MEXICO SETS SIGHTS ON CYBER SECURITY

A look into the potential and demand for new investment

WORDS RORY JACKSON

President Peña Nieto is spending big on defence

The reach of online hacking groups has not left Mexico untouched. Over half a dozen highly-publicised hacks of Mexican government websites have taken place, with attackers protesting over causes ranging from net neutrality to the deaths of journalists and students. In doing so, the hackers have helped draw attention to Mexico's vulnerability to cyber attacks, an issue often overshadowed by the country's ongoing drug wars.

Spreading security investment

This intense security situation already presents a particular burden on Mexico's economic ambitions. In recent years, the country's competitiveness has lagged behind its neighbours. Much of the blame is placed on a lack of investment in proper infrastructure.

To remedy this gap, President Peña Nieto's administration announced plans in April 2014 for investing $590bn across Mexican infrastructure, with energy and transport being of chief focus, and urban development, healthcare, tourism, and communications taking shares of the budget.

Even so, for Mexico's economic investments to pay off, they must survive and operate undisrupted long enough to inspire confidence in foreign investors. Financing defence and security is therefore essential to Mexican prosperity.

Little wonder that Peña Nieto has purchased over $3.5bn in military equipment from the U.S. Government and American companies in the past few years. More than two dozen Black Hawk helicopters and 2,200 Humvees were included, vastly augmenting the armed forces' reach and the scale of their firepower against surprisingly well-equipped cartels.

'Anonymous Mexico' has aligned itself with revolutionary group EZLN

'Cyber attacks in Mexico have increased exponentially over the last five years'

Mexico's cyber shortcomings

This impressive spending has done little however to address a glaring weakness in the security of Mexican infrastructure: the internet.

Cyber attacks in Mexico have increased exponentially over the last five years: 2012 saw a 40 percent increase in attacks from the previous year. 2013 saw a 113 percent increase over 2012, and 2014 bore an increase of more than 300 percent on the subsequent year.

The victims of these attacks are diverse. Government websites connected with Mexico's 2012 presidential elections were hit by 'hacktivists' conducting Distributed-Denial-of-Service (DDoS) attacks, cross-site-scripting (XSS) and injections of Structured Query Language (SQL) code. The hacker group 'Anonymous' disrupted the Mexican defence secretariat (SEDENA) website in 2013, while the Ministry of Interior (SEGOB) was listed as a prime customer in leaked documents after the infamous attack on cybersecurity firm Hacking Team.

Additionally, Critical National Infrastructure (CNI) is gradually turning towards using IT and networked industrial control systems that are highly vulnerable to infiltration and disruption. Power plants, airports, telecommunications, and oil rigs all remain at severe risk.

Last year, Ernst & Young revealed that over half of all Mexican companies were subject to minor or serious cyber attacks, including extortion and espionage. Mexico City-based security risk analyst, James Bosworth, pointed out that companies (particularly banks) routinely fail to share information on cyber attacks for fear of panicking shareholders. As a result, they miss crucial opportunities to learn who the major attackers are – and how to defend themselves.

Also worth noting is that the civilian population, widely operating pirated software with no security patches, remains at ever-increasing risk from various attack types, from 'virtual kidnappings', to identity theft and credit fraud, all of which have spiked.


Vulnerabilities in Mexico's critical infrastructure demand urgent attention

'Last year, over half of all Mexican companies were subject to minor or serious cyber attacks, including extortion and espionage'

Upgrades underway

The prospects have however seen some improvement.

For further analysis, *Defence IQ*'s **Rory Jackson** consulted a panel of experts, each with a unique perspective on the present and future of cyber security in Mexico: political and security risk analyst **Lloyd Belton** from Salamanca, special risks analyst for red24 **Nicole Elliot**, U.S. defence consultant **James Farwell**, OAS Secretary of Multidimensional Security and H.E. Ambassador **Adam Blackwell**, and Information Technology Security Manager for the Bank of Mexico **Arturo Garcia Hernandez**.

What, in your opinion, has been the most beneficial contribution to Mexican cyber security of the past two years?

JF: A growing recognition by the Mexican government that it actually needs to significantly improve its use of cyber, and to strengthen defences against infiltration by cartels whose $39bn a year profits and sophistication enable the cartels to hack into virtually any Mexican government entity and to use their financial influence and ability to corrupt and coerce the government.

AGH: The recognition of cyber security's importance in the National Plan of Development 2013-2018 (*Plan Nacional de Desarrollo*). Cyber security was already an important task for the country, as visible from previous efforts: postgrad courses in the field, the creation of a Mexican CERT, legal compliance for governmental organizations (for example, the MAAGTICSI document), international cooperation agreements, and so on. This recognition has enhanced cyber-defence throughout the country, especially in military organisations.

LB: One potential positive was the decision by Telmex to create the *Centro de Ciberseguridad* in October 2014. This institution, the first of its kind in Latin America, has set a precedent, which will hopefully be emulated by other telecommunications providers in the region. If it operates effectively, Telmex's cyber-security centre has the potential to partially mitigate the cyber-security risks threatening millions of its Mexican clients.

NE: Since 2012, the government has demonstrated its commitment to addressing this threat by investing in technical personnel and creating agencies dedicated to the fight against cybercrime. These include a national coordination centre and specialised police cyber response units. Mexico has also participated in several important regional and international cyber defence initiatives.

AB: The issue of cyber security has been promoted with greater impetus in the current federal administration. The dissemination of information has been strengthened in a way that has contributed greatly towards awareness in society. Currently, there are protocols for responding to large-scale cyber incidents, having strengthened coordination with various government agencies, private institutions, academia, and civil society.

'The issue of cyber security has been promoted with greater impetus in the current federal administration'

Amb. Adam Blackwell
Organization of American States

What group or sector of Mexican society, or the Mexican economy, do you feel merits special attention for further cyber defence investment?

AB: Critical infrastructure and law enforcement agencies must be strengthened.

JF: Law enforcement and civil society both need it.

NE: In broad terms, when it comes to cybercrime, the Mexican population bears the brunt. Locals are most frequently targeted and also experience the trickle-down effect of the loss of public sector funds due to extortive practices. Existing criminal and drug-cartel related activity, which includes Kidnap for Ransom and Extortion (KRE), extortion, and virtual kidnapping, has evolved due to technological advances and the growth in online and social media usage.

LB: Mexico's finance, pharmaceutical, automotive, retail and extractive sectors are most at risk of cyber breaches and this merits urgent examination. Many companies have yet to realise that investing in cyber security is a

strategic investment that could save them money, mitigate potential reputational risks, and protect their employees' identity, in the event of an attack. This mentality is changing, although not as quickly as hackers and criminals develop novel means to carry out their attacks. Mexico's organised criminal groups are increasingly more sophisticated and some now have the capacity to carry out cyber-attacks on large firms, stealing company and employee information, and then demanding extortion payments.

AGH: Organisations with CNI should be the most worried, and deserve special attention. There is a lot to be done in this area since there is no formal (or publicly available) catalogue of such organizations. Furthermore, most CNI is owned by private sector companies, which should be included. By the way, physical security and logical security are currently divided. For example, *Plataforma Mexico* is an excellent platform to integrate national security threats – however, it only processes issues from the physical world, without considering threats from the logical world, such as a DDoS attack affecting the financial sector. An integral outlook would be better if Mexico wants to deal with national threats.

'Organisations with CNI should be the most worried, and deserve special attention'

Arturo Garcia Hernandez
IT Security Manager,
Bank of Mexico

'As important as protecting high-value targets will be Mexico's efforts to reduce rampant criminality'

Nicole Elliot
Risk Analyst

What action or direction would you personally recommend that Mexico take next, in cyber defence policy or, indeed, in acquisition?

AGH: There are some actions that I personally consider must be attended promptly. There should be a full-time organisation that leads the information security area reporting directly to the President, as in some other countries. This institution should be in charge of all national strategies, controls, regulations, and so on. Today, this responsibility is distributed in several organisations with part-time staff. Legal regulation should be enforced, in accordance with international law. National security officials should also be trained by cyber security experts, and vice versa, to have an integral view of national security threats, how to face them, how to evaluate them and how to respond to them. I am currently studying a Masters in National Security at the Navy University (CESNAV, *Centro de Estudios Superiores Navales*) and I've identified some activities and projects that can be done in cyberspace and cyber defence. The migration from paper work processes to processes using IT should be properly accompanied by IT training. Some people that have never used the internet or do not know how to use it securely are required to perform activities in cyberspace.

'Recognition has grown that Mexico needs to significantly improve its use of cyber'

James P. Farwell
U.S. Defence Consultant

AB: Aside from strengthening critical infrastructure, Mexico absolutely must update the national legal framework and continue the work of integration into the international legal framework on cybercrime issues.

LB: As with other countries in the region, there needs to better coordination between the various cyber defence institutions operating in Mexico, including UNAM's *Centro Nacional de Respuesta a Incidentes Cibernéticos* (CERT-MX), the *Centro de Monitoreo y Respuesta a Incidentes de Seguridad en el Ciberespacio* (operated by the Secretariat of the Navy) and telecommunications regulators such as the *Instituto Federal de las Telecomunicaciones*. In line with its 2014-18 national security plan, the Mexican Government needs to demonstrate a serious commitment to building a concerted, and sufficiently-funded, cyber defence strategy. This process should include consultations between the private and public sectors, both of which remain highly exposed to cyber-attacks. Furthermore, Mexico, and existing CERTs within the country, should look to greater cooperation with international partners through information sharing.

NE: Looking ahead, the government is likely to focus its cyber defence efforts on high-value targets such as public institutions and interests, as well as critical infrastructure such as telecommunications, financial institutions, oil and gas, and transportation. However, arguably as important as protecting these prominent targets will be efforts to reduce rampant criminality, which most frequently impacts the local population. A sustained public education programme highlighting the potential risks posed by insufficient online privacy and security measures, coupled with further security force engagement may assist in providing citizens with concrete measures to respond to future attacks.

'The mentality is changing, just not as quickly as hackers' ability to develop means to carry out their attacks'

Lloyd Belton
Risk Analyst

Clearly, as Mexico modernises, and access to the internet becomes not just wider, but *fundamental* to the Mexican economy, the need for major efforts in cyber defence policy will become too evident to ignore.

Ambassador Adam Blackwell and Arturo Garcia Hernandez will speak further on Mexican national security and other concerns this November, at MEXSEC 15.

MEXSEC 15

03 - 05 November, 2015
Mexico City

SUPPORTING THE GOVERNMENT TO ACHIEVE "MEXICO IN PEACE" THROUGH SECURITY COOPERATION

MEXSEC 15 will continue a timely discussion on the national security current situation in Mexico, bringing together the most relevant governmental representatives and international experts to share their experiences over the contemporary challenges faced. Furthermore, MEXSEC 15 will provide the exclusive opportunity to all those attending to discuss an innovative multidimensional approach including relevant discussions about Intelligence Strategies, Narcotraffic, Safe Cities and Cybersecurity, to strengthen Homeland Security in Mexico from different perspectives.

It is clear that the adoption of a multidimensional and transnational position is essential. Therefore, experts from the Mexican Government and security institutions, including SEGOB, SEDENA and SEMAR, will meet with international and regional bodies including the OAS and UNODC along with neighboring countries and regional partners to discuss challenges and strategies for achieving a more secure Mexico.

Attend MEXSEC 15 to:

- Gain great insight into the Mexican Homeland Security Strategy and a complete overview of the security situation in Mexico and the many organisations involved in enhancing the security situation
- Engage with Mexican and regional security personnel at a time of heightened interest in tackling the problem of porous borders and the associated threat of organised and transnational crime
- Gain a comprehensive understanding of the different aspects linked to national security, such as integrated surveillances systems, cybersecurity, border control and private security
- Promote a wider inclusion of all private and public sectors involved in promoting security across the region

Key discussion topics include:

- Homeland security is a joint task
- National Security vs Public Order
- Safe Cities
- Private security supporting public security
- Control and Surveillance Centres
- Cybersecurity and digital security strategy

www.MEXSEC.com

+44(0) 20 7368 9737 enquire@defenceiq.com