Central American Observatory for Digital Security

-Annual Report 2018-

FUNDACIÓN Acceso

índice

A. Introduction

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

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

To achieve this goal, Fundación Acceso conducts initial and follow-up visits with people and organizations working to defend human rights that have reported a digital security incident. The foundation also maintains a registry of reported incidents and publishes an annual report with the information.

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

During the Observatory's period of registration and analysis (during 2018), we registered and documented 22 cases from Honduras (2), Nicaragua (14), and Guatemala (6).

A.I. Human rights and the Internet

It's important to emphasize that the right to privacy is protected by international law, including Article 12 of the Universal Declaration of Human Rights,[1] Article 17 of the International Covenant on Civil and Political Rights[2] and Article 11 of the American Convention on Human Rights.[3] These articles outline the right to be protected from arbitrary or illegal interference in private life as well as to obtain relevant legal protection at a national level.

In addition to being important for the strengthening of a democratic society, the right to privacy is vital for other fundamental rights, including open access to information, freedom of expression and freedom of association and protest. In the context of defending human rights, it becomes even more necessary to protect these rights. As such, it requires an intersectional analysis of international and national legal frameworks, which transcends the digital realm.

In the last decade, and particularly following revelations by Edward Snowden, it has become clear due to these and other leaks that governments around the world, including several in Latin America, have acquired the means and the software to conduct mass surveillance of communications. These surveillance tools primarily target members of the political opposition, human rights defenders and various activists with the goal of intimidating and censoring their causes based on the nature of information in their possession.

Clearly, the use of surveillance mechanisms infringes on international standards of human rights affirmed by different treaties and laws, primarily the rule of law, due process, necessity and proportionality, among others. Governments use several unregulated digital surveillance tools as part of new social repression strategies.

---

1 United Nations. **Universal Declaration of Human Rights.** Available at: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

2 United Nations. **International Covenant on Civil and Political Rights.** Available at: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

3 Organization of American States. **American Convention on Human Rights.** Available at: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

These principles form part of the International Principles on the Application of Human Rights to Communications Surveillance,[4] developed by civil society organizations such as the Electronic Frontier Foundation, Article 19, Privacy International and others.

These broadly developed principles also serve as a best practice guide for governments that have decided to update their legal framework related to communications surveillance to guarantee the protection of human rights. These 13 principles comprise an analysis based on international standards (Inter-American[5] and universal) and of the appropriate manner in which they should be applied to communications surveillance. They serve as a guide for governments to develop a regulatory framework and a means for regulating mass surveillance activities. They also provide civil society with oversight capacity when faced with possible arbitrariness. In this context, the Inter-American Court of Human Rights has determined that one of the direct results of monitoring human rights defenders' communications without appropriate legal oversight is that it causes fear and hinders the right of free association.[6] This is harmful for the activity of defending human rights in the region.

Despite most constitutions in Central American countries recognizing, to some extent, that privacy is an inherent right, the region's lawmakers easily forget these constitutional provisions when introducing and passing new legislation. The Electronic Frontier Foundation created a series of recommendations[7] for Latin American governments, including Central America. The recommendations detail the laws governing mass communications surveillance that should be abolished or reformed, and to what extent. Specifically, they outline how laws addressing the Internet should not include vague definitions that could subsequently allow unreasonable violations of fundamental rights.

Michel Forst, United Nations Special Rapporteur on the situation of human rights defenders, has expressed deep concern in his reports about the mechanisms governments use to restrict freedom of expression and other fundamental rights involving the Internet. Forst believes that the Internet is one of the most relevant platforms to facilitate information and to demand transparency. Nevertheless, governments have conducted multiple activities to censor the voices of human rights defenders, from limiting Internet access to removing content to deploying spyware.

One of the main concerns is the effect these mechanisms have had on human rights defenders, who use technologies like the Internet and social media to promote the respect of fundamental rights. Governments have accused human rights defenders of defamation, and they have waged smear and harassment campaigns to suppress the expression of opinions.

David Kaye, U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, also has warned in his annual reports that governments recently have shown a tendency toward controlling, limiting or monitoring freedom of expression on the Internet. They have interfered

4 Electronic Frontier Foundation (2014). **Necessary and Proportionate: International Principles for the Application of Human Rights to Communications Surveillance (Necesarios y Proporcionados: Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones).** Available at: https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf

5 Electronic Frontier Foundation and Digital Rights (Derechos Digitales, 2016). **International Principles for the Application of Human Rights to Communications Surveillance (Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones) and the Inter-American System of Human Rights Protection.** Available at: https://necessaryandproportionate.org/files/2016/08/23/iachr-sp-agosto2016.pdf

6 Inter-American Commission on Human Rights (2016). **Report on the Criminalization of Human Rights Defenders (Informe Criminalización de defensoras y defensores de derechos humanos).** Available at: https://www.oas.org/es/cidh/informes/pdfs/criminalizacion2016.pdf

7 Electronic Frontier Foundation (2016). **Comparative Analysis of Surveillance Laws and Practices in Latin America (Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica).** Available at: https://necessaryandproportionate.org/files/2016/10/07/comparative_report_october2016_es_0.pdf

with connections and intercepted private communications, generally with the assistance of actors from the private telecommunications sector, such as Internet service providers. Other tactics have included content filtering, censorship, prioritization of content or applications, and infringement of net neutrality, an invariant of the Internet.

Edison Lanza, the Inter-American Commission on Human Rights' Special Rapporteur for Freedom of Expression, has described the Internet as a tool that people can use to search for, to receive and to distribute information, facilitating the right to freedom of expression in their communities. However, he has denounced several examples of violence and intimidation directed at journalists and human rights defenders. Examples include mass surveillance tactics, state-sponsored censorship and cyberattacks. He reiterated "the need for States to protect journalists and to prevent and investigate attacks on people who provide information through the Internet."[8] Lanza emphasized that protection of freedom of expression on the Internet should be extended to code, protocols, hardware and telecommunications infrastructure.

In its 2017 annual report,[9] Amnesty International expressed deep concern about the disproportionate means that governments use to harass and intimidate people dedicated to protecting human rights, and the role that new technology plays. Several governments are known to have acquired various types of software – such as malware and spyware – to spy on human rights defenders. They also have carried out smear campaigns and promoted fictitious news reports on social media against activists and human rights defenders.

In its 2016 annual report,[10] Front Line Defenders expressed concern about the questionable practices that governments use to silence and persecute human rights defenders. These include using digital tools to restrict access to the Internet and applications, blocking content, hiring users (via fake social media profiles) to spread rumors, false information and slander, and acquiring software and other mass surveillance tools to target activists and human rights defenders.

A.2. ¿What is a digital security incident?

Activities carried out by the Central American Observatory for Digital Security include registering incidents that affect human rights defenders in Central America. These incidents are related to digital information and/or communications that are stored, in transit or part of certain services

Accordingly, based on the principles set forth by the United Nations, human rights defenders are defined as individuals, groups and institutions known to work in the defense of human rights in their villages and for the people. In the context of this project, this includes those working in Guatemala, Honduras, El Salvador and Nicaragua, irrespective of gender, age, place of origin, professional background or any other type of characteristic.[11] Additionally, within the framework of the Inter-American System of Human Rights, the Inter-American Commission on Human Rights (IACHR) recognizes the existence of the right of defenders to protect human rights.[12]

---

8 Inter-American Commission on Human Rights (2017). **Report on Silenced Zones: Regions of High Risk for Freedom of Expression (Informe Zonas Silenciadas: regiones de alta peligrosidad para ejercer la libertad de expresión).** Available at: https://www.oas.org/es/cidh/expresion/docs/publicaciones/ZONAS_SILENCIADAS_ESP.pdf P. 122.

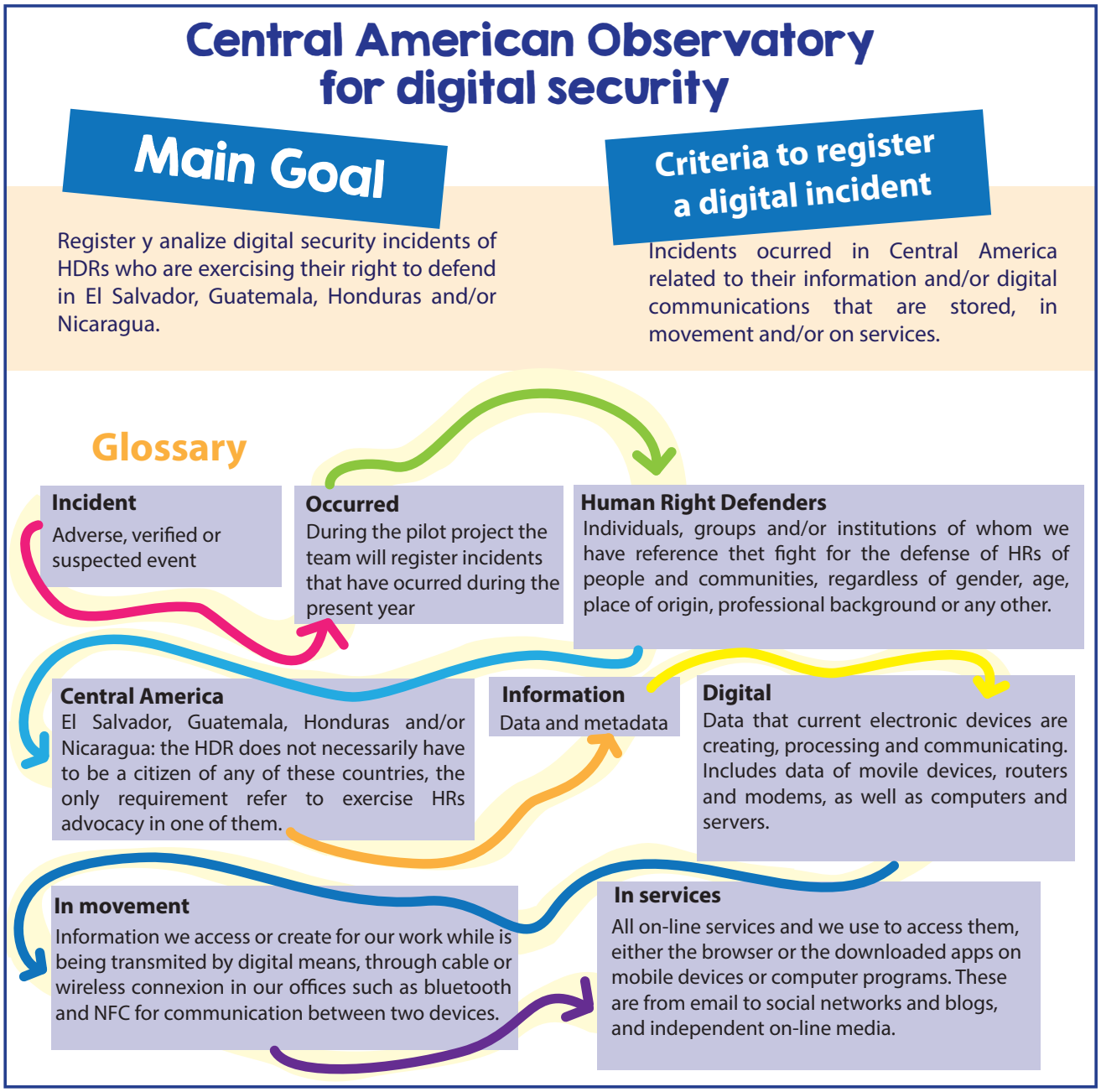
9 Amnesty International (2017). **Annual Report 2016/2017: The State of the World's Human Rights (La situación de derechos humanos en el Mundo).** Available at: https://www.amnesty.org/es/documents/pol10/4800/2017/es/

10 Front Line Defenders (2016). **Annual Report: Human Rights Defenders at Risk in 2016.** Available at: https://www.frontlinedefenders.org/en/resource-publication/2016-annual-report

11 United Nations. **Resolution 53/144 March 8, 1999.** Available at: http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf

12 Inter-American Commission on Human Rights. **Report on the Situation of Human Rights Defenders in the Americas (Informe sobre la situación de las defensoras y defensores de los derechos humanos en las Américas).** Available at: https://www.cidh.oas.org/countryrep/Defensores/defensoresindice.htm

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



In order to be considered digital, this information and/or communication must be created, processed and communicated by current electronic computational devices (systems devices) and can be stored, transmitted or part of an online service or any of the applications used to access it (including email, social media, blogs and independent online media).

If an incident is identified that does not meet the Observatory's criteria for registration, Fundación Acceso will provide the necessary technical assistance if information may have been compromised or if an incident involves a different security variable – whether physical, legal or psychosocial – so that the case may be referred to partner organizations or other entities, either national or regional, that specialize in the specific field.

A.3. Classification of incidents

Incidents are registered based on the following categories:

- **LAN attacks:**[13] Blockage of data traffic circulating on a local network, interruption of connections between network computers, or denial of network service and traffic generation. One example is the reconfiguration of routers or modems to block specific pages.
- **Remote attacks:** Taking control of equipment or extracting information remotely by obtaining access via an Internet connection or a network. Remote attacks exploit vulnerabilities of the modem[14] or operating system.
- **Web attacks:** Any attack on, or monitoring of, the Internet services we use. These could be blogs, news services, online radio, websites, YouTube channels or others. It also includes the monitoring of 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 the Internet Service Provider's (ISP) censorship of specific websites, traffic monitoring, identity theft on the web, website hijacking, the appearance of non-authorized publications on a website, changes to the Domain Name System (DNS), and the inadequate updating and backup of a website.
- **Compromised accounts:** This is a special category that should be included in "Web attacks" but specifically involves hacking our credentials to access the services we use. We decided to separate this category due to the frequent number of these types of incidents.[15] One of the primary techniques for this type of attack is phishing,[16] or identity theft, which involves an attempt to acquire confidential information in a fraudulent manner, particularly passwords of any email account, Internet subscriptions, social media accounts, hosting administration and websites, bank accounts, credit cards, etc.
- **Malware[17] or malicious software:** Any type of software[18] that is installed on devices to interrupt operations and collect sensitive information without the consent of the user/administrator. These can be installed simultaneously, and covertly, as complementary extras of programs that appear to be legitimate, legal, in good faith or without third parties or hidden intentions.

  One of the most dangerous pieces of malware is known as **spyware**,[19] which collects information stored on a device and transmits it to an external entity without the consent of the user/administrator. Programs installed on cellphones that eavesdrop on calls or activate video and audio also are considered malware.

---

13 LAN refers to local area network, a group of computers located in a determined space (such as the offices of an organization) that share files among them as well as the Internet.

14 A modem is a device provided by the Internet service provider. It converts digital information generated by computers into sound frequencies transmitted through telephone networks. In other words, it is the device through which computers connect to the Internet.

15 Recommendation of the Access Now team based on experience with Help Desk. https://www.accessnow.org/linea-de-ayuda-en-seguridad-digital/

16 Ed Skoudis. Phone phishing: The role of VoIP in phishing attacks.

17 *Definition of malware taken from techterms.com: http://techterms.com/definition/malware*

18 Software is defined as any intangible component through which set instructions or routines are executed to allow a device to be used.

19 FTC Report (2005). Available at: http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf

- **Loss of hardware:** Theft, robbery, destruction or extraction of equipment. One example is the destruction of equipment during an illegal raid.
- **Seized hardware:** Equipment seized, confiscated and/or retained by agents of the State, with or without a legal warrant and with or without legitimate justification.

Central American Observatory for Digital Security

Intervention Moments

Whether by phone call, video call, email, text messaging, instant messaging, or personally. During initian contact the technician will decide if it could be a digital attack, and/or if he/she should visit the organization and/or HDR (Module 1 of registration format).

The technician visits the organization and/or HDR to determine if it is indeed an incident or a false alarm (Module 2 of registration format).

If it is indeed an incident, there will be a second visit with the technician an the lawyer for a pre-diagnosis procedure. The team, in conversation and agreement with the organization and/or HDR, will decide the strategy to follow, including if it will only be a single record or a possible legal case (Module 3 of registration format).

Lawyer and technician perform the actions that they commited during the strategy (Module 4 of registration format).

Lawyer and technician decide whether to solicit and external examination of the incident (forensic analysis for example) (Module 5 will be added to registration format)

Forensic analysis results (Include in Module 6 of registration)

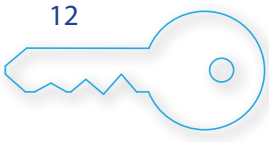
A.4. Procedure for incident registration

Once the Fundación Acceso team becomes aware of a possible digital security incident, it registers the incident and provides technical assistance to protect the person's or organization's information.

The process starts when the team obtains informed consent to ensure the affected person understands the actions that will be taken regarding their equipment. Then, authorization is obtained to conduct a technical inspection (depending on the type of incident, this could take hours or even weeks).

During the duration of the analysis, the digital defender should keep a log in which all actions conducted with the equipment are registered to show that during the intervention only actions aimed at determining the origin of the problem were performed on the equipment. Finally, the end of the inspection is registered, and the equipment is returned, along with the conclusions of the analysis and possible follow-up actions.

The cases the Observatory registered this year are the result of the knowledge and relations the Fundación Acceso team has with diverse organizations and people working in human rights defense in each country.



B. GUATEMALA CHAPTER

B.I. Legal Context: Internet and Human Rights in Guatemala

In 2015, Fundación Acceso conducted a research titled, "Digital privacy for defenders of human rights?"[20] This investigation discussed the applicable legal framework for the right to privacy in Central America. It established applicable parameters at a national level that continue mostly unchanged today.

In general, the findings established that constitutional recognition of the right to privacy exists at a general level,[21] but current criminal legislation does not protect the right to digital privacy.

Since 2009, Bill 4090, known as the Law to Protect Personal Information,[22] has generally been viewed favorably. The bill has been awaiting, since 2010, a third and final debate before the full Congress prior to its passage. The existence of a legal framework to govern the protection of personal information would also favor the adequate protection of human rights defenders' online privacy, as they would have mechanisms to exercise their rights against government or private companies.

Throughout 2017, numerous bills were presented to Congress that, in one form or another, could jeopardize the exercising of various human rights on the Internet, especially for the country's human rights defenders. Among which are cited:

Bill 5239, which seeks passage of the Law Against Terrorist Acts,[23] already has received approval of the Committee on Governance and awaits being called to the floor of the full Congress. In general, this bill seeks to criminalize citizen protests.[24] It seeks prison terms of 10 to 20 years for the crime of "cybernetic terrorism or cyberterrorism." Additionally, it calls for the establishment of an intelligence network to monitor the movements of suspected terrorists. But it fails to outline minimum standards to regulate this control, which could result in potential mass surveillance.

Bill 5254, which seeks passage of the Law against cyber-crime,[25] already has received a favorable opinion and awaits approval by the congressional Committee on Governance. However, the content of this bill lacks a focus on human rights and seeks to criminalize conduct that at some point could affect user activities and the work of human rights defenders, or those who denounce human rights violations.

From the perspective of government and the creation of public policy on the issue of the Internet and information and communications technologies, some efforts have been undertaken throughout the year that should be mentioned due to their potential impact – whether positive or negative – on defenders in Guatemala.

---

20 Fundación Acceso (2015). **Digital privacy for defenders of human rights? (¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos).** Available at: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

21 *Ibid. Page* 175.

22 Congress of the Republic of Guatemala. **Bill 4090, Law to Protect Personal Information.** Available at: http://old.congreso.gob.gt/uploadimg/archivos/dictamenes/988.pdf

23 Congress of the Republic of Guatemala. **Bill 5239, Law Against Terrorist Acts.** Available at: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=3607

24 Prensa Libre. **A dangerous bill (Una peligrosa propuesta de ley).** Available at: http://www.prensalibre.com/opinion/opinion/una-peligrosa-propuesta-de-ley

25 Congress of the Republic of Guatemala. **Bill 5254, Law Against cyber-crime.** Available at: http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf

The Superintendence of Telecommunications (SIT) has developed a digital agenda called "Nación Digital" ("Digital Nation"), with the help of other government entities.[26] Its main strategies include the use of information and communications technologies in health, education, security, development and transparency. However, the agenda lacks specific objectives. To date, the sectors or entities that are supposed to execute these strategies haven't been defined, and the agenda's focus doesn't include protecting human rights on the Internet.

Since 2018, with support from the Organization of American States (OAS), the Interior Ministry – via the Vice Ministry of Information and Communications Technologies – has been promoting the creation of a National Cybersecurity Strategy.[27] In general terms, this strategy seeks to generate and coordinate a medium- and long-term road map to design and implement specific actions to protect the national security from cyber-crime. Various sectors, including government agencies, the judicial sector, the private sector, academia, the technical community and civil society, have been asked to help create the strategy. Nevertheless, the current draft lacks a focus on human rights. Additionally, the protection of online privacy and personal information isn't a priority.

This latter point is important to highlight. The creation of public policies related to the Internet and new technologies requires national recognition of minimum standards of fundamental digital protections. The lack of participation by organizations dedicated to defending human rights is detrimental to the process and creating the strategy should involve key sectors. Additionally, it's troubling that the public policies it embraces were only created with a focus of "national security," which could disrupt the activities of human rights defenders. This is primarily due to the tradition the government has of classifying these organizations as destabilizing or terrorist groups. It's also dangerous if the strategy is approved in its current form because it would serve as the basis of future development and implementation of public policies related to cybersecurity.

During 2018, there hasn't been made any major advancements in terms of discussing the Internet and human rights. On one hand, the international organization The World Wide Web Foundation conducted a collaborative and decentralized process to promote dialogue about human rights online among the different civil society sectors. That process was called the Charter of Internet Rights in Guatemala.[28]

The Alliance for Affordable Internet (A4AI) is promoting the Guatemalan Coalition for Affordable Internet[29] to create dialogue between the public and private sectors and civil society. The goal is to develop and implement public and regulatory policies so that access to the Internet is affordable in the country.

Additionally, on October 25, 2018, the second Guatemalan Internet Governance Forum[30] was held, where issues related to protecting the user's digital privacy and freedom of speech in the electoral context were discussed, although the discussions were very basic and didn't include the protection of human rights defenders.

These types of events increasingly demonstrate the need to foster dialogue about protecting human rights online. They also show that citizens demand these rights to be recognized and respected. Citizens

26 Nación Digital. https://www.naciondigital.gob.gt/

27 Interior Ministry. **Conclusions to improve the draft of the National Cybersecurity Strategy** (**Presentan conclusiones para mejorar Borrador de la Estrategia Nacional de Ciberseguridad).** Available at: http://mingob.gob.gt/presentan-conclusiones-para-mejorar-el-borrador-de-la-estrategia-nacional-de-ciberseguridad/

28 World Wide Web Foundation. **Charter of Internet Rights in Guatemala** (**Carta de Derechos de Internet en Guatemala).** Available at: http://1e8q3q16vyc81g8l3h3md6q5f5e.wpengine.netdna-cdn.com/wp-content/uploads/2017/06/Carta-de-Derechos-de-Internet-para-Guatemala.pdf

29 Alliance for Affordable Internet. (**Coalición Guatemalteca para una Internet Asequible).** Available at: http://a4ai.org/guatemala/

30 Internet Governance Forum in Guatemala (Foro de Gobernanza de Internet de Guatemala). http://igf.gt/

also demand that human rights defenders be included in these types of discussions. This creates a unique situation of vulnerability, because without the appropriate laws, it's likely that these types of attacks, along with the perpetrators whether they are companies or government agents, will remain in impunity.

B.2. Attacks against human rights defenders

In its recent biannual report[31] (*January to June 2017*), the Human Rights Defenders Protection Unit of Guatemala (UDEFEGUA) stated that in only six months, 236 acts of aggression were reported that targeted human rights defenders in Guatemala. Most of these cases involved assassinations, intimidation, defamation, criminal complaints, arbitrary and illegal detentions and threats. Of these, 72 attacks targeted people who defend the human right to a healthy environment (land, territory and natural resources), and 45% targeted women human rights defenders.

This situation also was denounced in Amnesty International's annual report,[32] which noted that human rights defenders continue to be targeted by threats, stigmatization, intimidation, aggression, and in some cases, homicide. The most vulnerable groups to these types of attacks are organizations that defend land, territory and the environment.

In his reports, Michel Forst, United Nations Special Rapporteur on the situation of human rights defenders, has expressed concern "over the lack of independent and diligent investigations of the aggression committed against environmental human rights defenders, as they are usually linked to a lack of resources, corruption and collusion among perpetrators. States rarely have been able to bring perpetrators to justice and ensure that they are appropriately punished."[33]

The role social media platforms have played for human rights defenders, members of the news media and independent investigators is important to highlight. Social media is a means to circulate opinions and announce activities, particularly in the context of increasing protests against government corruption. They also play a role in defending territory, enhancing the right to prior consultation, protecting the environment and accessing justice when other human rights are violated.

In the past year, Twitter has been fundamental for people and civil society to mobilize citizens to demand that high-ranking public officials – including the current President of the Republic – resign, among other things. In response, an increase in profiles considered bots or net centers[34] has spread disinformation (from spreading false news to defamation against activists and independent media). This is primarily to weaken the investigative work conducted by the International Commission Against Impunity in Guatemala (CICIG),[35] the Public Prosecutor's Office (MP)[36] and several national human rights organizations (particularly women human rights defenders).

---

31 Amnesty International (2017). **Annual Report 2016/2017: The State of the World's Human Rights (Informe annual 2016/2017: La situación de derechos humanos en el Mundo).** Available at: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ P. 217.

32 Amnesty International (2017). **Annual Report 2016/2017: The State of the World's Human Rights.** Available at: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ P. 217.

33 United Nations Special Rapporteur on the situation of human rights defenders. **Report on the situation of human rights defenders, 2016 (Informe sobre la Situación de los defensores de los derechos humanos 2016).** Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/247/12/PDF/N1624712.pdf?OpenElement

34 Soy502. **Net Centers of Impunity (Los netcenteros de la impunidad).** Available at: http://www.soy502.com/articulo/netcenteros-impunidad-20878

35 International Commission Against Impunity in Guatemala (Comisión Internacional contra la Impunidad en Guatemala). http://cicig.org/

36 Nómada. **#JimmySeQueda: el netcenter de @rodrigopolo, @rmendezruiz y @pirulismo.** Available at: https://nomada.gt/asi-se-fabrico-el-jimmysequeda-el-netcenter-de-rodrigopolo-rmendezruiz-y-pirulismo/

In 2017, a group of 12 news organizations requested that the Public Prosecutor's Office investigate attacks against them on social media networks, primarily by net center accounts. The organizations said they were targeted by "hacks, net center attacks and direct threats, especially against women."[37] Clearly, several governments, either directly or indirectly, are using bots against activists and independent media to defame or destabilize them. One of the biggest difficulties is identifying if public funding exists for these types of activities. On the other hand, unfortunately, the Public Prosecutor's Office lacks the technical capability to determine which profiles are "false or bots," which could lead to an even greater risk.

In 2017, an interesting article was published titled, "Net Centers: Luis Assardo's Business of Manipulation" ("Los Netcenters: negocio de manipulación de Luis Assardo"), which detailed how they have operated in Guatemala and what effect they have had.[38]

In the context of investigations into various cyber-crimes, the Ministry of Defense has publicly expressed the intention of tasking the Guatemala military with conducting investigations of cyber threats to protect the country's economy and its institutions.[39] The danger of having the military conduct investigations of cyber threats is considerable for the public, as a great possibility exists that the military will focus on spying and collecting information from citizens, activists and defenders of human rights.

During august 2018, the Nuestro Diario newspaper released a series of investigative articles on government surveillance in Guatemala[40], proving the capacity they have and the different surveillance strategies used against different social and political actors, including the use of spyware.

B.3. Main findings in Guatemala

Following are the main findings by the Central American Observatory for Digital Security for Guatemala. These findings have been registered between March and September 2018. For registration, a series of technical and legal tools were created to define the criteria used in documenting digital incidents.

B.4. Registered cases

During this period mentioned before, a total of **six** cases and incidents were registered, with different components and motives, all of them taking place in Guatemala City.

B.5. Profile of the people/organizations that reported incidents

The first case involves an independent media journalist from Guatemala. The second case relates to an artist and defender who contacts the Observatory through a national human rights organization.

The third and fourth case involves two defenders who are in a process of access to justice for a trial for crimes against humanity. The fifth case relates to a defender who does research for advocacy in

37 Soy502. **Journalists demand Public Prosecutor's Office Investigate 'Net Centers' (Periodistas exigen que el MP investigue a los "net centers").** Available at: http://www.soy502.com/articulo/periodistas-exigen-investigacion-ataques-cibernet-icos-149

38 Medium.com. **Net Centers: The Business of Manipulation (Los Netcenters: Negocio de Manipulación)**. https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulacion-2140cf7262fc

39 Soy502. **The military wants to handle cyber threats (El Ejército quiere encargarse de las amenazas cibernéticas).** Available at: http://www.soy502.com/articulo/ejercito-quiere-encargarse-amenazas-ciberneticas-63338?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter#link_time=1511180394

40 Nomada.gt https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/?utm_source=clipboard_share

Guatemala. The sixth case involves an organization that provides accompaniment to victims of crimes against humanity.

B.6. Types of attacks

Following is a brief description of the registered attacks.

In the first case, journalist, several incidents were registered and analyzed at the Observatory. Among them: a. phishing attacks targeting her iCloud account, b. a family member's picture upload to her Instagram account, c. Text messages indicating she was connected to another IP in a different region in Guatemala (from her Gmail account), d. Call history in her phone shows outgoing calls made to numbers she has never contacted before, as well as incoming calls she doesn't recognize, e. password change in her Gmail account. During the analysis process it was identified that the IP in which the phishing site was allocated was associated to various sites dedicated to performing phishing attacks. After analyzing the IP's linked to the messages, it was determined that indeed, the IP's are regularly used in phishing attacks targeted to Apple devices. The company is based in Panama, and so far, we know that the defender's phone number and details of her operative system are compromised. It is determined that this is an incident of "account compromise" and it is classified as a positive incident.

In the case of the defender/artist, this person was invited to join a group of recognized artists on Facebook. When she accessed the link, it redirected the person to a phishing site. The person then wrote fake information on the site, and when she clicked the "access" button, her cell phone turned off and wouldn't turn back on. Later, the person took her phone for repairing, but at the analysis time, her phone hasn't been given back. An analysis was to her social media accounts and emails looking for proof of intrusion, but there wasn't any. There was not any evidence of unauthorized logins into the person's accounts. It is determined that this is an incident of "account compromise" and is classified as false positive.

One of the defenders in the process of access to justice for a trial for crimes against humanity, contacted the Observatory through a digital defender from a national human rights organization. This defender's case consists of an email received stating someone had requested a password change to her Facebook account. However, she indicates she didn't request it and updates her account's password. The incident was chronologically analyzed, but the email was deleted by the defender, which restricted the digital defender from making more investigations about the incident. It is determined that this is an incident of "Web attack" and is classified as false positive.

Another one of the defenders in the process of access to justice for a trial for crimes against humanity, contacts the Observatory. The defender received a Facebook Messenger message with a video with her name and a description. A picture of her appeared in the video thumbnail. Later, she clicks on the video and it redirects her to a phishing site. The defender wrote down her credentials and then realized she's was making a mistake and updated the information she was giving. The links were copied at the Observatory to run a detailed analysis: the thumbnail of the video is actually an image allocated in a Blogger blog, which indicates that someone took the time to design an image with the defender's information to make her enter the fake link. The time and work required to do this confirms that the digital incident was a targeted attack. It is determined that this is an incident of "account compromise" and is classified as a positive incident.

With the fifth case, the Guatemalan defender who does research for advocacy, contacted the Observatory directly with the purpose of getting the digital defender to analyze her phone and computer in search of malware. Due to the article from the journalist Luis Angel Sas about the different programs the

Guatemalan government uses for surveillance, and since the defender herself has a very high profile, a visit was made to the defender to analyze and register her case. An inspection was made to her phone and computer's network traffic, with the purpose of checking if there was any data breach in it. All her networks were analyzed, and it was established that all the IP addresses the devices were connected to were legitimate, therefore they don't represent any danger. It is determined that this is an incident of "Malware "and is classified as false positive.

Regarding the sixth and last case registered in Guatemala, the organization that provides accompaniment to victims of crimes against humanity contacted the Observatory's digital defender directly. The director and team members received an email from their own institutional domain, containing an extortion message. The message states someone had *hacked* their server and asked for money in return, and if not they would publish intimate information about the people working at the organization. The director was asked by the digital defender to send the header of the email in order to determine whether it came from their server or not, to see if their accounts were indeed compromised or not. By checking the headers, the digital defender was able to determine that the emails were actually sent from their internal network, which confirmed that their accounts were in fact compromised. There is going to be further investigation, and the organization is going to be asked to let the digital defender check all the logs, which will help determine the nature of the attack.

B.7. Possible perpetrators

Identifying the possible perpetrators of the attacks is a task that interests the Observatory for Digital Security, but it should be noted that it is not always possible. Attackers often remain anonymous by using technical and methodological resources that assist this type of attack.

For more complex cases, this type of investigation requires technical resources and access to services that are out of the organization's capabilities. Nevertheless, based on the evidence recovered from the attacks a possible technical profile of the attacker and their objectives can be established.

In the first case the incidents occurred after various "hacking" attacks towards defenders in late 2017, and after the theft of the defender's phone in January 2018. The multiple account compromising incidents indicate a constant attack pattern towards the defender. Additionally, through this case we were able to identify an IP used with Phishing purposes and tracked it to a specific region in Guatemala (Mazatenango). Also, we were able to confirm that the IP addresses linked to the text messages are addresses dedicated to performing hacking and phishing attacks to Apple devices from Panama.

With the second and third case, due to them being classified as false positives because of the lack of data needed for an analysis, the possible perpetrators or their mechanisms couldn't be identified.

With the fourth case we couldn't identify the attacker's origin. What we did determine, is that it was directly targeted towards the defender, and that the perpetrator had time and technological resources to set up the video's image. Due to the active participation of the defender in the "crimes against humanity" case, we can infer that this attack was paid by, or made by the persons (or relatives of them) who are on trial for these crimes.

Regarding the fifth case, it is declared as false positive, therefore there are no possible perpetrators. However, it is important to note that the defenders are more aware of the possibilities of digital attacks and are using observation as a preventive step in the matter of digital incidents. The fact that a case is classified as a false positive should not be understood as a failure, but instead should be interpreted as an alert that was answered on time, in which the intentionality of external subjects is discarded.

Finally, with the sixth case, the perpetrator can't be identified until the log's analysis is complete.

B.8. Protection Mechanisms

In this section, we present the legal framework that may have been violated in cases registered by the Central American Observatory for Digital Security in Guatemala. We also analyze possible strategies that could be developed to protect the digital rights of human rights defenders.

B.9. Possible human rights violated

The right to digital privacy is contemplated in the Constitution of the Republic of Guatemala. Here is its legal base:

> Article 24: **"Inviolability of Correspondence, Documents, and Publications".** The correspondence of any person, his [or her] documents, and books are inviolable. They may only be inspected or seized, by virtue of a firm resolution dictated by a competent judge and with the legal formalities. The secrecy of correspondence and telephone, radio, and cablegram communications and of other products of the modern technology is guaranteed.
>
> Article 31: **"Access to Archives and State Registries".** All persons have the right to take cognizance of what the archives, records, or any other form of State registries contain about them, and [regarding] the purpose for which such data is used, as well as their correction, rectification, and updating. Registries and records of political affiliation, except for those pertaining to the electoral authorities and to the political parties are prohibited.

In other words, the inviolability of correspondence, documents and publications in any format that attempts against personal privacy, is prohibited, unless there is a firm resolution dictated by a competent judge and with the legal formalities.

B.10. Possible penal classification

A 2015 investigation of the country's legal framework by Fundación Acceso[41], updated in 2018, noted that the penal framework is still insufficient to establish integral safeguards to protect the right of digital privacy for human rights defenders. Despite this, the last modifications of the Decree N# 17-73[42], Chapter VII of the Guatemalan Criminal Code, extends those actions relative to crimes against Copyright, Industrial Property, and Informatic crimes, to the commission of damages or losses to legal entities and natural people.

Through a third person or software that damages one's digital integrity, following articles may be applied:

- **Destruction of computer records**. Article 274 "A" states: "Any individual who were to destroy, delete, or in any way alter computer records, will be imposed with imprisonment going from six months to four years, and a fine going from two hundred to two thousand quetzals.
- **Software alteration**. Article 274 "B" states: "Any individual who were to delete, alter, or destroy computer programs or software, will receive the same punishment stated in the previous article.
- **Computer software reproduction**. Article 274 "C" states: "Any individual who were to reproduce or copy computer software in any manner, will be imposed with imprisonment going from six months to four years, and a fine going from five hundred to twenty-five hundred quetzals.

41 Fundación Acceso (2015). Digital privacy for defenders of human rights? (¿Privacidad Digital para Defensores y Defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensores y defensoras). http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf

42 http://www.oas.org/es/sla/ddi/docs/G6%20Codigo%20Penal%20de%20Guatemala.pdf

- **Prohibited records.** Article 274 "D" states: "Imprisonment going from six months to four years, and a fine going from two hundred to two thousand quetzals, will be imposed to any individual(s) who were to create a data bank or a digital record using information and data that may affect a person's privacy.
- **Manipulation of information**. Article 274 "E" states: "Imprisonment going from one to five years and a fine going from five hundred to three thousand quetzals will be imposed to any individual who were to use computer registries and software to hide, alter, or distort any kind of information required for a commercial activity, the fulfillment of an obligation with the State, or to conceal, falsify or alter financial statements or patrimonial situation of a natural person or legal entity.
- **Use of information**. Article 274 "F" states: "Imprisonment going from six months to two years and a fine of two hundred thousand quetzals will be imposed to any individual(s) who were to use another individual's digital registries, or, by any means, access another individuals bank account information, or to its digital files.

However, regarding personal data, the current legislation in criminal matters does not regulate the crimes of identity theft or impersonation in social networks or other digital media.

B.II. Legal response strategies

The people or organizations affected will have to plan strategic litigations through substantiated cases. These cases can be presented to jurisdictional organizations, or to the Public prosecutor's office. Strategical litigation has been being used in the region for many years to promote human rights advocacy in the region, being a tool that can be used by the victims, civil organizations, and certain State branches (like the public prosecutor).

These are some of the legal tools that could be used in some of the incidents registered by the Observatory:

1. Denouncements/Complaints to the Public Prosecutor's Office

With cases registered in Guatemala, it is constitutionally required to file complaints and denouncements with the Public Prosecutor. This office promotes the prosecution of the aforementioned cyber-crimes and will direct the investigation of crimes committed against persons or organizations defending human rights.

Under its chain of custody and presenting physical and digital evidence, it will be able to resolve the digital incidents of extortion and threats, identified as means to interrupt the work of organizations and individuals in the defense of human rights.

2. Other actions/ Legal protection appeal

Guatemalan Constitution establishes the legal protection with cases regarding privacy and personal intimacy violations. This appeal is presented to the Supreme Court, with a strategic process that demands a specialized lawyer's representation. **Its legal base is down below:**

> *Article 24:* ***"Inviolability of Correspondence, Documents, and Publications".*** *The correspondence of any person, his [or her] documents, and books are inviolable. They may only be inspected or seized, by virtue of a firm resolution dictated by a competent judge and with the legal formalities. The secrecy of correspondence and telephone, radio, and cablegram communications and of other products of the modern technology is guaranteed.*

Article 31: ***"Access to Archives and State Registries".*** *All persons have the right to take cognizance of what the archives, records, or any other form of State registries contain about them, and [regarding] the purpose for which such data is used, as well as their correction, rectification, and updating. Registries and records of political affiliation, except for those pertaining to the electoral authorities and to the political parties are prohibited.*

3. Habeas Data resources

Habeas data resources are presented by victims or their defenders in case their personal information is subtracted from a state-owned database. Decree number 57-2008, contained in the Access to Public Information Law, Chapter six, articles 30 to 34, details the habeas data resource. This legislation restricts personal data commercialization without the proper approval of the individual. To use this resource, the victim or defender must prove that the person in charge of managing the data has shared or commercialized sensitive information. If this is proven, the person will be sanctioned with 5 to 8 years, according to Art.66, which specifies responsibilities and sanctions related to the handling of information.

4. Complaints to the Human Right's Procurator Office

This is the main human rights defense office in Guatemala, in which denounces regarding fundamental human rights are made, and at the same time, it defends and pleads for the fulfillment of these rights. This office is in charge of investigating and denouncing behaviors that can be harmful or injurious against individuals or organizations.

However, this office has a moral nature and is designed to function as a Court of Conscience, although it has the legal capacity to present complaints and denouncements to other legal and/or judiciary institutions.

5. Inter-American System of Human Rights

The Inter-American System of Human Rights has certain requirements that must be met before cases can be brought before its regional bodies. Nevertheless, in extremely serious and urgent situations, protective measures can be requested from the Inter-American Commission on Human Rights so that the State takes steps to prevent irreparable damage to the people or the object of a petition or a pending case.

Additionally, it is a good forum to document these and other cases to identify patterns of behavior by organizations and governmental agencies that might be using surveillance against human rights defenders. This information can be shared with the respective rapporteurs so that it can be included in periodical reports to shed light on the region's digital security situation.

B.I2. Conclusions and Recommendations

Conclusions

1. An adverse climate persists for the defense of human rights defenders, along with legal gaps in the protective framework for digital security for their work, which were identified in the 2015 research by Fundación Acceso, and its update in 2018. Various bills have been proposed and are being debated in the Congress of the Republic that lack a human rights perspective. If they are approved in their current form, they could jeopardize the work of organizations dedicated to the defense, protection and promotion of human rights. Current Cyber Security strategies must focus on analyzing not only the incidents, but also focus on the motives and reasons of these attacks. The current approach could be affecting human rights defenders' work directly. By not

establishing citizen oversight mechanisms, this puts their personal information, work, and even their lives exposed to intrusive surveillance programs.

2. The issue of digital security continues to be absent in many national and international reports about the security of human rights defenders, causing areas of vulnerability through which they can be attacked.
3. A Personal data Law, including clear Habeas Data procedures and restricts undue use of personal information present in social media or Internet must be approved as soon as possible.

Recommendations

1. Reform of the legal framework is needed to improve the safeguards and levels of protection for human rights defenders, with an emphasis on the need for digital security tools, including international standards for the Internet and human rights.
2. Institutions in charge of Human Rights Defense and Justice must develop different approaches to raise awareness of digital rights and their application. Currently, court rooms and justice institutions lack strategic litigation techniques regarding cyber-crime and new technologies, making it a poorly developed area in Guatemalan legislation.
3. The collectives and organizations dedicated to the defense of human rights should generate internal mechanisms and protocols focused on digital security, which can be achieved by developing skills on this issue within their own collectives.
4. In the reports on the situation of human rights defenders it's important to include sections dedicated to digital security, to highlight its importance for integral security and protection.
5. A national round table focused on analysis of the Internet and human rights called by human rights organizations with the participation of academic and technical communities is an important strategy to pursue. Global trends on Internet regulations that usurp the right to privacy are rapidly promulgating throughout the congresses of our Central American nations.

C. HONDURAS CHAPTER

C.I. Legal Context: Internet and Human Rights in Honduras

In 2015, Fundación Acceso conducted an investigation titled, "Digital privacy for defenders of human rights?"[43] This investigation discussed the applicable legal framework pertaining to the right to privacy in Central America. It established applicable parameters at a national level that continue mostly unchanged today.

In general, the investigation established that constitutional recognition of the right to privacy exists at a general level,[44] but current penal legislation does not protect the right to digital privacy.

Moreover, in February 2017, the Honduran Congress passed the Law for the Strengthening and Effectiveness of Security Policy, Decree No. 6-2017, which includes a collection of various legislative reforms, such as to the Criminal Code and the Procedural Code; the Law Against Terrorism Financing; the National Intelligence Law; the Law Limiting Telecommunications Services in National Correctional Facilities, Prison Farms and Internment Centers for Children; the Special Law for Private Communications Surveillance; the Incentives Law; and the National Penitentiary System Law. The law was approved in the context of fighting crime, with a series of provisions and modifications in criminal matters. However, several local and international organizations[45] oppose the law because it lacks a focus on human rights.

Reforms were enacted to the Criminal Code that modified the crimes of extortion and terrorism, and to the Law of Correctional Facilities. This was one of the most criticized reforms, and one of the more troubling, as it addresses the crime of terrorism. The regulation is overly broad, and many fear it could be used as a "gag law" that violates freedom of expression by potentially labeling public protests as terrorism.[46] Reforms to the Criminal Code broaden the definition of "terrorist" conduct to include those who damage property; or those who have not directly participated in damaging property, but who participate in an act to intimidate or cause terror to the government or to the public.

Additionally, the approved text ascribes advocacy and incitement of terrorist acts to those who publicly, or via media, incite others to commit the crime of terrorism. Both reforms should be analyzed from the perspective of social mobilization against acts of corruption, as those who convene public demonstrations or participate in them could be targeted for criminal prosecution under this type of crime. This violates the human rights of expression, association and demonstration that are enshrined in Honduras' Constitution, including for human rights defenders, who play an important role in defending territory and democracy. It is alarming that the criminalization of public protests and the work of human rights defenders would be contained in legislation that limits fundamental liberties and rights.

---

43 Fundación Acceso (2015). **Digital privacy for defenders of human rights? (¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos).** Available at: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

44 *Ibid.* P. 192.

45 Amnesty International. **Public Declaration AMR 37/5587/2017, Jan. 27, 2017** (**Declaración Pública AMR 37/5587/2017 del 27 de enero de 2017)**.

46 El Heraldo. **Honduras: National Congress Approves 2 More Controversial Penal Reforms (Honduras: Congreso Nacional aprobó los dos artículos más polémicos de las reformas penales).** Available at: http://www.elheraldo.hn/pais/1046584-466/honduras-congreso-nacional-aprob%C3%B3-los-dos-art%C3%ADculos-m%C3%A1s-pol%C3%A9micos-de-las-reformas

In the reforms of the Special Law for Private Communications Surveillance, the Communications Surveillance Unit (UIC, for its name in Spanish) was created to define the procedure for tracking / recording incoming and outgoing phone calls of those under investigation, with a competent judge's order. Additionally, it obligates telephone operators to guarantee the UIC immediate access – without limitation – to all information related to the surveillance and the extraction of telecommunications content.

In 2018, National Assembly presented a project called "Law of National Cybersecurity Strategy for the Prevention of Hate and Discrimination Campaigns on Social Networks" (Ley de Estrategia de Ciberseguridad Nacional de Prevención de Campañas de Odio y Discriminación en redes sociales)[47]. Opening up the debate about its legality, the Office of the Special Rapporteur for Freedom of Expression expressed concerns about the approach and scope of the project[48]. Despite this, Honduran government has signed a Cooperation Agreement with Israeli Government for the strengthening of the National Directorate of Research and Intelligence for the implementation of a CERT[49] in the country. Both actions threaten human rights such as digital privacy and freedom of expression in Honduran cyberspace.

C.2. Attacks towards Human Rights Defenders

Since 2009, Honduras has fostered an environment of systematic violence against human rights defenders, as highlighted in a report by the International Advisory Group of Experts.[50] Global Witness[51] has labeled Honduras the most dangerous country in the world for environmentalists due to the high rates of persecution, detention and assassination of people who defend the rights to access clean water and a healthy environment.

Organizations that defend human rights and independent news outlets have been targets of surveillance, harassment, threats, theft of equipment and information, persecution and even physical attacks and attempts on their lives.

In his reports, Michel Forst, the United Nations Special Rapporteur on the situation of human rights defenders, has expressed his concern "over the lack of independent and diligent investigations of aggression against environmental human rights defenders, which typically is linked to a lack of resources, corruption and collusion among the perpetrators. The States have nearly universally failed to bring the perpetrators to justice and to sanction them."[52] This is especially true in Guatemala and Honduras, where impunity persists, and defenders of human rights do not trust jurisdictional bodies when seeking judicial reparations.

According to Global Witness, following the 2009 coup d'état, more than 120 defenders of the land and the environment were assassinated in Honduras.[53] The majority of these cases remain in impunity

47 Telesur. Medios piden No aprobar Ley de Ciberseguridad en Honduras. Available at: https://www.telesurtv.net/news/medios-rechazan-ley-ciberseguridad-honduras-20180212-0038.html

48 La prensa. Ley de Cicerseguridad Amenaza la libertad de expresión. Available at https://www.laprensa.hn/honduras/1187050-410/ley-ciberseguridad-amenaza-libertad-expresion-cidh

49 El Heraldo. **Israel dotará de unidades en contra del cibercrimen en Honduras.** Available at: http://www.elheraldo.hn/pais/1115476-466/israel-dotar%C3%A1-de-unidades-en-contra-del-cibercrimen-en-honduras

50 International Expert Advisory Group (Grupo Asesor Internacional de Personas Expertas, 2017). **Dam of Violence: The Plan to Assassinate Berta Cáceres (Represa de violencia: El plan que asesinó a Berta Cáceres).** Available at: https://www.cejil.org/sites/default/files/represa_de_violencia_es_final_.pdf P. 11.

51 Global Witness (2017). **Honduras: The most dangerous place to defend the planet (Honduras: el lugar más peligroso para defender el planeta).** Available at: https://www.globalwitness.org/documents/18802/Spanish_single_v6.pdf

52 United Nations Special Rapporteur on the situation of human rights defenders. **Report on the Situation of Human Rights Defenders (Informe sobre la Situación de los defensores de los derechos humanos 2016).** Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/247/12/PDF/N1624712.pdf?OpenElement

53 *Ibid*. P. 5.

for different reasons, ranging from a lack of will to corruption in the government, the military, and the private companies that extract natural resources. The Honduran government, through its security forces, has institutionalized tactics of control and repression at all levels.

At the same time, in its 2017 report on press freedom, Freedom House classified Honduras as not free.[54] The report's methodology includes parameters such as the legal, political and economic climates that media outlets – including print media, radio and digital media – conduct their work of informing the public without fear of retaliation from private and political actors including members of organized crime. It added that Honduras continues to be one of the most dangerous countries in the world for journalists.[55]

In its annual report,[56] Amnesty International highlighted that the military has been accused of infiltrating social movements as well as attacking human rights defenders. The country's Law to Protect Human Rights Defenders, Journalists, Social Communicators and Justice Operators[57] has not been adequately enforced.

The State has invested more than 2 billion lempiras (some US$85 million) on intelligence and spying activities[58] targeting members of the political opposition under the banner of combating crime. These intelligence activities include telephone wiretaps, malware attacks and tailing activists and journalists. It's important to note that the Intelligence Directorate uses these tactics without a judge's warrant.

In the context of the presidential election of Nov. 26, 2017, these tactics of political violence and repression against social protests have extended to the general public. A state of emergency was declared[59] that restricted constitutional guarantees after public protests against election results and possible electoral fraud. That prompted citizen protests and excessive use of force by public security forces. These clashes resulted in several arrests, injuries and deaths across the country.[60]

During February 2018, the Honduran Congress was debating a law to regulate discrimination and hate acts through social media. This law was representing a high level of risk to the right of freedom of expression and access to information in the country, it also was not aligned with international standards of Human Rights, such as necessary, proportional, due process and transparency, which are fundamental to the respect of freedom of expression. This law was national and internationally condemned by 55 digital rights organizations with the campaign led by Access Now.

---

54 Freedom House (2017). **Freedom of the Press: Press Freedom's Dark Horizon.** Available at: https://freedomhouse.org/sites/default/files/FOTP_2017_booklet_FINAL_April28.pdfP. 24.

55 *Ibid.* P. 21.

56 Amnesty International (2017). **Annual Report 2016/2017: The State of the World's Human Rights (Informe anual 2016/2017: La situación de derechos humanos en el Mundo).** Available at: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ PP. 225-226.

57 Honduran National Congress. **Law to Protect Human Rights Defenders, Journalists, Social Communicators and Justice Operators (Ley de Protección para las y los Defensores de derechos humanos, Periodistas, Comunicadores Sociales y Operadores de Justicia).** Available at: http://www.tsc.gob.hn/leyes/Ley_Proteccion_defensores_der_humanos_periodistas_op_just.pdf

58 ConfidencialHN. **JOH spent nearly 2 billion to spy on the opposition (JOH gastó casi dos mil millones para espiar a opositores).** Available at: http://confidencialhn.com/2017/08/28/joh-gasto-casi-dos-mil-millones-para-espiar-a-opositores/

59 Reuters. **Honduras suspends constitutional guarantees amid strong protests following elections (Honduras suspende garantías constitucionales en medio de fuertas protestas tras elecciones).** Available at: https://lta.reuters.com/article/domesticNews/idLTAKBN1DV4UW-OUSLD

60 Amnesty International. **Honduras: Violent repression following elections (Honduras: represión violenta después de elecciones).** Available at: https://www.amnesty.org/es/documents/amr37/7550/2017/es/

C.3. Main findings in Honduras

Following we present the Central American Observatory for Digital Security's main findings for the case of Honduras. These have been registered between May and June of 2018. For registration, a series of technical and legal tools were created to define the criteria used in registering digital incidents.

C.4. Registered cases

During this period, a total of **two** cases of digital security incidents were registered, all of them in Tegucigalpa, Francisco Morazán.

C.5. Profile of the people/organizations that reported incidents

The first case involves a well-known journalist that collaborates with various international news channels, working in Honduras. The second case involves a defender from an international accompaniment organization.

C.6. Types of attacks

Following is a brief description of the registered attacks.

With the first case, the journalist contacts the Honduran Defenders Network, which contacts the Observatory's digital defender. The journalist states she has been receiving threats, insults, and constant harassment in her social networks from a specific profile. The profile was then checked, along with the messages sent from it, and then blocked from the defender's account. The defender was then encouraged to denounce the incident to a freedom of expression organization. Although it is not a digital incident but direct harassment and threats, it is classified as a false positive.

Regarding the second case, the defender contacts the Observatory's digital defender directly, because his organization has received at least 3 emails in different days, containing ransomware threats, asking them money in exchange of not publishing their computer's information. The digital defender inspected the source code of the defender's email and his computer. No vulnerabilities were found on his device. The incident is registered as a "Malware" and classified as false positive. Note that a false positive shouldn't be understood as a mistake, but as an early alert taken care of on time.

C.7. Possible perpetrators

In the first case, the profile of an individual posing as "Ramon Jérez" was identified. In the second case, the perpetrator was identified as a common "cracker" or "group of crackers" who usually send this type of electronic mail for electronic scams.

C.8. Protection mechanisms

In this section, we present the legal framework that could have been violated in the cases registered by the Central American Observatory for Digital Security in the Honduras chapter. We also analyze possible strategies that could be developed to protect the digital rights of human rights defenders.

C.9. Possible human rights violated

Honduran Constitution guarantees digital privacy's rights in:

> *Article 76: The right to honor, to personal privacy, to family, and to one's dignity is guaranteed.*

The Constitution also guarantees other fundamental rights like freedom of speech, through the Expression of Thought law, which protects the diffusion of thoughts and ideas in any digital media or social networks, encouraging the right of information transmission, acknowledged in:

> *Article 72: Expression of thought shall be free, and be expressed through any means of dissemination, without prior censorship. Those who abuse this right, and those who by direct or indirect methods restrict or limit the communication and circulation of ideas and opinions shall be liable before the law.*

Both constitutional precepts guarantee the protection of individual liberties, even if the State and power groups desired to censor information deposited in cell phones, computer equipment and smart devices of individuals and organizations that defend human rights.

C.10. Possible penal classification

From the legal framework investigation done by Fundacion Acceso in 2015 (and updated in 2018)[61], we could establish that even with the penal code alterations from 2017, this matter still continues to be insufficient when it comes to protecting human rights like digital privacy, and to applying legal defense mechanisms to protect human rights defenders in the country. In other words, the same sentence imposed to a person who violates postal mail can be applied to a person who vulnerates another individual's email.

Because cyber-crime can be adopted by multiple criminal figures in the analyzed legislation, Chapter VI talks about Constraints and Threats. Some of its legal base:

> *Article 207.- The individual who threatens another with causing an evil to him or his family, in his person, honor or property, whether it constitutes a crime or not, shall be punished with imprisonment of six (6) months to two (2) years, and in addition, to the security measures that the Judge determines.*

Fraud executed through an computer program, is also regulated in Chapter VI, which delimit the Scam and Fraud concepts. Its legal base:

> *Article 240. Commits the crime of fraud, any individual(s) who, with false names, influence or simulated quality, abuse of trust, pretending to be the owner of property, credits, business or negotiation or using any artifice, trickery or deception, were to induce and deceive another individual, for their own benefit or that of others.*

The sanctions vary in terms of amounts defrauded and their sanction with imprisonment are between two and seven years in prison.

---

61 Fundación Acceso (2015). ¿Privacidad Digital para Defensores y Defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensores y defensoras. http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf y "Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos en Guatemala, El Salvador, Honduras y Nicaragua" https://medium.com/@facceso.ca/privacidad-y-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-en-l%C3%ADnea-para-defensores-y-defensoras-de-derechos-5690330c3762

Other crimes that could be punished are hacking incidents, if this incident exposes information and shares private data that puts people's integrity in danger.

C.II. Legal response strategies

The people or organizations affected will have to plan strategical litigations through substantiated cases. These cases can be presented to jurisdictional organizations, or to the Public Prosecutor's Office. Strategical litigation has been used in the region for many years to promote human rights advocacy, being a tool that can be used by the victims, civil organizations, and certain State branches (like the Public Prosecutor).

These are some of the legal tools that could be used in some of the incidents registered by the Observatory:

1. Denouncements/Complaints to the Public Prosecutor's office

With cases registered in Honduras, it is constitutionally required to file complaints and denouncements with the Public Prosecutor. This organism promotes the prosecution of the aforementioned cyber-crimes and will direct the investigation of crimes committed against persons or organizations defending human rights.

Under its chain of custody and presenting physical and digital evidence, it will be able to resolve the digital incidents of extortion and threats, identified as means to interrupt the work of organizations and individuals in the defense of human rights.

2. Habeas data appeals

Honduran constitution describes Habeas Data as an immediate application appeal designed and made to cease human rights violation, specifically rights of honor, and personal and family intimacy. This appeal is presented to Supreme Court, with a strategic process that demands a specialized lawyer's representation. Article 76 supports it:

Article 76: The right to honor, to personal privacy, to family, and to one's dignity is guaranteed.

Legislative Decree No. 381-2005, which changed Chapter I, Title IV, from the Honduran Constitution, recognizes the warrant of the Habeas Data Appeal: that "Any individual has the right to access information about him/her self, or its goods, in an easy and not burdensome manner, if it is stored in a public or private registry, and in any case, can update or rectify it "

3. Denounces to the National Mechanism for the Protection of Human Rights Defenders

Honduras has a National Mechanism for the Protection of Human Rights Defenders and is obligated to investigate crimes and to protect the personal safety of defenders, as well as to avoid the obstruction of these defenders as they conduct their work. However, this mechanism only outlines measures of physical, psychological and legal protection, but it does not outline protection related to the digital security of its beneficiaries.

4. Inter-American System of Human Rights

The Inter-American System of Human Rights has certain requirements that must be met before cases can be brought before its regional bodies. Nevertheless, in extremely serious and urgent situations, protective measures can be requested from the Inter-American Commission on Human Rights so that the State takes steps to prevent irreparable damage to the people or the object of a petition or a pending case.

Additionally, it is a good forum to document these and other cases to identify patterns of behavior by organizations and governmental agencies that might be implementing surveillance against human rights defenders. This information can be shared with the respective rapporteurs so that it can be included in periodical reports to shed light on the region's digital security situation.

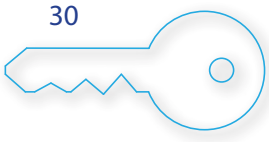
C.I2. Conclusions and Recommendations

Conclusions

1. While Honduras has a National System to Protect Human Rights Defenders, Journalists, Social Communicators and Justice Operators, it is still in its infancy. It has many shortcomings in terms of effective and efficient response. Honduras has been described as one of the most dangerous countries in the world for this type of work.
2. At the same time, the absence of adequate legal frameworks persists to protect digital privacy, which was outlined by the 2015 investigation by Fundación Acceso and updated in 2018.
3. The Honduran government has invested millions of lempiras to implement an intelligence system without including mechanisms of control and vigilance according to international standards in the field of human rights.
4. The threats directly faced by human rights defenders and independent journalists in the country range from physical to digital. The danger these defenders face at their daily jobs includes threats to their physical safety and their lives, as well as to the information generated throughout the course of their work and their daily efforts.
5. The issue of digital security continues to be left out of reports that address the security of human rights defenders, leaving areas of vulnerability through which they could be attacked.
6. Honduras lacks an adequate legislation when it comes to criminal matters, which sets limits in the classification of digital privacy and digital attack related crimes. This makes the Public Prosecutor's work more difficult when it comes to pursuing and stopping these crimes.

Recommendations

1. Reform to the judicial framework is needed to improve the mechanisms and levels of protection for human rights defenders, with an emphasis on including digital security tools, using international standards governing the issues of the Internet and human rights.
2. The public should demand transparency and accountability in respect to the various intelligence and surveillance tools, as well as to their regulation so that they are used in the context of need, legality and proportionality.
3. Human rights collectives and organizations should create internal protocols and mechanisms focused on digital security, which can be accomplished by training within these same organizations and collectives.
4. It is important to include sections in reports about the situation of human rights defenders that are dedicated to digital security. This will highlight the importance of the issue in terms of integral protection.
5. A national round table would be an important strategy to promote. This round table would feature analysis of the Internet and human rights and would be convened by local organizations with the participation of academic and technical communities. Global trends in Internet regulation that sacrifice the right to privacy are quickly echoing throughout the congresses of our Central American countries.



D. NICARAGUA

D.I. Legal Context: Internet and Human Rights in Nicaragua

In 2015, Fundación Acceso conducted an investigation titled, "Digital privacy for defenders of human rights?"[62] This investigation discussed the applicable legal framework for the right to privacy in Central America. It established applicable parameters at a national level that continue mostly unchanged today.

In general, the investigation established that constitutional recognition of the right to privacy exists at a general level,[63] but current penal legislation does not protect the right to digital privacy.

It's important to highlight the Sovereign Security Law of the Republic of Nicaragua, Law No. 919 from Dec. 2, 2015. Article 8 states that attacks against cybersecurity, primarily those that affect national communications systems, are considered national security threats. However, the law isn't clear about what is considered a "cyberattack," which could be problematic with a legal framework that is overly broad and ambiguous.

Article 13 **prohibits** public agencies that are part of the National Security System from the following: conducting political spying, obtaining or storing sensitive information or data from social organizations, or intercepting communications without a judge's order. The latter prohibition reflects, at least in legal text, that mass surveillance tactics should comply with some international standards and principles, such as legality, competent judicial authority and due process.

On Nov. 14, 2017 the First Forum on Internet Governance and Computer Security was held in Nicaragua.[64] At the forum, discussions between several sectors were held on issues related to digital privacy, although they were very general and did not include the need to protect human rights defenders.

A lack of other forums demonstrates that it is increasingly important to promote dialogue about the protection of human rights online, and for the public to demand that these rights are recognized and respected. The protection of human rights defenders also should be included in these types of discussions.

This creates a unique situation of vulnerability, because without the appropriate laws, it's likely that these types of attacks, along with the perpetrators whether they are companies or government agents, will remain in impunity.

D.2. Attacks towards Human Rights defenders

During 2018 Nicaragua has lived a deep social and political crisis that has impacted all the population and to date the crisis is ongoing. Different events such as massive civic manifestations in April 2018 were strongly repressed, including assassinations, illegal detentions, torture and forced disappearances. The CIDH stated that from April to the 19th of June 2018 they had registered 212 people dead due to State repression, along with 1337 injured and 507 imprisoned. Recent reports increase these numbers[65], and a national dialogue is not succeeding.

---

62 Fundación Acceso (2015). **Digital privacy for defenders of human rights? (¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos).** Available at: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf

63 *Ibid.* P. 260.

64 Internet Society, Nicaragua chapter. http://isoc.org.ni/

65 http://gieinicaragua.org/giei-content/uploads/2018/12/GIEI_INFORME_DIGITAL.pdf

On Jan. 10, 2017, Daniel Ortega was elected president for the third time and his wife, Rosario Murillo, became vice president. The concentration of power in Nicaragua has affected various areas of institutionality, from the arbitrary firing of different public officials who are members of the opposition[66] to the curbing of fundamental rights.

In Nicaragua, human rights defenders continue to be targeted by intimidation and threats due to their work. According to Amnesty International's Annual report,[67] indigenous and afro-descendent peoples have reported different violations of their fundamental rights, specifically in the context of the construction of a multibillion-dollar Interoceanic Canal, which was approved following a series of irregularities. Several communities and human rights organizations expressed concern about the impact the canal would have on their lives. The Interoceanic Canal's negative consequences for human rights have been compiled in a report by the Nicaraguan Human Rights Center (CENIDH) and the International Federation for Human Rights (FIDH).[68] The report clearly documents the criminalization of social protests, the harassment of the public and the militarization of the communities along the proposed canal route.

CENIDH's annual report for 2016[69] on the human rights situation in Nicaragua includes a section about the situation of human rights defenders. It indicates that, "The majority of cases of aggression, threats, stigmatization and litigation against human rights defenders have stemmed from the dissemination of denigrating and defamatory information on websites and social media networks, where not only photos and personal information is published, but also information about family members and home addresses. This exposes the subjects to the presumed aggressors, which places their security greatly at risk, as well as to constant threats both directed at them and their children."

In its recent report from 2017, Front Line Defenders also mentions that they have registered multiple attacks against human rights defenders in Nicaragua, particularly against women defenders. In two years, from 2015 to 2017, the Nicaraguan Initiative for Human Rights Defenders has registered **3**89 attacks against 202 defenders. Of those, 45 percent of the aggressors who were identified were government officials disguised as police.[70]

D.3. Main findings in Nicaragua

Following are the main findings by the Central American Observatory for Digital Security for the case of Nicaragua. These were registered between January and May 2018. For registration, a series of technical and legal tools was created to define the criteria used in registering digital incidents.

66 CEJIL (2017). **Nicaragua: How were institutional reforms passed to concentrate power? (Nicaragua: ¿cómo se reformó la institucionalidad para concentrar el poder?)** Available at: https://www.cejil.org/sites/default/files/informe_cejil_sobre_nicaragua_-_derechos_politicos.pdf P. 22.

67 Amnesty International (2017). **Annual report 2016/2017: The State of the World's Human Rights (Informe annual 2016/2017: La situación de Derechos Humanos en el Mundo).** Available at: https://www.amnesty.org/es/documents/pol10/4800/2017/es/ P. 328.

68 FIDH (2016) – Interoceanic Canal Concession in Nicaragua: Serious impact on human rights (Concesión del Canal Interoceánico en Nicaragua: Grave Impacto en los derechos humanos). Available at: https://www.cenidh.org/media/documents/docfile/informe_nicaragua_canal_esp1.pdf

69 CENIDH (2016). Human Rights in Nicaragua 2016 (Derechos Humanos en Nicaragua 2016). Available at: https://www.cenidh.org/media/documents/docfile/Informe_Cenidh_2016_Final2017.pdf

70 IM-Defenders (2017). Hearing 164 of the IACHR. Available at: https://www.youtube.com/watch?v=c4Pr6A3Yiq8

D.4. Registered cases

During the previously mentioned period, a total of 14 cases and security incidents were registered with different elements and motives in Leon and Managua, as well as an incident directed towards a Nicaraguan defender living in Mexico City.

D.5. Profile of the people/organizations that reported the incidents

First case has to do with a defender from an organization known for its work towards defending land and water sovereignty. The second case is linked to a director of an organization that carries out work to promote and defend the rights of women and girls, and to accompany victims of femicide. Third case involves an independent journalist, and the fourth case involves a defender from a women's organization. Fifth and sixth case are linked to two defenders from a human rights coalition. Seventh case corresponds to a social activist, and the eighth case, to a feminist activist. Ninth case is related to a woman's rights defender. Tenth and eleventh case are related to a male and a female defender. Twelfth case is related to a trans woman activist. Thirteenth and fourteenth case are about a female activist and male activist from Leon.

D.6. Types of attacks

Following is a brief description of the digital incidents registered.

First case: A solidarity organization informs Fundacion Acceso that the deputy director of one of their co-parties' organizations in Nicaragua is receiving calls from her office in Costa Rica, which are not done from it. Fundacion Acceso's director contacts the Observatory's digital defender in Nicaragua to arrange a meeting between the defender and her. According to the defender, she received a call from a landline from Costa Rica, which wasn't registered in her phone. When she answered the phone, it was directly hung up by the other part. After this, the calls from this number stopped.

The other incident mentioned by the defender is related with two video-calls via Whatsapp, which she received from her dad's number. She answered but there was no video showing (only a black screen). As she answered, a message popped on the screen stating that she had a weak connection. After this incident, the defender hasn't received any strange messages or calls. Her phone was analyzed by the digital defender but didn't have anything unusual in it. The defender was encouraged to ask for the call log of her cellphone and the organization's landline. We still don't have the call log, so the analysis can't go further for now.

Second case: A defender who knows about the Observatory sends us information about an organization who suffered a "computers theft incident." The organization informs the digital defender that in the computers' stolen is vital information about one of their projects, which is about girls suffering violence, and that they are afraid the perpetrator boycotts the project or uses the data to stop the organization's work. The defender expressed that in early February unknown subjects broke into the main offices and stole two computers belonging to the countability area. They forced the locks and broke a fence. They only stole financial information and left other equipment intact. Members of the organization are concerned about the possibility of hackers breaking into the accounting system or intimidating defenders to stop them from supporting the project. They took financial reports, bank account status and general accounting.

As an investigation can't be made without the equipment, a visit was made to support and guide them in creating safe backups of their information. This type of incidents can only be analyzed by the Observatory once the equipment is recovered. If it is recovered, the Observatory would then proceed to analyze if there was any data loss, malware installation or modifications to the operating system. This attack is reported as a "Hardware Loss" and classified as a false positive.

Third case: The journalist contacts the Observatory's digital defender directly to report that in early February, when he was investigating some denounces from syndicate workers from a mining zone in Leon, he couldn't access the mining company's webpage. Using a safe browser, the Observatory's digital defender was able to enter the page. With the help of the "Inspect element" tool that is integrated in several web browsers like Firefox and Google Chrome, she was able to detect the use of a plug-in called Geolify inside the webpage. This service is in charge of redirecting people into the welcome page, or into the localhost (null), based on the IP's location. We concluded that this is part of the site's configuration and has nothing to do with intentional blockage of the information. This incident is reported as a "Web Attack" and classified as false positive.

Fourth case: A women's organization contacts the Observatory's digital defender, reporting that one of the defenders of the organization had her equipment stolen. A TV and a tablet containing confidential information were subtracted from her house. It was a theft with intimidation, because the defender was home when the perpetrator broke in. The defender indicated that she has changed her passwords. Although the tablet was encrypted, she is not sure if it was completely protected. In 2016 and 2017, her organization also suffered an equipment theft. This incident is reported as a "Hardware Loss" and is classified as a positive incident.

Fifth case: A defender contacts the Observatory's digital defender, reporting that she has received international phone calls where they would hang up after she answered. This happened in January 2018 and hasn't happened again. The defender changed her mobile phone and the number linked to it. This incident is reported as a "Remote Attack" and is classified as a false positive.

Sixth case: A defender contacts the Observatory's digital defender, reporting that in two occasions, she received international phone calls where they would hang up after she answered. She also received unusual calls via Whatsapp. The incident was registered but the digital defender couldn't analyze the phone because the defender had already changed her device. This incident is reported as a "Remote Attack" and is classified as a false positive.

Seventh case: A social activist contacts the Observatory's digital defender directly. The defender reported that her Twitter accounts were suspended due to suspicious activity. The activist tries to recover her accounts, but the verification codes didn't show up in her phone. After this, she contacts the helping line of Access Now. The activist recovered her accounts access, and we suspect that the incident was caused by massive reports on her accounts, from pro-government users, due to the crisis in Nicaragua and the various mechanisms they use to censor and block freedom of speech in the Internet. This incident is reported as an incident of "Account compromise" and is classified as positive.

Eighth case: A feminist activist living in Mexico contacted the Observatory's digital defender via chat. The activist reports that her Facebook account is suspended due to massive reports coming from pro-government bots and accounts. Her account was suspended because of the content she was posting about the situation in Nicaragua. The Observatory did follow up the case until the defender got her account back. This incident is reported as an incident of "Account compromise" and is classified as positive.

Ninth case: A Women's Right's defender contacted the Observatory's digital defender. She reports that her Facebook account has been blocked. It seems like her password wasn't very strong, and someone

managed to log into her account. The case is shared to the Help Line from Access Now. We followed up her case and tried to visit her, but it wasn't possible due to the country's crisis. After this, we encouraged the defender to activate two step verification on her accounts to avoid another incident.

A feminist activist living in Mexico contacted the Observatory's digital defender via chat. The activist reports that her Facebook account is suspended due to massive reports coming from pro-government bots and accounts. Her account was suspended because of the content she was posting about the situation in Nicaragua. The Observatory did follow up the case until the defender got her account back. This incident is reported as an incident of "Account compromise" and is classified as positive.

Tenth case: A feminist activist contacted the Observatory's digital defender directly via chat. The activist indicates that she uploaded some protests pictures to her Facebook account, had lots of trouble uploading them, and after 15 minutes, Facebook reported unusual activity in her account. When she checked, she found a log in from an unknown IP address (which was later proven to be near Luis Alfonso Velásquez Park). She closed all the active sessions and changed her password, but the page wouldn't load on her phone. She turned off her phone and logged in again after a while. An option showed up on her account, asking if she wanted to close her account due to a hacking incident. She sent some screen-shots that confirmed the unusual log in. Additionally, she reported that another unknown active session was showing up in her Telegram account. Furthermore, she received a Whatsapp message from her boyfriend that he hadn't sent. The activist deleted the Whatsapp account. The digital defender recommended a visit to analyze the mobile phone, but this wasn't possible due to the country's crisis. This incident is reported as an incident of "Account compromise" and hasn't been classified as false or positive

Eleventh case: A male activist working with the mediating commission of the national dialogue reports that the official Facebook page of a known religious individual had been suspended due to massive reports from pro-government groups. At the same time, at least 3 pages and 3 fake profiles have been put up with the objective of getting the people's attention and deviating it from the authentic page. The male activist asks for support with the account's recovery and verification. The case was shared to the Access Now Help Line, and we followed up the case until the Facebook and Twitter accounts were recovered and verified. The fake pages and profiles were reported, and the people were advised to double check the pages they were following. We tried to arrange a visit between the Observatory's digital defender and the defender, but this wasn't possible due to the country's crisis and the attacks from police forces. This incident is reported as an incident of "Account compromise" and is classified as positive.

Twelfth case: A trans women defender contacts the Observatory's digital defender. The defender was intercepted by two persons on a motorbike, who stole her cellphone. This defender had been threatened before by a police officer, who has a relative with a high rank of power inside the police. This officer confessed to the defender about the murdering of the students, and later started threatening her, following her with vehicles and harassing her constantly. The incident happened at night, and the defender was not able to block her SIM card soon enough. At the next day, with technical support, she tried to log into her email accounts but neither Gmail or iCloud recognized the passwords. The digital defender then confirmed that the passwords had been recently changed, and that she had 2 steps verification. Analyzing the situation, it is presumed that the perpetrators managed to get into her accounts due to her not being able to block her SIM card right away. The case was shared with the Access Now Help Line. This incident is reported as "Hardware Loss" and classified as positive.

Thirteenth case: A human rights defender contacts the Observatory's digital defender informing that her husband's phone has been stolen, who works in an international cooperation organization. His husband reports that he was in a road blockage (*tranque*), and two persons on a motorbike snatched his phone.

They tried to access his accounts to change passwords because he had 2 step verification and called the cellphone carrier asking to disable the SIM card. The defender and her husband were advised to access the accounts from the house computer and delete them. This incident is reported as “Hardware Loss” and classified as positive.

Fourteenth case: A female activist contacts the Observatory’s digital defender directly. The activist informs about another activist’s computer theft, who runs the page of a social movement. The digital defender contacted the activist involved, and he states that the robbery’s circumstances were unclear, as they only took the computer and left other valuable stuff. He indicated he had his information safe and was able to access his accounts with his phone. This incident is reported as “Hardware Loss” and classified as positive.

D.7. Possible perpetrators

The identification of the possible perpetrators of the attacks is a task that interests the Digital Security Observatory, but it should be pointed out that this is not always possible. This is especially true in the context of common crime, which has become a frequent occurrence in the countries of the Central American region. For these types of complex cases, technical resources and access to services are needed that are outside the scope of the organization.

The general context of the country and the crisis going on, as well as the clear identification of the repressive methods are present in the seventh and eighth cases, in which the account compromise incident occurred because of massive reports on social media platforms against the accounts of activists and defenders. In this case, the perpetrators were pro-government groups.

In the Hardware Loss incidents, although the perpetrators are not identified, in several of these cases, the presence of motor bike riders is notable. In the crisis context, motor bike riders are linked to para-police groups in Nicaragua.

In the tenth case, an IP was identified, located near Luis Alfonso Velázquez Park in the middle of Managua. However, there’s no further information about the perpetrator.

D.8. Protection Mechanisms

In this section, we present the legal framework that could have been violated in the cases registered by the Central American Observatory for Digital Security in the Nicaragua chapter. We also analyze possible strategies that could be developed to protect the digital rights of human rights defenders.

D.9. Possible Human Rights Vulnerated

The Constitution of the Republic of Nicaragua envisages and regulates the right to privacy, in which the inviolability of correspondence, documents and books in any format is established, except under order from a competent judge. The common denominator of the positive incidents that were registered is the infringement on the constitutional right to digital privacy, compromising personal information, accounts, email content and passwords. Its legal base is stated in:

> Article 26 - All persons have the right to:
>
> 1. privacy and the privacy of their family;
>
> 2. the inviolability of their home, correspondence, and communications;
>
> 3. respect for their honor and reputation.

A private home may be searched only with a warrant from a competent judge or expressly authorized official to prevent a crime from being committed or to avoid damage to persons or goods, in accordance with the procedures established by law. The law shall determine the cases and the procedures for an examination of private documents, fiscal records and related documents, when such is indispensable for the investigation of matters before the Courts or for fiscal reasons. Illegally seized letters, documents and other private papers shall be null and void in legal proceedings or elsewhere.

Because of this, national authorities can't retain computer equipment, smartphones or any digital device from any individual.

D.10. Possible penal classifications

Based on the 2015 investigation by Fundación Acceso, updated in 2018 [71], it is clear that the penal framework continues to be insufficient to establish integral safeguards to protect the right of digital privacy for human rights defenders in the country. Nonetheless, criminal legislation prohibits any individual from using an computer program to access personal data and information stored in any smart device or computer equipment:

> Article 192 regulates the Opening or Illegal Interception of Communications.
>
> Who illegitimately opens, intercepts or by any other means finds out the contents of a letter, a closed sheet or a telegraphic, telematic, electronic or other document that is not addressed to him, will be punished by imprisonment from six months to two years.
>
> If he also disseminates or discloses the content of the communications indicated in the previous paragraph, imprisonment of one to three years will be imposed.
>
> Article 193 regulates Subtraction and Diversion of Communications
>
> Who without knowing its contents, illegally seizes, destroys or deviates from its destiny a communication that is not addressed to it, will be punished with imprisonment of six months to a year.
>
> Who knowing or presupposing the content of the communication carries out the behavior foreseen in the previous paragraph, will be punished with imprisonment of one to two years.
>
> Article 194 regulates the improper Capture of Communications from Others
>
> Who illegitimately record the words or conversations of others, not intended for the public, or who through technical procedures listen to private communications or telephone that are not directed, will be punished with imprisonment of one to two years.
>
> Article 195: Propagation
>
> Who is legitimately in possession of a communication, private documents or recordings, and makes them public without proper authorization, even if they have been directed, will be penalized from sixty to one hundred and eighty days of fine.

71 Fundación Acceso (2015). ¿Privacidad Digital para Defensores y Defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensores y defensoras. http://acceso.or.cr/assets/files/Investigacion-Privacidad-Digital-FA.pdf y "Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos en Guatemala, El Salvador, Honduras y Nicaragua" https://medium.com/@facceso.ca/privacidad-y-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-en-l%C3%ADnea-para-defensores-y-defensoras-de-derechos-5690330c3762

Article 197: Prohibited records

Whoever, without the authorization of law, promotes, authorizes, finances, creates or markets a data bank or a computer registry with data that may affect natural or legal persons, will be punished with imprisonment of two to four years and three to five hundred days of fine.

Article 198: Access and unauthorized use of information

Who, without proper authorization, use the computer records of another, or enter, by any means, the data bank or electronic files of someone, will be punished with imprisonment of one to two years, and a fine of two hundred to five hundred days.

Article 199: Aggravation due to abuse of authority or charge

The authority, official or public employee who, outside the cases authorized by law and taking advantage of his position or function, performs any of the conducts established in this chapter, will be imposed with the penalty of three to six years of prison and disqualification from exercising the position or public employment

Article 245: Destruction of Computer Records

Whoever destroys, erases or in any way renders computer records unusable, will be punished with imprisonment of one to two years or a fine of between ninety and three hundred days.

The penalty will be raised from three to five years, when such information is necessary for the provision of a public service or it is an official record.

Article 246: Regulates the Use of Destructive Programs

Who, with the intention of producing damage, acquires, distributes or puts into circulation destructive computer programs or instructions, which may cause damage to records, programs or computer equipment, will be punished with imprisonment of one to three years and a three to five hundred days of fine.

Article 250: Regulates the Protection of Computer Programs.

It will be sanctioned from three hundred to five hundred days of fine or imprisonment from one to three years, who, contravening the law of the matter, manufactures, distributes or sells mechanisms or systems that allow or facilitate the unauthorized suppression of technical devices that have been used to prevent reproduction of computer programs.

D.II. Legal response strategies

The people or organizations affected will have to plan strategical litigations through substantiated cases. These cases can be presented to jurisdictional organizations, or to the Public prosecutor's office. Strategical litigation has been being used in the region for many years to promote human rights advocacy in the region, being a tool that can be used by the victims, civil organizations, and certain State branches (like the public prosecutor).

These are some of the legal tools that could be used in some of the incidents registered by the Observatory:

1. Denouncements/Complaints to the Public Prosecutor's office

With cases registered in Nicaragua, it is constitutionally required to file complaints and denouncements with the Public Prosecutor. This organism promotes the prosecution of the aforementioned cyber-

crimes and will direct the investigation of crimes committed against persons or organizations defending human rights.

Under its chain of custody and presenting physical and digital evidence, it will be able to resolve the digital incidents of 1. Remote attacks, 2. Account compromise, and 3. Electronic equipment theft, identified as means to interrupt the work of organizations and individuals in the defense of human rights.

2. Appeal of Amparo

The Appeal of Amparo also is used as a legal mechanism to demand the protection of rights guaranteed under the Constitution. Because the privacy of communications is a constitutional right, an appeal could be attempted to safeguard this and other rights.

The Appeal of Amparo in Nicaragua is presented to the Constitutional Chamber of the Supreme Court. The process requires sponsorship by an attorney, preferably an expert in this type of action, which in some cases impedes human rights defenders and the general public from accessing constitutional justice.

3. Habeas data appeal and other actions

Any person or entity, whether it's public or private, can access the mechanisms from the Personal Data Protection Office, ascribed to the Ministry of Finance and Public Credit, as the highest authority that the Personal Data Protection Law establishes in its application section. It serves to guarantee the right to personal and familiar privacy, and the right of informative self-determination. It is contemplated in the Article 9, 12-15, and the sanctions in articles 47-52.

Another legal action to protect digital privacy is contemplated in the General Law on Telecommunications and Postal Services, which regulates the telecommunication and postal services, and establishes the rights and duties of the users and operators, in terms of quality, equality, equity, and development. Article 2 numeral 6 of this law guarantees and protects communication privacy and security of the transmitted information.

Depending on the case, the regulatory organ may impose sanctions and financial infractions as established in Art. 82 These are considered very serious infractions: numeral 3) Interfere or intentionally intercept telecommunications services, affect their operation and intentionally violate laws, regulations, treaties, international telecommunications agreements or agreements in which Nicaragua is a party, provided that manifest fraud is proven.

4. Denounces to the Procurator for the Defense of Human Rights

In matter of denunciations of violation to the Human Rights, Nicaragua regulates the figure of the ombudsman. This figure is determined by the Procurator for the Defense of Human Rights, before whom violations of fundamental freedoms and rights can be interposed for the effective fulfillment of the fundamental rights that the constitution establishes.

The Procurator's office, depending on the case, would take the denounce in the investigative phase. This process goes according to what is established in Law 212 "Law of the Procurators Office for the Defense of Human Rights"

However, this organism has a moral nature and is designed to function as a Court of conscience, although it has the legal capacity to present complaints and denouncements to other organs.

5. Inter-American System of Human Rights

The Inter-American System of Human Rights has certain requirements that must be met before cases can be brought before the regional bodies. Nevertheless, in extremely serious and urgent situations, protective measures can be requested from the Inter-American Commission on Human Rights so that the State takes steps to prevent irreparable damage to the people or the object of a petition or a pending case.

Additionally, it is a good forum to document these and other cases to identify patterns of behavior by organizations and governmental agencies that might be surveilling human rights defenders. This information can be shared with the respective rapporteurs so that it can be included in periodical reports to shed light on the region's digital security situation.

D.I2. Conclusions and Recommendations

Conclusions

1. It could be observed that in Nicaragua, the inadequate application of the legal framework regarding digital privacy, which was identified in the investigation done by Fundación Acceso in 2015 and updated in 2018 persists. In the cases analyzed, Nicaraguan Constitution recognizes the right of privacy through articles 26,27,96 and 188. Also, Personal Data Protection Law eases the usage of the Habeas Data appeal, followed by a series of rules and measures that prohibit civilian surveillance in any way. However, all these measures become ineffective due to the current institutional and political uncertainty in the country.
2. The threats directly faced by defenders of human rights and independent journalists in the country range from physical to digital. The danger that these people face at their daily jobs includes threats to their physical safety and even their lives, as well as to the information they generate in the course of their work.
3. It could be observed that in Nicaragua, privacy and information security institutionality is still necessary. The Personal Data Protection Office, ascribed to the Ministry of Finance and Public Credit, as the highest authority that the Personal Data Protection Law establishes in its application section, doesn't manage to fulfill its constitutional obligations regarding control and protection of personal data. For this reason, digital privacy will continue to be absent in human right defenders' security, causing vulnerabilities.

Recommendations

1. Reform of the legal framework is needed to improve the safeguards and levels of protection for human rights defenders, with an emphasis on the need for digital security tools, including international standards for the Internet and human rights.
2. The collectives and organizations dedicated to the defense of human rights should generate internal mechanisms and protocols focused on digital security, which can be achieved by developing skills within their own collectives.
3. In reports on the activities of human rights defenders, it's important to include sections dedicated to digital security to highlight its importance for integral security.
4. Even though Nicaragua has a Personal Data Protection Law, a national space of analysis and consultation must be arranged to discuss human rights and the sovereignty of the Internet. In the current context no reasonable dialogue is possible between any actor (state institutions,

judiciary institutions, civil society, academia, tech communities, etc); therefore any effort to engage discussions or change public policies is at this time useless.

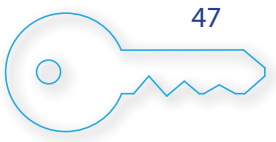
E. Bibliography

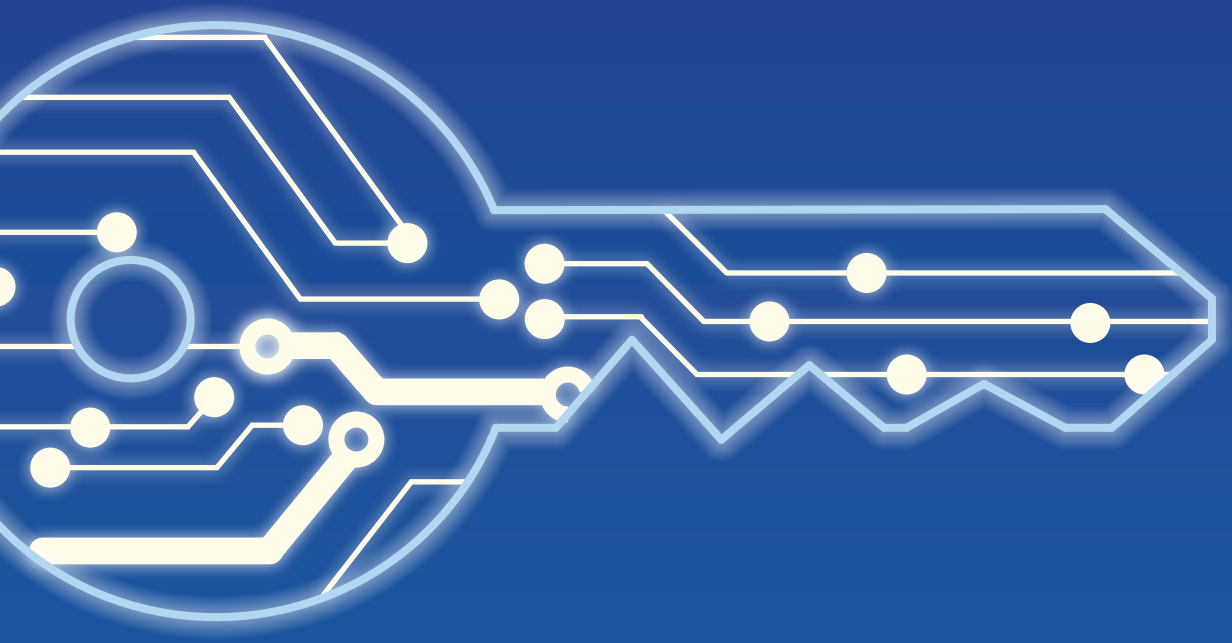
- Alliance for Affordable Internet. (**Coalición Guatemalteca para una Internet Asequible).** Available at: http://a4ai.org/guatemala/
- Amnesty International (2017). **Annual report 2016/2017: The State of the World's Human Rights.** Available at: https://www.amnesty.org/es/documents/pol10/4800/2017/es/
- Civil Rights Association (Asociación de Derechos Civiles, 2015). **Educate to Monitor: An investigation of the state's institutional training on surveillance and investigation in the digital realm (Educar para vigilar: Una investigación acerca de la formación institucional estatal en vigilancia e investigación en el entorno digital).** Available at: https://adcdigital.org.ar/wp-content/uploads/2016/01/Educar-para-vigilar.pdf
- Inter-American Development Bank and Organization of American States (2016). **Cybersecurity: Are We Prepared in Latin America and the Caribbean?** Available at: https://publications.iadb.org/handle/11319/7449?locale-attribute=es&
- CELE-UP (2012). **Toward an Internet Free of Censorship (Hacia una Internet libre de censura: propuestas para América Latina).** Available at: http://www.palermo.edu/cele/pdf/Internet_libre_de_censura_libro.pdf
- CELE-UP (2014). **Internet and Human Rights: Discussions for Latin America (Internet y derechos humanos: aportes para la discusión en América Latina.)** Available at: http://www.palermo.edu/cele/pdf/InternetyDDHH.pdf
- CENIDH (2016). **Human Rights in Nicaragua (Derechos Humanos en Nicaragua, 2016).** Available at: https://www.cenidh.org/media/documents/docfile/Informe_Cenidh_2016_Final2017.pdf
- Congress of the Republic of Guatemala. **Bill 4090, Law to Protect Personal Information.** Available at: http://old.congreso.gob.gt/uploadimg/archivos/dictamenes/988.pdf
- Congress of the Republic of Guatemala. **Bill 5230**. Available at: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=2636
- Congress of the Republic of Guatemala. **Bill 5239, Law Against Terrorist Acts.** Available at: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=3607
- Congress of the Republic of Guatemala. **Bill 5254, Law Against cyber-crime.** Available at: http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf
- UN Human Rights Council (2014). **The Right to Privacy in the Digital Age (El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los derechos humanos).** Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjYmJj-8M3MAhXEHR4KHVVcCQYQFggdMAA&url=http%3A%2F%2Fwww.ohchr.org%2FEN%2FHRBodies%2FHRC%2FRegularSessions%2FSession27%2FDocuments%2FA-HRC-27-37_sp.doc&usg=AFQjCNGT_BPxxWGqFMXjIlOkF80ao6-TkA
- Inter-American Commission on Human Rights (2006). **Report on the situation of human rights defenders in the Americas (Informe sobre la situación de las defensoras y defensores de los derechos humanos en las Américas).** Available at: https://www.cidh.oas.org/countryrep/Defensores/defensoresindice.htm

- Inter-American Commission on Human Rights (2013). **Report on Freedom of Expression on the Internet (Informe Libertad de Expresión e Internet).** Available at: https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf
- Inter-American Commission on Human Rights (2015). **Report on the Situation of Human Rights in Guatemala (Informe Situación de los derechos humanos en Guatemala: Diversidad, desigualdad y exclusión).** Available at: https://www.oas.org/es/cidh/informes/pdfs/Guatemala2016.pdf
- Inter-American Commission on Human Rights (2016). **Report on the Criminalization of Human Rights Defenders (Informe Criminalización de defensoras y defensores de derechos humanos).** Available at: https://www.oas.org/es/cidh/informes/pdfs/criminalizacion2016.pdf
- Inter-American Commission on Human Rights (2017). **Report on Standards for a Free, Open and Inclusive Internet (Informe Estándares para una Internet Libre, Abierta e Incluyente).** Available at: https://www.oas.org/es/cidh/expresion/docs/publicaciones/Internet_2016_ESP.pdf
- Inter-American Commission on Human Rights (2017). **Report from the Rapporteur for Freedom of Expression (Informe de la Relatoría para la Libertad de Expresión).** Available at: https://www.oas.org/es/cidh/expresion/docs/informes/anuales/InformeAnual2016RELE.pdf
- Inter-American Commission on Human Rights (2017). **Report on Silenced Zones: Extremely dangerous regions to practice freedom of expression (Informe Zonas Silenciadas: regiones de alta peligrosidad para ejercer la libertad de expresión).** Available at: https://www.oas.org/es/cidh/expresion/docs/publicaciones/ZONAS_SILENCIADAS_ESP.pdf
- Digital Rights (Derechos Digitales, 2016). **Hacking Team: Malware for spying in Latin America.** Available at: https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf
- Electronic Frontier Foundation (2014). **Necessary and Proportionate: International Principles for the Application of Human Rights to Communications Surveillance (Necesarios y Proporcionados: Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones).** Available at: https://necessaryandproportionate.org/files/2016/03/04/spanish_principles_2014.pdf
- Electronic Frontier Foundation and Digital Rights (Derechos Digitales, 2016). I**nternational Principles for the Application of Human Rights to Communications Surveillance (Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones) and the Inter-American System for the Protection of Human Rights.** Available at: https://necessaryandproportionate.org/files/2016/08/23/iachr-sp-agosto2016.pdf
- Electronic Frontier Foundation (2016). **Comparative analysis of surveillance laws and practices in Latin America (Análisis comparado de las leyes y prácticas de vigilancia en Latinoamérica).** Available at: https://necessaryandproportionate.org/files/2016/10/07/comparative_report_october2016_es_0.pdf
- Freedom House (2017). **Freedom of the Press: Press Freedom's Dark Horizon.** Available at: https://freedomhouse.org/sites/default/files/FOTP_2017_booklet_FINAL_April28.pdf P. 24.
- Front Line Defenders (2015). **Annual Report 2015: Human Rights Defenders on a Tightrope (Defensores (as) de derechos humanos en la cuerda floja).** Available at: http://www.coljuristas.org/documentos/adicionales/defensores_de_ddhh_en_la_cuerda_floja.pdf

- Front Line Defenders. **Annual Report, Human Rights Defenders at Risk in 2017.** Available at: https://www.frontlinedefenders.org/en/resource-publication/annual-report-human-rights-defenders-risk-2017
- Internet Governance Forum in Guatemala (Foro de Gobernanza de Internet de Guatemala). http://igf.gt/
- Fundación Acceso (2015). **Digital privacy for defenders of human rights? (¿Privacidad digital para defensores y defensoras de derechos humanos?: Un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos).** Available at: http://acceso.or.cr/files/Investigacion-Privacidad-Digital-FA.pdf
- Medium.com. **Net Centers: The Business of Manipulation (Los Netcenters: Negocio de Manipulación).** https://medium.com/@luisassardo/los-netcenters-negocio-de-manipulacion-2140cf7262fc
- Interior Ministry. **Conclusions to improve the draft of the National Cybersecurity Strategy (Presentan conclusiones para mejorar Borrador de la Estrategia Nacional de Ciberseguridad).** Available at: http://mingob.gob.gt/presentan-conclusiones-para-mejorar-el-borrador-de-la-estrategia-nacional-de-ciberseguridad/
- Motherboard. **The 'Illegal' Empire of Hacking Team in Latin America (El imperio 'ilegal' de Hacking Team en América Latina).** Available at: https://motherboard.vice.com/es/article/wngqmx/el-imperio-ilegal-de-hacking-team-en-america-latina-5886b78158d4ae45b7112d84
- Nación Digital. https://www.naciondigital.gob.gt/
- Nómada. **#JimmySeQueda: el netcenter de @rodrigopolo, @rmendezruiz y @pirulismo.** Available at: https://nomada.gt/asi-se-fabrico-el-jimmysequeda-el-netcenter-de-rodrigopolo-rmendezruiz-y-pirulismo/
- Organization of American States. **American Convention on Human Rights.** Available at: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm
- United Nations. **Universal Declaration of Human Rights.** Available at: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf
- United Nations. **International Covenant on Civil and Political Rights.** Available at: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx
- United Nations (1999). **Resolution 53/144 from March 8, 1999.** Available at: http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf
- Prensa Libre. **A Dangerous Bill (Una peligrosa propuesta de ley).** Available at: http://www.prensalibre.com/opinion/opinion/una-peligrosa-propuesta-de-ley
- United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2016). **Annual Report.** Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/51/PDF/G1707751.pdf?OpenElement
- United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2017). **Annual report.** Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/51/PDF/G1707751.pdf?OpenElement

- United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2017). **Report.** Available at: http://www.un.org/ga/search/view_doc.asp?symbol=A/72/350
- United Nations Special Rapporteur on the situation of human rights defenders. **Report on the Situation of Human Rights Defenders (Informe sobre la Situación de los defensores de los derechos humanos, 2016).** Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/247/12/PDF/N1624712.pdf?OpenElement
- Factum Magazine. **Extermination: The Complicit State (Exterminio: El Estado cómplice).** Available at: http://revistafactum.com/exterminio-el-estado-complice/
- Soy502. **The military wants to handle cyber threats (El Ejército quiere encargarse de las amenazas cibernéticas).** Available at: http://www.soy502.com/articulo/ejercito-quiere-encargarse-amenazas-ciberneticas-63338?utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter#link_time=1511180394
- Soy502. **Net Centers of Impunity (Los netcenteros de la impunidad).** Available at: http://www.soy502.com/articulo/netcenteros-impunidad-20878
- Soy502. **Journalists demand an investigation of "net centers" (Periodistas exigen que el MP investigue a los "net centers").** Available at: http://www.soy502.com/articulo/periodistas-exigen-investigacion-ataques-ciberneticos-149
- Udefegua. **Situation of Human Rights Defenders in Guatemala (Situación de Defensoras y Defensores de derechos humanos en Guatemala Un Reflejo del Deterioro de los derechos humanos en el País).** Available at: http://udefegua.org/wp-content/uploads/2017/10/201709-Sit-Defensores-DH-SEMESTRAL.FIN_.pdf
- Web We Want. **Charter of Internet Rights in Guatemala (Carta de Derechos de Internet en Guatemala).** Available at: https://webwewant.org/es/guatemala/





FUNDACIÓN Acceso