SCASSI.
be secure

comet

Cybersecurity in Space Systems Operations

19 septembre 2019

Bringing together "cyber spatial" and "cyber space"

« and how cybercrime wants to benefit from it ... »

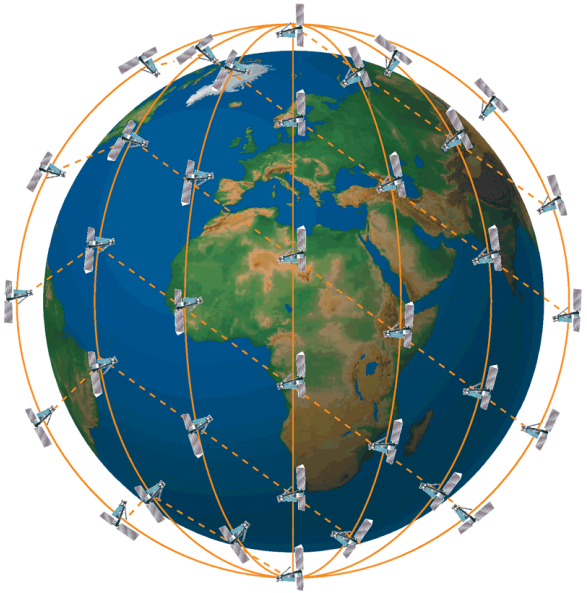
Fabrice CRASNIER

Senior Expert Consultant- Head of legal expertise activities (FORENSIC) - SCASSI-CYBER Laboratory - SCASSI Conseil - Doctoral student in artificial intelligence

- **After 27 years in the service of research units of the Gendarmerie Nationale, 17 of which were spent tracking cyber-delinquency, I joined SCASSI as a Senior Expert Consultant.**
- **I am in charge of forensic computer expertise activities at the SCASSI-CYBER Laboratory.**
- **Interested in companies and the issues related to security incidents, I aim to make people and property understand the impact this has on them.**

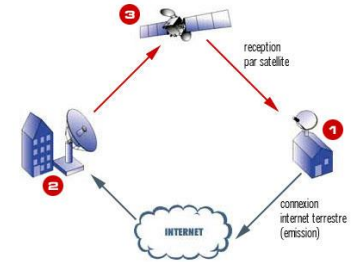
3 Presentation

- **Bringing together "cyber spatial" and "cyber space"**
  - Physical proximity
  - Strategic bringing
  - Economic activities
- **Paradigm shift**
  - The Internet's architecture
  - The Internet everywhere in the world
  - Increased transfer speed
- **The use of satellite data in cybercrime**
  - Satellite data in cyberspace
  - Cyber-threat
  - Trust in satellite data



4 Bringing together "cyber spatial" and "cyber espace"

- **Physical proximity**
  - Low Earth Orbit satellites are not new!
  - Low orbit's sensitivity to ground attack
- **Strategic bringing**
  - How France is preparing for real star wars
- **Economic activities**
  - Convergence of satellite and infra cloud data availability



5 Physical proximity

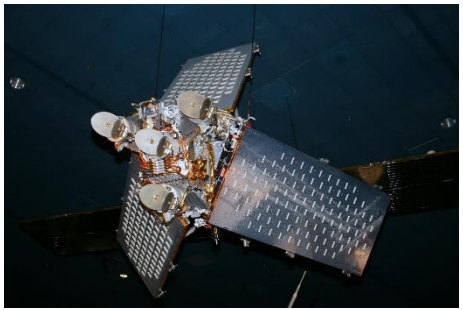
- **Low Earth Orbit satellites are not new!**

Take for example the Iridium project is a satellite telephone system. (*https://www.iridiumnext.com/*)

- This system was **designed in the early 1990s** by engineers from the American company Motorola
- environ **90 satellites** dont 66 actifs.
- Lack of customers and the company filed for **liquidation in August 1999**

The company was taken over in 2001 by a group of private investors,

The battle of space has begun.
Satellite cyber attacks, detection, interception, jamming of satellite communications



First generation Iridium satellite.

The Krassoukha-4 mobile electronic warfare complex.

6 Physical proximity

- **Low orbit's sensitivity to ground attack**

China conducted an ASAT weapon test last week by destroying one of its aging low-earth orbit weather satellites with a ballistic missile, creating a large amount of space debris.
China is thus showing its ability to destroy satellites in low orbit from the ground.
(CBC News · Posted: **Jan 18, 2007**)

https://www.cbc.ca/news/world/canada-voices-concern-over-chinese-missile-test-1.675488

Only a government has the weapons to carry out a ground attack to paralyze the constellation

7

Physical proximity

- **Satellites in low Earth orbit for institutional use**

Take for example the Iridium project is a satellite telephone system. (*https://www.iridiumnext.com/*)

In 2015, Iridium has just over 800,000 subscribers

The main users are professionals

- in the maritime, oil and air transport sectors,
- employees of government agencies (including the military),
- researchers and frequent travellers (journalists, sailors, rally or expedition organizers, and the military).
- **Machine to Machine connections represent more than half of all subscribers in 2015.**

Deployment of the 5th cluster of the Iridium Next constellation

Only one government could be interested in mounting a cyber attack to allow it to monitor another user government and would have the means to do so

8

Strategic bringing

- ## How France is preparing for real star wars

On **13 July 2019**, under the responsibility of the Air Force, **the large Space Command** was createdand will be **based in Toulouse**. .

Space is a new front to defend

how?

- **An evolution of the law in accordance with international law**
- **Actively defend French military and civilian satellites**
- **Creation of new means of monitoring**
- **Creating new defences from space.**
  - nano patrol satellites
  - power lasers for dazzling
  - Frequency jammer, etc,

The Cyber Defence Command (COMCYBER) was created on **May 4, 2017**. He is responsible for the protection of information systems under the responsibility of the Chief of the Defence Staff.

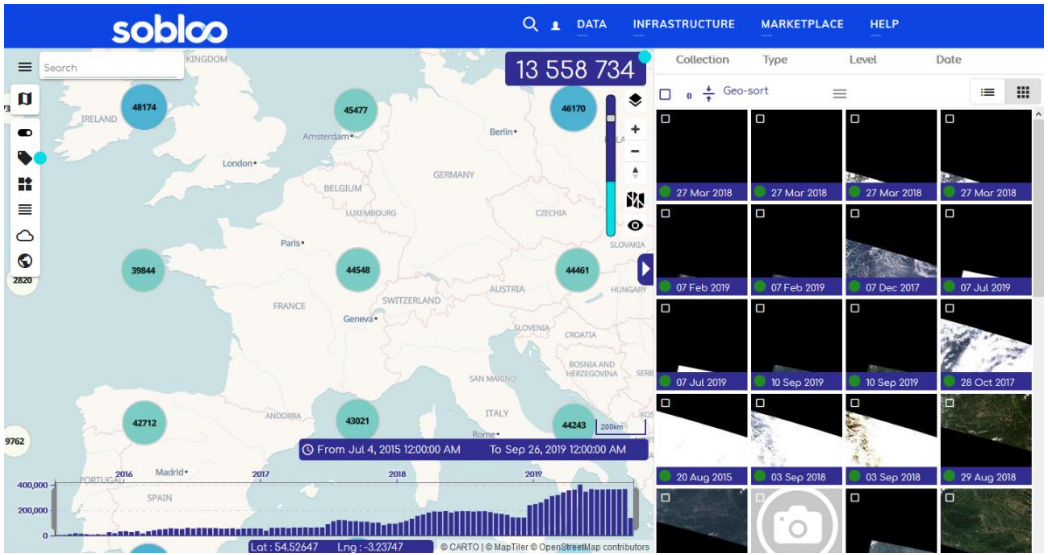
9

Economic activities

- **Convergence of satellite and infra cloud data availability,**

Space programs are intrinsically collections of data of all kinds (spatial, terrestrial, maritime, agricultural, etc.)

- Programme **COPERNICUS** (*https://copernicus.cnes.fr/fr*)
- Plateforme d'Airbus DS : **sobloo** (*https://sobloo.eu/*)
- plateforme d'Atos : **Mundi web services** https://mundiwebservices.com/



10

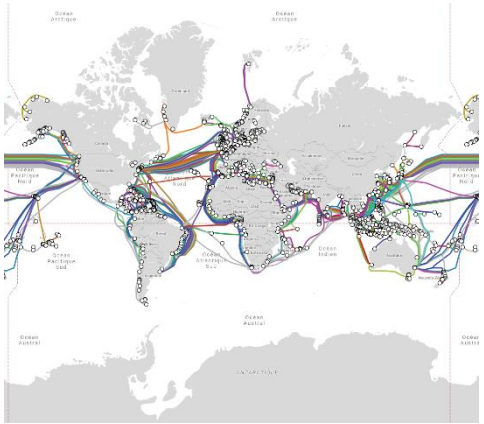
Paradigm shift

- **The Internet's architecture**
  - A mapping of the physical network of cyberspace
- **The Internet everywhere in the world**
  - The end of white zones
  - Increase of the number of Internet users worldwide
- **Increased transfer speed**
  - Un monde en HYPER-CONNEXION

11

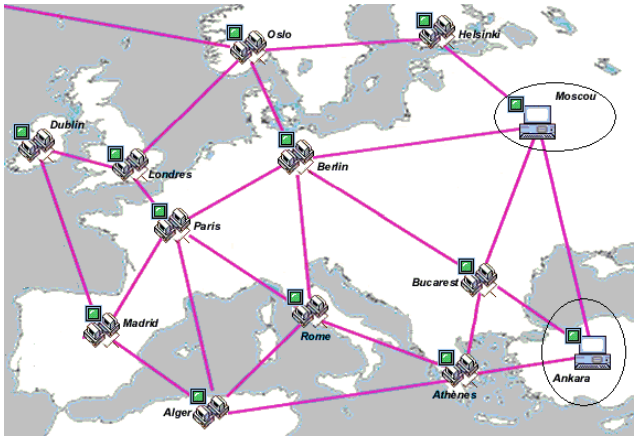
The Internet's architecture

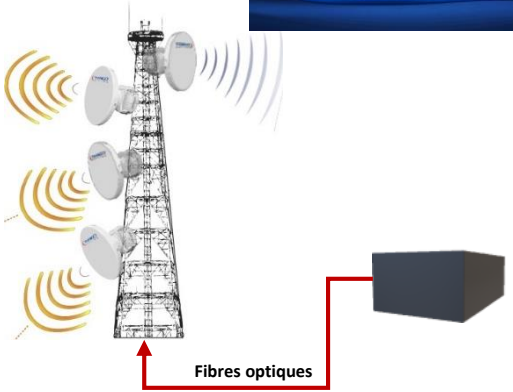
- **A mapping of the physical network of cyberspace**



https://www.submarinecablemap.com/

Vision 2D
of Cyberspace





https://www.antennesmobiles.fr/
https://www.cartoradio.fr

12

The Internet everywhere in the world

- **The end of white zones**

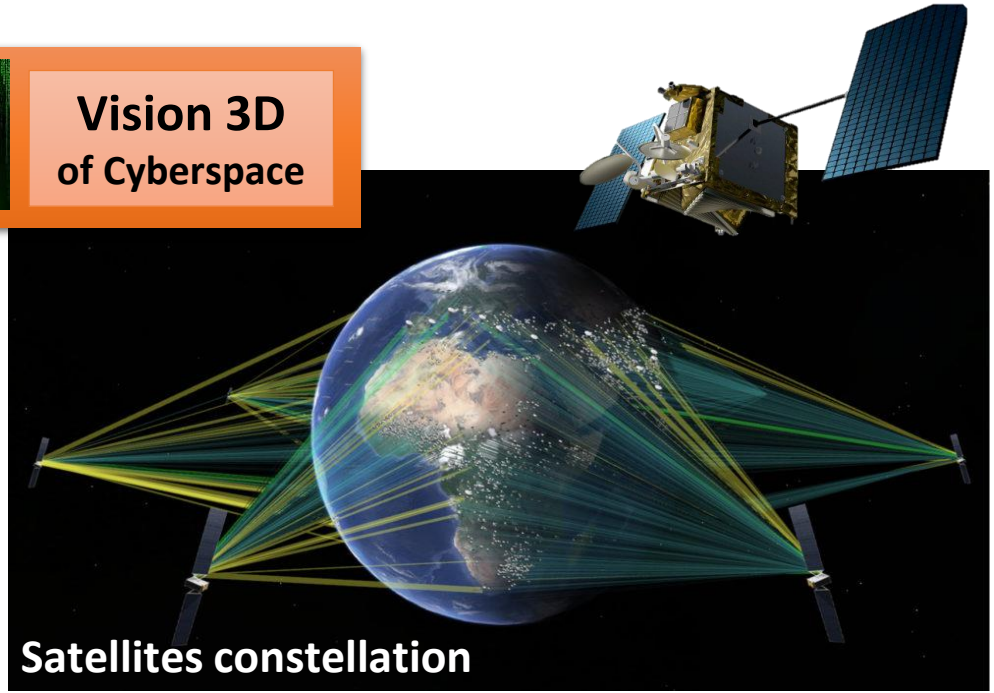
by boat fishing

in the countryside

in the desert

in the mountains

Vision 3D
of Cyberspace



13

The Internet everywhere in the world

- **Increase of the number of Internet users worldwide**

The arrival of constellations such as OneWeb, SpaceX and O3b will give :

- a second wind to this growth,
- new use,
- and new service possibilities.

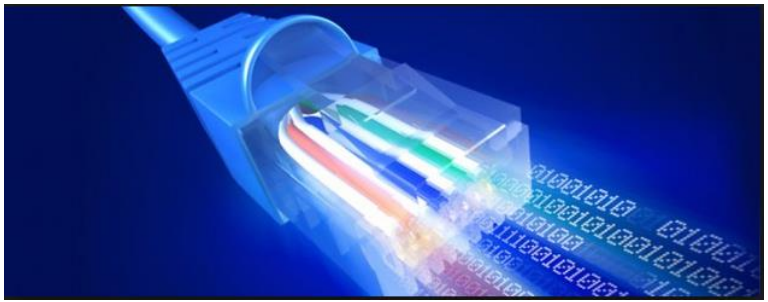
- **But also a new playground for cybercrime**

WORLD INTERNET USAGE AND POPULATION STATISTICS
2019 Mid-Year Estimates

World Regions	Population (2019 Est.)	Population % of World	Internet Users 30 June 2019	Penetration Rate (% Pop.)	Growth 2000-2019	Internet World %
Africa	1,320,038,716	17.1 %	522,809,480	39.6 %	11,481 %	11.5 %
Asia	4,241,972,790	55.0 %	2,300,469,859	54.2 %	1,913 %	50.7 %
Europe	829,173,007	10.7 %	727,559,682	87.7 %	592 %	16.0 %
Latin America / Caribbean	658,345,826	8.5 %	453,702,292	68.9 %	2,411 %	10.0 %
Middle East	258,356,867	3.3 %	175,502,589	67.9 %	5,243 %	3.9 %
North America	366,496,802	4.7 %	327,568,628	89.4 %	203 %	7.2 %
Oceania / Australia	41,839,201	0.5 %	28,636,278	68.4 %	276 %	0.6 %
WORLD TOTAL	7,716,223,209	100.0 %	**4,536,248,808**	58.8 %	1,157 %	100.0 %

14 Increased transfer speed

About 50 megabits per second in 2019



This speed will reduce end-to-end latency (ping), a key element to ensure a better user experience when using Internet services

technology	Speed
UMTS 3G	0.144 à 2 Mbit/s
ADSL1	1 à 8 Mbit/s
Internet Satellite NOVA	2 à 20 Mbit/s
ADSL2+	3 à 20 Mbit/s
LTE 4G	10 à 300 Mbit/s
Satellite constellation	**50 Mbit/s**
Optical fiber ISP	30 Mbit/s à 1 Gbit/s
Local network	100 Mbit/s à 1 Gbit/s
Local network in Optical fiber	10 Gbit/s à 1 Pbit/s
5G ?	

15

Paradigm shift - Conclusion

- Un monde en HYPER-CONNEXION

Manifeste du Cyberespace

You are no longer alone!

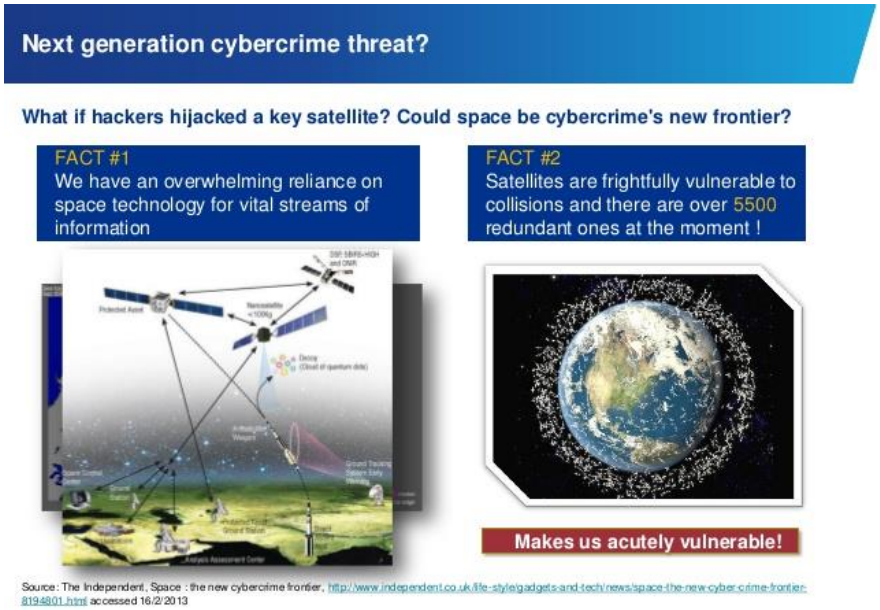
You are in the CYBERESPACE!

4,5 B  ***+ ~ 50 B*** 

16

The use of satellite data in cybercrime

- **Satellite data in cyberspace**
  - The site search
  - The tracking
  - Institutional use
- **Cyber-threat**
  - Are cyber attacks possible?
  - Satellites data in cyberspace
- **Trust in satellite data**
  - Digital evidence
  - Regulations in the « cyber spatial »
  - Satellite data is investing in our applications

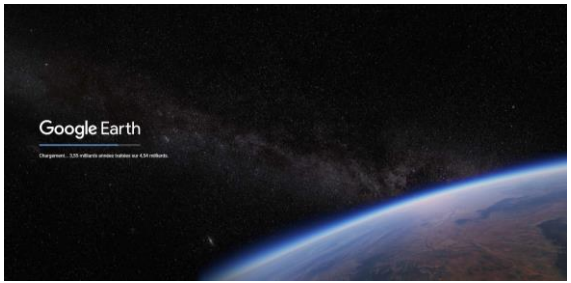


17

Satellite data in cyberspace

The site search

- Google Earth



- Google Maps

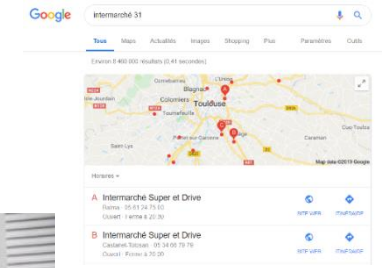
- Google Street view

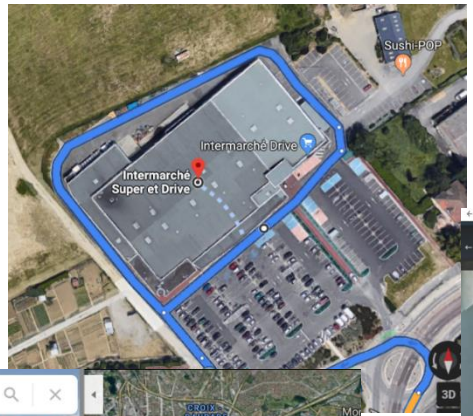
18

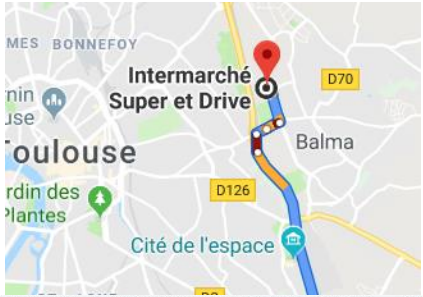
Satellite data in cyberspace

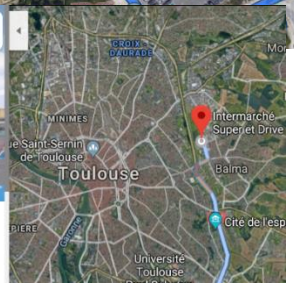
The tracking

- Armed robbery
- Burglary









19

Satellite data in cyberspace

Institutional use

Legal investigations

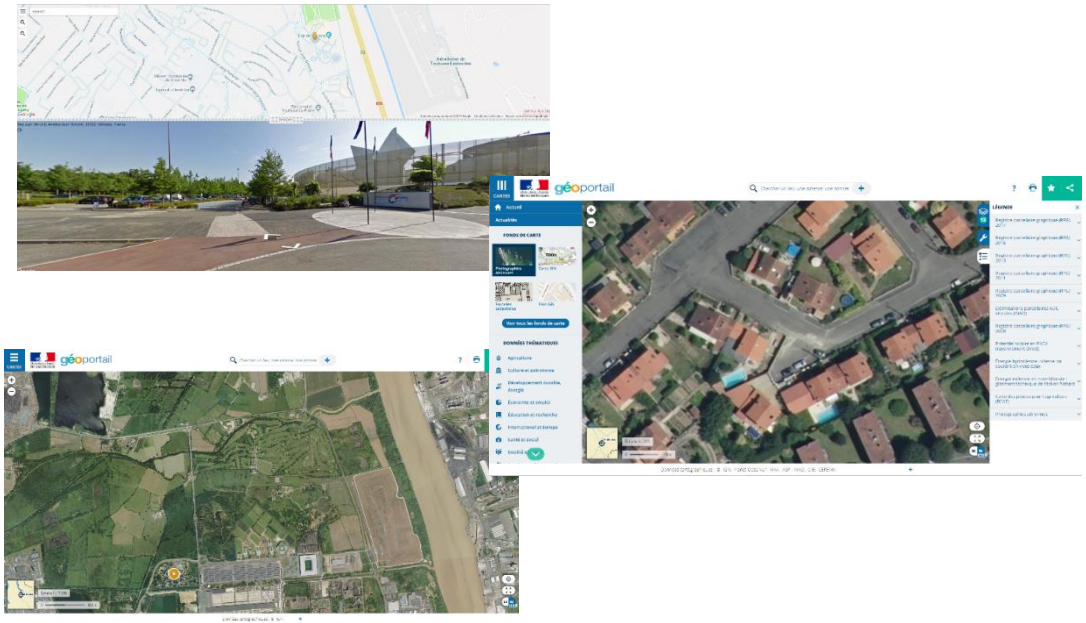
action plan

Tax investigations

Patrimonial environment

Legal proceedings

geolocated data



20

Cyber-threat

- **Are cyber attacks possible?**

Thousands of High-Risk Vulnerabilities Found in NOAA Satellite System

September 10, 2014 Swati Khandelwal

The informational systems that the National Oceanic and Atmospheric Administration (NOAA) run are loaded with several critical vulnerab...

https://thehackernews.com/2014/09/thousands-of-high-risk-vulnerabilities_9.html

Satellite Communication (SATCOM) Devices Vulnerable to Hackers

April 18, 2014 Swati Khandelwal

The growing threat of cyber-attacks and network hacking has reached the satellite-space sector, posing a growing challenge to the satel...

https://thehackernews.com/2014/04/satellite-communication-satcom-devices.html

Turla

Russian Hackers Hijack Satellite To Steal Data from Thousands of Hacked Computers

September 10, 2015 Swati Khandelwal

A group of Russian hackers, most notably the Turla APT (Advanced Persistent Threat) is hijacking commercial satellites to hide command...

https://thehackernews.com/search/label/satellite%20hacking

Satellites have different protection gradients against cyber threats

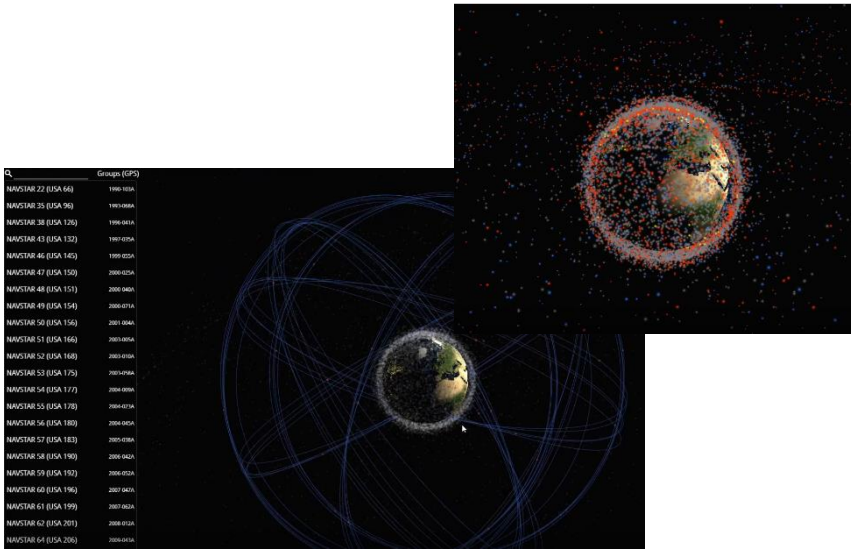
Satellite is no longer reserved for the government

Micro service satellite
Tractor, UAV

21

Cyber-threat

- **Satellite data in cyberspace**



http://stuffin.space

https://cybermap.kaspersky.com/fr

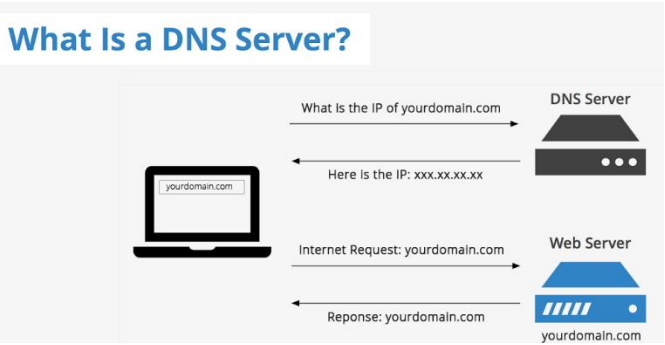
22

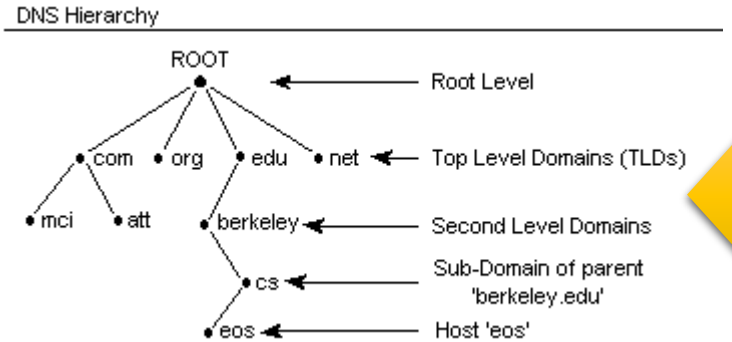
Cyber-threat

- **attack on ISP infrastructures in cyberspace**

https://www.**comet-cnes.fr**/

Can we paralyze an infrastructure ?





DNSpionage
Campaign Targets
Middle East

A global cyber attack on the international organization that assigns Internet addresses, **ICANN**.

four major attacks
between 13 December 2018 and 2 January 2019

SOURCE : https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html

23

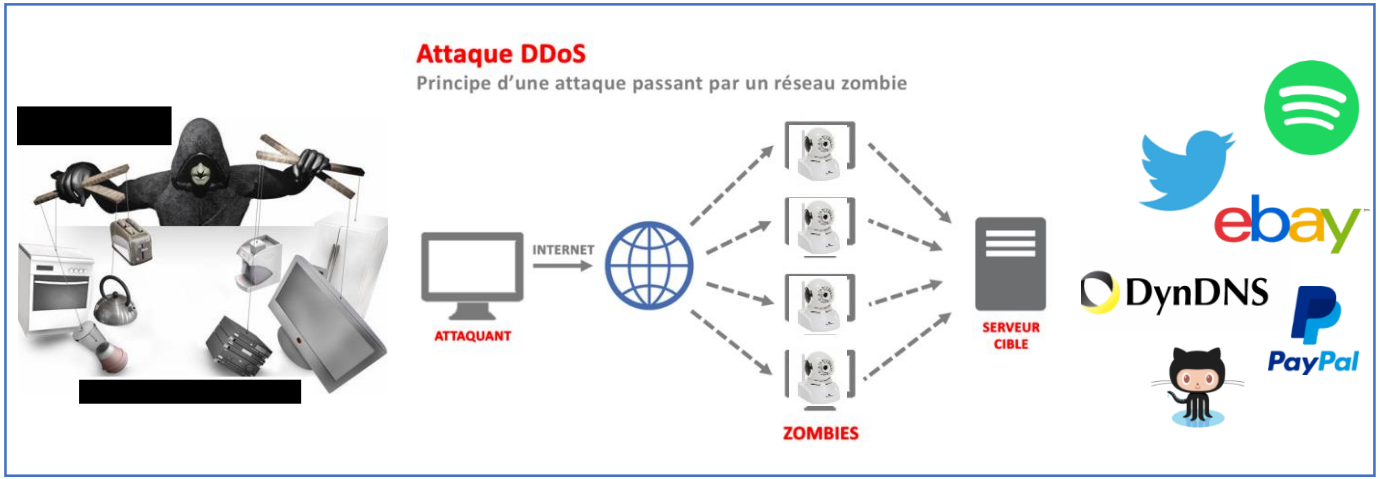
Cyber-threat

- ## DDoS (Distributed Denial of Service)

DDOS ATTACK, on October 21, 2016, which saw the appearance of a botnet named "**Mirai**" composed of connected objects (145,000 cameras) targeting the Dyn Managed DNS service that use this service (different from DynDNS), such as **Twitter, Ebay, Netflix, GitHub, PayPal, Spotify**.

telnet login

login: vstarcam2015
passwd: 20150602



Cyber-threat

- **DDoS (Distributed Denial of Service)**

  DDOS ATTACK, on October 21, 2016, which saw the appearance of a botnet named "**Mirai**" composed of connected objects (145,000 cameras) targeting the Dyn Managed DNS service that use this service (different from DynDNS), such as **Twitter, Ebay, Netflix, GitHub, PayPal, Spotify**.

25

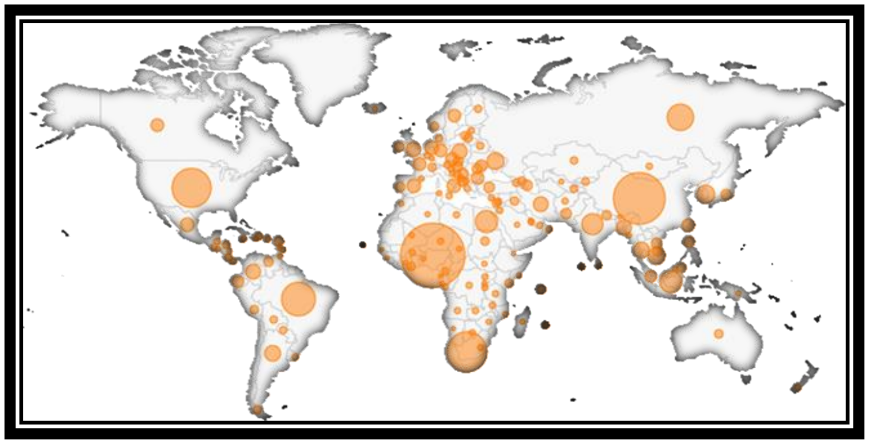
Cyber-threat

- **attack on clouds in cyberspace**

Cybercrime: **Cloud application attacks have exploded** in recent months (16 March 2019) with a 65% increase

Two common techniques

- **brute force attacks** come mainly from China (53%), Brazil (39%) and the United States (31%)
- **Phishing attacks**, on the other hand, come mainly from Nigeria (63%), South Africa (21%) and the United States (11%), via VPNs.



Volume of successful malicious connection sources (Source: Proofpoint)

26

Trust in satellite data

Digital evidence

Digital evidence refers to any digital information that can be used as evidence in a court case.

Admissibility

Computer forensic expertise is a forensic digital investigation that collects digital evidence to provide a person with the ability to support a **legal action or have a legal right**.

27

Trust in satellite data

Regulations in the « cyber spatial »

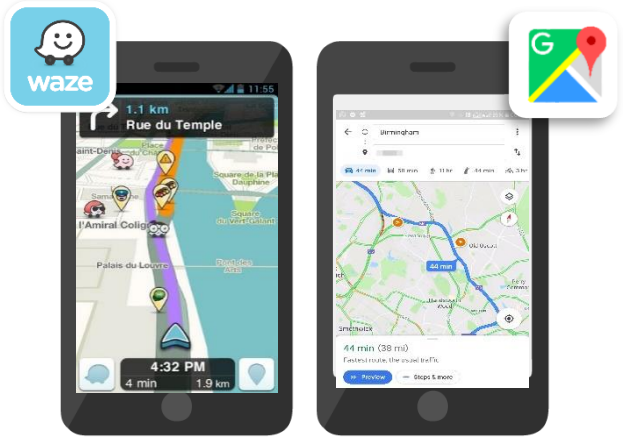
The laws and regulations in "cyberspace are similar to those of "cyberspace"

28

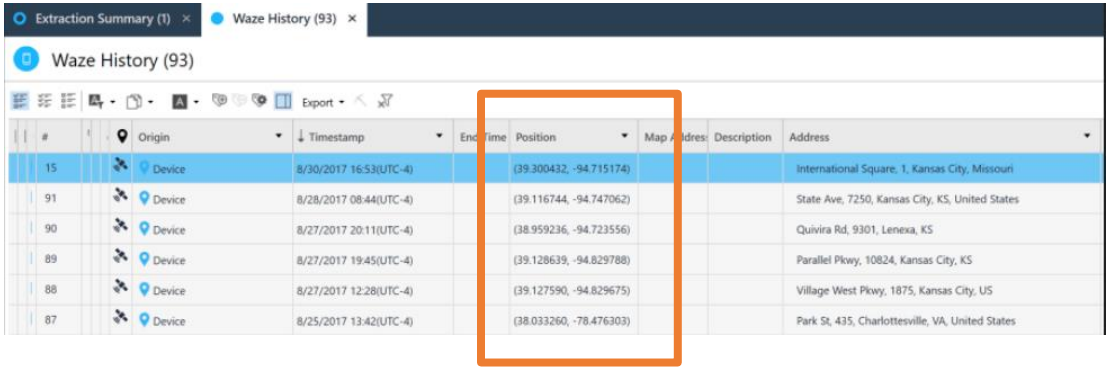
Trust in satellite data

Satellite data is investing in our applications

the trails from travels



non-répudiation

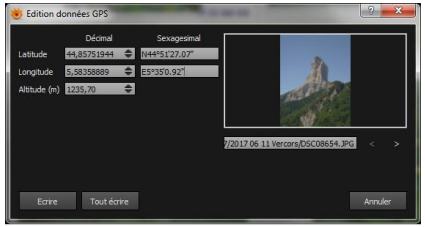


29

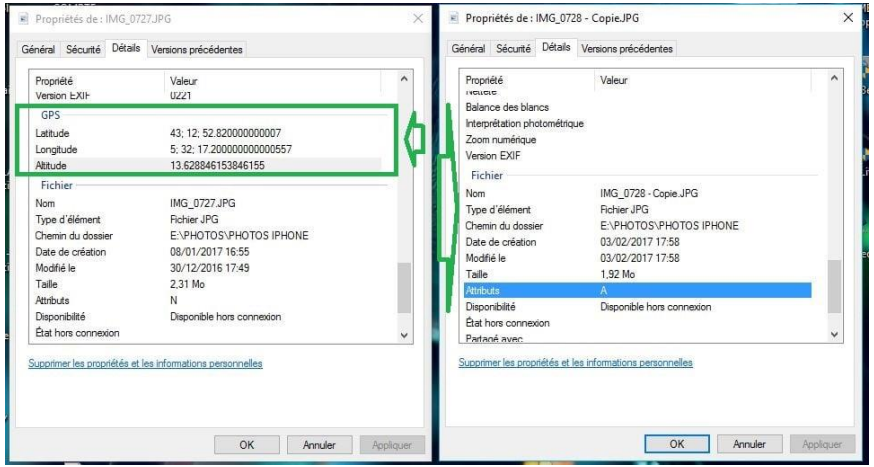
Trust in satellite data

Satellite data is investing in our applications

EXIF metadata of pictures



non-répudiation

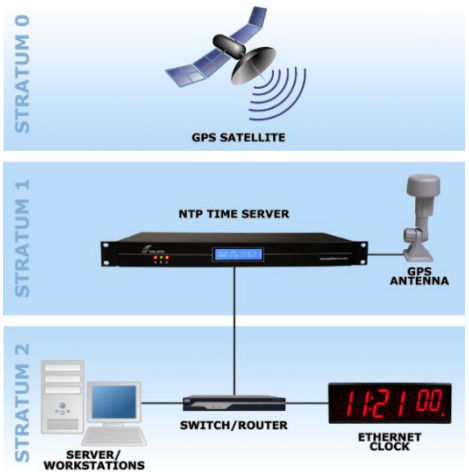


30

Trust in satellite data

Satellite data is investing in our applications

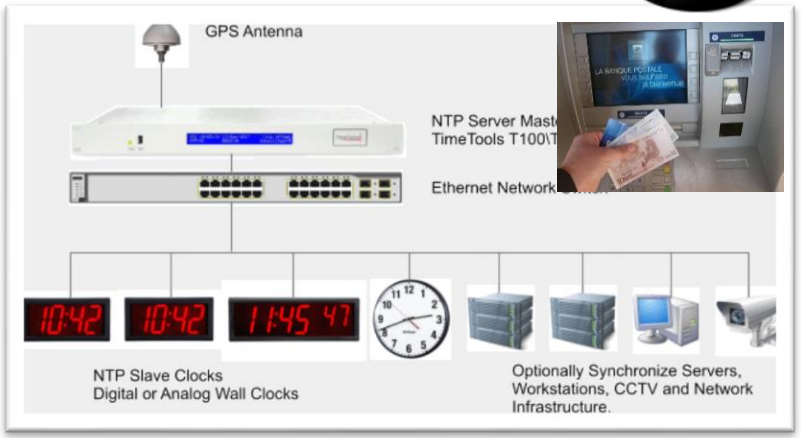
Time signal



Solution

The **EGNOS** service is based on the distribution of correction data from positioning systems while **guaranteeing the integrity of the signal and its confidence level**.

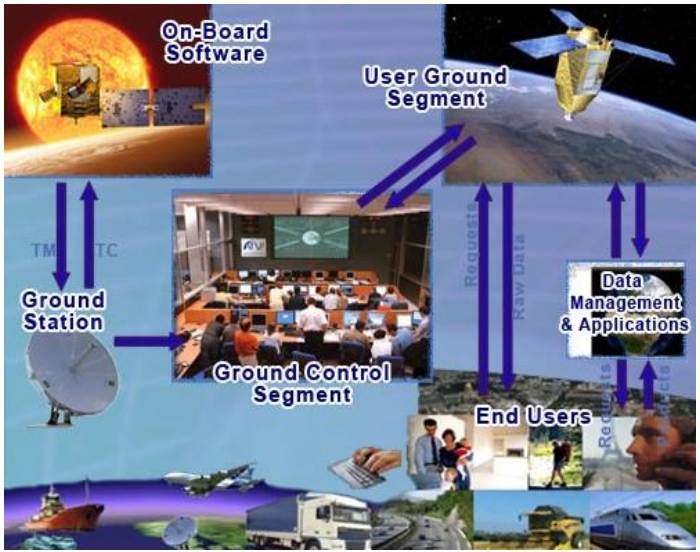
non-répudiation



31

Conclusion

- **What needs to be protected?**



- **How to protect our assets?**

Cybersecurity is a continuous process

In an increasingly uncertain environment, ensuring business continuity requires more proactive and integrated approaches. By applying the latest standards and best practices, to ensure the protection of "by design" systems and to guarantee the trust of organizations in digital technology, cyber-resilience becomes fundamental.

32

Conclusion

- **Cybersecurity a major asset for cyberspace**
  - Risk analysis, EBIOS (civil / military)
  - Study and securing of collaborative platforms such as GED/CMS processing sensitive information and on components in ground segments or payload
  - Study and analysis of network and data center
  - Support for the accreditation of information systems
  - Contribution to approval dossiers
  - Assistance towards compliance with the LPM
  - Development of attack scenarios to test cybersecurity actors

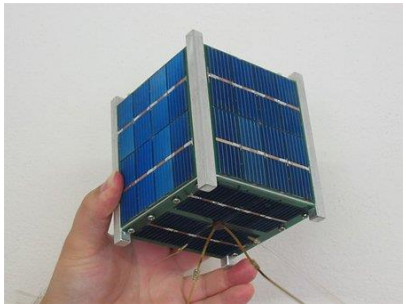
DÉFENSE & SPATIAL

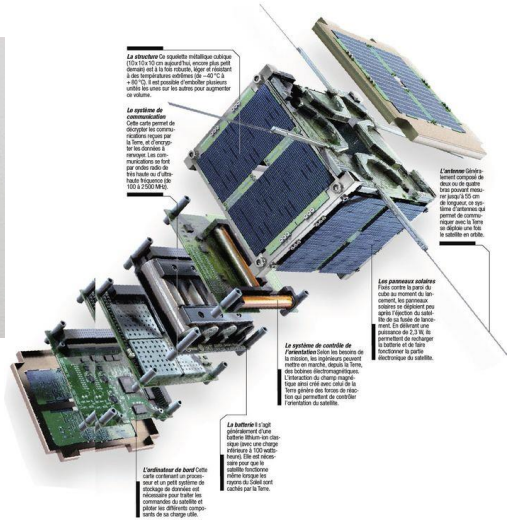
SCASSI. be secure

33 Conclusion

- **Révolution des microsatellites**

The revolution in microsatellites will require more vigilance on **embedded components** (*lowcost*) in terms of **cybersecurity**.





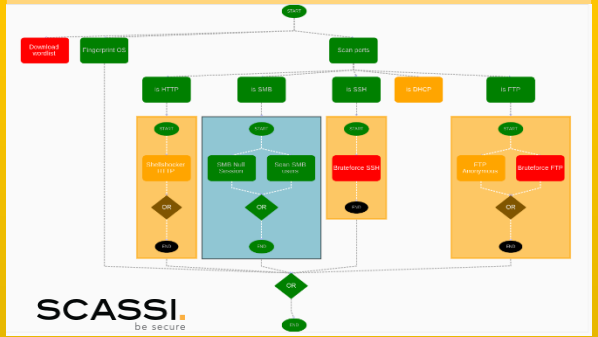
Solution

To add cybersecurity, it is necessary to use :

- personnel qualified in intrusion testing and specialized in IoT
- tools dedicated to cybersecurity of embedded components

Passed

for cybersecurity of embedded components



See you later into our agencies

MADRID

Votre contact :
jesus.friginal@scassi.com

TOULOUSE

Votre contact :
jean.reau@scassi.com

PARIS

Votre contact :
pierre.nicolas@scassi.com