investigate cases of any type of attack against human rights defenders.

Currently the National Mechanism for Protection, both in its law and its regulations, only contemplates physical protection measures, partial psychological measures and legal measures, but it does not contemplate the protection of its beneficiaries' digital security.

The implementation of some of the protection measures contemplated by the National Mechanism could place at risk the digital security of its beneficiaries, as one security measure includes panic buttons, a device installed on the mobile phones of the mechanism's beneficiaries that is controlled by private security companies hired by the Honduran government.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

1.In Honduras, the work of defending human rights is carried out in an adverse context for defenders, and legal gaps exist in the framework of digital security protection in the work that these defenders carry out which were identified in 2015 Fundación Acceso investigation.

2. Digital security incidents exist, and these directly affect the work of human rights defenders, placing their information, their work and even their lives in danger.

3.The issue of digital security continues to be absent in reports that discuss the security of human rights defenders, prompting areas of vulnerability through which they could be attacked.

Recommendations

1. A reform of the legal framework is needed to improve protection provided to human rights defenders, protecting above all their digital security.

2. Human rights defenders should create internal protocols to strengthen their digital security in order to comprehensively strengthen their security in general.

3.A specific section should be included on digital security in reports on the situation of human rights defenders in order to create more awareness about its importance to the concept of comprehensive security.

BIBLIOGRAPHY

•C-Libre. “ACI Participa victim of cyberattack.” Alert 162-15.Sept. 24, 2015. Available at: http://www.clibrehonduras.com/alerta/aci-participa-sufre-ciberataque

•Criterio. “COFADEH denounces hacking of its website and construction of false positives.” December 16, 2016. Available at: http://criterio.hn/2016/12/16/cofadeh-denuncia-hackeo-pagina-construccion-falsos-positivos/

•Fundación Acceso. “General Framework for the functioning of the Observatory for Digital Security.” San José, C.R., 2016.

•Fundación Acceso. “Digital privacy for human rights defenders? A study of how the legal framework in El Salvador, Guatemala, Honduras and Nicaragua can be used for the digital protection, criminalization and/or surveillance of human rights defenders.” San José, C.R., 2015.

•Court of Sentencing in Tegucigalpa, Honduras. “Lesbia Pacheco Case.” Case 68-2013.

HlqVRomqggh
j86Z/sIDhll vy5

j86Z/sIDhll vy5Wvrrsk

FUNDACIÓN Acceso