Central American Observatory for Digital Security

- Annual Report 2017 -

Fundación Acceso, 2018

Central American Observatory for Digital Security- 2017 Report

Written by: Sara Fratti

Revised by: Tanya Lockwood

In collaboration with: Alejandro Durón, Gema Jiménez y David Oliva

Translation: David Boddiger

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 (from June to November 2017), we documented 24 cases in Honduras, Nicaragua and Guatemala. In El Salvador, two cases were reported but not analyzed due to the inability to communicate with the affected defenders or organizations. Therefore, the El Salvador chapter lacks analyzed cases. However, it will be included, with descriptions of relevant legal context.

A.1. 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 and this important work, which transcends the digital realm.

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

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.

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 practices 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

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 derecho**s 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). 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 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

recommendations[7] for Latin American governments, including in 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 Frost, 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. Frost 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 utilize 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 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.

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

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.

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]

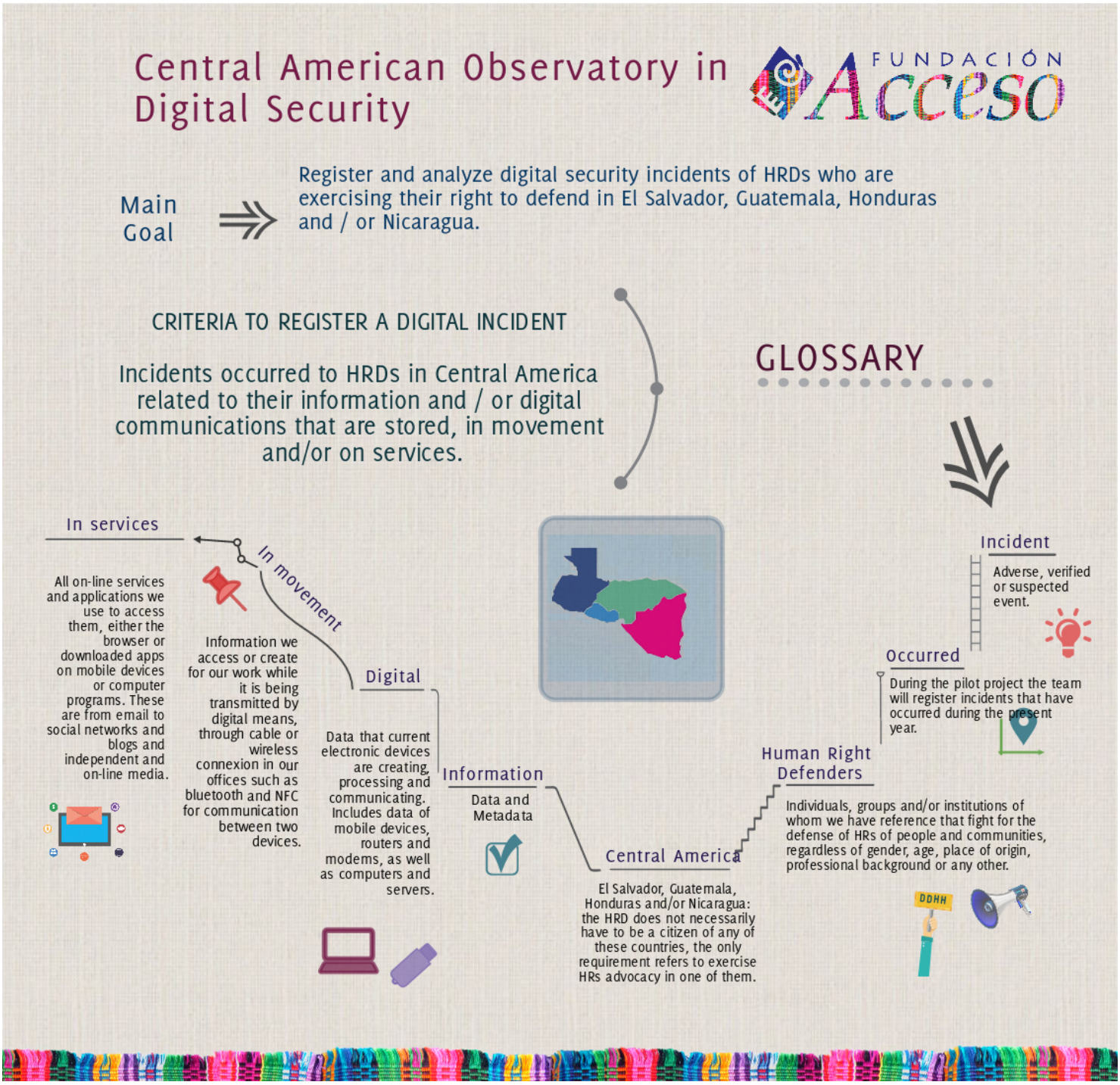
An incident is defined as any adverse event (verified or suspected) related to digital information (including data and metadata) and/or communications.

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



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

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.

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.

•**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.

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

Central American Observatory in Digital Security

Intervention Moments:

FUNDACIÓN Acceso

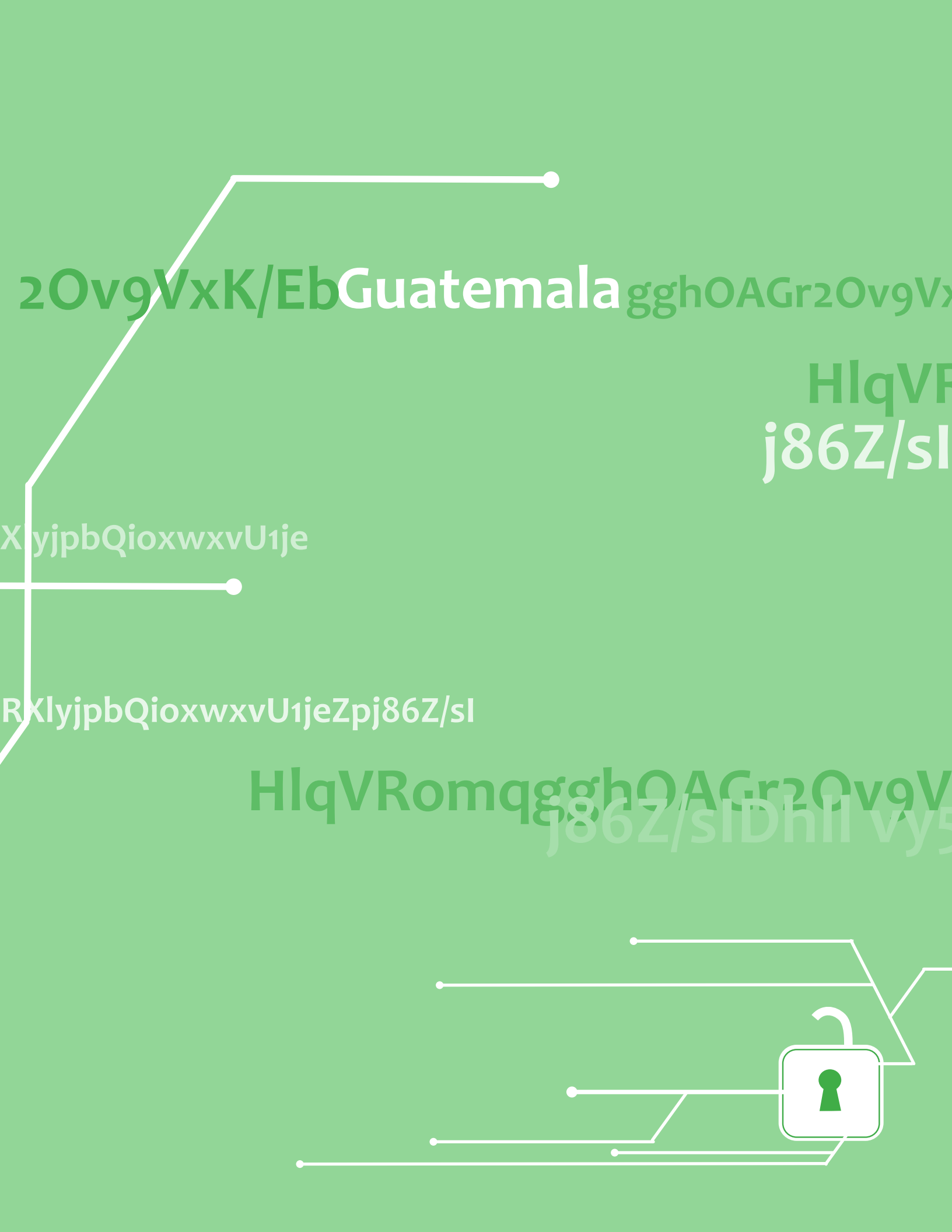
A.4. Procedure for incident registration

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 inspection, the investigating technician 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 inspection 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 Guatemala.


2Ov9VxK/EbGuatemalagghOAGr2Ov9Vx
HlqVR
j86Z/sI
XlyjpbQioxwxvU1je
RXlyjpbQioxwxvU1jeZpj86Z/sI
HlqVRomqgghOAGr2Ov9V
j86Z/sIDhII vy5

B. GUATEMALA CHAPTER

B.1. Legal Context: Internet and Human Rights in Guatemala

In 2015, Fundación Acceso conducted an investigation 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 investigation established that constitutional recognition of the right to privacy exists at a general level,[21] but current penal 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 the 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.

Bill 5230,[23] which seeks to reform Decree No. 17-73 of the Penal Code of the Congress of the Republic, would specifically modify section d) of Article 274 outlining the crime of defamation. The reform would criminally classify the creation of a "data bank, an account or user of a virtual social network, social software, or an information registry with information that could affect the privacy, repute or dignity of a person," except that which is regulated by Article 35 of the Constitution regarding the free expression of thought. The reform would impose a penalty of four to eight years in prison for this proposed violation.

While this bill was presented as a means to protect the dignity, honor and privacy of citizens, its primary outcome would be to prevent citizens from protesting on social media against the corrupt acts of public officials. Because of this, the bill could eventually become a threat to freedom of

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 5230.** Available at: http://www.congreso.gob.gt/iniciativa-de-ley-detalle/?id=2636

expression on the Internet. Additionally, human rights defenders would not feel safe sharing their opinions on social media networks. This bill already has received approval from the Committee on Legislative and Constitutional Matters, and it awaits a third debate before the full Congress.

Bill 5239, which seeks passage of the Law Against Terrorist Acts,[24] 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.[25] 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 Cybercrime,[26] 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.

The Superintendency of Telecommunications (SIT) has developed a digital agenda called "Nación Digital" ("Digital Nation"), with the help of other government entities.[27] 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.

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.[28] 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

24. 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

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

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

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

28. 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/

national security from cybercrime. 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 the year under review, important advances were made 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.[29]

The Alliance for Affordable Internet (A4AI) is promoting the Guatemalan Coalition for Affordable Internet[30] 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 July 27, 2017, the first Guatemalan Internet Governance Forum[31] was held, where issues related to digital privacy 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 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.

29. 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

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

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

B.2. Attacks against human rights defenders

In its recent biannual report[32] (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. The majority 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,[33] 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 Frost, 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."[34]

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[35] 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

32. 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.

33. 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.

34. 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

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

Commission Against Impunity in Guatemala (CICIG),[36] the Public Prosecutor's Office (MP)[37] and several national human rights organizations (particularly for women human rights defenders).

Recently, 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."[38] 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, such as spying and the possible criminalization of activists and defenders of human rights.

As this report by the Observatory was being finalized, 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.[39]

In the context of investigations into various cybercrimes, 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.[40] 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.

B.3. Main findings in Guatemala

Following are the main findings by the Central American Observatory for Digital Security for Guatemala. These findings were registered between June and November 2017. For registration, a series of technical and legal tools was created to define the criteria used in documenting digital incidents.

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

37. 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/

38. Soy502. J**ournalists 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-ciberneticos-149

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

40. 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

B.4. Registered cases

During this period, a total of four cases and incidents were registered with various elements and motives, all in Guatemala City.

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

The first case involved a foundation focused on demanding that human rights be respected and contributing to the struggle for transparency and against impunity in the country. Two cases involved an independent news organization devoted to investigative journalism, and the last case involved an organization that provides international accompaniment for cases involving human rights violations in the country.

B.6. Types of attacks

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

In the first case, an incident that occurred on social media, the human rights defender was a victim of identity theft on one of the platforms.

In the case of the media outlet, screenshots of private messages from the director were leaked by an anonymous profile and later on an external website. Beyond the compromised account, it also could be considered a phishing attack because the screenshots do not coincide with those of his mobile device. On the other hand, the official website of this media outlet was subject to several service denial attacks throughout the year.

In the fourth case, the organization lost all of the information on its server twice, but fortunately that information was backed up on hard drives.

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.

The first and second cases occurred in the context of defamation and harassment campaigns targeting activists, human rights defenders and influencer's of public opinion demanding justice

against impunity and transparency, among others. As a consequence, the objective was to smear the work that these people carry out, along with their respective organizations and media outlets. This was done by impersonating their identities on social media, in the first case, and by leaking private communications in the second case. These activities seek to create a state of fear and to influence people and organizations to self-censor their activities.

In the third case, during the year in question, the digital media published investigations related to various corruption cases involving the current government, which clearly has made several sectors that favor impunity uncomfortable. As a result, activities that amount to censorship, such as denial of service attacks against the website, prevent the public from accessing information that is of public interest.

In the fourth case, the elimination of all information on an organization's servers potentially was carried out to stop the organization from continuing its work. Files with sensitive and important information were deleted.

B.8. Safeguards

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 Constitution of the Republic governs the right to privacy, which establishes the inviolability of correspondence, documents and books, in any format, except as ordered in advance by a competent judge.

B.10. Possible penal classification

A 2015 investigation of the country's legal framework by Fundación Acceso[41] noted that the penal framework is still insufficient to establish integral safeguards to protect the right of digital privacy for human rights defenders.

In the case of information that was lost from a server, the Penal Code outlines in Article 274 "A" the crime of destruction of computer records, which results in a prison sentence and fine for anyone who illegally deletes or destroys computer records in any manner.

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

In the case of the screenshots that were leaked and disseminated, the conduct could be punished under the crime of unlawful interception or reproduction of communications as regulated by Article 219 of the Penal Code.

However, for the other crimes, current criminal legislation does not regulate the crimes of identity theft or web denial of service attacks.

B.11. Legal response strategies

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

Criminal complaints

Cases registered in Guatemala should be reported to the Public Prosecutor's Office, which is tasked with conducting criminal prosecutions. In other words, it is the justice agency in charge of investigating crimes committed against human rights defenders.

Other actions

Guatemala oversees at the constitutional level and at the general level the figure of ombudsman – more specifically the human rights ombudsman – where complaints can be filed over violations of fundamental rights and freedoms. This fulfills the role as guarantor that these rights are protected. However, the type of sanction this office imposes is of a moral character, because it's designed to be a tribunal of conscience, although it can file complaints with relevant jurisdictional bodies.

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 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.

B.12. 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 investigation by Fundación Acceso. 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.

2.Digital security incidents exist and they directly affect the work of human rights defenders, placing at risk their information, work and even their lives.

3.The issue of digital security continues to be absent from reports about the security of human rights defenders, causing areas of vulnerability through which they can be attacked.

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 on this issue within their own collectives.

3.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.

4.A national round table focused on analysis of the Internet and human rights called by


vzaa9VxK/EbHondurasgghOAGr2Ov9V
HlqVR
j86Z/sI
XlyjpbQioxwxvU1je
RXlyjpbQioxwxvU1jeZpj86Z/sI
HlqVRomqgghOAGr2Ov9V
j86Z/sIDhll vy5Wvrrs

C. HONDURAS CHAPTER

C.1. Legal Context: Internet and Human Rights in Honduras

In 2015, Fundación Acceso conducted an investigation titled, "Digital privacy for defenders of human rights?"[42] 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,[43] 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 included a collection of various legislative reforms, such as to the Penal 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. This 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[44] oppose the law because it lacks a focus on human rights.

Reforms were enacted to the Penal 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.[45] Reforms to the Penal 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.

42. 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

43. *Ibid.* P. 192.

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

45. 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

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.

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 surveilling 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.

Honduras has not yet initiated the process of elaborating a Cybersecurity Strategy.[46] However, the government has signed a cooperation agreement with the government of Israel to strengthen the National Investigation and Intelligence Office to implement a CERT[47] in the country.

C.2. Attack against 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.[48] Global Witness[49] 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.

46. El Heraldo. **16 Institutions to Be Protected from Cybercriminals in Honduras (Unas 16 instituciones serán protegidas de los cibercriminales en Honduras).** Available at: http://www.elheraldo.hn/pais/1115813-466/unas-16-instituciones-ser%C3%A1n-protegidas-de-los-cibercriminales-en-honduras

47. El Heraldo. **Israel to Equip Units that Combat Cybercrime in Honduras (Israel dotará de unidades en contra del cibercrimen en Honduras).** Disponibe en: http://www.elheraldo.hn/pais/1115476-466/israel-dotar%C3%A1-de-unidades-en-contra-del-cibercrimen-en-honduras

48. 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.

49. 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

In his reports, Michel Frost, 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."[50] 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.[51] The majority of these cases remain in impunity 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.[52] 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.[53]

In its annual report,[54] 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[55] has not been adequately enforced.

The State has invested more than 2 billion lempiras (some $85 million) on intelligence and spying activities,[56] targeting members of the political opposition under the banner of combatting crime. These intelligence activities include telephone wiretaps, malware attacks and tailing activists and

50. 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

51. *Ibid.* P. 5.

52. 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.

53. *Ibid.* P. 21.

54. 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/ PP.. 225-226.

55. 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

56. 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/

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[57] 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. [58]

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 June and November of 2017. For registration, a series of technical and legal tools was created to define the criteria used in registering digital incidents.

C.4. Registered cases

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

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

All eight cases involved university students and directors who were victims of the crime of theft. As a consequence, their personal information and digital accounts were compromised.

C.6. Types of attacks

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

The eight cases constituted the theft, robbery or pilfering of mobile telephones from different leaders of the Honduran student movement throughout the year and in different contexts. As an immediate result of these acts, the personal information, accounts and passwords of these eight people were compromised.

However, it is important to highlight that with today's wide use of smartphones, people store a large amount of information – in some cases sensitive data – ranging from contacts to photos. This information includes all types of documents and personal conversations. Therefore, the

57. 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

58. 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/

compromising of passwords, email accounts, social media accounts, and instant messaging is one of the biggest concerns.

C.7. Possible perpetrators

In some of the mobile phone thefts, the perpetrators of the digital security incidents were members of Honduras' National Police. In other cases, the devices were stolen during an assault, making identification of the perpetrator impossible.

C.8. Safeguards

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

The right to private property is constitutionally recognized. In the eight cases, the objects of the crimes were cellphones that comprise people's tangible items. As a direct consequence of these actions, the intimacy and privacy of communications were violated.

C.10. Possible penal classifications

In the registered cases, the act of theft of private property – in this case of cellphones – could be classified, according to the case and the specific circumstances, as crimes of robbery and theft as outlined by the Penal Code, articles 217 and 223, respectively.

C.11. Legal response strategies

Following are some of the legal mechanisms that could be implemented in response to the incidents registered by the Observatory:

Criminal complaints

For the cases registered in Honduras, the first step is to file a criminal complaint with the Public Prosecutor's Office to prompt an investigation of the crimes committed against the student human rights defenders.

Furthermore, 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.

C.12. 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. 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.

2. 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.

3.The threats directly faced by human rights defenders and independent journalists in the country range from physical to digital. The danger these workers 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.

4. 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.

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.


El Salvador

D. EL SALVADOR CHAPTER

D.1. Legal Context: Internet and Human Rights in El Salvador

In 2015, Fundación Acceso conducted an investigation titled, "Digital privacy for defenders of human rights?"[59] 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,[60] but current penal legislation does not protect the right to digital privacy.

However, since 2016, El Salvador has enacted the Special Law Against Computer and Related Crimes,[61] Decree No. 260. The law outlines several crimes including computer espionage, identity theft and the misuse of personal information, which to some extent protect digital privacy.

The Justice and Public Security Ministry currently is developing a national cybersecurity strategy, but it hasn't made the preliminary proposal public. The country has CSIRT and CERT[62] to respond to cyberattacks and to coordinate regional strategies.

In El Salvador, forums don't exist for dialogue among multiple sectors about the Internet and human rights. As a result, public discussion about everyone's right to online privacy, especially for human rights defenders, is scarce.

This leaves the country in an especially vulnerable situation, as these gaps in legislation and public policy make it more likely that these types of attacks, and the perpetrators of them whether they are companies or agents of the state, remain in impunity.

D.2. Attacks against human rights defenders

In its 2017 report on press freedom, Freedom House described El Salvador as partially free.[63] The report's methodology includes parameters such as the legal, political and economic climates that media outlets – including print, radio and digital media – carry out their work of informing the

59. 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

60. *Ibid.* P. 75.

61. El Salvador's Legislative Assembly. **Special Law Against Information and Related Crimes (Ley Especial contra los Delitos Informáticos y Conexos).** Available at: https://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-especial-contra-los-delitos-informaticos-y-conexos

62. Inter-American Development Bank and Organization of American States (2016). **Cybersecurity: Are We Prepared in Latin America and the Caribbean? (Ciberseguridad: ¿Estamos preparados en América Latina y El Caribe?)** Available at: https://publications.iadb.org/handle/11319/7449?locale-attribute=es& P.72,

63. 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.

public without fear of retaliation from private and political actors including members of organized crime. Despite El Salvador traditionally having low rates of violence against journalists, threats against media organizations has increased recently.[64]

In 2017, Factum Magazine was targeted by surveillance and intimidation after publishing a journalistic investigation of death squads in the elite national police units. This type of attack also was reported in 2015 by El Faro under similar circumstances (following a report about the national police).[65]

In its annual report,[66] Amnesty International reported the case of a human rights defender who faced a criminal process for libel and defamation brought by a private company. The case was prompted by statements the defender made about the environmental impact and deterioration caused by the company's project. The defender was cleared of all charges, but the company filed a procedural appeal of the verdict.

Human rights defenders, activists and members of independent media outlets also have been the target of threats, stigmatization, intimidation and aggression, and in some cases, government officials were involved.

Front Line Defenders also mentions in its 2017 report that several attacks have been reported against human rights defenders in El Salvador, particularly against women defenders and defenders of the LGBTQ community.

D.3. Main findings in El Salvador

Throughout 2017, Fundación Acceso did not register any digital security incidents among human rights defenders in El Salvador. The technician assigned to the country was initially contacted only twice. After attempting to reach out to those involved to learn more details about the possible digital security incidents, the technician was unable to reestablish contact with the human rights defenders.

64, *Ibid.* P. 21.

65, Revista Factum (2017). **Extermination: The Complicit State (Exterminio: El Estado cómplice).** Available at: http://revistafactum.com/exterminio-el-estado-complice/

66. 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. 173.

J4A1dbQioxwxvU

Nicaragua

aOv9VxK/Eb

gghOAGr2Ov9V

HlqVR

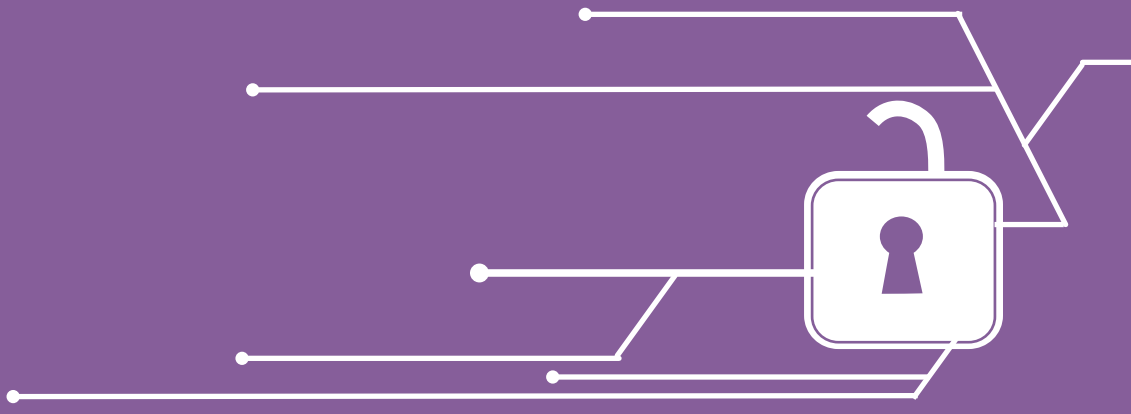
j86Z/sI

XlyjpbQioxwxvU1je

RXlyjpbQioxwxvU1jeZpj86Z/sI

HlqVRomqgghOAGr2Ov9V

j86Z/sIDhll vy5



E. NICARAGUA CHAPTER

E.1. Legal Context: Internet and Human Rights in Nicaragua

In 2015, Fundación Acceso conducted an investigation titled, "Digital privacy for defenders of human rights?"[67] 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,[68] 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 and surveilling 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.[69] 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.

67.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

68. *Ibid.* P. 260.

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

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.

E.2. Attacks against human rights defenders

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[70] 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,[71] 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).[72] 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[73] 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."

70. 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.

71. 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.

72. FIDH (2016) – I**nteroceanic 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

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

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 389 attacks against 202 defenders. Of those, 45 percent of the aggressors who were identified were government officials disguised as police.[74]

E.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 June and November 2017. For registration, a series of technical and legal tools was created to define the criteria used in registering digital incidents.

E.4. Registered cases

During the previously mentioned period, a total of **11** cases and security incidents were registered with different elements and motives in León, Managua, Matagalpa and Bilwi. Among them, five incidents were positively confirmed and six were determined to be false positives. In this section, we will discuss only the positively confirmed incidents.

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

The first case involved an organization that investigates the country's political and economic situation. The second case involved an organization that promotes social and cultural rights, focused primarily on the right to health and its relation to other issues. The third case involved a collective that demands respect for the rights of women in Nicaragua. The fourth case targeted a member of a collective that defends the rights of the LGBTQ community. In the fifth case, the victim asked to remain anonymous, so no general profile of the person or organization is available.

E.6. Types of attacks

Following is a brief description (not technical) of the registered attacks. First, the positive incidents will be described, followed by the false positives registered.

In the first incident against the organization that investigates the country's political and economic situation, the leaking of emails on a website was reported to Fundación Acceso. Beginning in early 2017, this website has been publishing defamatory content against some of the organizations in the country. It mainly leaks excerpts of emails from various organizations. On one hand, it is believed that the information was taken from a hard drive that was stolen from the organization

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

years ago. However, the publication of more recent emails has led some to believe that the emails are being leaked by someone from within the organization.

The second case, involving the organization that promotes the right to health, also is related to the previous case, as emails from one of the members of the organization also were published on the same website.

In the same context, the registered incident against the women's rights collective also involves defamation and leaked emails.

The fourth incident, targeting a member of a collective that defends the rights of the LGBTQ community, involves the systematic harassment of a former partner in which this person had remote access to the victim's mobile phone in order to harass and spy on them. In this case, in addition to remote access, the sending of threatening messages and vulgarities also was registered. As an immediate consequence of the remote access of the device, personal information, accounts and passwords were compromised.

The fifth incident refers to the theft of a device, and as an immediate consequence, the compromising of information, accounts and passwords of this person or organization.

E.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.

Only in the fourth incident was the possible perpetrator identified. In this case, the person was the former partner of the defender of the rights of the LGBTQ community. The objective was to exercise control and commit gender violence against this person.

E.8. Safeguards

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.

E.9. Possible human rights violated

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.

Additionally, the right to private property was violated as in one of the cases, the object of the crime was digital devices, which are tangible goods belonging to people.

E.10. Possible penal classifications

Based on the 2015 investigation by Fundación Acceso, 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.

Beyond the cases involving the theft or robbery of devices that had information belonging to people or an organization, robbery and theft are punished by articles 219, 220, 223, 224 and 225 of Nicaragua's Penal Code.

In the case involving harassment and threats by a former partner, the crimes committed were psychological violence and intimidation or threats against the woman, which are governed by articles 11 and 13 of the Integral Law Against Violence Toward Women.

E.11. Legal response strategies

Following are some of the legal mechanisms that could be implemented in response to the incidents registered by the Observatory:

Criminal complaints

For the cases registered in Nicaragua, a criminal complaint should be filed with the Public Prosecutor's Office to prompt an investigation of the crimes committed against the human rights defenders.

Constitutional actions

The writ 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, a writ could be attempted to safeguard this and other rights.

The writ 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.

Other actions

Nicaragua has the figure of an ombudsman, established formally as the Ombudsman for the Defense of Human Rights, to whom complaints can be filed involving violations of fundamental liberties and rights. The role of the ombudsman is to ensure that these rights are complied with. However, sanctions are of a moral character, as the office is designed to fulfill the role of a tribunal of conscience. It does, however, have the legal ability to file complaints with relevant jurisdictional bodies.

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.

E.12. Conclusions and Recommendations

Conclusions

1. Nicaragua lacks mechanisms for the physical and digital protection of human rights defenders. Equally, the absence of adequate legal frameworks to protect digital privacy, which were identified in the investigation by Fundación Acceso in 2015, persists.

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. The issue of digital security continues being left out of reports that address the security of human rights defenders, leaving areas of vulnerability through which they could be attacked.

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.

F. 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). T**oward 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 Cybercrime. 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). **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 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/

HlqVRomqggh
j86Z/sIDhll vy5

j86Z/sIDhll vy5WvrrskJ