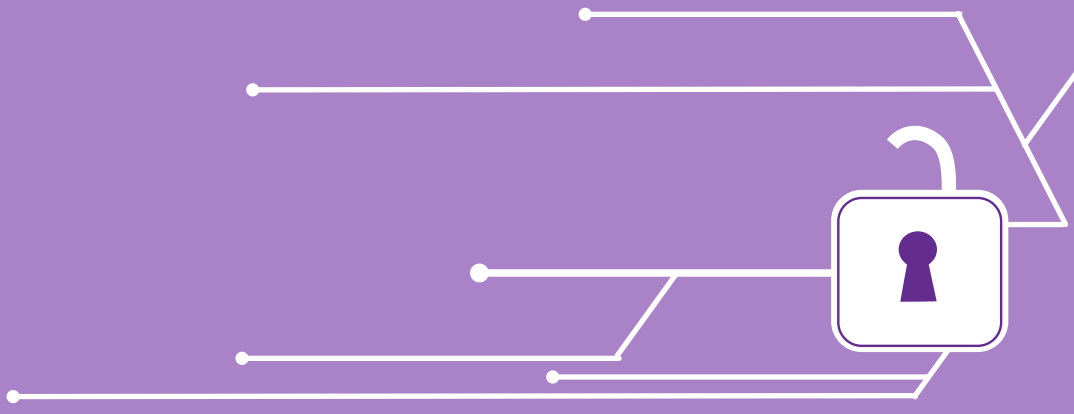
Central American Observatory for Digital Security

- Annual Report 2016 -

Nicaragua



HlqVRomqgghOAC
j86Z/sIDhll vy5Wvr

Central American Observatory for Digital Security

- Annual Report 2016 -

Nicaragua

Central American Observatory for Digital Security

Annual Report 2016

Nicaragua[1]

INTRODUCTION

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

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

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

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

a) What is a digital security incident?

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

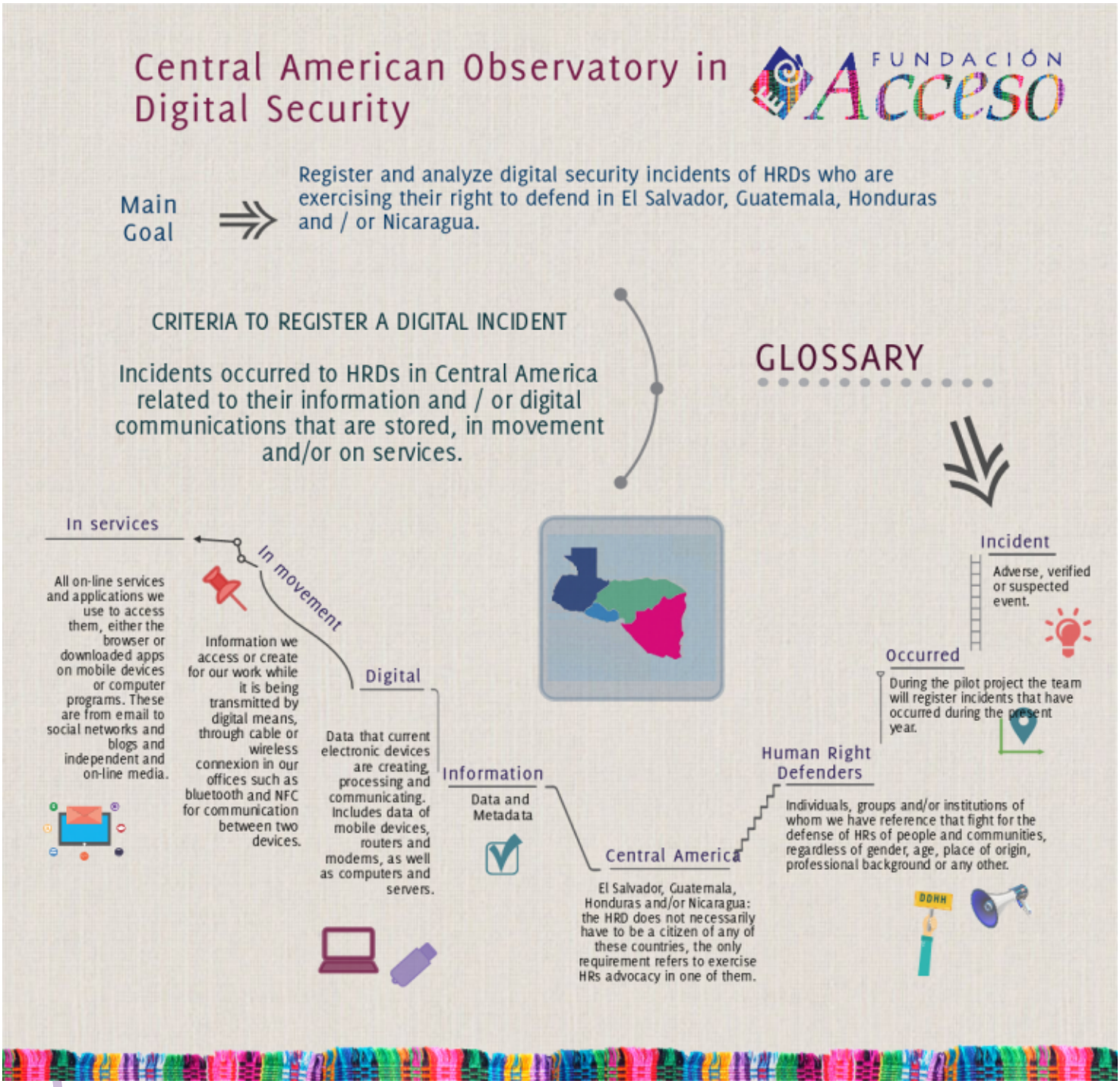
For human rights defenders, we use the broad concept defined by the United Nations[2], Declaration, including individuals, groups and institutions that are known to work in the defense of human rights in their villages and for the people of El Salvador, Guatemala, Honduras and/or Nicaragua, irrespective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

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

1. The Nicaragua chapter was compiled by in-country legal adviser Isbelia Ruiz Perdomo with support from technicians in the country and the Director of Organizational Development Luciana Peri.

2. United Nations, Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms. Available at: http://www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration_sp.pdf

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



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

b) Incident typology

Registered incidents are catalogued according to the following typology:

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

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

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

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

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

- **Web attacks:** Any attack on Internet services that we use and the monitoring of the same.

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

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

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

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

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

These can be blog or news services, our websites, blocking our YouTube channel or others, as well as monitoring our behavior based on the sites we visit.

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

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

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

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

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

Central American Observatory in Digital Security

Intervention Moments:

FUNDACIÓN Acceso

c) National context

Attack on human rights defenders

The human rights situation in Nicaragua in recent years has caused great concern among diverse national and international organizations. During 2016, the Inter-American Commission on Human Rights (IACHR) admonished the Nicaraguan government for several alarming situations. IACHR press releases, for example, expressed concern over cases of violence involving communal land conflicts and the failure by the government to protect indigenous communities in the northern Caribbean region.[10] The rights commission also expressed concern over the situation of institutional weakness across the country following the removal of opposition lawmakers in July 2016.[11]

In its 2015-2016 Annual Report, Amnesty International shared further details of the human rights situation, in addition to those shared in the IACHR press release, among them the persecution of human rights defenders:

> Human rights defenders, along with indigenous groups and Nicaraguans of African heritage faced threats and intimidation in retaliation for their work, particularly public protests. Some members of the news media and civil society organizations were victims of harassment. Several people died violently and hundreds were forcibly displaced as a consequence of intensified land conflict on the northern Caribbean coast. [...][12]

In a 2015 report, the Nicaraguan Human Rights Center (CENIDH) described a climate of persecution that human rights defenders confront:

> In Nicaragua, human rights defenders face a hostile environment characterized by threats, aggression, persecution, defamation and stigmatization because of the work they do. That environment impedes and makes difficult, according to each specific case, the exercise of the right to defend with necessary guarantees for their protection. It's even worse when government policy is focused on delegitimizing, disqualifying, attacking and criminalizing those who defend and promote human rights.[13]

At an Inter-American Court of Human Rights hearing in which allegations were presented in the case of María Luisa Acosta vs. Nicaragua (involving the failure of the State to investigate the assassination of Acosta's husband as a means to intimidate and halt the work of defending the rights of indigenous and Afro-Caribbean people in the Caribbean region), the Nicaraguan State alleged that the persecution of human rights defenders does not exist. Nevertheless, several

10. IACHR. "IACHR Urges Nicaragua to Protect Members of the Miskitu Indigenous Peoples." Press release 18/16, Feb. 23, 2016.
11. IACHR. "IACHR Expresses Concern over Removal of Opposition Legislators in Nicaragua." Press release 111/16, Aug. 8, 2016.
12. Amnesty International. 2015/2016 Report. Situation of human rights in the world. Page 323.
13. Nicaraguan Human Rights Center. 2015 Report, page 175.

human rights defenders have insisted that in Nicaragua they face persecution, threats and other actions that disrupt the work of human rights defenders.[14]

Digital Security and human rights defenders

Digital security and its defense are issues related to human rights that are not strongly positioned in Nicaragua, as is the case in the other countries of the region.[15] In the past year in Nicaragua, some cases related to possible incidents of digital privacy have been documented by social and news media. In the following, we present some of the cases compiled by news media and others as a result of investigation by the Central American Observatory for Digital Security for Nicaragua.

Radio Camoapa Case

Radio Camoapa is a communications media in the country's central region whose objective is to "promote the democratization of communications to benefit freedom of expression and contribute to equitable development and sustainability of the communities within the radio's reach."[16] As part of its journalistic work, the radio station broadcast a report related to the use of the municipal budget in Camoapa and administration of budgetary line items. During the radio program's broadcast, the municipality's IP was blocked, and according to witnesses, no one could access the website. Later, the radio station director reported that his email was hacked.

Elizabeth Romero Case

Elizabeth Romero is a journalist at the daily La Prensa[17] covering the public security beat. According to the Nicaraguan Human Rights Center, or CENIDH, "she is being subject to spying and harassment due to her journalistic coverage of armed groups operating in the country."[18] Romero's journalistic work has exposed the existence of armed groups in the north of the country. According to La Prensa, the journalist has been targeted by defamation and accusations on websites and Facebook.[19]

14. La Prensa, Oct. 11, 2016, "Government: In Nicaragua there is no persecution of human rights defenders." http://www.laprensa.com.ni/2016/10/11/nacionales/2115370-en-nicaragua-no-hay-persecucion-a-defensores-alega-gobierno. See also: La Prensa, Nov. 3, 2016, "Human rights defenders fear for their lives." http://www.laprensa.com.ni/2016/11/03/nacionales/2128164-defensores-de-derechos-humanos-temen-por-sus-vidas ; La Prensa, Aug. 30, 2016 "Human rights defenders denounce impunity and governmental silence." http://www.laprensa.com.ni/2016/08/30/nacionales/2091823-defensores-de-derechos-humanos-denuncian-impunidad-y-silencio-gubernamental

15. Fundación Acceso, *Digital Privacy for human rights defenders?*

16. Radio Camoapa. "Who are we?" http://www.radiocamoapa.com/quienes-somos/

17. La Prensa website: http://www.laprensa.com.ni/

18. In the following Nicaraguan Human Rights Center link, you can read the complaint filed by the journalist before this organization: http://www.cenidh.org/noticias/720/

19. La Prensa, Nov. 15, 2014: The intimidation of Elízabeth Romero. http://www.laprensa.com.ni/2014/11/15/editorial/217643-la-intimidacion-a-elizabeth-romero; Additional information on the case: La Prensa journalist Elizabeth Romero denounces "spying" [YouTube video] https://www.youtube.com/watch?v=2YTntZLtZKo La Prensa journalist Elizabeth Romero: Journalism, harassment and spying in Nicaragua, Elizabeth Romero, [YouTube video] https://www.youtube.com/watch?v=bipAjJH02zc La Prensa, Nov. 13, 2014, "LA PRENSA journalist denounces harassment and spying" http://www.laprensa.com.ni/2014/11/13/nacionales/1387565-periodista-de-la-prensa-denuncia-acoso-y-espionaje

Carlos Fernando Chamorro / Diario Confidencial Case

Journalist Carlos Fernando Chamorro, director of Confidencial magazine and the television programs “Esta Semana” (“This Week”) and “Esta Noche” (“Tonight”), reported that members of his editorial team were solicited by agents of the Nicaraguan army and political operatives from the governing party to leak information related to digital protection mechanisms within the office and registries of people who visit the office. The journalist publicly reported these interventions to the Nicaraguan Human Rights Center.[20]

20.La Prensa, Oct. 7, 2016 “Carlos Fernando Chamorro denounces intimidation and political spying” http://www.laprensa.com.ni/2016/10/07/nacionales/2113347-ntimidacion-y-espionaje-politico-por-operadores-politicos-y-del-ejercito-denuncia-en-cenidh-carlos-fernando-chamorro CENIDH, Oct. 7, 2016, “Confidencial and Esta Semana journalism team denounces spying and intimidation” http://www.cenidh.org/noticias/946/ El Nuevo Diario, Oct. 8, 2016, “Chamorro denounces alleged spying” http://www.elnuevodiario.com.ni/nacionales/406694-chamorro-denuncia-supuesto-espionaje/

1. MAIN FINDINGS IN NICARAGUA

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

1.1) Procedure for the registration of incidents

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

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

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

1.2) Registered cases

Although awareness of the Digital Security Observatory was spread to several important organizations that work to defend and promote rights, as well as to independent human rights activists, we did not manage to receive from connected organizations or activists complaints that entail digital security violations. This could be due to a lack of sufficient awareness by organizations and activists regarding the issue. One case was registered related to the destruction of computers at the Centro de la Mujer Acción Ya ("Action Now Center for Women") office in the city of Estelí in July 2016; however, this case was the result of contact with the organization by one of the Observatory's technicians.

a) Profile of people/organizations that reported incidents

Centro de la Mujer "Acción Ya." A space created by the civil foundation to support women in situations of violence. It was founded 15 years ago in Estelí, Nicaragua, in the context of the Women's autonomy movement, with the goal of promoting [h]ealth and [r]ights.21 This civil

society feminist organization promotes and provides assistance in legal and administrative processes for women who seek the Center's support.

b) Types of attacks

Initial contact was made with the organization by IT specialists from the observatory via a telephone call.

Acción Ya reported an illegal search, perpetrated in July 2016, in the organization's local office in Estelí, in which equipment (computers) was destroyed. However, when the IT specialist visited the scene of the crime, the destroyed equipment was no longer there because the organization had decided to get rid of it because "it no longer worked."

Once the organization Centro de la Mujer "Acción Ya" was contacted, the Digital Security Observatory visited the site that had been searched and the computers had been destroyed, along with network equipment and cables. Nevertheless, the evidence obtained did not permit technical expertise to be applied or to proceed to other stages of the intervention beyond the first technical visit.

The reported incidents could involve a **loss of hardware**. However, Observatory staff could not verify the type of damage to the computer equipment or if due to this damage, another type of attack could have been perpetrated, such as theft of the hard drives from the destroyed equipment. The reason is that the organization decided before the in situ visit by the technician to get rid of the destroyed equipment because it was no longer useable for the Center's work.

c) Possible perpetrators

The identity of the perpetrators is unknown. According to registered information, the Centro de la Mujer Acción Ya filed complaints against State agencies including the Ministry of the Family for alleged illegal adoptions. Members of the Center believe that the perpetrators could have been people linked to the State in order to block or delay legal and administrative processes.

2. PROTECTION MECHANISMS

In this section we present the legal framework that could have been violated in the case registered in the Nicaraguan chapter by the Central American Observatory for Digital Security.

2.1) Rights violations

a) Possible fundamental/human rights violated

Of the various incidents reported by the Centro de Mujeres Acción Ya, several represent fundamental rights violations. In terms of the illegal search of the residence, the right to the inviolability of the home established in Article 26.4 of the Nicaraguan Political Constitution. In terms of the loss of hardware, caused by the destruction of the computers, constitutional Article 44 was violated, which guarantees the right to private property and its inviolability. As stated previously, it is believed that the purpose of the search and destruction of the equipment was to obstruct the litigation work the organization carries out in courts to denounce irregularities in the process of adoptions against the Ministry of the Family, violating Article 52 of the Constitution that establishes the exercise of the right to petition to denounce anomalies to the powers of State: "Citizens have the right to file petitions, denounce anomalies and provide constructive criticism, in an individual or collective manner, to Powers of the State or any authority; to obtain a swift resolution or response and to receive notification of the result in periods established by law."

Also, the incidents described could be considered a form of violation to the right of freedom of association established by Article 49 of the constitutional text, as the acts committed affect the normal development of this citizens' association.

b) Possible penal classifications

Because the identity of the perpetrators is unknown, the types of crime could vary. If the illegal entry into the Center's office was committed by individuals, the Penal Code of the Republic, Law 641 from 2007 punishes the crime with a prison term of six months to one year for whoever remains or enters the offices of a legal entity; and this represents the crime of "invasion of residence" established in Article 200 of the same legal document. If the illegal entry into Acción Ya's offices was perpetrated by agents of the State without meeting the legal requirements to do so, Article 201 of the Penal Code classifies this conduct as an "illegal search," stipulating a sentence of three to five years in prison, plus barring them from public office for the same period of time.

The act of destroying the computers during a residency invasion is classified as a crime of "destruction," according to Article 243 of the Penal Code, which establishes prison terms of six months to two years. If three or more people caused the destruction, the criminal guidelines call

for prison terms of two to four years. In that case, the classification of the crime would be "aggravated destruction" (Art. 244, lit. h).

c) Possible administrative infractions

Because more details are unknown regarding the circumstances of the incidents or actions that occurred after the visit by an Observatory technician to the office of the searched organization, the concrete existence of administrative infractions cannot be determined.

2.2) Response strategies

In this section we present the different response strategies that can be implemented to address the case that was registered with the Observatory and prevent future digital security incidents from happening to human rights defenders.

a) Legal

- Criminal complaints

  For the acts described and compiled, a criminal complaint would be filed with the National Police or the Public Prosecutor's Office, according to the Penal Process Code, who should begin the process of investigation to determine the perpetrators of the acts against the organization.

b) Non-legal

Turning to civil society organizations that defend human rights in some situations would be effective in the country to help make visible patterns of aggression that target human rights organizations and activists as well as to pressure State entities to take action when confronted with situations like that of Acción Ya. Among these organizations are the Nicaraguan Human Rights and the Permanent Commission on Human Rights.

CONCLUSIONS AND RECOMMENDATIONS

Conclusions

1.Of the cases of context related to and beginning with the case documented by the Observatory, the presence of the Nicaraguan State and its agents can be noted in the perpetration of the incidents.

2.The incidents contextualized and registered in this report allow us to affirm that threats to digital security are being used to obstruct the free exercise of the work of defending rights, as well as to violate other rights such as the freedom of expression of journalists.

3.While the use of the digital environment to jeopardize the rights of human rights defenders and activists is evident, an awareness of denouncing these incidents still does not exist among these defenders in order to make known the threats they have experienced in terms of their digital security.

Recommendations

1.The organizations that defend human rights should document and denounce the digital security incidents they suffer, especially in the Nicaraguan case where the State or its agents seem to be using digital media to violate the rights of organizations, activists and other people who denounce or criticize the State, such as the case of journalists and media mentioned in this report.

2.The organizations that defend human rights should develop an awareness, mechanisms of warning and the denouncing of incidents that place at risk or violate their digital security.

BIBLIOGRAPHY

•Acción Ya: "What should we do?" http://accionyame.blogspot.com.ar/

•Amnesty International: 2015/2016 Report. The world's human rights situation.

•NIDH, Oct. 7, 2016, "Editorial team at Confidencial and Esta Semana report spying and intimidation" http://www.cenidh.org/noticias/946/

•Nicaraguan Human Rights Center: 2015 report.

•IACHR: "IACHR expresses concern over dismissal of opposition lawmakers in Nicaragua." Press release, 111/16, Aug. 8, 2016.

•IACHR: "IACHR urges Nicaragua to protect members of the Miskitu indigenous community." Press release, 18/16, Feb. 23, 2016.

•El Nuevo Diario, Oct. 8, 2016, "Chamorro denounces alleged spying." http://www.elnuevodiario.com.ni/nacionales/406694-chamorro-denuncia-supuesto-espionaje/

•Fundación Acceso: "Digital privacy for human rights defenders? A study of the legal framework in El Salvador, Guatemala, Honduras and Nicaragua that can be used for the protection, criminalization and/or digital surveillance of human rights defenders." San José, Costa Rica: 2015.

•http://www.laprensa.com.ni/2016/10/07/nacionales/2113347-ntimidacion-y-espionaje-politico-por-operadores-politicos-y-del-ejercito-denuncia-en-cenidh-carlos-fernando-chamorro

•La Prensa, Nov. 3, 2016, "Human rights defenders fear for their lives." http://www.laprensa.com.ni/2016/11/03/nacionales/2128164-defensores-de-derechos-humanos-temen-por-sus-vidas ;

•La Prensa, Oct. 7, 2016 "Carlos Fernando Chamorro denounces intimidation and political spying."

•La Prensa, Oct. 11, 2016, "Government: There is no persecution of human rights defenders in Nicaragua." http://www.laprensa.com.ni/2016/10/11/nacionales/2115370-en-nicaragua-no-hay-persecucion-a-defensores-alega-gobierno.

•La Prensa, Nov. 13, 2014, "LA PRENSA reporter denounces harassment and spying." http://www.laprensa.com.ni/2014/11/13/nacionales/1387565-periodista-de-la-prensa-denuncia-acoso-y-espionaje

•La Prensa, Nov. 15, 2014, Intimidation of Elízabeth Romero. http://www.laprensa.com.ni/2014/11/15/editorial/217643-la-intimidacion-a-elizabeth-romero

•La Prensa, Aug. 30, 2016, "Human rights defenders denounce impunity and government silence." http://www.laprensa.com.ni/2016/08/30/nacionales/2091823-defensores-de-derechos-humanos-denuncian-impunidad-y-silencio-gubernamental

•La Prensa Reporter, Elizabeth Romero, Journalism, harassment and spying in Nicaragua, Elizabeth Romero, [video youtube] https://www.youtube.com/watch?v=bipAjJH02zc

•La Prensa Reporter, Elizabeth Romero, denounces "spying" [video youtube] https://www.youtube.com/watch?v=2YTntZLtZKo

ioxwxvU

Eb

HlqVRomqggh
j86Z/sIDhll vy5

j86Z/sIDhll vy5Wvrrsk

FUNDACIÓN Acceso