Foro sobre el fortalecimiento de la transformación digital en América Latina

7-8 de julio de 2022

Antigua, Guatemala

SIT Superintendencia de Telecomunicaciones Guatemala

comtelca Comisión Técnica Regional de Telecomunicaciones

ITU

First of all, congratulations, we have managed to **survive Covid-19**. My respects and condolences to all of us who have lost friends and family in these difficult times.

CENTRO DE CIBERSEGURIDAD INDUSTRIAL

INDUSTRIAL CYBERSECURITY CENTER

Serie Smart OT. Número 2 | Smart OT Series. Number 2

Smart Cities ante el desafío de la seguridad

La ciudad inteligente, escenario clave para el despliegue de las smart OT

Smart Cities before the security challenge

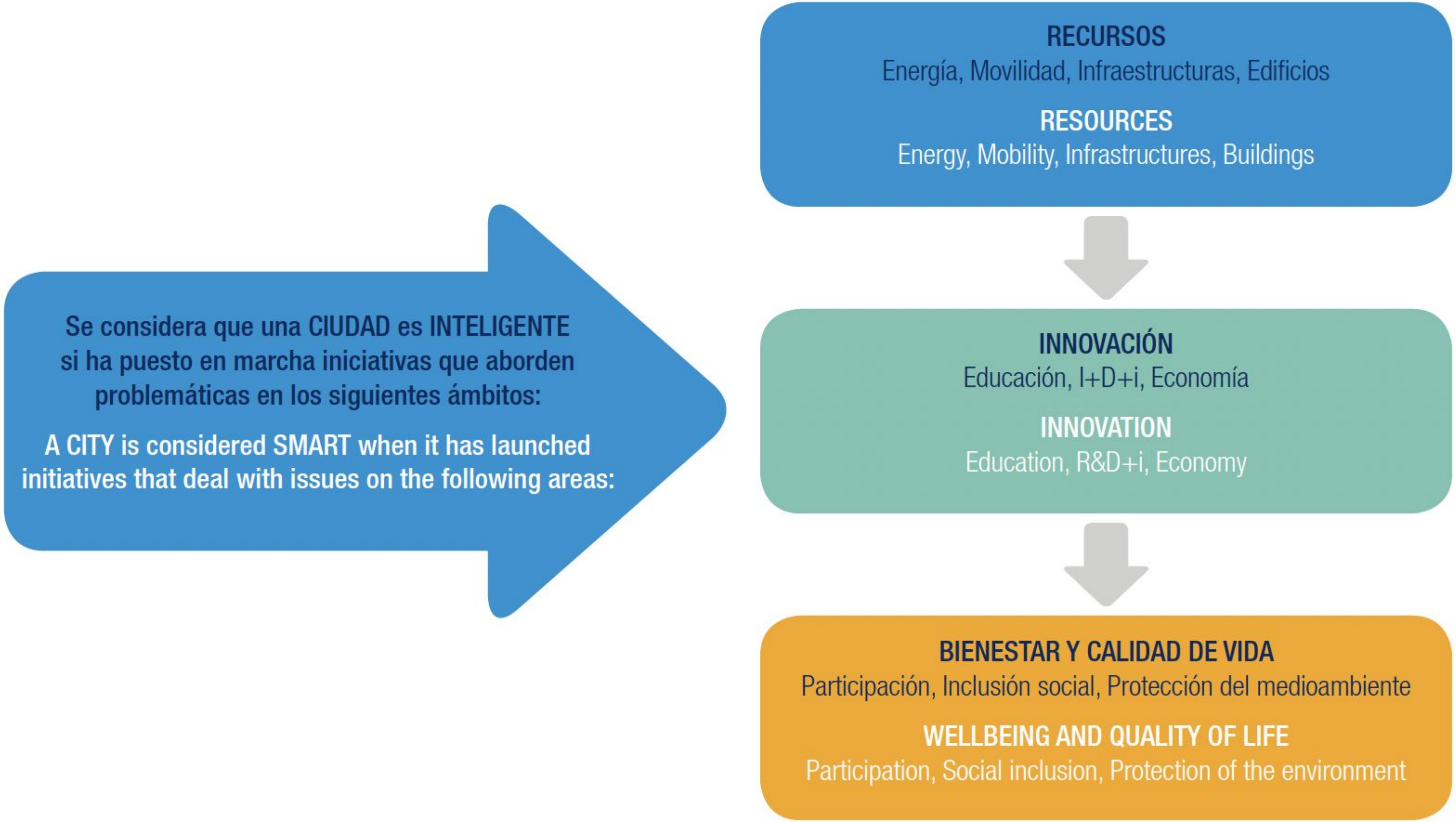
Smart cities, key scenario for deploying 'smart OT'

https://www.cci-es.org/activities/smart-cities-ante-el-desafio-de-la-seguridad_serie-smart-ot_2/

SIT Superintendencia de Telecomunicaciones Guatemala

comtelca Comisión Técnica Regional de Telecomunicaciones

ITU



Se considera que una CIUDAD es INTELIGENTE si ha puesto en marcha iniciativas que aborden problemáticas en los siguientes ámbitos:

A CITY is considered SMART when it has launched initiatives that deal with issues on the following areas:

RECURSOS
Energía, Movilidad, Infraestructuras, Edificios

RESOURCES
Energy, Mobility, Infrastructures, Buildings

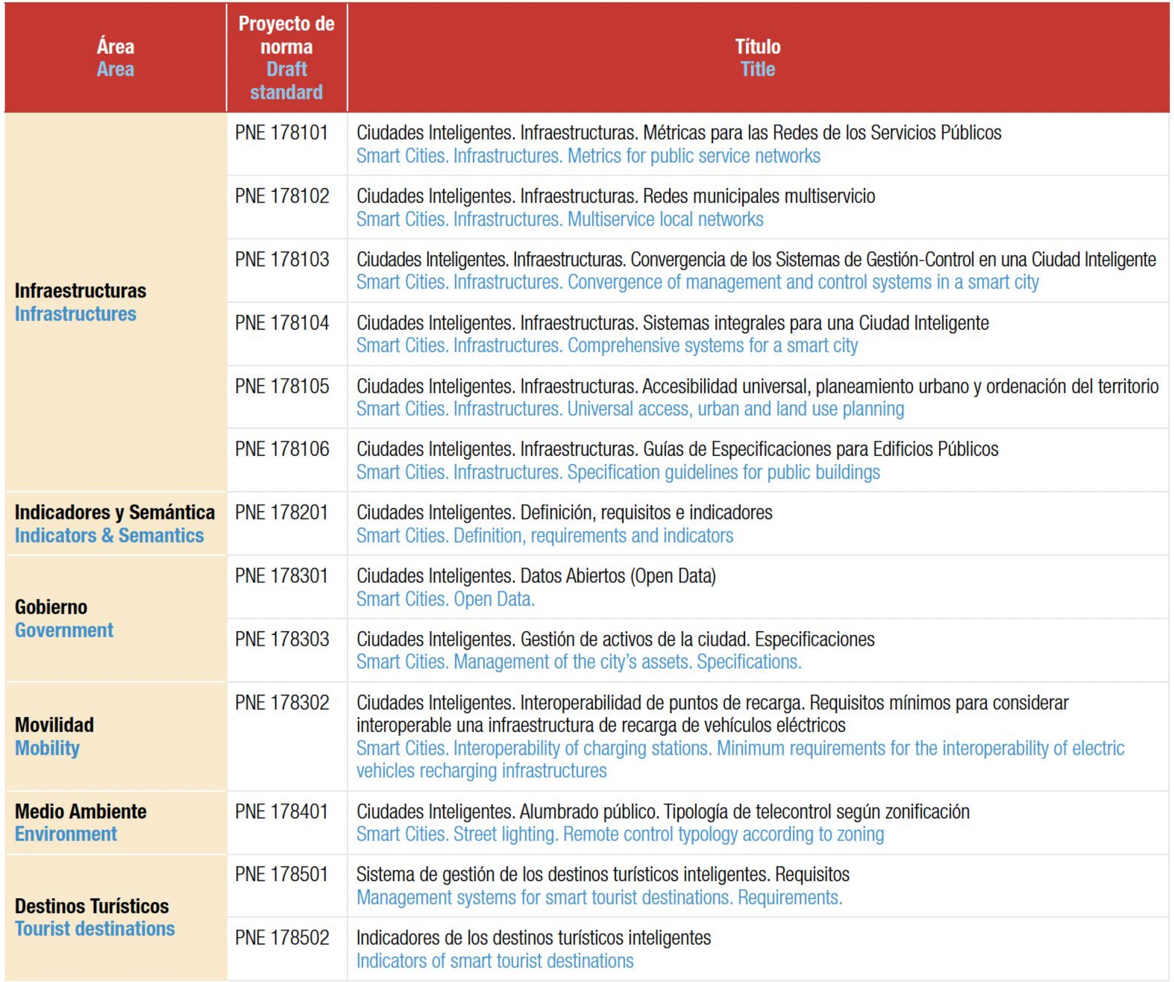
INNOVACIÓN
Educación, I+D+i, Economía

INNOVATION
Education, R&D+i, Economy

BIENESTAR Y CALIDAD DE VIDA
Participación, Inclusión social, Protección del medioambiente

WELLBEING AND QUALITY OF LIFE
Participation, Social inclusion, Protection of the environment

https://www.cci-es.org/activities/smart-cities-ante-el-desafio-de-la-seguridad_serie-smart-ot_2/

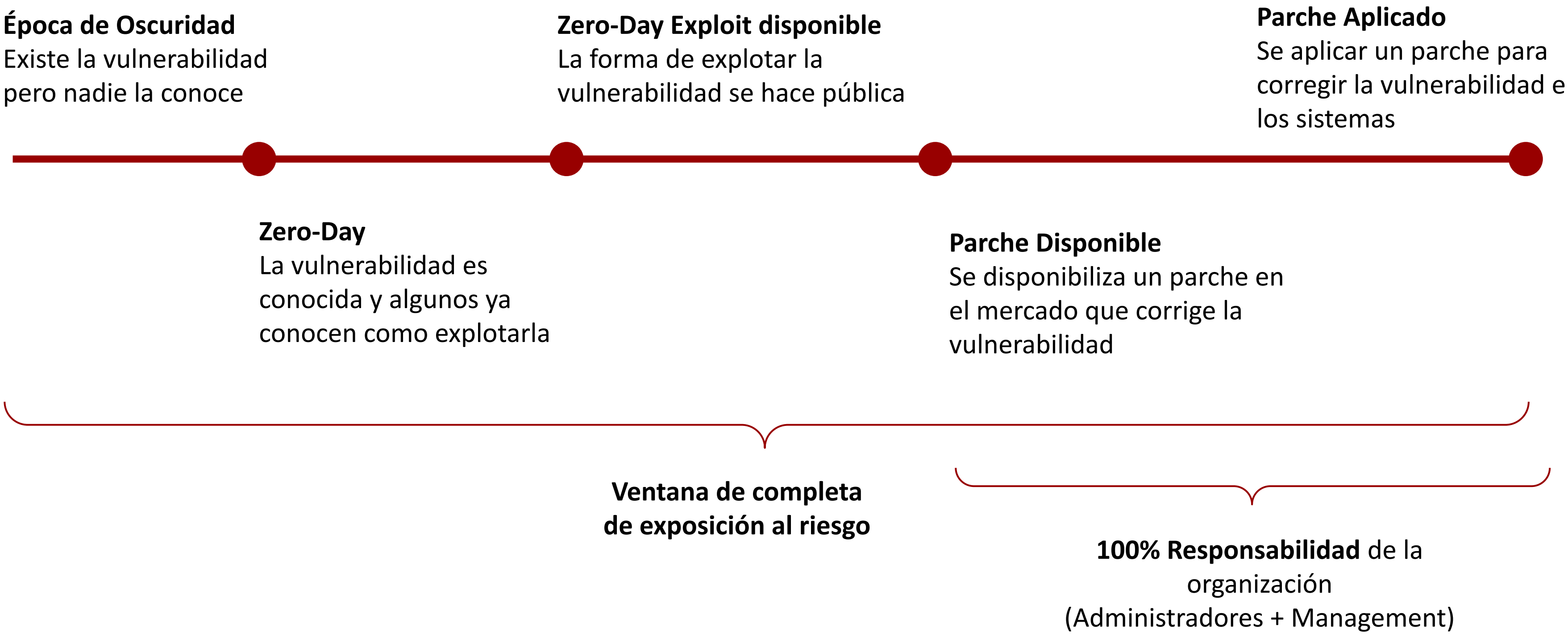


Área Area	Proyecto de norma Draft standard	Título Title
Infraestructuras **Infrastructures**	PNE 178101	Ciudades Inteligentes. Infraestructuras. Métricas para las Redes de los Servicios Públicos Smart Cities. Infrastructures. Metrics for public service networks
	PNE 178102	Ciudades Inteligentes. Infraestructuras. Redes municipales multiservicio Smart Cities. Infrastructures. Multiservice local networks
	PNE 178103	Ciudades Inteligentes. Infraestructuras. Convergencia de los Sistemas de Gestión-Control en una Ciudad Inteligente Smart Cities. Infrastructures. Convergence of management and control systems in a smart city
	PNE 178104	Ciudades Inteligentes. Infraestructuras. Sistemas integrales para una Ciudad Inteligente Smart Cities. Infrastructures. Comprehensive systems for a smart city
	PNE 178105	Ciudades Inteligentes. Infraestructuras. Accesibilidad universal, planeamiento urbano y ordenación del territorio Smart Cities. Infrastructures. Universal access, urban and land use planning
	PNE 178106	Ciudades Inteligentes. Infraestructuras. Guías de Especificaciones para Edificios Públicos Smart Cities. Infrastructures. Specification guidelines for public buildings
Indicadores y Semántica **Indicators & Semantics**	PNE 178201	Ciudades Inteligentes. Definición, requisitos e indicadores Smart Cities. Definition, requirements and indicators
Gobierno **Government**	PNE 178301	Ciudades Inteligentes. Datos Abiertos (Open Data) Smart Cities. Open Data.
	PNE 178303	Ciudades Inteligentes. Gestión de activos de la ciudad. Especificaciones Smart Cities. Management of the city's assets. Specifications.
Movilidad **Mobility**	PNE 178302	Ciudades Inteligentes. Interoperabilidad de puntos de recarga. Requisitos mínimos para considerar interoperable una infraestructura de recarga de vehículos eléctricos Smart Cities. Interoperability of charging stations. Minimum requirements for the interoperability of electric vehicles recharging infrastructures
Medio Ambiente **Environment**	PNE 178401	Ciudades Inteligentes. Alumbrado público. Tipología de telecontrol según zonificación Smart Cities. Street lighting. Remote control typology according to zoning
Destinos Turísticos **Tourist destinations**	PNE 178501	Sistema de gestión de los destinos turísticos inteligentes. Requisitos Management systems for smart tourist destinations. Requirements.
	PNE 178502	Indicadores de los destinos turísticos inteligentes Indicators of smart tourist destinations

Tabla 1: Proyectos de Norma Española impulsados desde el comité AEN/CTN 178 (Fuente: AENOR)
Table 1: Spanish Draft Standards by the AEN/CTN 178 Committee (Source: AENOR)

https://www.cci-es.org/activities/smart-cities-ante-el-desafio-de-la-seguridad_serie-smart-ot_2/

Ventana de Exposición al Riesgo



Época de Oscuridad
Existe la vulnerabilidad pero nadie la conoce

Zero-Day
La vulnerabilidad es conocida y algunos ya conocen como explotarla

Zero-Day Exploit disponible
La forma de explotar la vulnerabilidad se hace pública

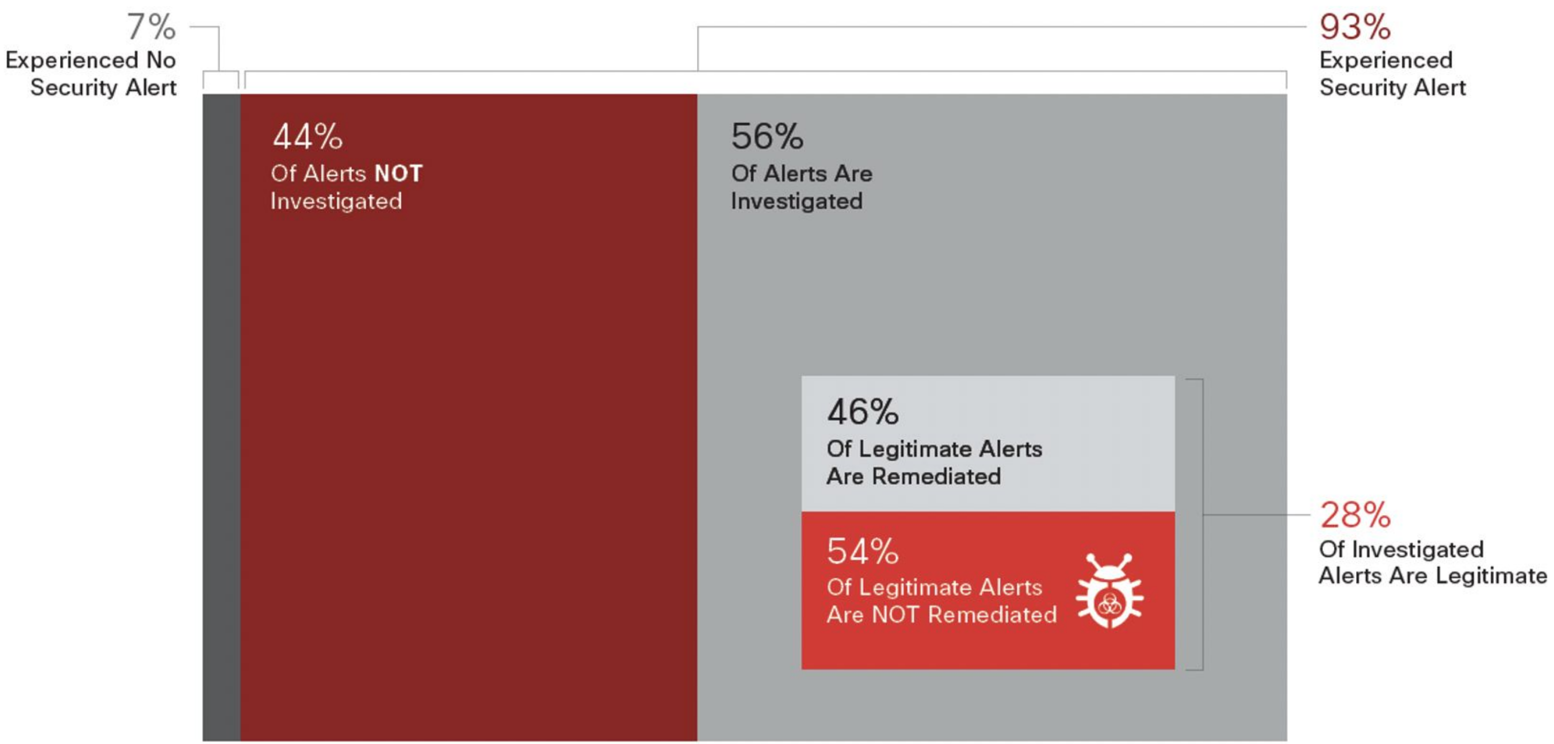
Parche Disponible
Se disponibiliza un parche en el mercado que corrige la vulnerabilidad

Parche Aplicado
Se aplicar un parche para corregir la vulnerabilidad en los sistemas

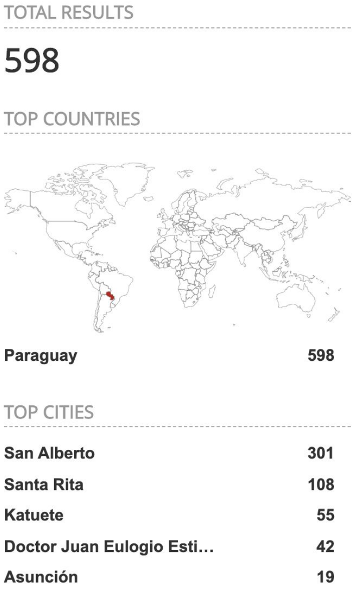
Ventana de completa de exposición al riesgo

100% Responsabilidad de la organización
(Administradores + Management)

Alertas


7%
Experienced No Security Alert
93%
Experienced Security Alert
44%
Of Alerts **NOT** Investigated
56%
Of Alerts Are Investigated
46%
Of Legitimate Alerts Are Remediated
54%
Of Legitimate Alerts Are NOT Remediated
28%
Of Investigated Alerts Are Legitimate

Monitoreo



TOTAL RESULTS

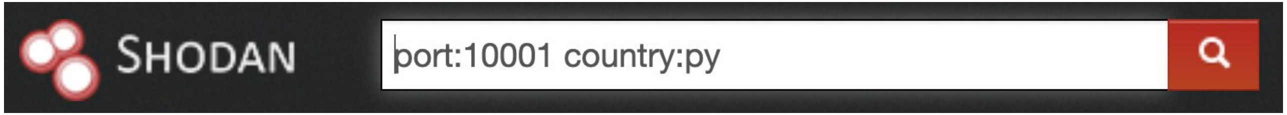
598

TOP COUNTRIES

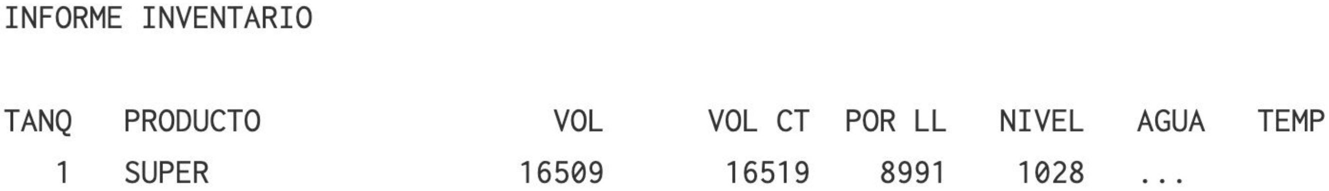
Paraguay	598

TOP CITIES

San Alberto	301
Santa Rita	108
Katuete	55
Doctor Juan Eulogio Esti…	42
Asunción	19

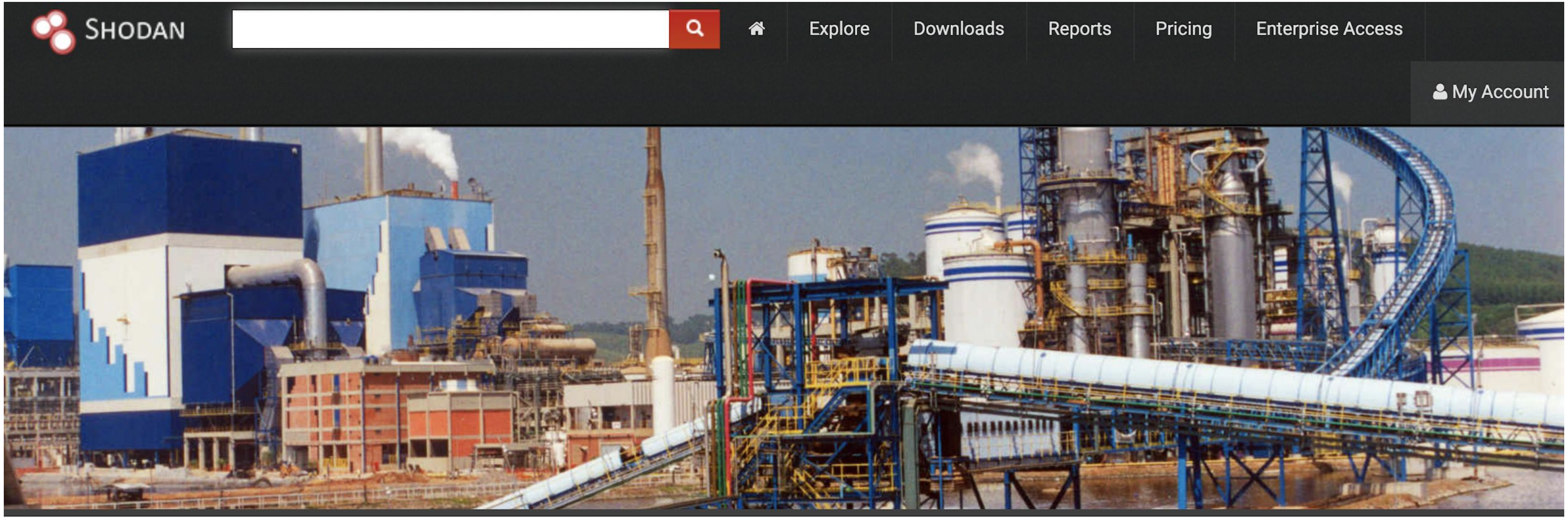


```
port:10001 country:py
```



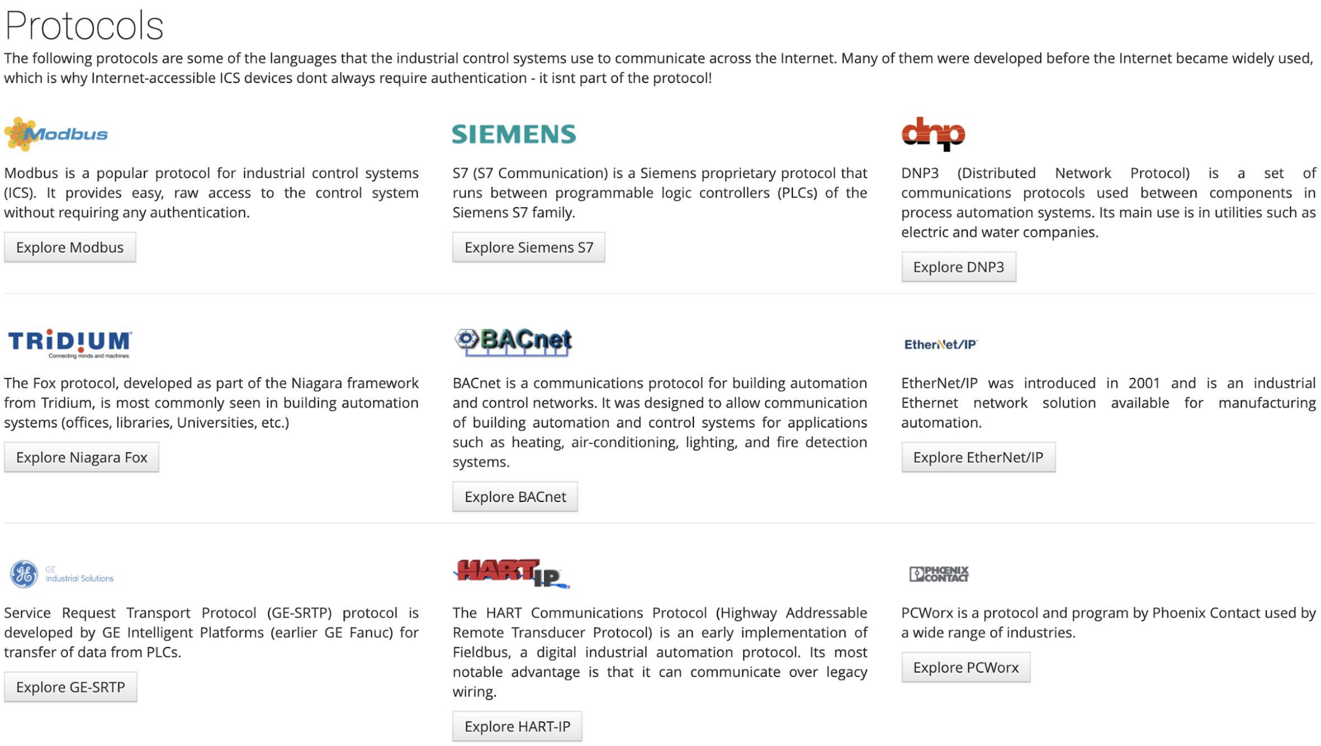
```
INFORME INVENTARIO

TANQ   PRODUCTO             VOL      VOL CT   POR LL    NIVEL    AGUA    TEMP
   1   SUPER              16509       16519     8991     1028    ...
```

Monitoreo



Industrial Control Systems

Monitoreo



Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices dont always require authentication - it isnt part of the protocol!

Modbus

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

Explore Modbus

SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

dnp

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

TRiDIUM
Connecting minds and machines

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

Explore Niagara Fox

BACnet

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

Explore BACnet

EtherNet/IP

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

Explore EtherNet/IP

GE
Industrial Solutions

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

Explore GE-SRTP

HART IP

The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

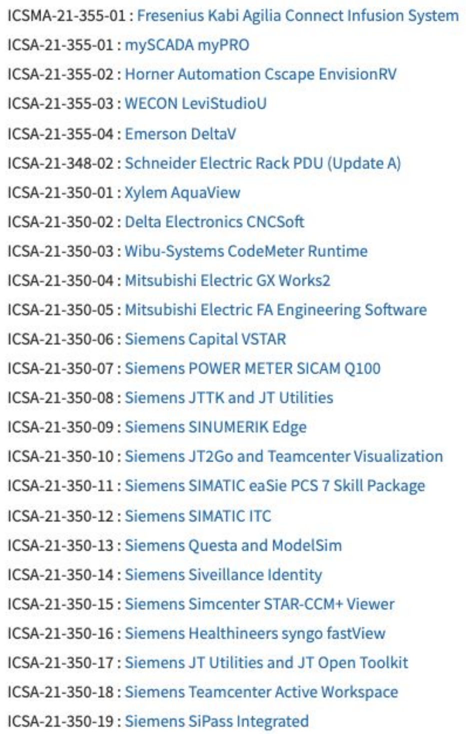
Explore HART-IP

PHOENIX CONTACT

PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

Explore PCWorx

Alertas



ICSMA-21-355-01 : Fresenius Kabi Agilia Connect Infusion System

ICSA-21-355-01 : mySCADA myPRO

ICSA-21-355-02 : Horner Automation Cscape EnvisionRV

ICSA-21-355-03 : WECON LeviStudioU

ICSA-21-355-04 : Emerson DeltaV

ICSA-21-348-02 : Schneider Electric Rack PDU (Update A)

ICSA-21-350-01 : Xylem AquaView

ICSA-21-350-02 : Delta Electronics CNCSoft

ICSA-21-350-03 : Wibu-Systems CodeMeter Runtime

ICSA-21-350-04 : Mitsubishi Electric GX Works2

ICSA-21-350-05 : Mitsubishi Electric FA Engineering Software

ICSA-21-350-06 : Siemens Capital VSTAR

ICSA-21-350-07 : Siemens POWER METER SICAM Q100

ICSA-21-350-08 : Siemens JTTK and JT Utilities

ICSA-21-350-09 : Siemens SINUMERIK Edge

ICSA-21-350-10 : Siemens JT2Go and Teamcenter Visualization

ICSA-21-350-11 : Siemens SIMATIC eaSie PCS 7 Skill Package

ICSA-21-350-12 : Siemens SIMATIC ITC

ICSA-21-350-13 : Siemens Questa and ModelSim

ICSA-21-350-14 : Siemens Siveillance Identity

ICSA-21-350-15 : Siemens Simcenter STAR-CCM+ Viewer

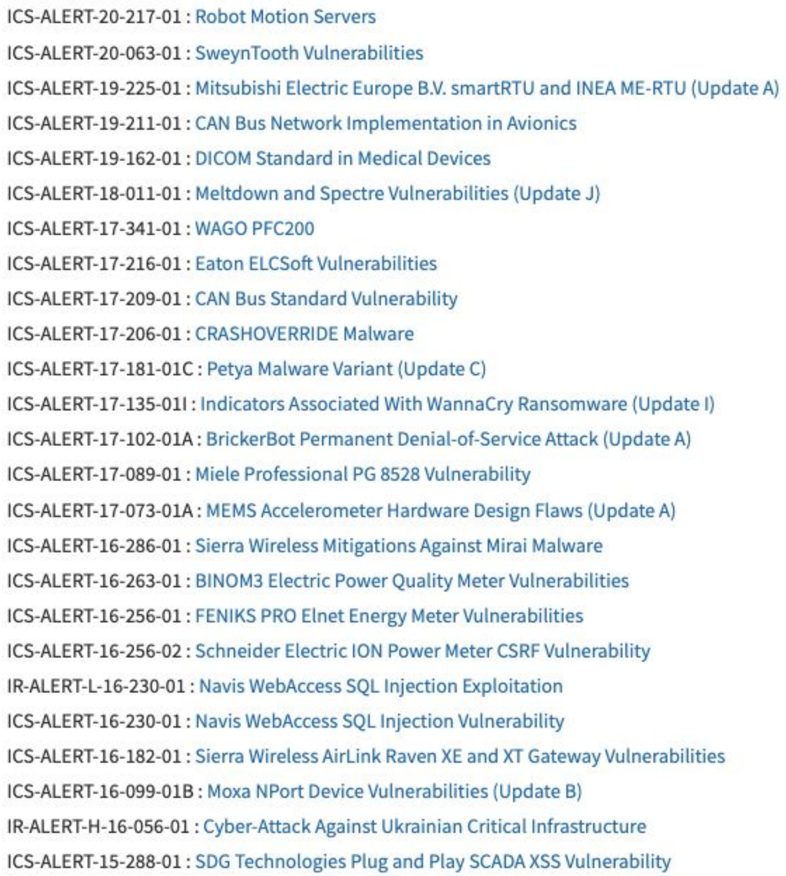
ICSA-21-350-16 : Siemens Healthineers syngo fastView

ICSA-21-350-17 : Siemens JT Utilities and JT Open Toolkit

ICSA-21-350-18 : Siemens Teamcenter Active Workspace

ICSA-21-350-19 : Siemens SiPass Integrated

https://us-cert.cisa.gov/ics/advisories



ICS-ALERT-20-217-01 : Robot Motion Servers

ICS-ALERT-20-063-01 : SweynTooth Vulnerabilities

ICS-ALERT-19-225-01 : Mitsubishi Electric Europe B.V. smartRTU and INEA ME-RTU (Update A)

ICS-ALERT-19-211-01 : CAN Bus Network Implementation in Avionics

ICS-ALERT-19-162-01 : DICOM Standard in Medical Devices

ICS-ALERT-18-011-01 : Meltdown and Spectre Vulnerabilities (Update J)

ICS-ALERT-17-341-01 : WAGO PFC200

ICS-ALERT-17-216-01 : Eaton ELCSoft Vulnerabilities

ICS-ALERT-17-209-01 : CAN Bus Standard Vulnerability

ICS-ALERT-17-206-01 : CRASHOVERRIDE Malware

ICS-ALERT-17-181-01C : Petya Malware Variant (Update C)

ICS-ALERT-17-135-01I : Indicators Associated With WannaCry Ransomware (Update I)

ICS-ALERT-17-102-01A : BrickerBot Permanent Denial-of-Service Attack (Update A)

ICS-ALERT-17-089-01 : Miele Professional PG 8528 Vulnerability

ICS-ALERT-17-073-01A : MEMS Accelerometer Hardware Design Flaws (Update A)

ICS-ALERT-16-286-01 : Sierra Wireless Mitigations Against Mirai Malware

ICS-ALERT-16-263-01 : BINOM3 Electric Power Quality Meter Vulnerabilities

ICS-ALERT-16-256-01 : FENIKS PRO Elnet Energy Meter Vulnerabilities

ICS-ALERT-16-256-02 : Schneider Electric ION Power Meter CSRF Vulnerability

IR-ALERT-L-16-230-01 : Navis WebAccess SQL Injection Exploitation

ICS-ALERT-16-230-01 : Navis WebAccess SQL Injection Vulnerability

ICS-ALERT-16-182-01 : Sierra Wireless AirLink Raven XE and XT Gateway Vulnerabilities

ICS-ALERT-16-099-01B : Moxa NPort Device Vulnerabilities (Update B)

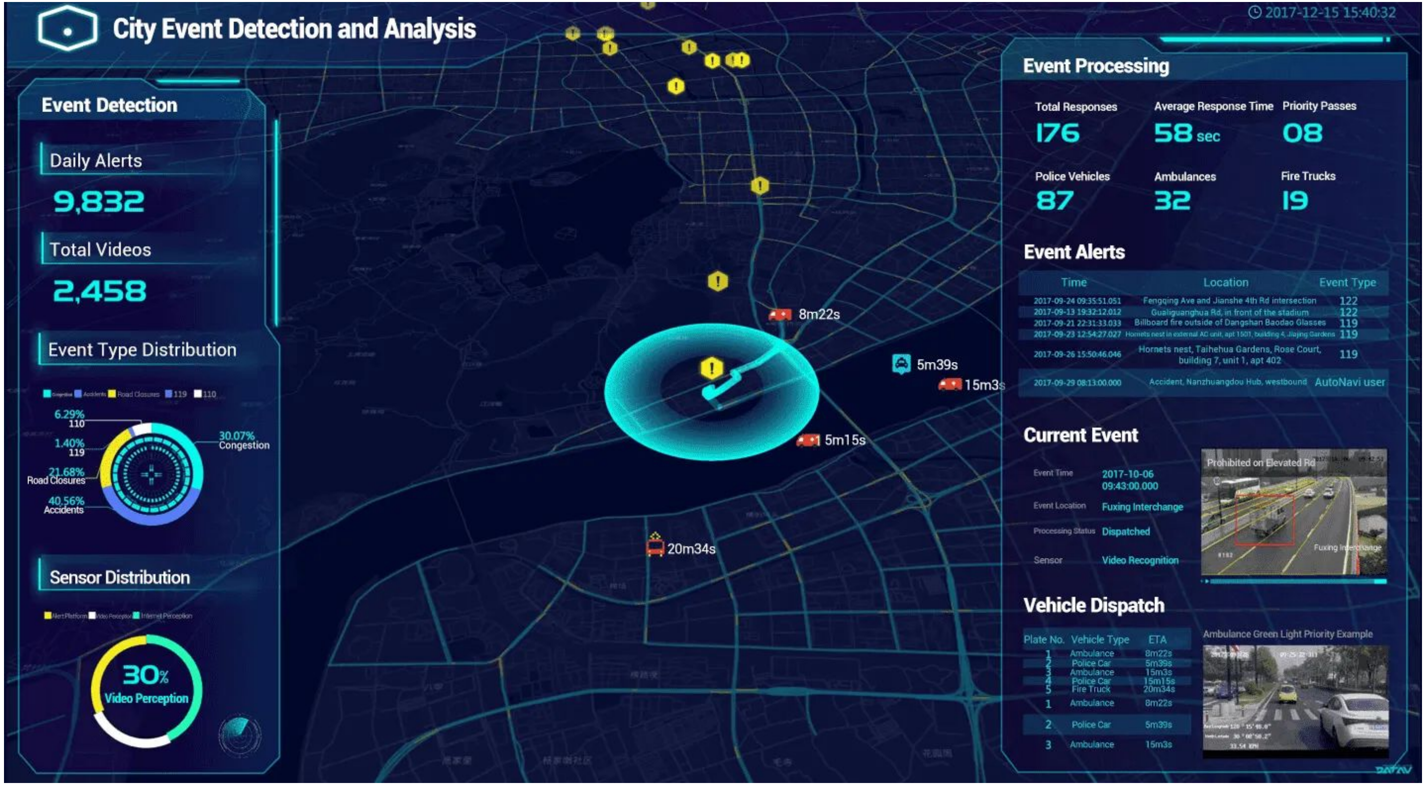
IR-ALERT-H-16-056-01 : Cyber-Attack Against Ukrainian Critical Infrastructure

ICS-ALERT-15-288-01 : SDG Technologies Plug and Play SCADA XSS Vulnerability

https://us-cert.cisa.gov/ics/alerts

In China, Alibaba's data-hungry AI is controlling (and watching) cities

City Brain monitors every vehicle in the Chinese city of Hangzhou, and has helped reduce traffic jams by 15 per cent. Now it is heading for Kuala Lumpur.



City Event Detection and Analysis

2017-12-15 15:40:32

Event Detection

Daily Alerts: 9,832

Total Videos: 2,458

Event Type Distribution

Sensor Distribution

Event Processing

Total Responses	Average Response Time	Priority Passes
176	58 sec	08

Police Vehicles	Ambulances	Fire Trucks
87	32	19

Event Alerts

Time	Location	Event Type
2017-09-24 09:35:51.051	Fengqing Ave and Jianshe 4th Rd intersection	122
2017-09-13 19:32:12.012	Gualiguanghua Rd, in front of the stadium	122
2017-09-21 22:31:33.033	Billboard fire outside of Dangshan Baodao Glasses	119
2017-09-23 12:54:27.027	Hornets nest in external AC unit, apt 1501, building 4, Jiajing Gardens	119
2017-09-26 15:50:46.046	Hornets nest, Taihehua Gardens, Rose Court, building 7, unit 1, apt 402	119
2017-09-29 08:13:00.000	Accident, Nanzhuangdou Hub, westbound	AutoNavi user

Current Event

Event Time: 2017-10-06 09:43:00.000

Event Location: Fuxing Interchange

Processing Status: Dispatched

Sensor: Video Recognition

Vehicle Dispatch

Plate No.	Vehicle Type	ETA
1	Ambulance	8m22s
2	Police Car	5m39s
3	Ambulance	15m3s
4	Police Car	15m15s
5	Fire Truck	20m34s
1	Ambulance	8m22s
2	Police Car	5m39s
3	Ambulance	15m3s

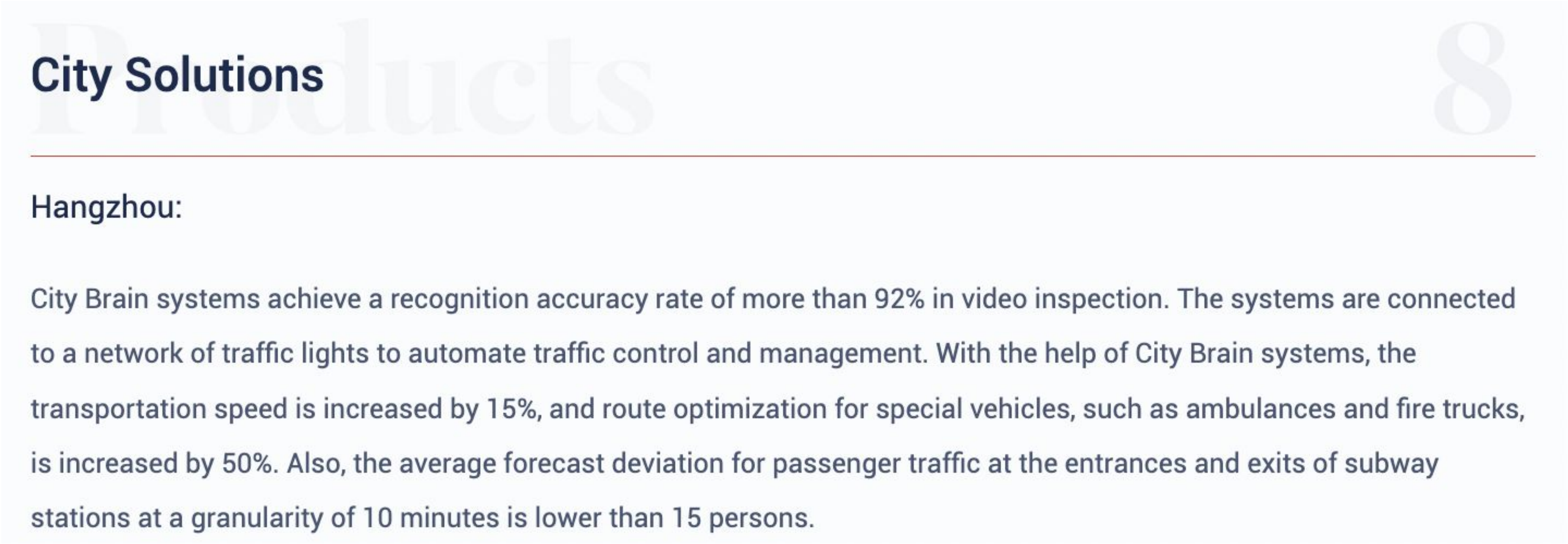
Ambulance Green Light Priority Example

https://www.wired.co.uk/article/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur

Machine Intelligence

City Brain Lab

The City Brain Lab is committed to building new infrastructure for future cities by using data, also opening up a "pipeline" of city data. The solutions have been deployed in Hangzhou, Suzhou, Shanghai, Macau, Malaysia and etc., which assists to solve problems of transportation, security, municipal construction, urban planning and etc. Framework "City Brain" is one of the largest public artificial intelligence systems worldwide.

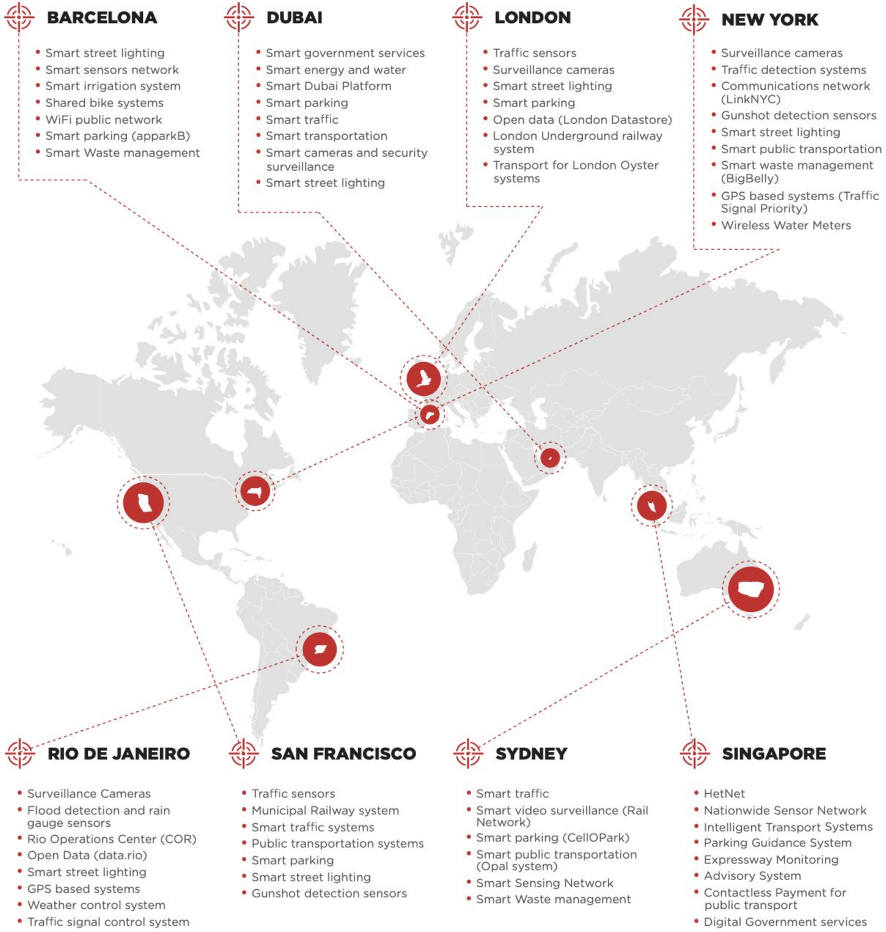


City Solutions

Hangzhou:

City Brain systems achieve a recognition accuracy rate of more than 92% in video inspection. The systems are connected to a network of traffic lights to automate traffic control and management. With the help of City Brain systems, the transportation speed is increased by 15%, and route optimization for special vehicles, such as ambulances and fire trucks, is increased by 50%. Also, the average forecast deviation for passenger traffic at the entrances and exits of subway stations at a granularity of 10 minutes is lower than 15 persons.

https://damo.alibaba.com/labs/city-brain



BARCELONA

- Smart street lighting
- Smart sensors network
- Smart irrigation system
- Shared bike systems
- WiFi public network
- Smart parking (apparkB)
- Smart Waste management

DUBAI

- Smart government services
- Smart energy and water
- Smart Dubai Platform
- Smart parking
- Smart traffic
- Smart transportation
- Smart cameras and security surveillance
- Smart street lighting

LONDON

- Traffic sensors
- Surveillance cameras
- Smart street lighting
- Smart parking
- Open data (London Datastore)
- London Underground railway system
- Transport for London Oyster systems

NEW YORK

- Surveillance cameras
- Traffic detection systems
- Communications network (LinkNYC)
- Gunshot detection sensors
- Smart street lighting
- Smart public transportation
- Smart waste management (BigBelly)
- GPS based systems (Traffic Signal Priority)
- Wireless Water Meters

RIO DE JANEIRO

- Surveillance Cameras
- Flood detection and rain gauge sensors
- Rio Operations Center (COR)
- Open Data (data.rio)
- Smart street lighting
- GPS based systems
- Weather control system
- Traffic signal control system

SAN FRANCISCO

- Traffic sensors
- Municipal Railway system
- Smart traffic systems
- Public transportation systems
- Smart parking
- Smart street lighting
- Gunshot detection sensors

SYDNEY

- Smart traffic
- Smart video surveillance (Rail Network)
- Smart parking (CellOPark)
- Smart public transportation (Opal system)
- Smart Sensing Network
- Smart Waste management

SINGAPORE

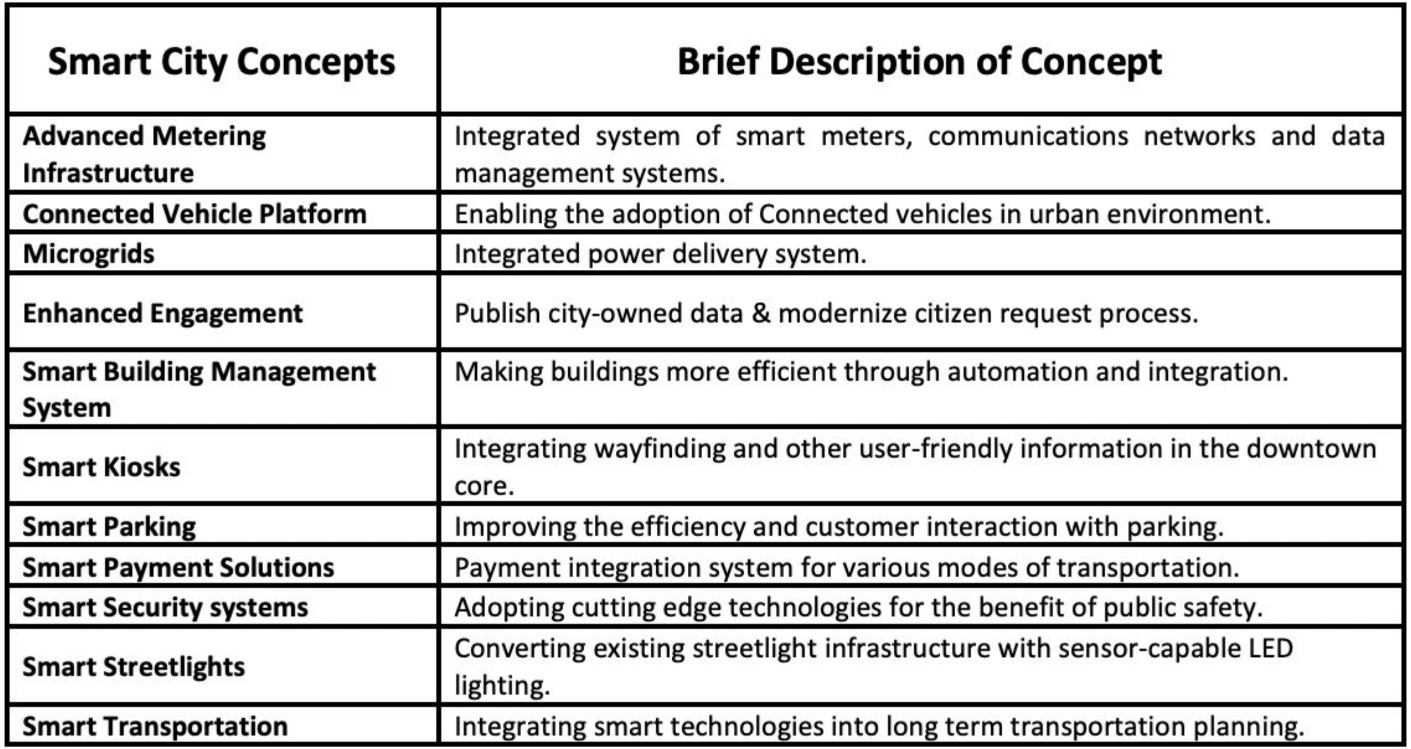
- HetNet
- Nationwide Sensor Network
- Intelligent Transport Systems
- Parking Guidance System
- Expressway Monitoring
- Advisory System
- Contactless Payment for public transport
- Digital Government services

https://securingsmartcities.org/wp-content/uploads/2019/01/SmartCities-cybersecurity-worries.pdf

SECURE SMART CITIES

The Secure Smart Cities team is a community focused initiative of the National Cyber Security Center 501(c)3. The strategy of the secure Smart Cities team is to garner interest of potential strategic partners, and spark innovative ideas. Smart city initiatives are becoming ubiquitous across the nation as population numbers continue to rise in urban environments and they are expected to jump from 54% to 66% by the middle of the century. In order to prepare for this transformation, cities are looking for answers to aid in the efficiency of transportation, housing, public health, and water. Those answers lie in the integration and interoperability of the Internet of Things (IoT) and Smart Technology, but this solution leaves the privacy and data of a city's critical infrastructure and the citizens more vulnerable to cyber attacks than ever before.

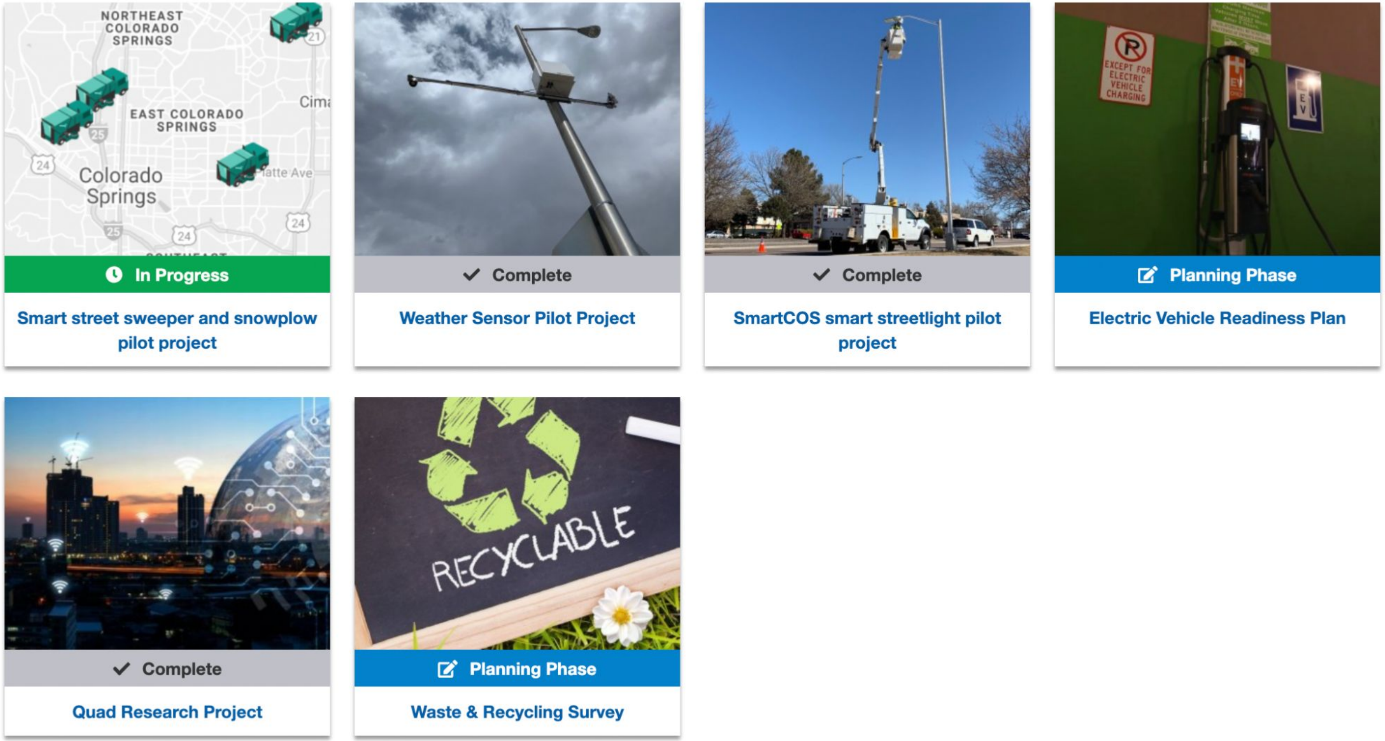
https://cyber-center.org/ssc/



Smart City Concepts	Brief Description of Concept
Advanced Metering Infrastructure	Integrated system of smart meters, communications networks and data management systems.
Connected Vehicle Platform	Enabling the adoption of Connected vehicles in urban environment.
Microgrids	Integrated power delivery system.
Enhanced Engagement	Publish city-owned data & modernize citizen request process.
Smart Building Management System	Making buildings more efficient through automation and integration.
Smart Kiosks	Integrating wayfinding and other user-friendly information in the downtown core.
Smart Parking	Improving the efficiency and customer interaction with parking.
Smart Payment Solutions	Payment integration system for various modes of transportation.
Smart Security systems	Adopting cutting edge technologies for the benefit of public safety.
Smart Streetlights	Converting existing streetlight infrastructure with sensor-capable LED lighting.
Smart Transportation	Integrating smart technologies into long term transportation planning.

The City of Colorado Springs
&
Colorado Springs Utilities
Smart City Strategy

https://coloradosprings.gov/sites/default/files/inline-images/smartcos_strategy_final_rdoc.pdf



In Progress
Smart street sweeper and snowplow pilot project

✓ Complete
Weather Sensor Pilot Project

✓ Complete
SmartCOS smart streetlight pilot project

Planning Phase
Electric Vehicle Readiness Plan

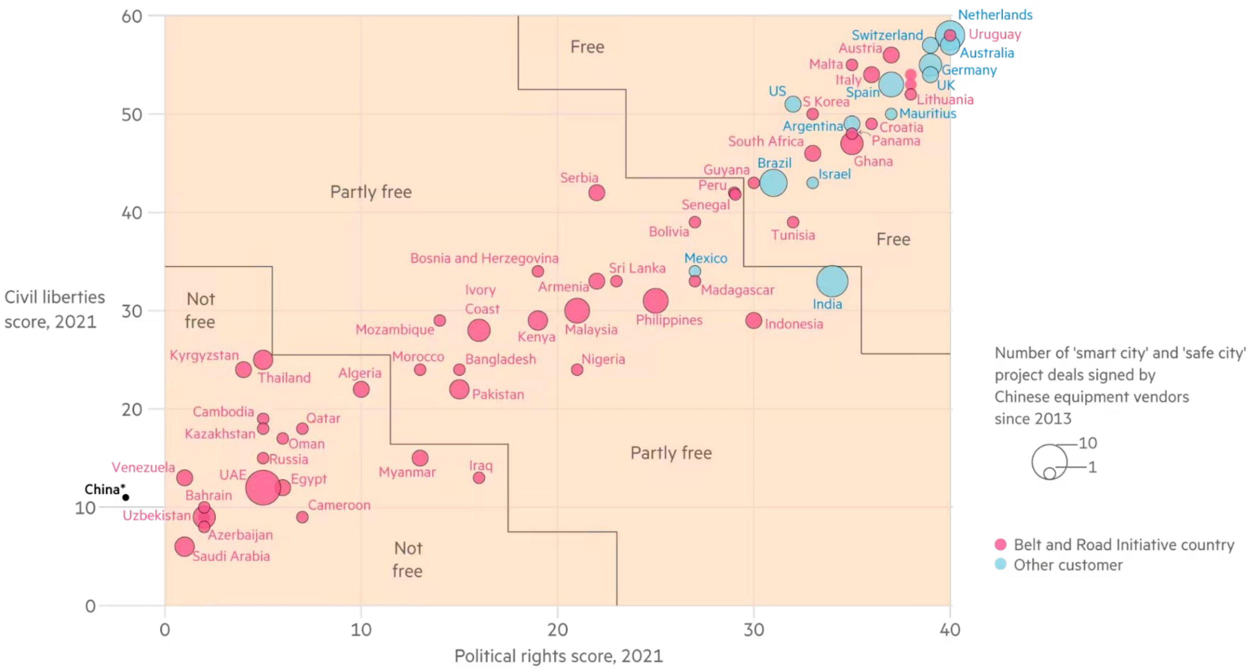
✓ Complete
Quad Research Project

Planning Phase
Waste & Recycling Survey

The City of Colorado Springs
&
Colorado Springs Utilities
Smart City Strategy

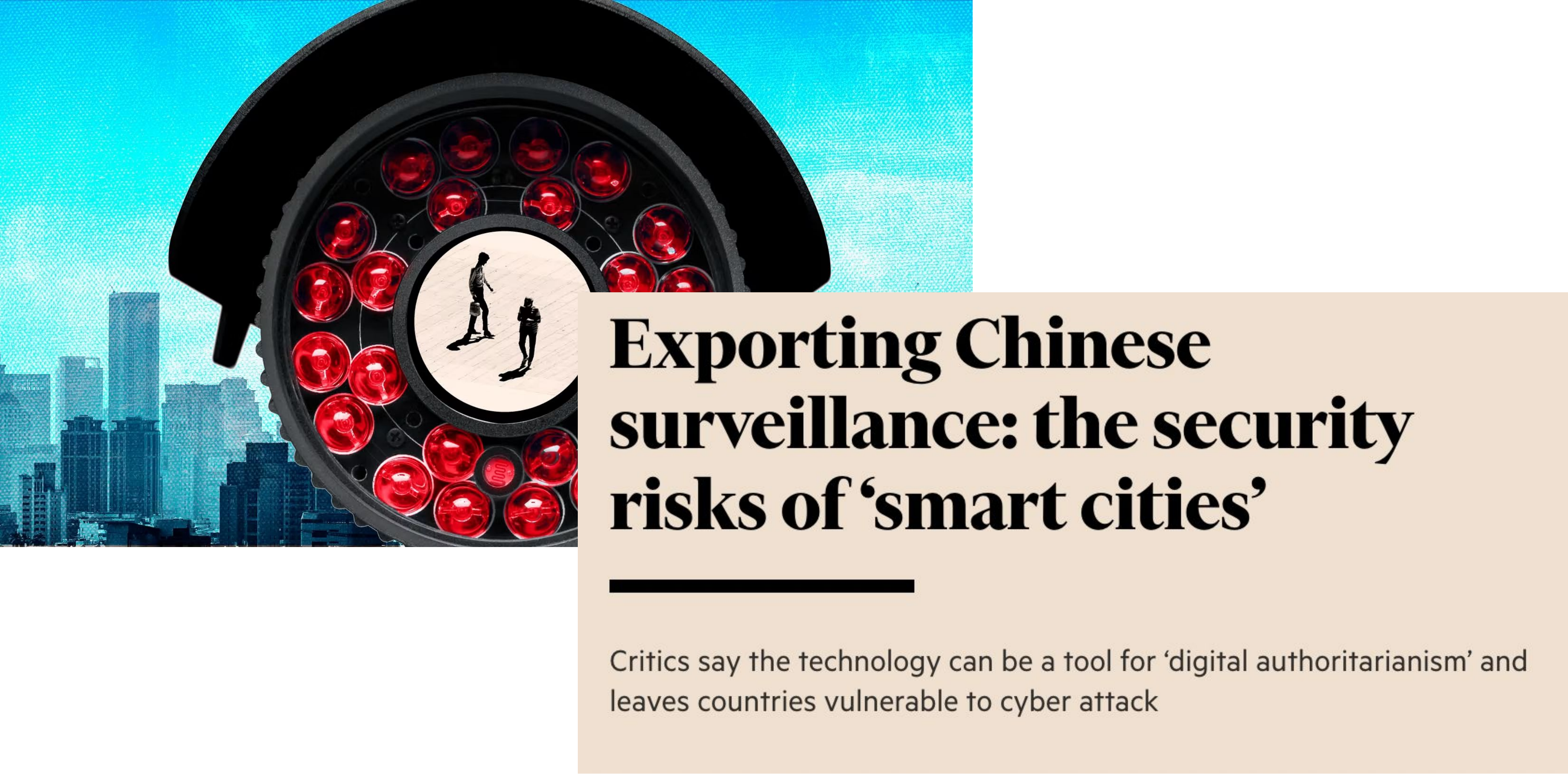
https://coloradosprings.gov/sites/default/files/inline-images/smartcos_strategy_final_rdoc.pdf

Authoritarian regimes are keen on China's surveillance technology — but they are not the only customers



*It is possible for a country's political rights score to be less than zero
Graphic: Alan Smith Sources: RWR Advisory, Freedom House
© FT

https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab

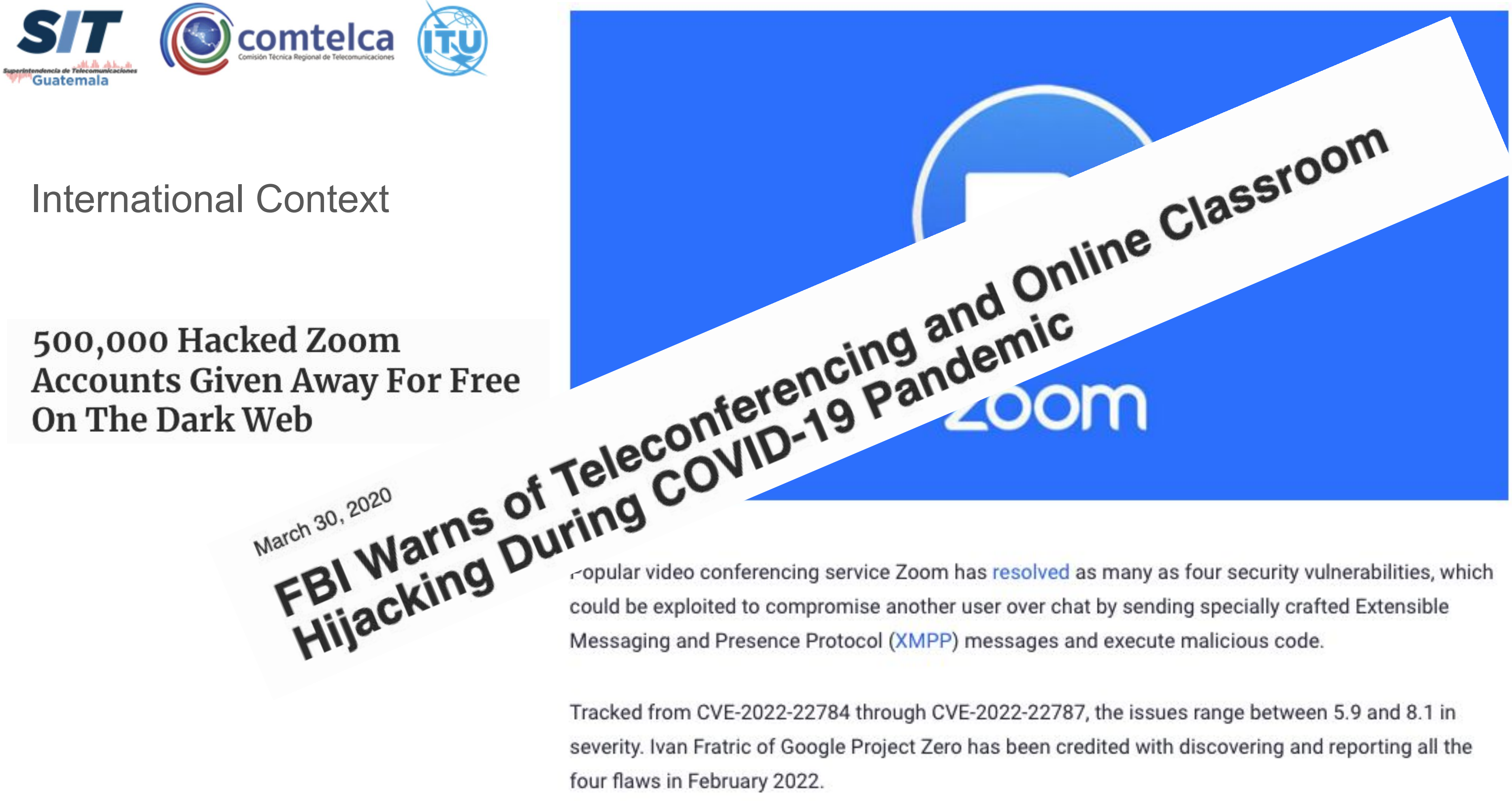


Exporting Chinese surveillance: the security risks of ‘smart cities’

Critics say the technology can be a tool for ‘digital authoritarianism’ and leaves countries vulnerable to cyber attack

https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab

International Context



500,000 Hacked Zoom Accounts Given Away For Free On The Dark Web

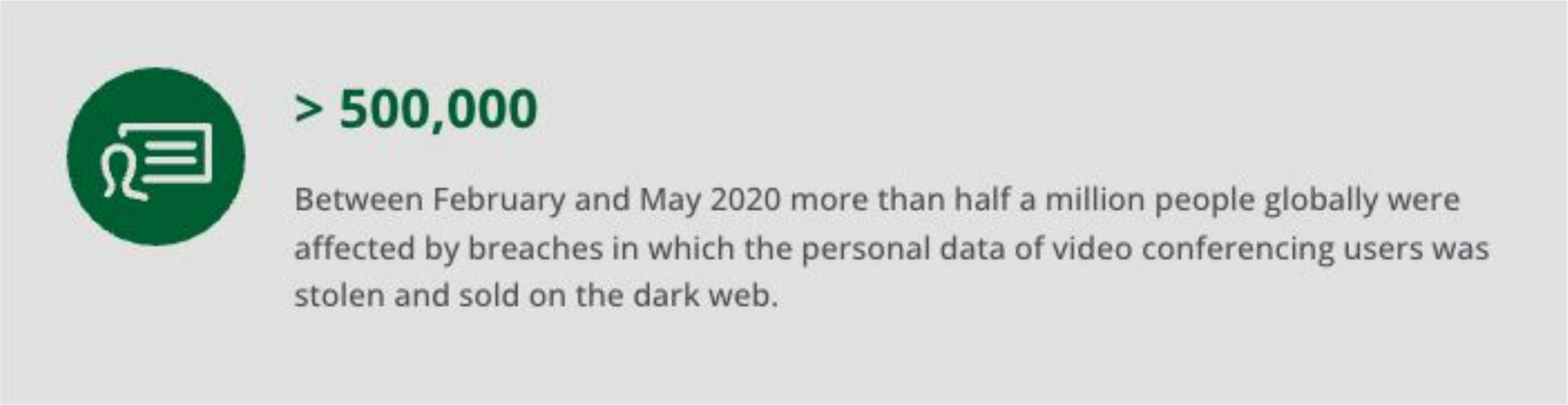
March 30, 2020

FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

ᴾopular video conferencing service Zoom has resolved as many as four security vulnerabilities, which could be exploited to compromise another user over chat by sending specially crafted Extensible Messaging and Presence Protocol (XMPP) messages and execute malicious code.

Tracked from CVE-2022-22784 through CVE-2022-22787, the issues range between 5.9 and 8.1 in severity. Ivan Fratric of Google Project Zero has been credited with discovering and reporting all the four flaws in February 2022.

International Context

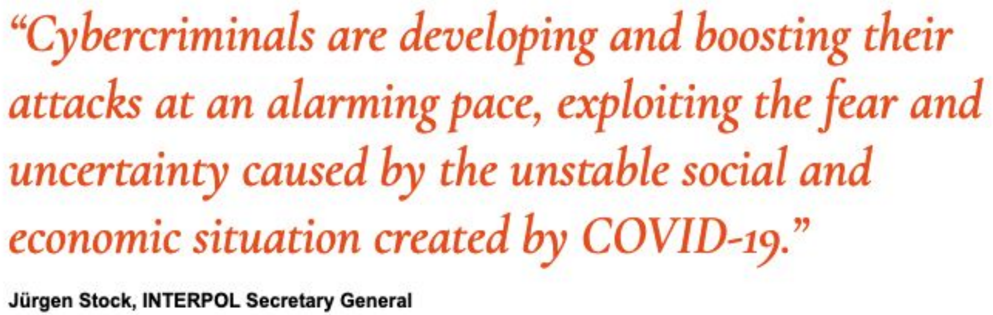


> 500,000

Between February and May 2020 more than half a million people globally were affected by breaches in which the personal data of video conferencing users was stolen and sold on the dark web.

Source: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

International Context



"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."

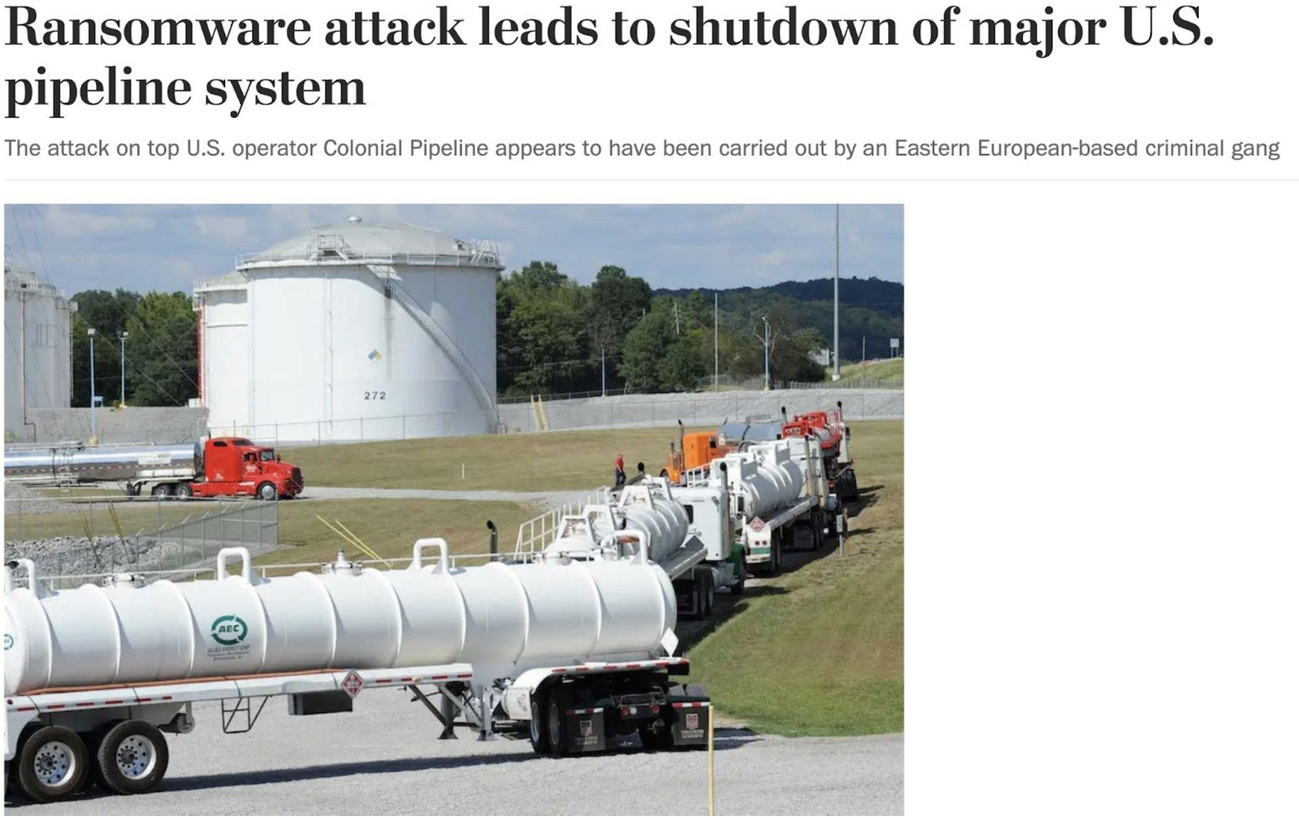
Jürgen Stock, INTERPOL Secretary General

INTERPOL report shows alarming rate of cyberattacks during COVID-19

4 August 2020

INTERPOL

Fuente: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19



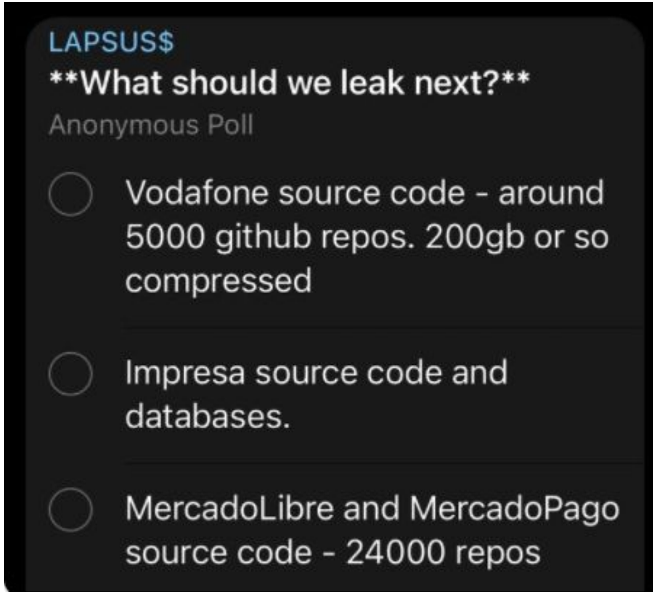
Ransomware attack leads to shutdown of major U.S. pipeline system

The attack on top U.S. operator Colonial Pipeline appears to have been carried out by an Eastern European-based criminal gang

Argentinian e-commerce giant Mercado Libre has confirmed "unauthorized access" to a part of its source code this week.

Mercado additionally says data of around 300,000 of its users was accessed by threat actors.

The company's announcement follows a poll by the data extortion group, Lapsus$ in which they threatened to leak data allegedly stolen from Mercado and other prominent companies.



LAPSUS$

What should we leak next?

Anonymous Poll

○ Vodafone source code - around 5000 github repos. 200gb or so compressed

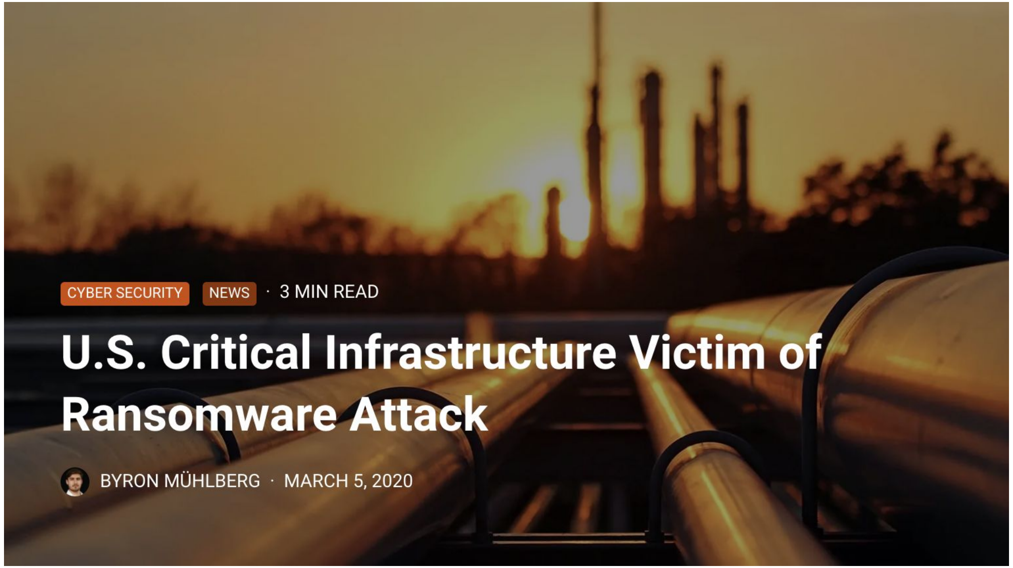
○ Impresa source code and databases.

○ MercadoLibre and MercadoPago source code - 24000 repos

Source: https://www.bleepingcomputer.com/news/security/e-commerce-giant-mercado-libre-confirms-source-code-data-breach/

0
DAYS
WITHOUT LOG4J CVE
imgflip.com

Contexto Internacional



CYBER SECURITY NEWS · 3 MIN READ

U.S. Critical Infrastructure Victim of Ransomware Attack

BYRON MÜHLBERG · MARCH 5, 2020

En febrero, CISA publicó un informe que describe un ataque de ransomware en una instalación de compresión de gas natural, que provocó el cierre de las operaciones en la instalación.

Contexto Internacional

"el aumento de las capacidades y la actividad de adversarios, la importancia crítica para la seguridad nacional de EE. UU. Y la vulnerabilidad de los sistemas OT, la infraestructura civil se convierte en objetivos atractivos para los actores extranjeros".

Contexto Internacional

REUTERS

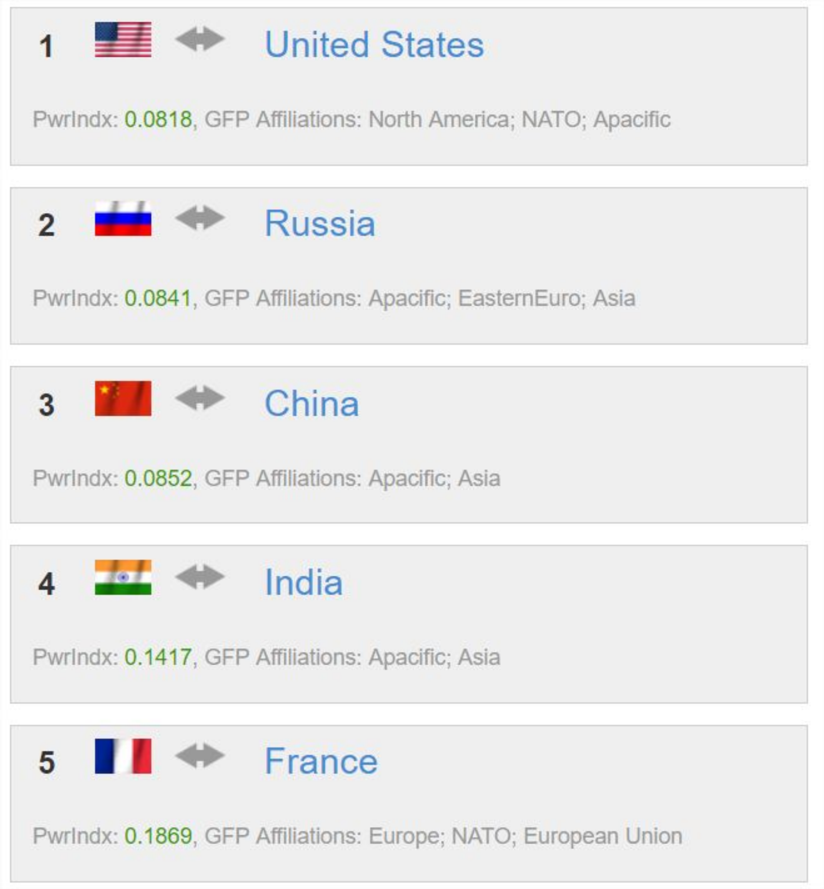
Ukraine has been forced to turn to back-up power sources in recent months following a spate of power cuts

El 23 de diciembre de 2015, tres empresas regionales de distribución de electricidad de Ucrania, Kyivoblenergo, Prykarpattyaoblenergo y Chernivtsioblenergo, sufrieron cortes de energía debido a un ciberataque.

Diferencias

- Infraestructuras críticas protegidas vs no protegidas no se diferencian en el ciberespacio
- Infraestructuras críticas humanitarias no tienen forma de ser “marcadas” en el ciberespacio
- Diferenciar objetivos civiles vs militares también es muy complejo
- Actores no estatales puede obtener alto poder en el ciberespacio
- Las ciberarmas poseen atributos no contemplados en leyes de guerra
- El desarrollo de ciberarmas se mantiene en secreto
- Las ciberoperaciones pueden mantenerse secretas e indetectables

Diferencias



1 United States

PwrIndx: 0.0818, GFP Affiliations: North America; NATO; Apacific

2 Russia

PwrIndx: 0.0841, GFP Affiliations: Apacific; EasternEuro; Asia

3 China

PwrIndx: 0.0852, GFP Affiliations: Apacific; Asia

4 India

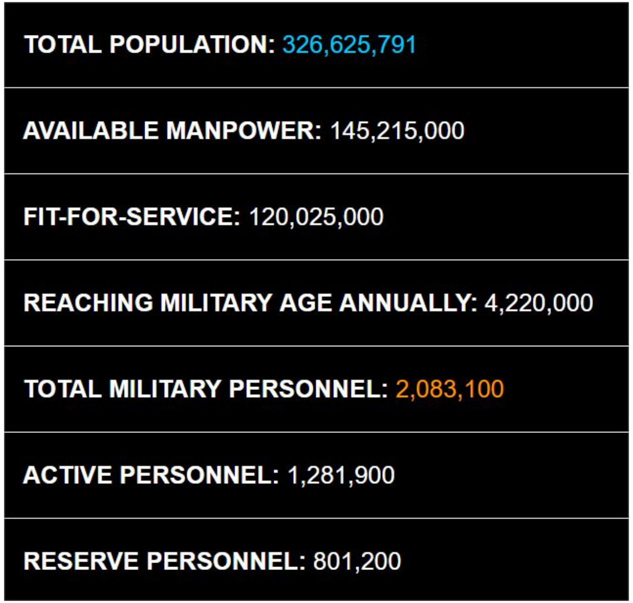
PwrIndx: 0.1417, GFP Affiliations: Apacific; Asia

5 France

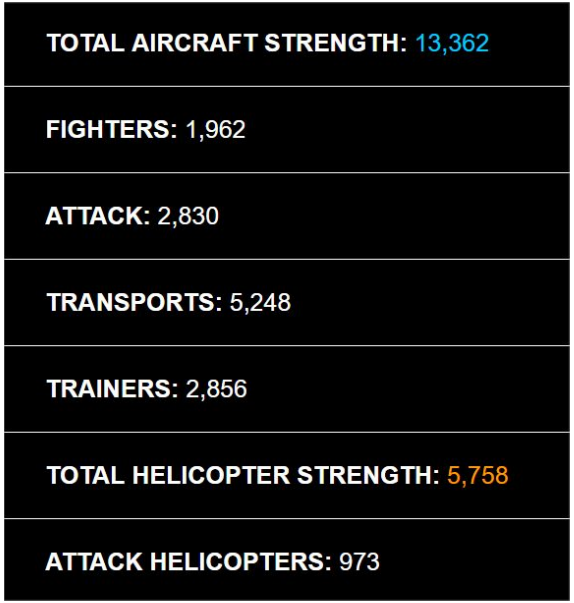
PwrIndx: 0.1869, GFP Affiliations: Europe; NATO; European Union

Fuente: https://www.globalfirepower.com

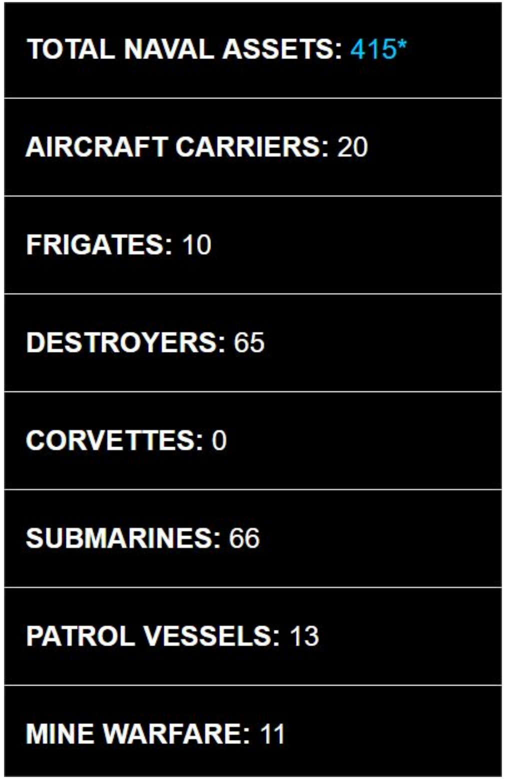
Diferencias



TOTAL POPULATION:	326,625,791
AVAILABLE MANPOWER:	145,215,000
FIT-FOR-SERVICE:	120,025,000
REACHING MILITARY AGE ANNUALLY:	4,220,000
TOTAL MILITARY PERSONNEL:	2,083,100
ACTIVE PERSONNEL:	1,281,900
RESERVE PERSONNEL:	801,200



TOTAL AIRCRAFT STRENGTH:	13,362
FIGHTERS:	1,962
ATTACK:	2,830
TRANSPORTS:	5,248
TRAINERS:	2,856
TOTAL HELICOPTER STRENGTH:	5,758
ATTACK HELICOPTERS:	973



TOTAL NAVAL ASSETS:	415*
AIRCRAFT CARRIERS:	20
FRIGATES:	10
DESTROYERS:	65
CORVETTES:	0
SUBMARINES:	66
PATROL VESSELS:	13
MINE WARFARE:	11

Fuente: https://www.globalfirepower.com

Infraestructuras Críticas

- Una falla en los sistemas de Infraestructuras Críticas puede tener consecuencias catastróficas.
- Al aumentar las dependencias entre los diferentes sistemas, como por ejemplo, el suministro de agua depende de la electricidad para las estaciones de bombeo, la banca moderna que depende de las TIC y los servicios de bomberos que dependen del suministro de agua.
- Los efectos en cascada de una avería en un sistema en otros sistemas interconectados también deben contemplarse.
- Surge de la necesidad de minimizar las interrupciones críticas del servicio, los accidentes y, en particular, las fallas en cascada.

Contexto Internacional

90% of OT security teams suffered at least one damaging cyber-attack in the last two years

Source: Ponemon

Infraestructuras Críticas

LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS Y LA CIBERSEGURIDAD INDUSTRIAL

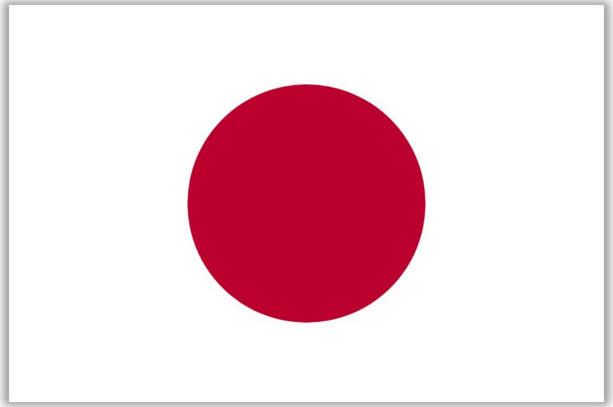
Infraestructuras Críticas

- Banca y Finanzas
- Gobierno Central y sus Servicios
- Comunicaciones y TICs
- Servicios de Emergencia y Rescate
- Energía/Electricidad
- Servicios de Salud
- Alimentos
- Transporte/Logística/Distribución
- Suministro de Agua

Australia

Infraestructuras Críticas

- Banca y Finanzas
- Gobierno Central y sus Servicios
- Comunicaciones y TICs
- Aviación
- Trenes
- Energía/Electricidad
- Gas
- Servicios de Salud
- Transporte/Logística/Distribución
- Suministro de Agua
-



Japón

Crearon en 2017 el Industrial Cyber Security Center of Excellente: https://www.ipa.go.jp

Infraestructuras Críticas

- Químicos
- Unidades Comerciales
- Comunicaciones
- Manufactura Crítica
- Represas Hidroeléctricas
- Bases de Defensa Industrial
- Servicios de Emergencia
- Energía
- Servicios Financieros
- Comida y Agricultura
- Gobierno
- Salud
- TICs
- Reactores nucleares, materiales y deshechos
- Sistemas de Transporte
- Suministro de Agua y Limpieza de Aguas

Estados Unidos

National Infrastructure Protection Plan: https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

Potential Increased Sources of Vulnerability

1. Most financial sector firms have already been using remote access facilities, however, **installed capacities may not have been enough to support most of the workforce** simultaneously, which increases potential security risks.
2. Cloud technologies are increasingly implemented and used to quickly deal with higher capacity needs. Under time and resource pressures, **inherent security risks coming with the usage of cloud services might not have been properly assessed** and existing controls might not be fully effective
3. Employees unfamiliar with working remotely and under stress caused by the pandemic, **can become easy targets of phishing** and social engineering attacks.
4. **Insecure endpoints** and **weak remote access authentication** are two main elements that increase the risk of such attacks succeeding.

Source: IMF Cybersecurity of Remote Work during the Pandemic

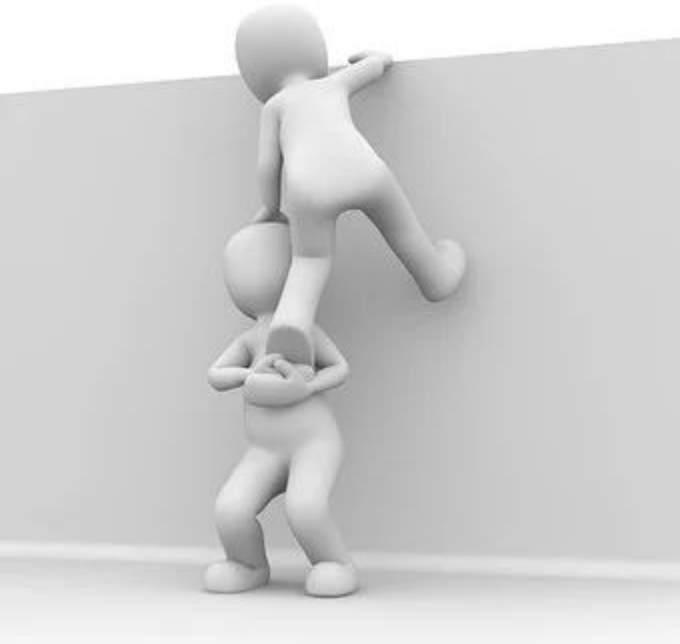
WFH Challenges

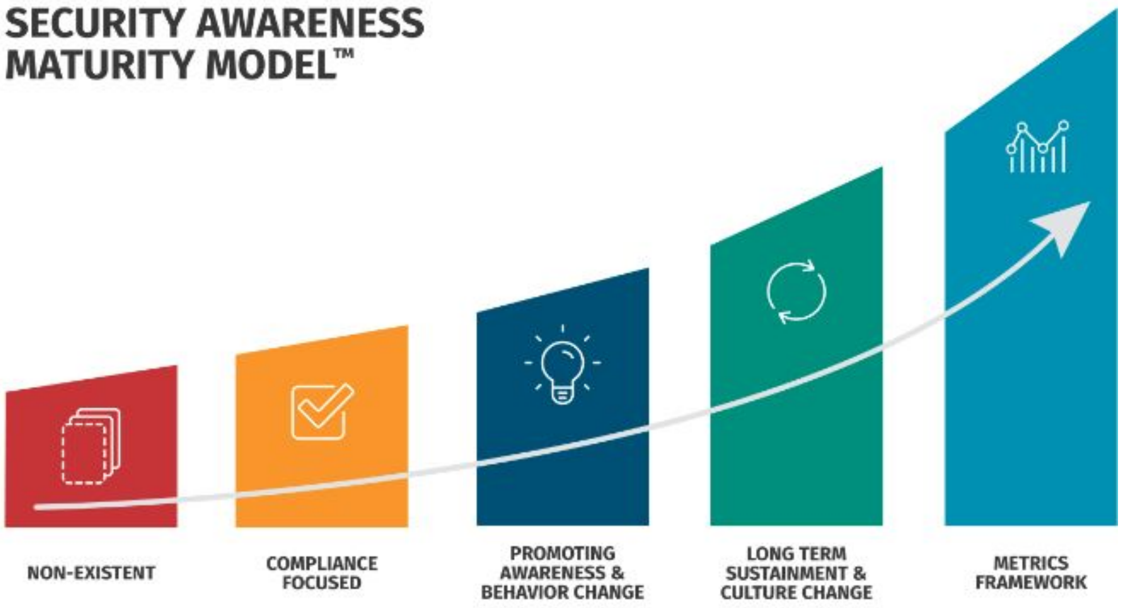
Personal Laptops

VPN Access & Secure Remote access

Zero Trust!

Trainings & Cybersecurity Awareness





SECURITY AWARENESS MATURITY MODEL™

NON-EXISTENT

COMPLIANCE FOCUSED

PROMOTING AWARENESS & BEHAVIOR CHANGE

LONG TERM SUSTAINMENT & CULTURE CHANGE

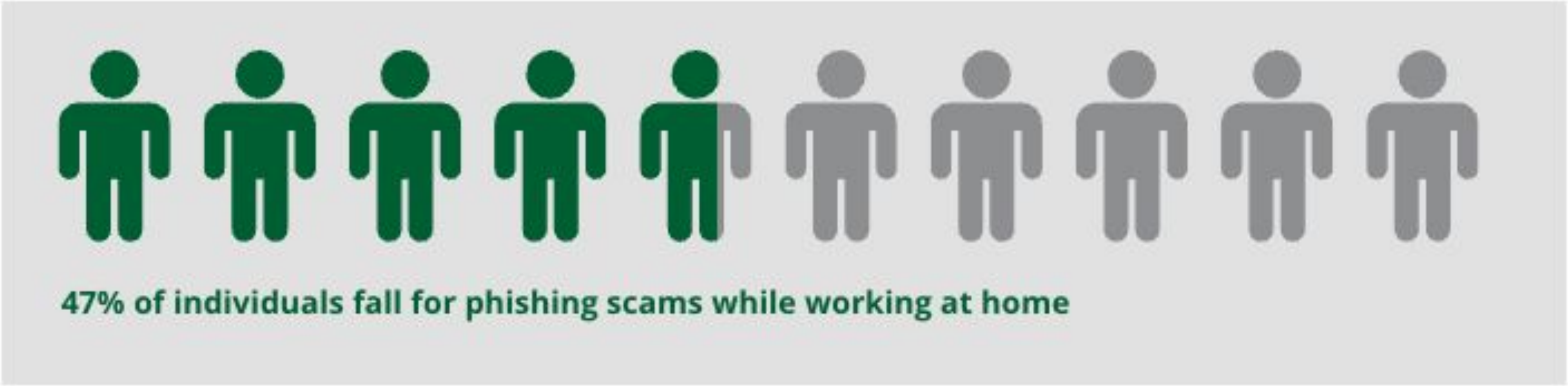
METRICS FRAMEWORK

Incident Response

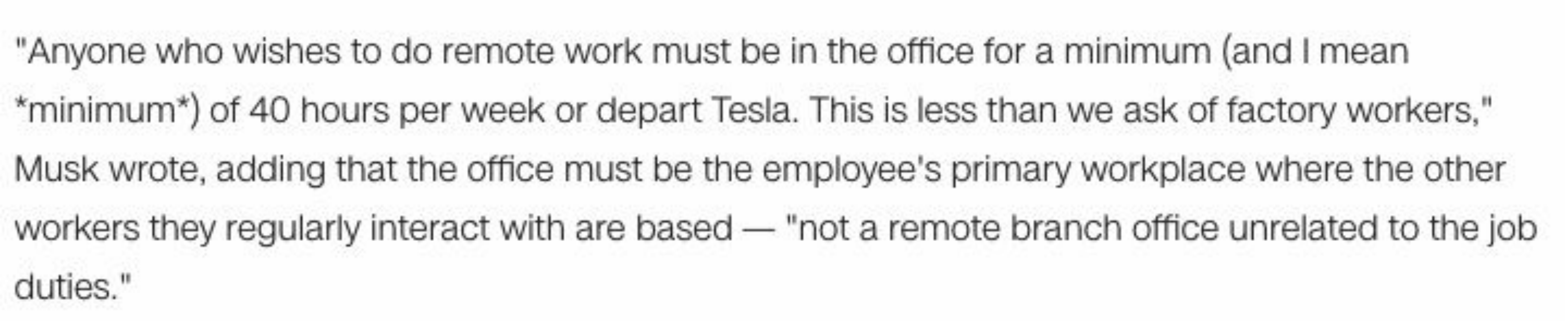
Far from home

No way home

No way home



47% of individuals fall for phishing scams while working at home hybrid?



"Anyone who wishes to do remote work must be in the office for a minimum (and I mean *minimum*) of 40 hours per week or depart Tesla. This is less than we ask of factory workers," Musk wrote, adding that the office must be the employee's primary workplace where the other workers they regularly interact with are based — "not a remote branch office unrelated to the job duties."

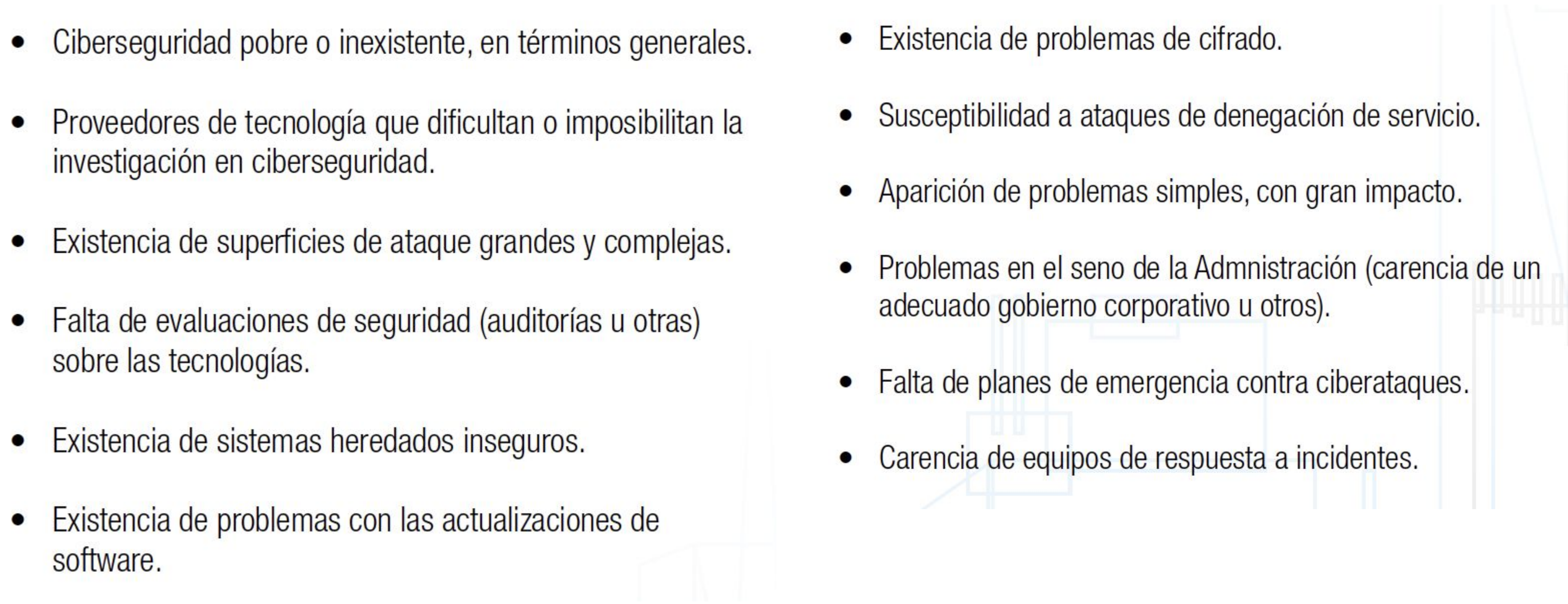
The cyber threat landscape is diverse

- **Malicious employees working from home with less supervision and fewer technical** controls may be tempted to carry out a fraud or other criminal activity
- Cybercriminals recognize that the **data security measures currently in place are ‘not fit for purpose’ or sufficiently robust** to prevent them from making successful cyberattacks
- The activities of **hacktivists** (hackers fighting for social and political issues) are adding to the cybersecurity threats
- **Script kiddies** (‘junior’ hackers with less technical skills) are testing out cyberattack packages on a variety of organizations and improving their skills.

During the pandemic, companies had to quickly adapt to new working conditions and thus opened new doors and more possibilities for cybercriminals. According to the European Union Agency for Cybersecurity, there are nine prime threat groups:

- **Ransomware** – attackers encrypt an organisation’s data and require payment to restore access
- **Cryptojacking** – when cybercriminals secretly use a victim’s computing power to generate cryptocurrency
- **Threats against data** – data breaches/leaks
- **Malware** – a software, which triggers a process that affects a system
- **Disinformation/misinformation** – the spread of misleading information
- **Non-malicious threats** – human errors and misconfigurations of a system
- **Threats against availability and integrity** – attacks that prevent the users of a system from accessing their information
- **Email-related threats** – aims at manipulating people to fall victims to an email attack
- **Supply chain threats** – attacking, for example a service provider, in order to gain access to a customer's data

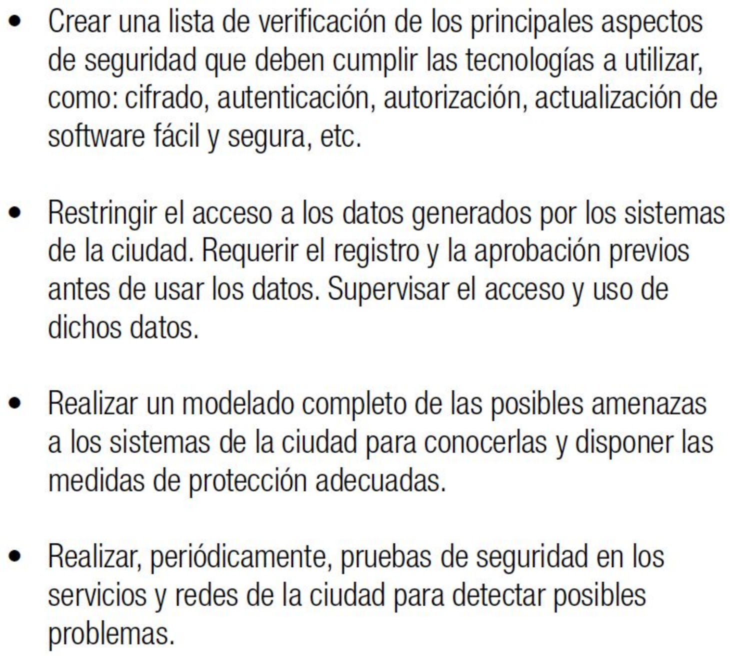
Desafíos de proteger una ciudad inteligente



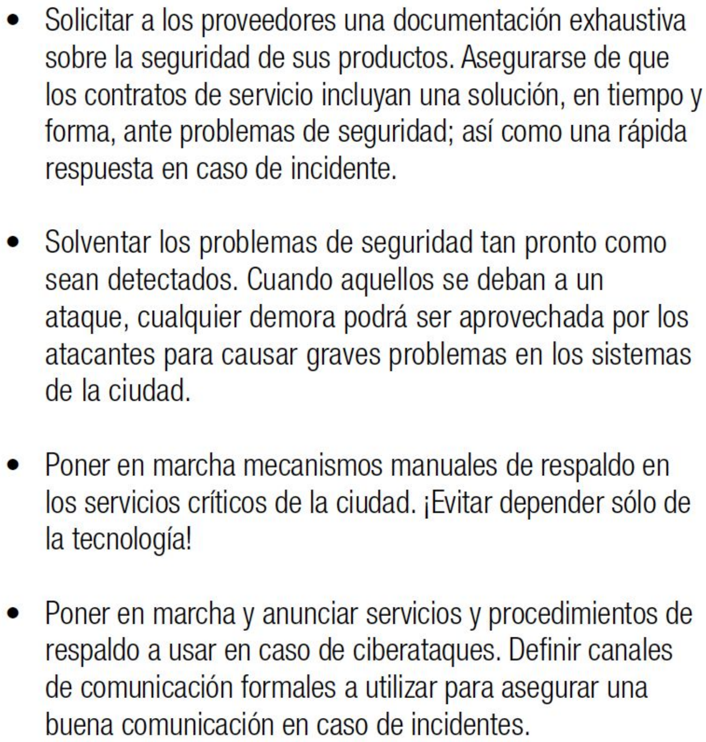
- Ciberseguridad pobre o inexistente, en términos generales.
- Proveedores de tecnología que dificultan o imposibilitan la investigación en ciberseguridad.
- Existencia de superficies de ataque grandes y complejas.
- Falta de evaluaciones de seguridad (auditorías u otras) sobre las tecnologías.
- Existencia de sistemas heredados inseguros.
- Existencia de problemas con las actualizaciones de software.
- Existencia de problemas de cifrado.
- Susceptibilidad a ataques de denegación de servicio.
- Aparición de problemas simples, con gran impacto.
- Problemas en el seno de la Admnistración (carencia de un adecuado gobierno corporativo u otros).
- Falta de planes de emergencia contra ciberataques.
- Carencia de equipos de respuesta a incidentes.

https://www.cci-es.org/activities/smart-cities-ante-el-desafio-de-la-seguridad_serie-smart-ot_2/

Recomendaciones para proteger una ciudad inteligente



- Crear una lista de verificación de los principales aspectos de seguridad que deben cumplir las tecnologías a utilizar, como: cifrado, autenticación, autorización, actualización de software fácil y segura, etc.
- Restringir el acceso a los datos generados por los sistemas de la ciudad. Requerir el registro y la aprobación previos antes de usar los datos. Supervisar el acceso y uso de dichos datos.
- Realizar un modelado completo de las posibles amenazas a los sistemas de la ciudad para conocerlas y disponer las medidas de protección adecuadas.
- Realizar, periódicamente, pruebas de seguridad en los servicios y redes de la ciudad para detectar posibles problemas.



- Solicitar a los proveedores una documentación exhaustiva sobre la seguridad de sus productos. Asegurarse de que los contratos de servicio incluyan una solución, en tiempo y forma, ante problemas de seguridad; así como una rápida respuesta en caso de incidente.
- Solventar los problemas de seguridad tan pronto como sean detectados. Cuando aquellos se deban a un ataque, cualquier demora podrá ser aprovechada por los atacantes para causar graves problemas en los sistemas de la ciudad.
- Poner en marcha mecanismos manuales de respaldo en los servicios críticos de la ciudad. ¡Evitar depender sólo de la tecnología!
- Poner en marcha y anunciar servicios y procedimientos de respaldo a usar en caso de ciberataques. Definir canales de comunicación formales a utilizar para asegurar una buena comunicación en caso de incidentes.

https://www.cci-es.org/activities/smart-cities-ante-el-desafio-de-la-seguridad_serie-smart-ot_2/

Foro sobre el fortalecimiento de la transformación digital en América Latina

7-8 de julio de 2022

Antigua, Guatemala

SIT Superintendencia de Telecomunicaciones Guatemala

comtelca Comisión Técnica Regional de Telecomunicaciones

ITU