MEMORANDUM FOR THE PRESIDENT OF THE UNITED MEXICAN STATES
ADDRESSING MEXICO'S CYBERCRIME
POLICY PROPOSAL FOR CARRYING OUT AN INFORMATION CAMPAIGN FOR
INCREASING AWARENESS ABOUT CYBERCRIME IN MEXICO

by
Iliana Araceli Briseño Angeles

A capstone project submitted to Johns Hopkins University in conformity with the
requirements for the degree of Master of Arts in Public Management

Baltimore, Maryland
December, 2014

TABLE OF CONTENTS

LIST OF FIGURES

I. ACTION FORCING EVENT

According to the 2013 Norton Report, illicit activities in the digital domain increased in Mexico during the year costing the economy three billion dollars. The average cost per victim increased from $197 to $238 dollars between 2012 and 2013.[1]

II. <u>STATEMENT OF THE PROBLEM</u>

In Mexico, cybercrime is growing rapidly, according to Ciro Humberto Ortiz Estrada, head of Mexico's Scientific Police Division.

The phenomenon of cybercrime has increasingly become a part of worldwide life in the last decade, yet there is not a clear definition of what constitutes cybercrime, either in Mexico or worldwide. The Budapest Convention states that cybercrime is any illicit activity that implies the use of a computer system on the Internet.[2] The Organization for Economic Cooperation and Development talks about computer–related crimes, defining them as any illegal, unethical or unauthorized behavior related to the automatic processing and the transmission of data.

In spite of the undecided definition of cybercrime, the use of the term is becoming more popular as the number of cybercrimes constantly grows. The most recurrent cases are: identity theft, malware, and child pornography. Identity theft is defined as the act of getting a person's identity information to commit fraud or other crimes; malware is defined as a set of malicious codes and programs including viruses, worms, spyware, bots

---

[1] Norton, Norton Report 2013. http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-data-sheet-mexico-es-mx.pdf . 2013. The Norton Report is a yearly research study, which looks at mindsets, consumers' online behaviors, security habits, and financial cost of cybercrime. It is one of the largest global studies of its kind.
[2] Michael A. Vatis. The Council of Europe Convention on Cybercrime. http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf. 6

and botnets, and child pornography is the commercial sexual exploitation of children on the internet.[3] In 2013, Jacobo Bello Joya, Coordinator of the Electronic Crime Unit of the Federal Police reported that the statistics of incidence of cybercrimes in Mexico were as follows: 41% identity theft, 54% of malware, and 5% is related to child pornography.

In 2012, criminal activities on the internet made an estimated $2 billion in Mexico, and saw an increase to $3 billion in 2013. According to the Organization of American States, throughout 2012 and 2013, cybercrimes have impacted more private and public institutions.[4]

In 2013, Mexico's Federal Police registered 23,543 cybercrime cases.[5] However, this number does not reflect accurate information of the cases of cybercrime, because many of them are not reported by the victims within the general public or small businesses.

Related to identity theft, a 2011 McAfee and CSIS Report stated that the most common thread was bringing down networks with distributed denial of service attacks (DDoS). This technique is of particular concern to Mexican banks. Banks lose as much as $93 million dollars each year due to this particular crime.

In terms of child pornography, Mexico is ranked as the top source of production and distribution of child pornography. It is a crime that is sourced, produced, and procured throughout the entire world.

---

[3] Alexander Seger, Identity theft and the Convention on Cybercrime, Italy 2007. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20UN%20id%20theft%20and%20CCC_en.pdf.
[4] Organization of American States and TREND Micro, Latin American and Caribbean Cybersecurity: Trends and Government Responses 2013, 17. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf
[5] Gustavo, Castillo Díaz, Ciberdelincuentes obtuvieron 3 mil mdd de pequeñas empresas durante 2013, La Jornada, 9 de abril 2014.

Different units to combat cyberthreats have been created by the Mexican government since 2000but as the levels of Internet penetration raised, the incidents have increased without a real mechanism of prevention or information about how to defeat or prevent these attacks. There is a need for a proposal to outline a roadmap for a comprehensive program of cybercrime which could fit in the National Digital Strategy of the National Development Plan (2013–2018), as presented by President Enrique Peña Nieto at the end 2012.[6]

Given previous failures to implement reforms to the law to address the growth of cybercrime in Mexico, and the lack of data from federal government to identify the extent of perpetration in the country, it is imperative to create new ways to raise awareness about the risks of theft on the Internet and diminish the likelihood of being a victim of delinquents.

III.   **HISTORY**

The growth of Internet use in Mexico had a significant increase from 5% –slightly more than 5 million users out of a total population of about 103 million in 2000– to 41%,[7] with approximately 50,923,060 Internet users in 2014. At the same time that the wireless connectivity generated economic transformations in Mexico, illicit cyber activities emerged as a new method of generating profit. Criminals obtained personal information of victims through several methods, including:

---

[6] Presidencia de la Republica. National Digital Strategy to transform Mexico. 2012 http://en.presidencia.gob.mx/national-digital-strategy-to-transform-mexico/
[7] Internet lives stats, Internet Users by Country. 2014. http://www.internetlivestats.com/internet-users-by-country/

- Softwares designed to collect personal information that can be secretly installed on personal computers or devices – fixed or mobile (i.e. malware).

- Deceptive e–mails or websites used to trick people into disclosing personal information (i.e. phishing –phishing e–mails are often mass–distributed via spam– more often those used to install malware on the computers of recipients).

- Computers or mobile devices that have been hacked to obtain personal data.[8]

Cybercrime's growth in Mexico. In 2006, the Cybercrime Police Unit received 1,229 complaints related to electronic commerce during that year. Six years later, there was an increased average of 670 complaints monthly for illegal behavior conducted through Internet,[9] seven times more than in 2006.

Mexico has been one of the countries most affected by cybercrime in Latin America in the last years.[10] According to the analysis of the security company ESET, Mexico went from 37th to 11th place globally in the incidence of illicit activities on the net perpetrated in 2013. The statistics obtained by ESET show that the number of lockscreen detections in Mexico has increased almost threefold compared to 2012.[11]

As shown in the map below, in 2012, Mexico occupied the second place after Brazil in allocating illicit activities in the digital domain, followed by Colombia in the third position. The number of victims at that time was 10 million in comparison to the 22

---

[8] OECD, Policy Guidance on online Identity theft, Seoul Korea, June 2008, p.3.
[9] Judith Pérez, Delinquen desde casa…en internet. La razón. Junio 1, 2013. http://www.razon.com.mx/spip.php?article174743
[10] Center for Strategic and International Studies and McAfee Report, Net Losses: estimating the global cost of cybercrime, June 2014. http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf. 8
[11] ESET Latin America's Research Team. Trends for 2014: "The Challenge of Internet Privacy", 2013. http://www.welivesecurity.com/wp-content/uploads/2013/12/Trends-for-2014.pdf. 25

million Brazilian people victimized in the same year. The percentage represents 25% of

the total number of Internet's users at that time; the number increased 50% the following

year.
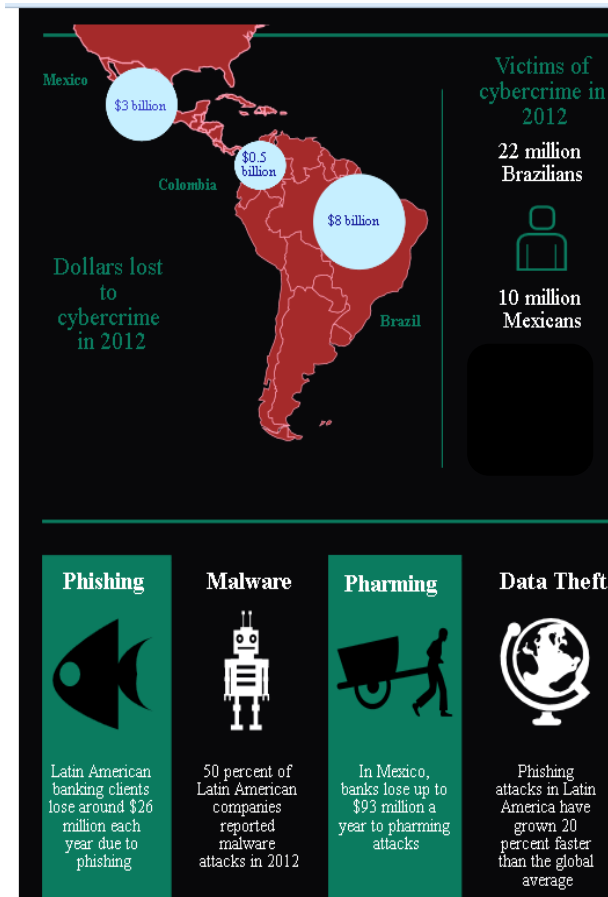
Source: Americas Society, Council of the Americas
http://www.as-coa.org/articles/infographic-cost-cybercrime-latin-america

Child pornography. Mexico is ranked as the top source countries producing and

distributing child pornography, although it is a crime that is sourced, produced and

procured the world over.[12] As for child pornography, from 2011 to 2013, Mexico jumped

---

[12] Global Initiative against Transnational Organized Crime, Stolen innocence: the online exploitation of children, http://www.globalinitiative.net/stolen-innocence-the-online-exploitation-of-children/

from third to first place as the world's number one distributor, and the second largest producer of child pornography, according to Mexican officials.[13]

The office of the Special Prosecutor for Crimes of Violence against Women and Human Trafficking (FEVIMTRA)[14] stated that the increase in the number of personal email accounts in Mexico disseminating pornography is rapidly growing. In 2010 Mexican authorities detected 580 accounts; it increased to 3000 in 2011. In the following year there were nearly 7000 more, and by 2013 more than 12 300 accounts were found.

Malware. In June 2013, Microsoft Security Intelligence Report recognized an increase of Malware and potentially unwanted software in Mexico. During the second quarter of 2013, the most common category was Worms. It was encountered in 17.7 percent of all computers inspected, up from 13.9 percent in the first quarter of 2013.

The second most common category was Miscellaneous Trojans. Trojans were found in 14.6 percent of all computers inspected, an increase of 11.9 percent compared to the first months of 2013. Finally, the third most common category was Trojan Downloaders & Droppers.

Costs generated by cybercrime. In 2013, the main incidents of cyber threats included: phishing, social engineering, and attacks targeting businesses through employees' personal devices. Small and medium size businesses were the most vulnerable to these attacks, since they do not have the sophisticated protection systems

---

[13] Marguerite Cawley, Mexico is world leader in child pornography: Officials, September 30 2013, http://www.insightcrime.org/news-briefs/mexico-is-world-leader-in-child-pornography

[14] París Martínez, México, primer lugar mundial en difusión de pornografía infantil, *Animal Político*, Junio 13, 2013, http://www.animalpolitico.com/2013/06/detectan-a-12-mil-300-pedofilos-mexicanos-que-operan-en-la-red/#ixzz371LPzrAd

that larger companies can afford, according to information reported by the head of Mexico's Scientific Police Division cybercrime in Mexico.

In these crimes, the criminals demanded payments –usually between $2,000 and $3,000 dollars– from the users to regain access to their systems. This kind of extortion is made by electronic transfer wires to national or foreign bank accounts.

In terms of child pornography, the Latin American and Caribbean Cybersecurity: Trends and Government Responses Report stated that in 2013 this activity generated an annual profit of more than 20 million of dollars in Mexico.

POLICY CHANGES IN MEXICO OVER TIME

First approach to combat illicit activities on the net. In 1999, the Mexican Congress approved the amendment to the Federal Criminal Code (federal legislation enforced across the country) proposed by President Ernesto Zedillo Ponce de León to include and punish criminal activities committed through the Internet.[15]

Creation of new institutions to combat cybercrime. In 2000, President Vicente Fox created the Cyber Police (part of Federal Preventive Police).[16] This police would be in charge to identify and dismantle organizations involved in identity theft, trafficking, and corruption of boys and girls. Some of its duties include:

- Identifying and monitoring the Internet to prevent criminal behavior.

---

[15] Francisco Iglesias, En México por lo menos hay 200 delitos informáticos tipificados: especialista, Octubre, 18, 2012. http://www.bsecure.com.mx/featured/en-mexico-por-lo-menos-hay-200-delitos-informaticos-tipificados-especialista/

[16] Sistema de Información Legislativa,Communications and transportation Commission in the Mexican Senate, Cybercrime in México, Mexican Senate, Abril 26, 2004. http://sil.gobernacion.gob.mx/Archivos/Documentos/2004/04/asun_979854_20040427_981312.pdf

- Managing cooperation with Internet service suppliers to neutralize sites and electronic pages that may harm public security, as well as preventing and fighting crimes in which electronic means are used.[17]

A year later, the Computer Emergency Response Team (CERT–MX) was created in order to augment government capabilities, to monitor and secure the federal government's digital assets, and to disseminate information and respond to network security incidents.[18]

In 2002, Vicente Fox's government created the Coordination Center for the Prevention of Electronic Crimes in response to the growth of cyber incidents. The center is responsible for managing cyber incident responses, investigating electronic crimes, analyzing digital evidence, protecting critical infrastructures, and responding to digital threats that would affect the integrity of critical networks.

In the same year, this unit identified and managed to remove around 200 sites of criminal organizations dealing with child pornography from the Internet. Said sites contained information, photography, films, or explicit sexual acts with boys and girls. In 2003, there was a daily average of 20 allegations related to pedophilia and child pornography, among others.[19]

Changing the legal framework. As the corruption of minors and promotion of child pornography increased, a new amendment was added in the Federal Criminal Law

---

[17] Consejo Nacional de Seguridad, Scientific Police Division. http://www.cns.gob.mx/portalWebApp/wlp.c?__c=7d1
[18] Cristos Velasco, The Legal Framework on Cybercrime and Law Enforcement in Mexico, Ciberdelincuencia. May, 2007. http://ciberdelincuencia.org/attachments/CristosMXContribution.pdf, 4.
[19] Ibid., 13.

these conducts also applied to online activities or through the use of networks, computer and electronic systems.

State level. Since the early 2000's, the Mexican government has been concerned about legislating on Cybercrime both at the federal and local levels. Sinaloa was the first state to typify user information protection.

States such as Baja California, Colima, Chiapas, State of Mexico, Durango, Guerrero, Jalisco Mexico City, Morelos, Nuevo León, Quintana Roo, Tabasco, Tamaulipas, Yucatan, and Zacatecas have included penalties in their various legislations to those who commit crimes through computer systems, such as fraud, forgery, corruption of minors, child pornography, kidnapping, revealing confidential information and indecent exposure.

Some states created their own local cyber police divisions. To this day twenty out of thirty two states already have these units, which work together with the Scientific Police Division cybercrime. The remaining states are already working to amend their local laws in order to create their own Cyber Police units.

The Calderon Administration. In response to the increase of illicit cyber activities, a new amendment presented by President Felipe Calderon Hinojosa was approved by the Congress in 2009. These modifications included: increasing prison sentences from a minimum of five to a maximum of ten years, instead of the previous two to eight years sentences, for state employees who obtained information from

Mexico's Platform[20] (Plataforma México). It also included fines from 1000 to 1500 days of the Mexican minimum wage –an approximate 5 dollars per day– to those that get information contained in computing and systems equipment related to the Public Security System.[21]

Still, according to Michel Rafael Estrada, head of the National Institute of Penal Sciences (INCP) in Mexico, and Maria Teresa Ambrosio at the Institute of Legal Research of the National Autonomous University of Mexico (UNAM), there are not enough regulations and laws that can prevent the occurrence of such cyber attacks. A very small number of misdemeanors are prosecuted.

Initiatives stalled in the Congress. Despite of the fact that the amendment to the Federal Criminal Code was supported by the majority of congressmen attending in the Chamber of Deputies (413 out of 500 members) in 1999, it has been difficult to incorporate a new typification of illicit activities in the digital domain into the Federal Criminal Code.

The main argument made by the Mexican Congress is that criminal activities on the net were already typified in the Federal Criminal Code. Even when comprehensive initiatives have been presented, problems in the digital domain not only remain

---

[20] Plataforma México is a set of databases in public security networks. http://www.ssp.gob.mx/portalWebApp/wlp.c;jsessionid=nyFRTspGkCNl4pG4ddHrBGf1D1hPbJt4ZtN5qP1NlBQKLwNyp1kf!-527600024?__c=105a

[21] Sistema de Información Legislativa, Que expide la Ley General del Sistema Nacional de Seguridad Pública y se adicionan diversos artículos del Código Penal Federal. Sistema de Información Legislativa, Octubre, 10 2008. http://sil.gobernacion.gob.mx/Busquedas/Avanzada/ResultadosBusquedaAvanzada.php?SID=7b136991d5dbfa1d8f0554a57afb4ce8&Serial=eae0d855515dc072d37f4caeb05fbaea&Reg=2&Origen=BA&Paginas=999#E2

unresolved, but have increased in the last years, affecting the integrity of institutions, citizens, and children.

Between 2001 and 2010, local Congresses and members of the national Congress have proposed some initiatives to reform the Federal Criminal Code and typify cybercrime in a better way; nonetheless, due to the complexity of the subject and the lack of data to support the problem, some of these regulations remain mired in Congress or were disapproved.

One of them is the amendment to the article 387 from Federal Criminal Code designed by Congressman Doring in 2009. This initiative punishes the misuse of any identification, password or bank PIN, as well as the use of any other identification document belonging to another person. The penalties for this illicit activity range from 3 days to 6 months of imprisonment, or fines from 30 to 180 days of minimum wage salary, when the value of the fraud does not exceed ten times the value of current minimum wage.

Another couple of initiatives were presented in 2011 and 2012 in the Senate. These initiatives amend the Federal Criminal Code that typify illegal activities against patrimonies or people's integrity such as fraud, extortion, child pornography, corruption of minors, and malware through networks, and on the Internet. These reforms were approved by the Senate on March 28, 2012 and sent to the Chamber of Deputies; nonetheless, said amendments were also stalled.

IV. BACKGROUND

Despite the multiple attempts to combat cybercrimes, they have been occurring more and more frequently. As the federal government has been implementing different strategies to combat these crimes, including new units created to address the problem not only at the federal level but also at the local level, and additionally the incorporation of illicit activities in the digital domain into the Federal Criminal Code, cybercrime is still running rampant.

In the next section, I will examine how the growth of illicit activities and the Internet penetration rates have impacted the economy of the country. I will explain the country's current strategies to combat these crimes in order to propose a new strategy to reduce the occurrence of cybercrime in the country.

More Internet users, more illicit activities on the Internet. The number of users who carry financial transactions, make use of government related services online, access networks and emails accounts, grows daily. More and more criminal and organized crime groups found the Internet to be an easy way to diversify their illicit activities. The bigger the number of Internet users, the bigger the number of possible victims of cybercrime.

In Mexico cybercrimes reached a peak in frequency of occurrences in 2012. The number of cyber incidents increased 40% according to the Latin American and Caribbean Cybersecurity Trends and Government Responses Report. The activities included the following: distributed denial–of–service (DDoS) attacks, defaced web pages, and carried

out cross–site scripting (XSS) and SQL injection attacks according to Mexican authorities.[22]

According to reports presented by specialists from the Organization of American States, during that same year Latino hackers developed a new cyber toolkit, PiceBOT, (malware programmed to steal financial information from Internet users). The kit included a malware that hackers could use to steal financial information from unsuspecting Internet users and target their bank accounts.

Experts believe that Latin America is a fertile ground for attacks because committing illicit cyber scams is far less costly than doing so in Europe or the United States. For instance, the creation of PiceBOT cost only $140 dollars, as it was most likely created in Peru, Mexico or Guatemala.[23] In fact, even though day–by–day more illicit activities in the digital domain are identified, over the last years these have not proportionately diminished.

The Growth of Internet users and demographics. The number of Internet users has grown considerably in the last years in Mexico, and it has stimulated the boom of illicit activities.

From 2006 to 2010 the penetration of Internet users grew an average of three percent annually. In 2006, Mexico had 20.2 million of users. Two years later it reached 27.6 million. Between 2010 and 2011, the growth was from 34.9 to 40.6%.

---

[22] Organization of American States, and TREND Micro, Latin American and Caribbean Cybersecurity Trends and Government Responses, 2013, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf, 11.
[23] Ibid., 14

On May 2014, the Mexican Association of Internet (AMIPCI) reported that from 2012 to 2013 the number of Internet users went up from 45.1 million to more than 50 million. The number of users is distributed by gender in equal proportions. From this figure, it was found that 57 percent of users are between 6 and 24 years old, 900,000 are under the age of 4, and 8.1 million are between 4 and 11 years. The age group between 12 and 18 years was estimated in 14.3 million.[24]

The multiple uses of Internet. (Job searching.) The Internet has become an essential tool to get a job among Mexican citizens. The 2013 survey from AMIPCI called "*Getting a job through the internet",* found that 63% of users were looking for a job on the Internet; while 58% of them had gotten their job through the net.

The number of bank transactions through the Internet rose in 2013 as well. For instance, 8 out of 10 users operated their banking accounts online, while 6 out of 10 made payments or transfers between their accounts on the Internet. The percentage of online shopping in Mexican websites also increased between 2012 and 2013, from 35 to 44 percent.

Government actions taken during the last two presidential terms (2006 to Present)

Felipe Calderon government. Consistent with the strategy of security led by the President Felipe Calderon Hinojosa, the National Program of Public Security (2008–2012) was launched during his mandate in response to the escalated violence in Mexico.

---

[24] Marisol Ramírez Olvera, Pequeños internautas, *El Universal*, Abril 2014.
http://www.eluniversal.com.mx/computacion-tecno/2014/ninos-tecnologia-nativos-digitales-87584.html

This program incorporated a paragraph establishing that the Ministry of Public Security would carry out workshops to prevent cybercrime countrywide. [25] Nevertheless, said workshops were almost imperceptible, since Calderon's administration made the war against drugs a top priority.[26]

As a consequence of Calderon's focus on drug war from 2006 to 2012 the Mexican government linked around sixty thousand homicides to organized crime. This violence occurred mainly along the central Pacific coast and in northern Mexico. It was increased as a result of the competition among cartels and from internal conflicts between criminal groups for the control of trafficking routes or "plazas" to the United States, and by the militarization on domestic public security.[27]

Regardless of this panorama of violence, the penetration of the Internet and the number of illicit activities increased without a realistic contention to prevent victimization or attain the detection of delinquents, because the security policy was focused on combating drug–trafficking and undermining the Mexican cartels.

Enrique Peña Nieto government. The strategy changed in 2012, when the Revolutionary Institutional Party won the presidential election. Mexico's security strategy was modified to adjust to Enrique Peña Nieto campaign promise to reduce the violence and protect citizens. These changes focused on reducing the violence that had erupted during the previous administration.

---

[25] Secretaria de Seguridad Publica, Programa Nacional de Seguridad Pública (2008-2012), p. 37. http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/414002//archivo
[26] Chistopher E. Wilson, Eric L. Olson et. al., New Ideas for a New Era: Policy options for the next stage in US-Mexico relations, Wilson Center, May 2013, p. 17.
[27] Shannon O´Neil, Two nations indivisible: Mexico and the United States 2013, Kindle edition.

The new strategy intended to adapt drug interdiction and the killing or capture of high–level drug traffickers, and redefine security strategy as a priority among security issues,[28] but not the predominating one.

As part of the new strategies, President Pena Nieto made the decision to increase the budget related to security. Important challenges for the government include prevention of crime and protection of users' data and devices from abuse. In that context, the budget for intelligence services increased from 200 to 580 million dollars for the 2013–2014 fiscal year.

The budget for intelligence was divided among institutions dedicated to preserve the integrity, stability, and permanency of the Mexican state. Some of their main concerns include the protection, preservation, and the upholding of the constitutional rights and the unity of the Mexican Federation.[29]

The Mexican National Development Plan 2013–2018. The Mexican National Development Plan 2013–2018[30] presented by President Enrique Peña Nieto specified that the Security Cabinet needed to increase funding to improve different areas of national security, such as communications security, weapons, training, land, air and sea vehicles, tactical teams, intelligence systems and cybersecurity. In the same regard, the National Development Plan states that crime prevention would be a central goal to public security.

---

[28] One Year after Enrique Peña Nieto's Election, Washington Office on Latin America, July 3rd 2013. http://www.wola.org/commentary/one_year_after_enrique_pena_nieto_s_election
[29] Mexican Constitution 2013. http://info4.juridicas.unam.mx/ijure/tcfed/9.htm?s
[30] Mexican National Development Plan 2013-2018 .2013. http://en.presidencia.gob.mx/national-development-plan-2013-2018/ p.9.

The National Security Program (2014 - 2018). The National Security Program (2014–2018) is the main rector of the security policy in Mexico. One of the main strategies is to develop a state policy on cybersecurity and cyber defense for protecting and promoting national interest and objectives. Its main actions are the following:

- Promote actions to prevent and combat cyber attacks.

- Strengthen mechanisms for preventing incidents in the federal executive sites.

- Promote compliance and development of procedures to evaluate and strengthen the performance of the response teams to incidents of cyber security in the federal executive branch.

- Improve human capital skills and technological infrastructure to address cyber security incidents.

- Establish international cooperation on cyber security and cyber defense to prevent and address attacks on the computer systems of the country.

The National Digital Strategy. As part of the new government actions, the "National Digital Strategy" was published in the Official Journal of the Federation, on May 3rd 2013 (Diario Oficial de la Federación, –DOF–).The Strategy sets out to tackle the challenges Mexico faces in the digital context, and the way it will cope with them through five objectives: government transformation, digital economy, quality education, universal, effective health, and public safety.[31]

It highlights that for achieving the goals of the strategy, it will be necessary for the government to analyze the legal framework surrounding issues such as: human rights protection, internet governance, information security and cybercrime.

---

[31] Ibid., 10

Agreement between the Mexican government and Microsoft. In May 2014, Microsoft and the Federal Police signed a business cooperation agreement to take actions against cybercrime, prevent illegal activities, and promote Internet security in Mexico. The statement was released by the National Security Commission (CNS). Enrique Galindo Ceballos, general commissioner of the Federal Police in Mexico announced that the coordination with Microsoft Mexico was aiming to reduce the digital gap to place it at the forefront, furthermore to promoting Internet security in Mexico.

The Budapest Convention. The government announced its adhesion to the Budapest Convention[32] which seeks to combat crimes on the Internet through April 2014. Its mains actions are the following:

- Harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber–crime.

- Providing domestic criminal procedural law enforces the powers necessary to investigate and prosecute such offences as well as other offences committed by means of a computer system.

- Setting up a fast and effective regime of international co–operation.[33]

In terms of cybercrime, both the adhesion to Budapest Convention, and the agreement with Microsoft represent significant advances. On the one hand, Budapest Convention will help to improve national capabilities for investigating such crimes, and

---

[32] José Antonio Belmont, México se adhiere al Convenio de Budapest, Abril 3, 2014. http://www.milenio.com/policia/Cibercriminalidad-Mexico-adhiere-Convenio_de_Budapest-PGR-delitos_informaticos-delitos_en_internet_0_274173006.html
[33] Council of Europe, Convention on Cybercrime p 1. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

increase cooperation on investigations. On the other hand, Microsoft will help the Federal Police to understand and manage diverse tools to prevent illicit activities on the net.

The agreement and the National Digital Strategy are important steps to move forward to raising penetration on the Internet in Mexico and improving skills and technological infrastructure to address cyber security incidents. However, as cybercrimes have increased in the last years, it is important the raise knowledge and awareness about these incidents through a culture on prevention in order to avoid more Internet users being victimized.

Process to reduce cybercrime

The Mexican system has multiple actors at different levels, and multiple interactions among them. To achieve an effective strategy to fight those illicit activities in Mexico through an information campaign, it is important to take into account the importance of the following main players.

Principal stakeholders and their responsibilities

Executive Branch. According to article 21 in the Mexican Constitution, the federal government will be in charge of public security in accordance to the distribution of jurisdictions established in the Constitution. Regarding this article, the Federal Police and FEVIMTRA are the government agencies (as Mexican security institutions) in charge of developing public policies related to a culture of prevention as well as evaluating the effectiveness of said policies.

The National Statistical and Geographic Information System (INEGI) according to article 26 in the Mexican Constitution establishes that this will be the public agency with technical and management autonomy responsible for producing, coordinating, and disseminating statistical and geographical information of national interest.

The General Directorate of Cinematography, Radio and Television (Dirección General de Radio Televisión y Cinematografía –RTC–) –conferring to the article 34th in the Internal Regulations of the Ministry of Interior– holds the responsibilities to regulate spaces available to the Mexican State in radio and broadcast television to spread messages to the population without any cost. This right is stipulated in the Radio and Television Law, article 59th.

Congress. Members from the following political parties are important pieces in building an information campaign, in cooperation with the Executive and Legislative branches. According to article 59th in the Radio and Television Law the Executive and the Congress can promote and disseminate information through media. They have 18 minutes on television and radio 35 minutes daily for the dissemination of campaigns.

- National Action Party (Partido Acción Nacional PAN),

- Democratic Revolution Party (Partido de la Revolución Democrática PRD),

- Ecologist Green Party (Partido Verde Ecologista de México, PVEM),

- Revolucionary Institutional Party (Partido Revolucionario Institucional PRI).

To decrease the number of cybercrimes in Mexico Analysts of the Organization of American States indicated in April 2014 that policymakers in Mexico face the following challenges in terms of cybercrime:

20

✓ Lack of Law enforcement against cybercriminals

✓ Lack of prevention, and awareness by Internet users

My proposal seeks to apply the latter point.

V. POLICY PROPOSAL

There is a wide range of illicit activities in the digital domain. The number of crimes is growing more and more by the day. For the purpose of this campaign, we will focus on three major issues that have been terribly recurrent in Mexico. These are identity theft, malware or child pornography which have increased in the last few years in Mexico, provoking an economic cost of three billion dollars on private sector, Internet users as well as damage to under–age users and those who lack the sound judgment to make decisions on their own.

While developing programs to combat and promote the culture of crime prevention is a government–wide mission, the current actions have neither combated crime nor generated awareness about the risk of illicit activities on the Internet.

Under this proposal the Mexican government would put in place a campaign to disseminate information about illicit activities on the Internet. The information campaign will broadcast images and messages related to illicit cyber activities and the risks of becoming a victim. These would include spots on television, radio and on the Internet. This proposal would be included as part of the annual federal campaign implemented by the Federal Police and the FEVIMTRA.

The presented proposal principally contains and explains the following elements: specific goal, target audience, campaign period, media used during the campaign, budget proposal, work plan and campaign break down based on Curt Lewin's theory of change, and law framework.

The proposal of the campaign "Keep safe on the internet" will be managing, developing, and sending the proposal and a plan to promote awareness among Internet users about ways to protect themselves from becoming victims by the Federal Police and FEVIMTRA. The INEGI will develop and distribute three surveys to evaluate effectiveness.

The government agencies in charge will carry out meetings to learn about the media campaign progress. They will present programs, strategies, messages costs concerning spots, and proposal to dissemination information to the Ministry of Interior. Additionally, reports will be presented to the Ministry of Interior, and said advances will be integrated in the State of Affairs Report 2015, 2016, and 2017.

The information campaign will promote preventive measures of victimization risks on the Internet. Within the population at risk, three different target audiences should be clearly identified. Vulnerable users include:

- Underage users and those who lack the sound judgment to make decisions on their own
- Corporate and public employees who may have access to confidential or privileged information
- All other users of Internet services

The campaign will have a duration of 35 months on radio and television, taking into account designing, organizing, and recording of advertisements. The broadcasting of

the spots in radio and television will not have any cost since the Federal Government has

the right to disseminate information related to advertising, programs or achievements.[34]

The Federal Police and FEVIMTRA websites, as Twitter and Facebook will serve

as an important vehicle for pointing constituent's information about preventive measures

and the risks of becoming victims. With frequent exposure to these spots, the population

will become aware of the information and will take more educated decisions when

making use of Internet websites. Increased public awareness represent an important

strategy in the prevention on any these crimes.

On budgets, the cost of each spot will be approximated million dollars. The

information campaign will have more than three spots to better disseminate information

and target the different age groups. This average information campaign cost was

calculated according to how much the federal government spent on campaigns in 2013.[35]

Based on Curt Lewin's theory of change, campaigns break down as follows:

First stage or Unfreezing. In this first stage, the INEGI will create and carry out a series

of surveys in order to evaluate the base level of awareness concerning illicit activities on

the net in Mexico among constituents.

The three surveys created by INEGI will address these specific functions.

1. **Baseline survey**: the first survey will evaluate the level of awareness concerning

   cybercrime in Mexico among the population; this will be distributed before the

---

[34] Secretaría de Hacienda y Crédito Público. Acuerdo por el que se publican las reglas de operación para el pago de impuestos de los concesionarios de radio y televisión. Diario Oficial de la Federación. Octubre 10, 2002.

[35]RedaccAnimal Político¿Quién hizo y cuánto costó la campaña Mover a México? (Who and how much did the *Moving Mexico* campaign cost?), *Animal Político*, Julio 9, 2013. http://www.animalpolitico.com/2013/07/quien-hizo-y-cuanto-costaron-los-spots-de-presidencia/

launching of the campaign. The data from this first survey will be use as the baseline later to measure the effectiveness of the campaign.

2. **Follow-up survey:** The second survey will intend to evaluate the progress of the policy implemented.

3. **Evaluation survey:** The last one will evaluate the impact of awareness concerning illicit activities on the Internet.

The data from the three different surveys will be compared and contrasted to better evaluate the effectiveness of the campaign. It will also be used to create new possible approaches. Because INEGI is the organization in charge of the statistical evaluation, it will be in charge of deciding the size of the population that will statically represent the whole country and it will also be in charge of creating a randomized selection of participants.

Federal agencies will analyze the results in order to articulate the importance of changing current behaviors. These messages should show the economic and social damages generated by illicit activities on the Internet in Mexican society. Messages must explain the main methods of victimization and the consequences as well as create the need for changing current attitudes.

Campaign Slogan: "Keep safe on the internet".

This first step will be focused on broadcasting economic and social damages. This will have a duration of twelve months.

Second stage or Transition. Federal agencies will broadcast the benefits of awareness of illicit activities in the digital domain, and how important complaints will be in order to put criminals in jail. This process would be the most significant period.

In this stage, reinforced support from stakeholders and interest groups will help to sustain the transition. The INEGI will carry out a second survey in order to evaluate the level of reception related to illicit activities on the net in Mexico and prevent measures on the Internet.

This second stage will have a duration of twelve months.

Third stage or Freezing. After disseminating information about how illicit activities on the net affect Mexican society, it will be time to internalize said information, through the broadcasting of a guide to keep safe on the Internet. This guide must have between five and ten recommendations on how individual can safely use the Internet. Finally, in this stage, INEGI will carry out a third survey in order to evaluate the level of awareness concerning illicit activities on the net in Mexico, and make sure that people have incorporated said information into everyday life.

The implementation for the plan will start on January 31, 2015, and will finish on December 31, 2017.

Law framework. The components of this campaign are completely supported by the law. It has also been thoroughly analyzed to assure the alignments to the constitutions rights and law for each component involved, as explained below.

Use of propaganda and media. According to the Mexican Constitution, article 134 establishes that propaganda that will be disseminated on any media from governments, agencies and public administration entities or any other entity of the three levels of government must take institutional and informational, educational or social orientation purposes. The propaganda should not include names, images, voices or symbols that imply personalized promotion of any public servant.

The National Development Plan 2013-2018. The National development Plan identifies as its second transversal strategy for national development, promoting mechanisms to improve their performance and quality of services; simplify regulations and governmental procedures and clearly accountable to citizens and timely manner.

The Ministry of the Interior. In terms of Article 27, Section XXXIX of the Organic Law of the Federal Government, the Ministry of the interior is responsible for developing, regulating, and conducting social communication policy of the Federal Government. It is in charge of coordinating, monitoring, and evaluating federal institutions' social communication programs.

Use of radio, television and internet for federal purposes. The article 38 Budget and Fiscal Responsibility law establishes that the Interior Ministry will approve both, campaigns and annual broadcast budget spending.

Federal Police and FEVIMTRA will develop their own campaign strategies and send it to the Directorate General of Norms and Communications (DGNC) from the Interior Ministry before January 31, as stipulated by the agreement of the federal government advertising campaigns for government.

VI. POLICY ANALYSIS — DISADVANTAGES

To begin with, there is a challenge in carrying out an information campaign to make Internet users aware of criminal activities on the net. First, there is a defiance related to priority concerns by Mexican consumers (i.e.: economic issues). Second, in terms of impact the campaign would be facing a challenge to reach its goal. Finally, in relation to enforcement tools for punishing criminal activities perpetrated through the net.

PRIORITIES FOR MEXICANS

Economic concerns. Prior to Peña Nieto's government the main concern for Mexicans was security, as a consequence of the wave of violence in the country.

Nevertheless, in August 2014, according to Buendia y Laredo survey, the issue that topped the list with the three most important priorities for Mexicans was economy followed by security, and politics.[36]

In the same way, the Pew Research Center survey showed that two out of three interviewees were displeased with the way things are going in Mexico in relation to economic issues. Majorities in all regions of Mexico conveyed displeasure, though those in the South (73% dissatisfied) and the federal district of Mexico City (78%) are especially disgruntled. Residents of urban areas (71%) are also particularly frustrated.[37]

Given that Internet security is not a major concern for Mexicans, the campaign may not be effective.

---

[36] Buendia y Laredo, August 2014. http://www.eluniversal.com.mx/nacion-mexico/2014/empleo-la-prioridad-para-mexicanos--1032800.html
[37] Pew Research Center. Mexican President Peña Nieto's Ratings Slip with Economic Reform. August 26, 2014. http://www.pewglobal.org/2014/08/26/mexican-president-pena-nietos-ratings-slip-with-economic-reform/

State media airtime yields. State´s media airtime yields could potentially have a lower impact to make a change in behavior among Internet users, due to the fact that the information campaign will be broadcast under the Ministry of Finance agreement.

According to said agreement, the State will be able to broadcast information only 18 and 35 minutes daily on television and radio, respectively. The schedules to broadcast spots are decided by the concessionaries, not by the government. This means that the government could schedule daily spots, but concessionaries can decide to not schedule them, or to broadcast them outside of primetime.

Finally, given the dependence on this arrangement, there is a high likelihood that its main goal of increasing among people knowledge and awareness about given activities would fail. Because the State media´s airtime must be shared among the executive, the legislative and judicial branches, de–concentrated and decentralized units, there is considerable competition for a limited number of slots.

Enforcement tools. Even when the Federal Criminal Code included different kind of penalties for criminals who perpetrated computer-systems, the rate of complaints and prosecutions for these of crimes is still low. The lack of unified procedures and methods of prosecution could open a window to criticize the federal government for running a campaign without the enforcement necessary to combat the problem.

New approaches. Regarding the concern level of Internet security in Mexico, the campaign should raise the knowledge and awareness through a complementary approach. Stakeholders at national and international level have suggested, and pointed out that partnership and teamwork are one of the best ways to develop effective policies.[38]

---

[38] Organisation for Economic Co-operation and Development. Cybersecurity policy making at a turning point. 2012. 13. http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

The agreement between the federal government and Microsoft would help to raise the concern level regarding internet security. If both the federal government, and Microsoft work together in broadcasting information about the problem, and at the same time involving more corporations as Google, Norton as well as public and private institutions.

In the same regard, a report from the IBM Center reaches a new approach, in order to redefine the relationship between citizens and government in problem-solving. This report identifies four distinct roles for citizens in public services co-creation and problem solving: as explorers, as ideators, as designers and as diffusers.

As explorers, citizens can identify/discover and define emerging and existing problems. As ideators, citizens can conceptualize novel solutions to well-defined problems. As designers, citizens can design and/or develop implementable solutions to well-defined problems. Finally, as diffusers, citizens can directly support or facilitate the adoption and diffusion of public.[39]

If the campaign involves the target audience into the campaign in one of said roles, it would probably help to raise awareness among them, since they will be part of the problem, and the solution. Although, this approach would implicate more budget, research, and as a new approach, there is a high risk that it may not work.

VII. POLICY ANALYSIS — ADVANTAGES

Increase knowledge and awareness through an information campaign may be a reasonable communication tool. Currently, diverse facts increase the feasibility of the

---

[39] IBM Center for the Business of Government, Engaging Citizens in Co-Creation in Public Services: Lessons Learned and Best Practices, 2013.
file:///C:/Users/Iliana/Downloads/Engaging%20Citizens%20in%20Co-Creation%20in%20Public%20Service%20(1).pdf

proposal. On the one hand, the growth of users and their concern for Internet security in Mexico. On the other hand, the constant progress of the use of Internet as both, social media and a new way of purchasing goods.

Information sources. Since the campaign will be broadcasted on television and the radio principally, it will be important to consider, if Mexicans are able to get information from these sources and how frequently they do.

In that case, the polling data by the INEGI shows that 94.9% of population in Mexico owns a TV set.[40] In this regard, the most recently World Values Survey (WVS) shows that daily the principal information source for Mexican people is television news followed by the radio news.

The information campaign would have a high impact in a large number of Mexican consumers, since the principal information source for the majority of Mexicans is television followed by radio. These are the principal media where the campaign will be carried out.

In view of the fact that the principal information source for the Mexican population is television and radio, disseminating warning information related to illicit activities on the Internet through commercials on television, and on the radio, could reduce the risks of being victimized, as well as shrinking the economic cost generated so far by criminals on the net.

Economic impact of the Internet. The Internet in Mexico is Latin America's second largest online retail market (after Brazil). As more Mexicans obtain Internet

---

[40] INEGI, Reporte sobre el número de usuarios de Internet en México, 2012. http://www.inegi.gob.mx/est/contenidos/espanol/temas/Sociodem/notatinf212.asp

access, online sales are projected to nearly triple to $4.4 billion by 2016.[41] The

workability of the proposal could have economic impact among both vulnerable and

aware users because it would motivate the use of Internet as a tool of consumption and

payments, but it could also help to prevent them to be victimized by criminals on the net.
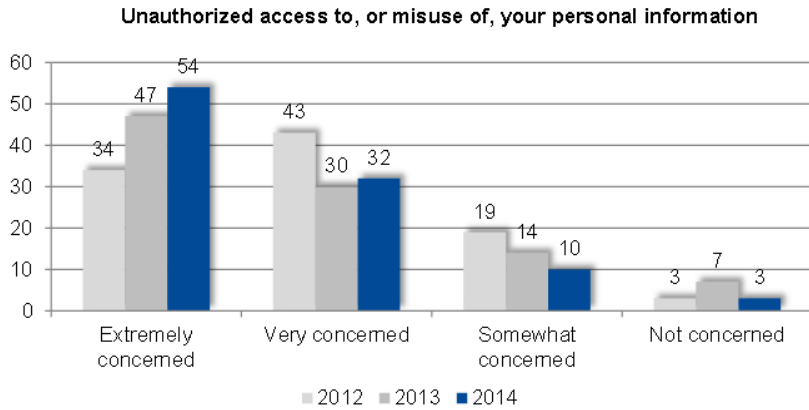
Growth of identity theft concerns. One the principal concerns for Mexican

people has been security since drug trafficking perpetrated, and increased the violence in

the nation. However, as the use of the Internet has boosted in the last years, concerns

related to personal safety involve identity theft as is mentioned in the Unisys Security

Index 2014.[42]

The graph below shows that in 2012, only 34 percent of the Mexican were

concerned about using unauthorized access to, or misusing personal information,

nonetheless two years later, this percentage increased twenty points. As the same graph

shows during the first semester in 2014, a total of 86% Mexicans are both, extremely

concerned and very concerned about these threats, not so far from previous years, but

increasing nine points perceptual from 2012-2013 to 2014.

---

[41] AT Kearney Consulting Firm, Kearney´s E-Commerce Index, June, 2012.
http://www.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/e-commerce-is-the-next-frontier-in-global-expansion/10192#sthash.tdyCoxp7.dpuf
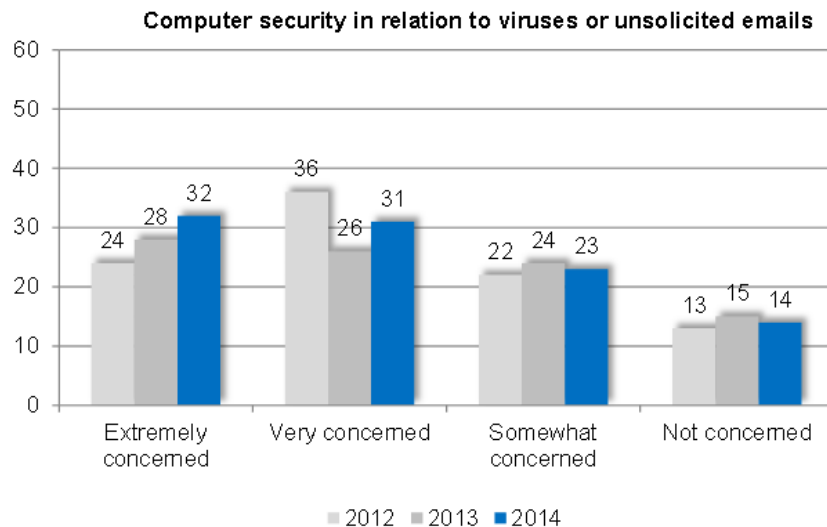[42] It is conducted by leading marketing research company Lieberman Research Group, the Unisys
Security Index provides a regular, statistically robust measure of concerns about eight areas of security.

Unauthorized access to, or misuse of, your personal information

Source: Unisys Security Index: MEXICO
http://www.unisyssecurityindex.com/system/reports/uploads/304/original/Unisys%20Security%20
Index%20Mexico%20May%202014.pdf?1399943793

The same Index indicates that Mexican consumers are now more concerned about
Internet security. As the figure below shows, more Mexicans are aware and concerned
about computer security. For example, the total between extremely concerned and very
concerned about computer security boosted nine points from 2013 to the first semester in
2014.

Computer security in relation to viruses or unsolicited emails

Source: Unisys Security Index: MEXICO
http://www.unisyssecurityindex.com/system/reports/uploads/304/original/Unisys%20Security%20
Index%20Mexico%20May%202014.pdf?1399943793

Campaign cost. The INEGI will be in charge of creating and carrying out surveys. The Federal Police and FEVIMTRA will be in charge of managing and developing the proposal and a plan to promote awareness on criminal activities on the net.

Since the federal government does not have publicity agencies, it will hire one agency in order to record the spots. Said activities will probably cost around three million dollars, in such case three spots will be recorded, under those circumstances, the cost for spots records would mean 0.01% of total economic cost that criminal activities on the Internet gained during 2013.

Disseminate information. The Mexican Federal Government has the right to broadcast public interest information including advertising, programs or achievements on radio and television without any cost.[43] As a result of the agreement that authorizes the Ministry of Finance (SHCP Secretaría de Hacienda y Crédito Público) to receive from radio and television concessionaries time on the media, the information campaign will not generate any additional cost for broadcasting the information.

---

[43] Secretaría de Hacienda y Crédito Público. Acuerdo por el que se publican las reglas de operación para el pago de impuestos de los concesionarios de radio y televisión. Diario Oficial de la Federación. Octubre 10, 2002.

VIII. POLITICAL ANALYSIS

As the information campaign will be part of activities related to the prevention of criminal activities, and will consequently be based on the National Security Plan, incorporating it into the national agenda would not represent a political risk insomuch as it will encourage awareness for Internet users.

The information campaign is a preventive and informative measure to combat cybercrime in Mexico. Thus it will not implicate questionability or contrary arguments by the opposition and principal political parties.

Since the proposal will be launched in 2015, it is important to consider that in July 2015, Mexico will be addressing the midterm elections. Nine Mexican states will be electing governors; seventeen states will elect local Congress and majors, as well as the members of the Chamber of Deputies will be renewed.[44]

As a consequence of the midterm elections the political dynamics will be split into competing factions, which are likely to include critical missions against the federal government to get the best ballot box results for each political party. The information campaign could open a window for criticism and denounce by political parties for using the State media´s airtime as propaganda not as public action to solve a public problem.

One more social factor is the Ayotzinapa case. At the present time, the problem related to 43 students disappearing from Ayotzinapa, Guerrero has generated alarm among the population for the possible involvement of the police, and because the students were not criminals. This case has generated a series of clashes among demonstrators and the police, as well as demonstrations nationwide and out of the country where Mexicans

---

[44] Instituto Nacional Electoral. Calendario Electoral 2015. http://www.ine.mx/docs/IFE-v2/DECEYEC/DECEYEC-ProcesosElectorales/Calendario-Docs/ISU_Cal_Elect-2015.pdf

are currently residing. Academic institutions, social media, stakeholders and general

public have reached a social indignation across the country and certainly without

precedent in recent decades. [45]

Launching a campaign cannot be taken lightly. After two months, the

Ayotzinapa´s case still does not have a clear solution. Launching a campaign would be a

risk not only for being criticized by the general public, and by political parties and

Congressmen, but the campaign also would not generate its principal goal, raise

knowledge among Internet users about illicit activities on the net.

Another factor in evaluating the proposal is the federal government low approval

ratings (particularly on economics terms). The Mitofsky survey found, that 42.2 percent

of midterm votes would be for the Revolutionary Institutional Party (Partido

Revolucionario Institucional PRI). Whereby, it is not possible to ignore the fact that there

is still a pending agenda in relation to economic issues.[46]

If the information campaign does have the criticism instead of support of political

parties will be difficult to get across new negotiations and cooperative actions among the

Executive and Legislative branches. At the same time, the result of midterm elections

will have no positive effect for the PRI, and the campaign goal would be diminished by

the effects of these events.

[45] Enrique Krauze. Mexico's Barbarous Tragedy. The New York Times. November 10, 2014.
http://www.nytimes.com/2014/11/10/opinion/enrique-krauze-mexicos-barbarous-tragedy.html

[46] Consulta Mitosfky. Porcentajes de votación para el año 2015. El Universal. Agosto 9, 2014.

IX. RECOMMENDATION

The growing use of the Internet has fostered a range of new criminal activities. The federal government has been able to convey a sense of urgency that would allow for a need for change. Users and general public are not yet aware of the risk posed by cybercrime. The use of communication tools such as information campaigns to raise awareness is a feasible solution.

After analyzing the ups and downs, cons and pros of the proposed campaign, I do recommend implementation and execution of the "Keep safe of the internet" campaign to protect internet user from becoming victims of cybercrime. Advice to Internet' users on cybercrime risks could mitigate the damage against them. As more Mexicans get Internet access the risk of becoming a victim of online predators could increase against consumers, campaigns as this could lower the risks.

Although, the information campaign would not eradicate the hazard of being a victim on the Internet, it could help to provide information about how people have been victimized and what they can do to avoid it. The information campaign among Internet´s users could also spur the development of new technologies and the use of new approaches such as the developed by the IBM Center in order to combat said crimes on the Internet in Mexico. The participation of academic institutions and private sector are important for preventing and developing these new technologies in the deterrence of cybercrime.

Regarding the campaign proposed spending the media airtime available to the Federal government, it will be worth considering investing more economical resources

into paying for more airtime. When paying for airtime media, government will have control of selecting the time of the day where these will be broadcasted. This way, we assure that the message will be effectively received and absorbed by the Mexican population, and the chances of creating a change of behavior increase.

This implicates an expense, but the results could make this expense become an investment. The money invested in the prevention of cybercrimes, will be nothing compared with the millions of dollars that are lost when we do not create awareness on cybercrimes.

Harnessing the potential of the information campaign would require active effort and support for reaching the results, the proposal would be the first step from many for diminishing economic damages for consumers for these activities, and the basis for protecting themselves from online threats.

BIBLIOGRAPHY

Animal Politico. ¿Quién hizo y cuánto costó la campaña Mover a México?. Animal

Político, Julio 9, 2013. http://www.animalpolitico.com/2013/07/quien-hizo-y-

cuanto-costaron-los-spots-de-presidencia/

AT Kearney Consulting Firm. 2012 A.T. Kearney´s E-Commerce Index. June 2012.

http://www.atkearney.com/paper/-/asset_publisher/dVxv4Hz2h8bS/content/e-

commerce-is-the-next-frontier-in-global-expansion/10192#sthash.tdyCoxp7.dpuf

Belmont, José Antonio. "México se adhiere al Convenio de Budapest", Milenio. Abril 3,

2014. http://www.milenio.com/policia/Cibercriminalidad-Mexico-adhiere-

Convenio_de_Budapest-PGR-delitos_informaticos-

delitos_en_internet_0_274173006.html

Buendia y Laredo. Empleo, la prioridad para Mexicanos. El Universal. August 2014.

http://www.eluniversal.com.mx/nacion-mexico/2014/empleo-la-prioridad-para-

mexicanos--1032800.html

Castillo Díaz, Gustavo. "Ciberdelincuentes Obtuvieron 3 Mil Mdd De Pequeñas

Empresas Durante 2013." La Jornada, April 9, 2014.

http://www.jornada.unam.mx/2014/04/09/politica/023n2pol

Cawley, Marguerite. Mexico Is World Leader in Child Pornography. September 30,

2013, http://www.insightcrime.org/news-briefs/mexico-is-world-leader-in-child-

pornography

Center for Strategic and International Studies and McAfee report. Net Losses: estimating

the global cost of cybercrime. June 2014.

http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf.

Consejo Nacional de Seguridad, Scientific Police Division. 2013.

http://www.cns.gob.mx/portalWebApp/wlp.c?__c=7d1

Consulta Mitofsky, Porcentajes de votación para el año 2015. El Universal, Nación sec. August 9, 2014.

Council of Europe. Convention on Cybercrime. 2012.

http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

ESET Latin America's Research Team, Trends for 2014: "The Challenge of Internet Privacy",ESET Latin America's Research Laboratory, 2013.

http://www.welivesecurity.com/wp/content/uploads/2013/12/Trends-for-2014.pdf.

Glickhouse, Rachel. Infographic: The Cost of Cybercrime in Latin America. Americas Society, Council of the Americas. November 14. 2013.

http://www.as-coa.org/articles/infographic-cost-cybercrime-latin-america

Global Initiative against Transnational Organized Crime, Stolen innocence: the online exploitation of children, http://www.globalinitiative.net/stolen-innocence-the-online-exploitation-of-children/

Iglesias, Francisco. "En México Por Lo Menos Hay 200 Delitos Informáticos Tipificados." October 12, 2012. http://www.bsecure.com.mx/featured/en-mexico-por-lo-menos-hay-200-delitos-informaticos-tipificados-especialista/.

IBM Center for the Business of Government. Engaging Citizens in Co-Creation in Public Services: Lessons Learned and Best Practices. By Satish Nambisan and Priya Nambisan. 2013.

http://www.businessofgovernment.org/sites/default/files/Engaging%20Citizens%20in%20Co-Creation%20in%20Public%20Service.pdf

Instituto de Investigaciones Juridicas, UNAM. Mexican Constitution 2013.

http://info4.juridicas.unam.mx/ijure/tcfed/9.htm?s

Internet Lives Stats."Internet Users by Country". January 1, 2014.

http://www.internetlivestats.com/internet-users-by-country/.

Instituto Nacional Electoral. Calendario Electoral 2015. Instituto Nacional Electoral.

2014. http://www.ine.mx/docs/IFE-v2/DECEYEC/DECEYEC-ProcesosElectorales/Calendario-Docs/ISU_Cal_Elect-2015.pdf

Krauze, Enrique. "Mexico's Barbarous Tragedy." The New York Times, November 10,

2014. http://www.nytimes.com/2014/11/10/opinion/enrique-krauze-mexicos-barbarous-tragedy.html.

Latin American and Caribbean Cybersecurity: Trends and Government Responses 2013.

Organization of American States. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Lieberman Research Group. Unisys Security Index: MEXICO. May, 15, 2014.

http://www.unisyssecurityindex.com/system/reports/uploads/304/original/Unisys%20Security%20Index%20Mexico%20May%202014.pdf?1399943793

National Statistical and Geographic Information System. Usuarios de Internet en México.

Inegi. Mexico, 2012.

http://www.inegi.gob.mx/est/contenidos/espanol/temas/Sociodem/notatinf212.asp

Norton Report 2013. http://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-data-sheet-mexico-es-mx.pdf. 2013

Martínez, París. "México, Primer Lugar Mundial En Difusión De Pornografía Infantil." Animal Político. June 13, 2013. http://www.animalpolitico.com/2013/06/detectan-a-12-mil-300-pedofilos-mexicanos-que-operan-en-la-red/#ixzz371LPzrAd

Organisation for Economic Co-operation and Development. Cybersecurity policy making at a turning point. 2012.

http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Organisation for Economic Co-operation and Development. "OECD Policy Guidance on Online Identity Theft." June 1, 2008.

http://www.oecd.org/sti/consumer/40879136.pdf.

O´Neil, Shannon. Two nations indivisible: Mexico and the United States. A Council on foreign relations book. University Press, Oxford. 2013. Kindle edition.

Organization of American States (OAS), and TREND Micro. Latin American and Caribbean Cybersecurity Trends and Government Responses. 2013.

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Pérez, Judith. "Delinquen Desde Casa…en Internet." La Razón, June 1, 2013.

http://www.razon.com.mx/spip.php?article174743.

Presidencia de la Republica. National Digital Strategy to transform Mexico. 2012.

http://en.presidencia.gob.mx/national-digital-strategy-to-transform-mexico/

Presentations/567 UN id theft and CCC_en.pdf.

Presidencia de la Republica. Mexican National Development Plan 2013-2018 .2013

http://en.presidencia.gob.mx/national-development-plan-2013-2018/

Pew Research Center. Mexican President Peña Nieto's Ratings Slip with Economic

Reform. August 26, 2014. http://www.pewglobal.org/2014/08/26/mexican-

president-pena-nietos-ratings-slip-with-economic-reform/

Ramírez Olvera, Marisol. "Pequeños Internautas." El Universal, April 28, 2014.

http://www.eluniversal.com.mx/computacion-tecno/2014/ninos-tecnologia-

nativos-digitales-87584.html.

Secretaría de Hacienda y Crédito Público. Acuerdo por el que se publican las reglas de

operación para el pago de impuestos de los concesionarios de radio y televisión.

Diario Oficial de la Federación. Octubre 10, 2002.

Secretaria de Seguridad Publica. Plataforma México: public security networks.

Septiembre 2013.

http://www.ssp.gob.mx/portalWebApp/wlp.c;jsessionid=nyFRTspGkCNl4pG4dd

HrBGf1D1hPbJt4ZtN5qP1NlBQKLwNyp1kf!-527600024?__c=105a

Secretaria de Seguridad Publica. Programa Nacional de Seguridad Pública (2008-2012).

http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repositor

y/414002//archivo

Seger, Alexander. Identity Theft and the Convention on Cybercrime. September 1, 2007.

http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Rep

orts-

Sistema de Información Legislativa. Communications and transportation Commission in

the Mexican Senate, Cybercrime in México. Mexican Senate, Abril 26, 2004.

http://sil.gobernacion.gob.mx/Archivos/Documentos/2004/04/asun_979854_2004
0427_981312.pdf

Sistema de Información Legislativa. Que expide la Ley General del Sistema Nacional de
Seguridad Pública y se adicionan diversos artículos del Código Penal Federal.
Octubre, 10 2008.

http://sil.gobernacion.gob.mx/Busquedas/Avanzada/ResultadosBusquedaAvanzad
a.php?SID=7b136991d5dbfa1d8f0554a57afb4ce8&Serial=eae0d855515dc072d37
f4caeb05fbaea&Reg=2&Origen=BA&Paginas=999#E2

Vatis Michael. The Council of Europe Convention on Cybercrime.
http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf.

Velasco, Cristos. "The Legal Framework on Cybercrime and Law Enforcement in
Mexico." May 1, 2007.
http://ciberdelincuencia.org/attachments/CristosMXContribution.pdf

Wilson, Chistopher E., and Eric L. Olson. New Ideas for a New Era: Policy Options for
the next Stage in US-Mexico Relations. Washington DC: Wilson Center, 2013.

Washington Office on Latin America. One Year after Enrique Peña Nieto's Election. July
3, 2013.
http://www.wola.org/commentary/one_year_after_enrique_pena_nieto_s_election

Curriculum Vita

Iliana A. Briseño was born in Mexico City, Mexico. She is a graduate from Johns Hopkins University with a Master in Arts of Public Management. She graduated from National Autonomous University of Mexico with a major in Political Science and Public Administration. She got a diploma in Government and Parliament from National Public Administration Institute in Spain.

She is a former director of Democratic Culture in the Secretariat of the Interior of Mexico (SEGOB) in Mexico. She has experience in developing and promoting Mexico's national civic culture campaigns to strengthen civic democratic participation, and civic cooperation, respect, and consciousness among population. She also has experience in researching legislative processes, and a marked interest in human rights.