Aerospace Cybersecurity Intelligence

CyberInflight

Space Cybersecurity

Challenges & the Importance of Collective Intelligence

November 8, 2021

florent.rizzo@cyberinflight.com

www.cyberinflight.com

comet

CyberInflight

ABOUT US

Unique player in Space & Aerospace Cybersecurity Market Intelligence

Independent company, employee owned

Founded in 2019 in France, headquartered in Toulouse

Specialized in the Space & Aerospace market

Member of:

SPACE ISAC

1st French member of the Space ISAC Chair member of the Supply Chain Working Group (SCWG)

Part of the catalog:

BOOST AEROSPACE

CYBER'OCC

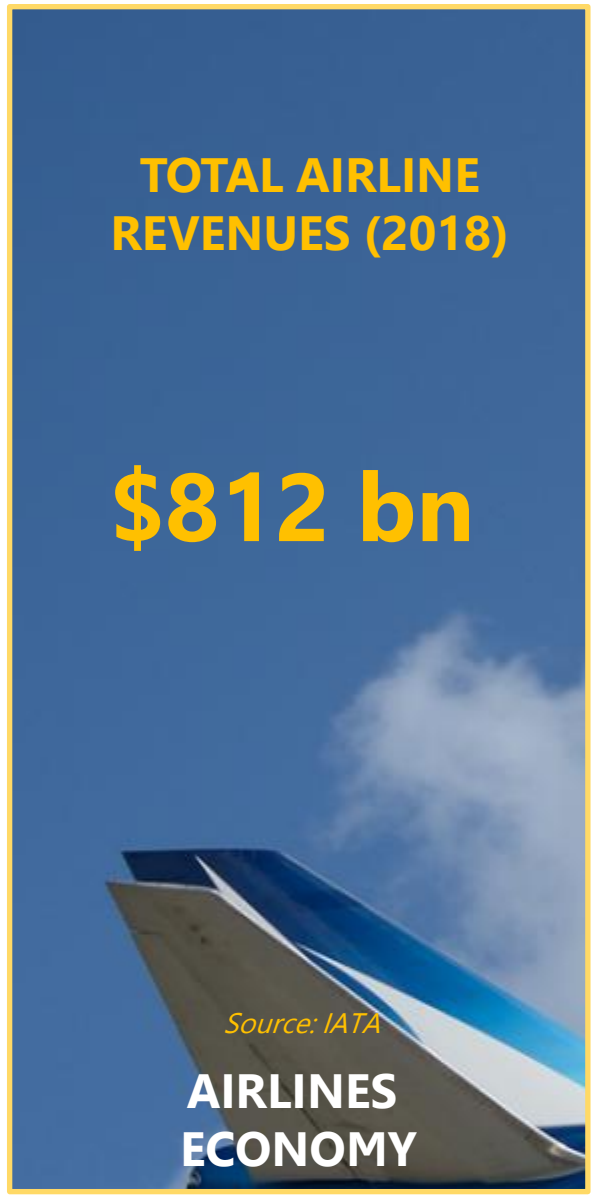
Aviation, Space and Cyberthreat economies

TOTAL AIRPORT REVENUES (2018)

$161 bn

Source: ACI

AIRPORT ECONOMY



TOTAL AIRLINE REVENUES (2018)

$812 bn

Source: IATA

AIRLINES ECONOMY

GLOBAL SPACE REVENUES (2019)

$366 bn

Source Euroconsult, Bryce, SIA

SPACE ECONOMY

TOTAL CYBERCRIME REVENUES - ILLICIT PROFIT(2018)

$1.5 Tn

Source: Bromium

≡ 10% of EU GDP rely on GNSS availability

CYBERTHREAT ECONOMY

Espionage $ vs IP

(APT, state sponsored)

Growing competition among ransomware groups (1/2)

WORK ETHIC/REPUTATION

(Source Balckmatter, Babuk, CloP)

About us

We are a team that unites people according to one common interest - money.
We provide the best service for our clients and partners compared to our competitors.
We rely on honesty and transparency in our dealings with our victims.
We never attack the company twice and always fulfill our obligations.
We invite the recovery companies to cooperate with, you can contact us through "*Contact Us*".

Rules

We do not attack:

- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Defense industry.
- Non-profit companies.
- Government sector.

We do not audit

next categories of organizations

Hospitals

Except private plastic surgery clinics, private dental clinics

Non-Profit

Any non-profitable charitable foundation

Schools

Except the major universities

Small Business

Companies with annual revenue less than 4 mln$ (info about revenue we take from zoominfo

ATTENTION!!!

We have never attacked hospitals, orphanages, nursing homes, charitable foundations, and we will not.

Commercial pharmaceutical organizations are not eligible for this list;

they are the only ones who benefit from the current pandemic.

If an attack mistakenly occurs on one of the foregoing organizations, we will provide the decryptor for free, apologize and help fix the vulnerabilities.

PARTNERSHIP/AFFILIATE PROGRAMS

(Source Avos, Lockbit2.0)

AvosLocker Partnership Program

Avos2, AvosLocker's latest Windows variant, is one of the fastest in the market, with highly scalable threading and selective ciphers.

CONDITIONS FOR PARTNERS

[Ransomware] **LockBit 2.0 is an affiliate program.**

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

Only you decide during communication how much the encrypted company will pay you. You get the payment to your personal ewallets in any currency, after which you transfer us the percentage of the foreclosure amount.

LockBit 2.0 does not function in post-Soviet countries.

We cooperate only with experienced pentesters who are real professionals in such tools as Metasploit Framework and Cobalt Strike.

Cooperation terms and conditions are determined for each Customer individually.

With our help you can easily get more targets over the weekend than with any other affiliate program over the week.

Growing competition among ransomware groups (1/2)

COMPETITION ON COMPUTATION SPEED

(Source Lockbit2.0)

Encryption speed comparative table for some ransomware - 02.08.2021

PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD

Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30 KB	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59 KB	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061 KB	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292 KB	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200 KB	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124 KB	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661 KB	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930 KB	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909 KB	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17 KB	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31 KB	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121 KB	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460 KB	random extension
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402 KB	79486

Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44s
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S
Rclone yandex.ru free	0,52 MB/s	No	No	No	5H 20M 30S	2D 05H 25M 7S	222D 13H 52M 49S

Encryption speed :

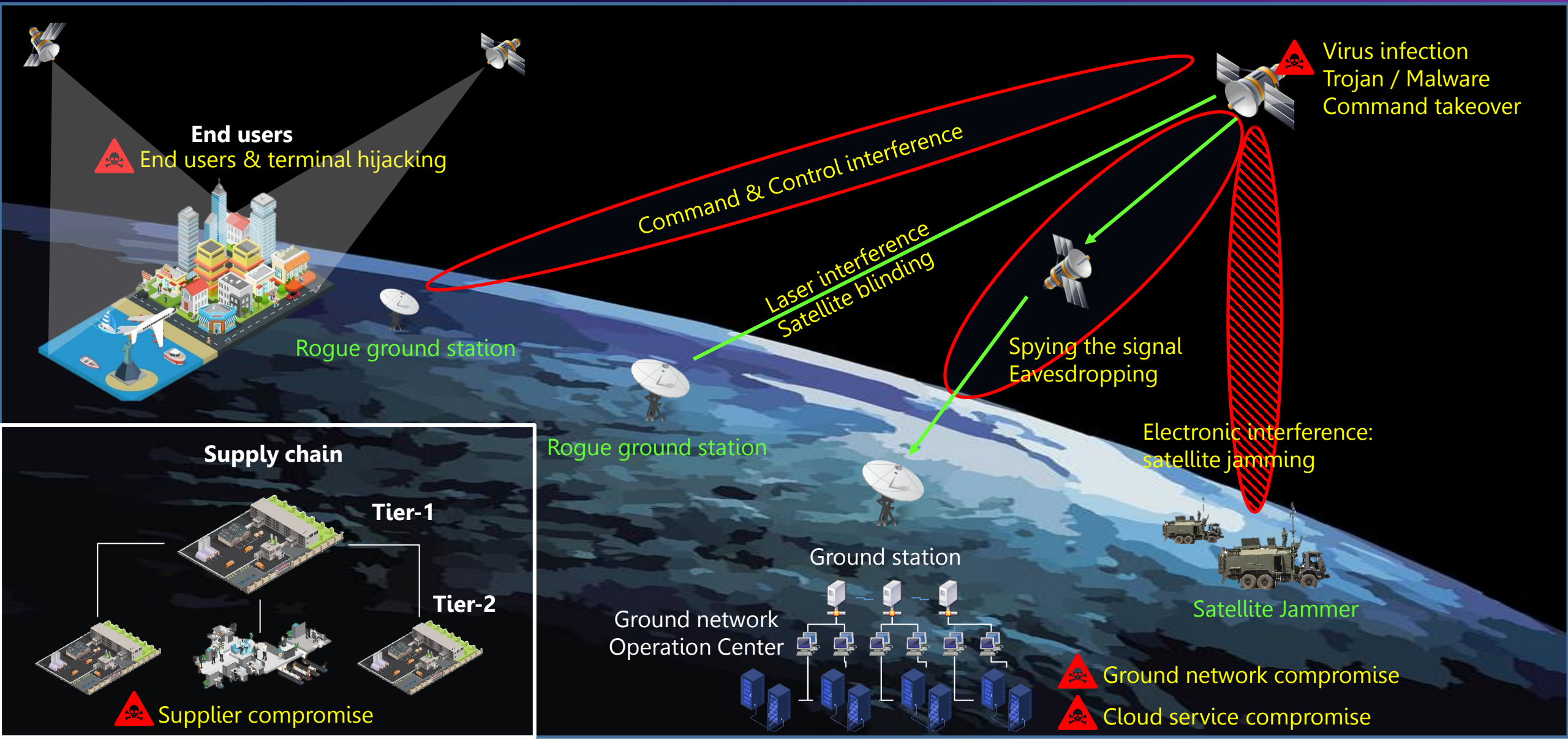
- **lockbit**: 266 MB/s
- **Lockbit 2.0**: 373 MB/s
- **Others**: Max. speed ~185 MB/s

Download speed speed :

- **StealBIT by Lockbit:** 83.46 MB/s
- **Others:** 4.82 MB/s

Qualitative & Quantitative demonstrations

Overview of cyberattacks on space ecosystem



Example: Supply chain compromise

ILLUSTRATION OF THE SUPPLY CHAIN COMPROMISE IN THE SPACE INDUSTRY

I

During the production, a chip has been compromised. The compromise happened at an atomic level which suppose significant means and capabilities, probably a state.

Case mentioned by ESA during a conference
Declassified at YE2018
Detection of the flaw took ~6 months
Could have had catastrophic consequences

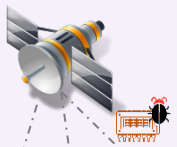
- Test showed that the blueprint of the chip was exactly compliant with specification and expectations

II

The supplier distributed the chip to satellite operator. In this case, the chipset was used for a military satellite managing using cryptographic keys.

- Used in sophisticated military satellite
- Management of cryptographic key exchanges

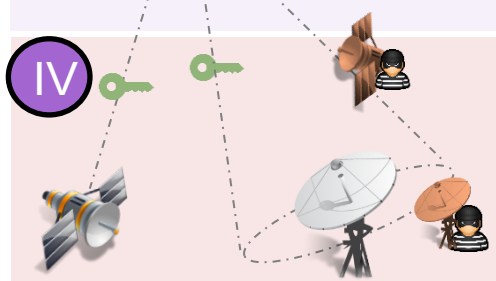
III



The operating satellite embedding the chipset performed key exchange with other satellites or ground stations to allow confidentiality of exchange information. The random code generator is used to generate keys.

- The random code generator proved not random
- Key could be guess in less than 30 minutes.
- According to ESA, this type of attack was obviously super power which has developed this kind of capabilities.

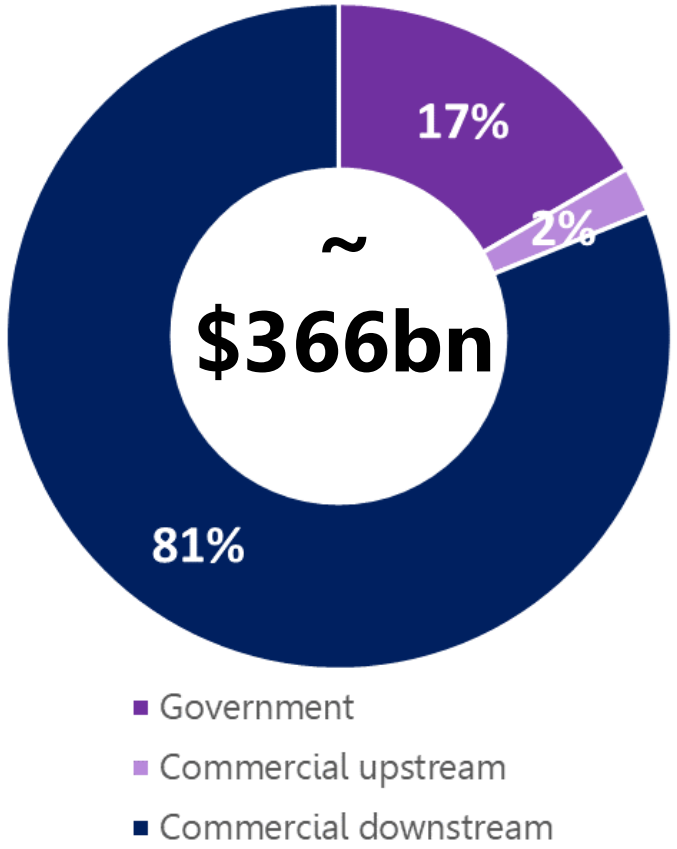
IV



The key is compromised by the faulty chipset. The code generator being not "random" some pattern can be guessed after several tries, ultimately allowing rogue satellites or ground stations to read intercepted satellite communications.

Space Cybersecurity Economy: A rough estimate

GLOBAL SPACE REVENUES
(2019)

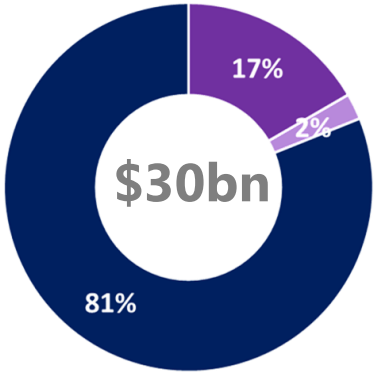


Source Euroconsult, Bryce, SIA

Weighted average of IT spend as % of revenue

8.2%

Rough estimate of Space IT budget



https://www.flexera.com/blog/technology-value-optimization/it-spending-by-industry/

Recommended averaged cybersecurity budget as % of IT budget

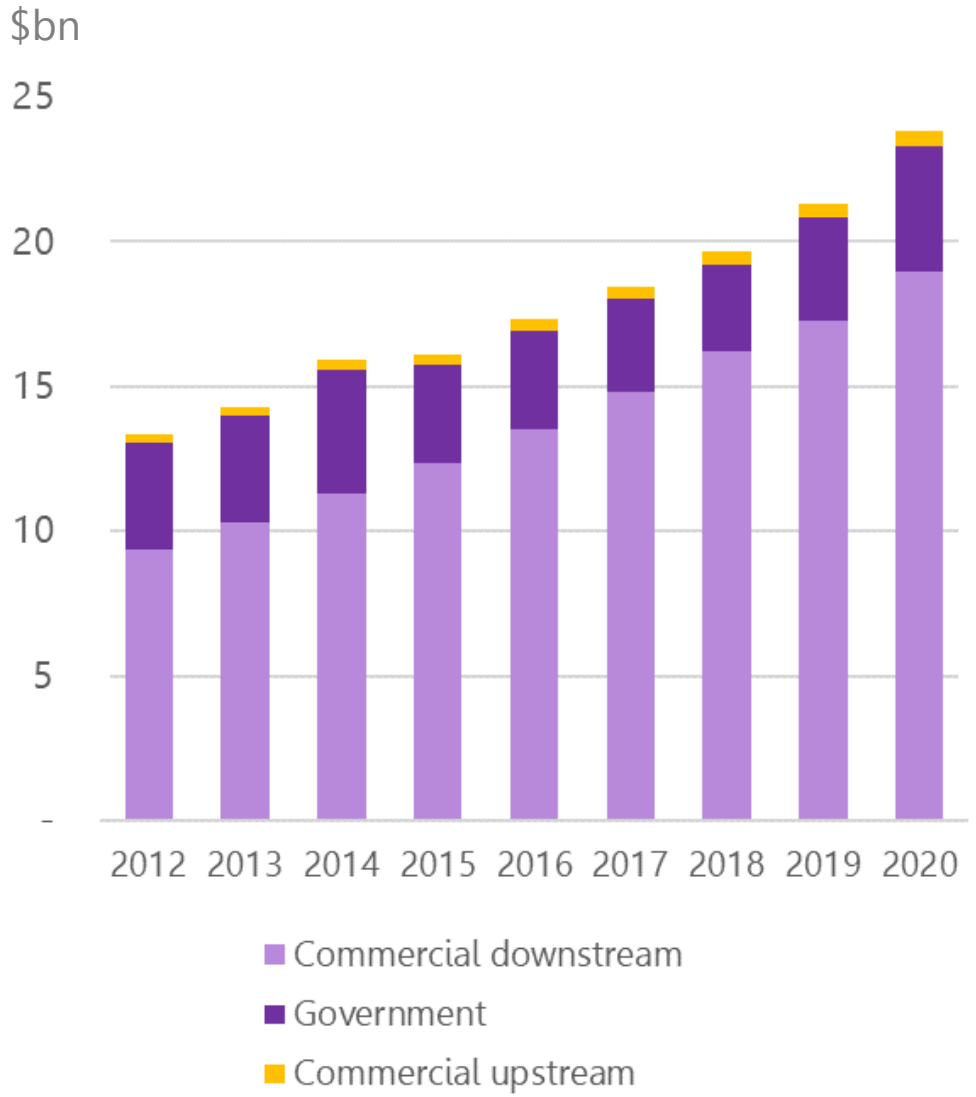
10%

Space cybersecurity economy rough estimate

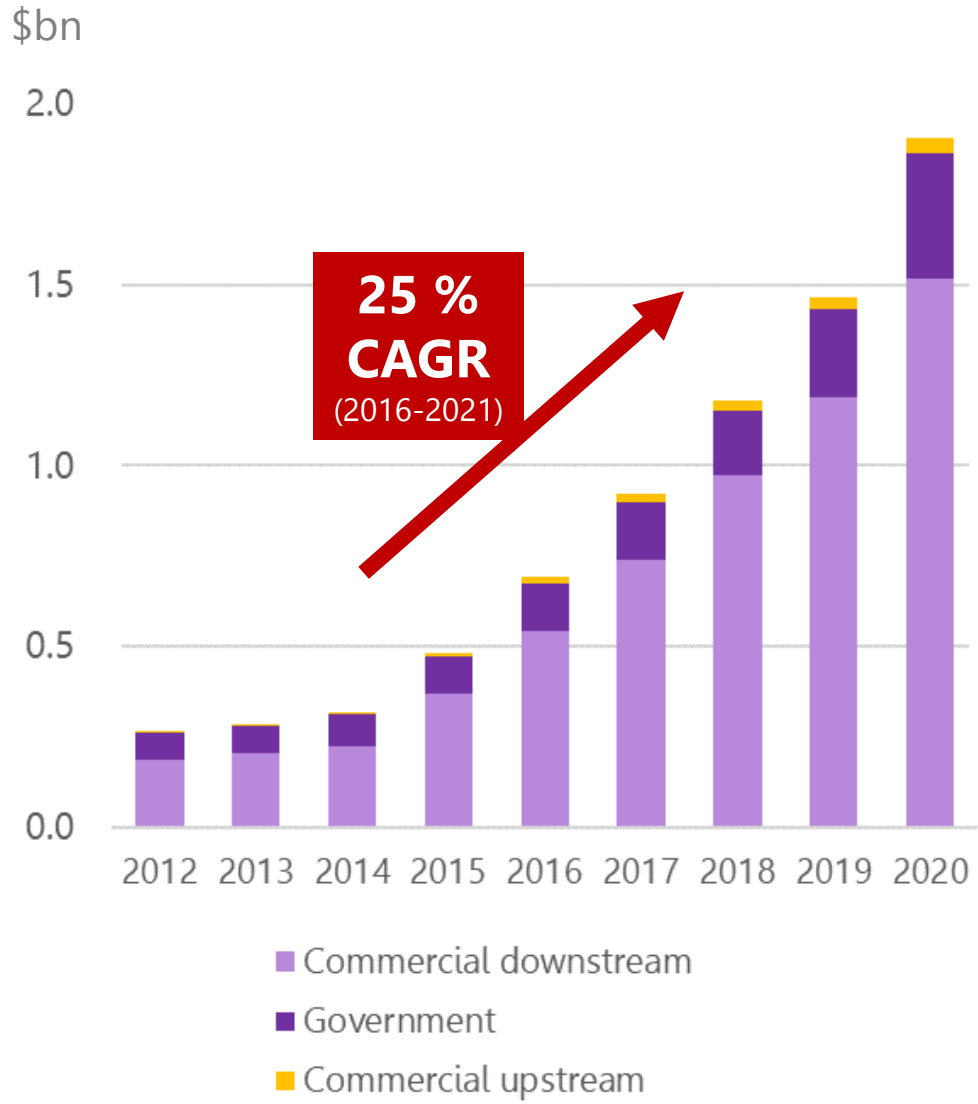
< $3bn

Evolution of Space IT and Cybersecurity budgets

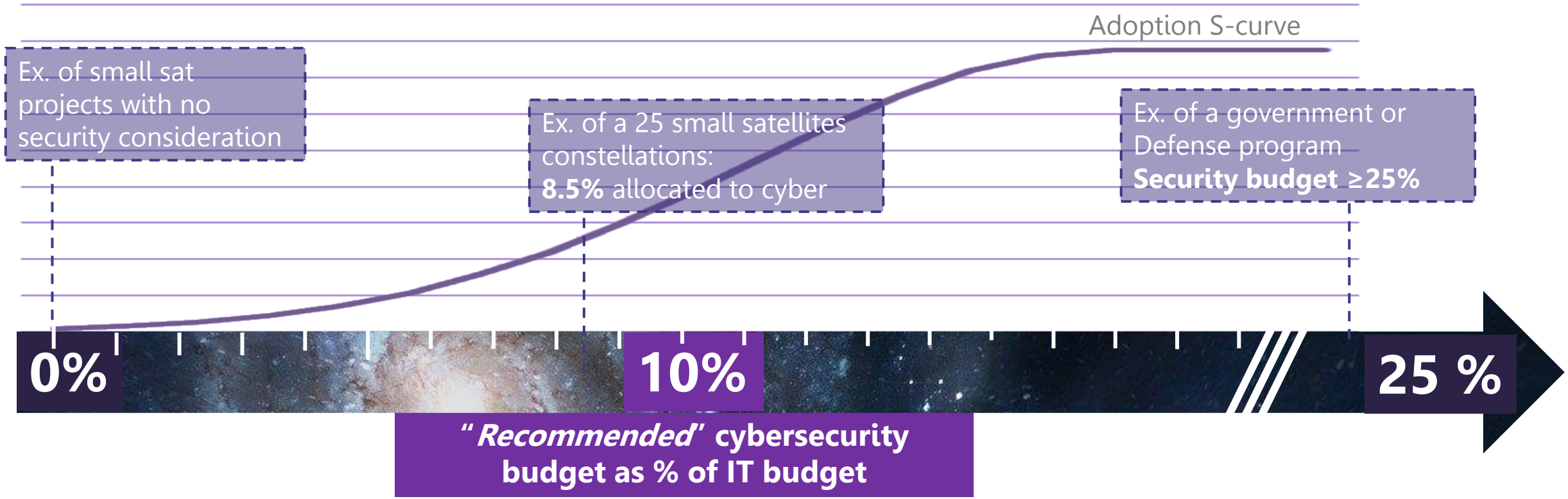
EVOLUTION OF IT BUDGET



EVOLUTION OF CYBERSECURITY BUDGET



Adoption curve & factors



FACTORS IMPACTING CYBERSECURITY LEVEL

(From sat. manufacturer perspective)

- Maturity
- Security Cost
- Time to market
- SWaP compromise
- Recommendations/guidance from industry or security agencies
- Regulatory level
- Threat level
- Commercial/Gov/Def

Internal External

Information sharing landscape: 2 main ecosystems

Space-ISAC:
HQ Colorado Springs
14 founding members
Around 25 current members
Start activities 2020
Numerous partner agencies
Part of NCIs
US-centric PPP open to international

national council of ISACs

Booz | Allen | Hamilton · Lockheed Martin · Northrop Grumman · Aerospace · KRATOS · Parsons · Space Dynamics Laboratory · Johns Hopkins Applied Physics Laboratory · Microsoft · MITRE · Purdue · SES · UCCS University of Colorado Colorado Springs

EU institutions:
CCSE/ESA: Cybersecurity Center of Excellence "*the enabler for collaborative cyber information sharing*" under the Technology and Product Phase of ESA's ARTES
ESPI: EU Space Policy Institute
ENISA: foster the creation of ISACs, encourage collaboration
EUROCONTROL: ESA partner, REX on aviation
EDA: European Defense Agency: enabler for ministries of defense

EU collaborative groups:
COMET Cyber: CNES initiative, expert community
SGAC: Supported by the UN though very active in EU
Various independent communications groups (discords, slacks, etc.)

Status for MEA, CIS, APAC ?

Space-ISAC internals *(public info.)*

FOUNDING MEMBERS

SES, Lockheed Martin, Northrop Grumman, Purdue University, Kratos, Aerospace, Parsons, Booz | Allen | Hamilton, Space Dynamics Laboratory, MITRE, Johns Hopkins Applied Physics Laboratory, University of Colorado Colorado Springs, L3Harris, Microsoft

COMMUNITIES OF INTEREST

- Smallsats COI
- Blockchain COI
- Workforce COI

WORKING GROUPS

- Information Sharing Working Group
- Analyst Working Group
- Supply Chain Working Group

(CyberInflight part of on the chair)

PARTNER AGENCIES

DoJ, DoD, NSA, DHS, Dept. of State, US Space Force, Space Command, Missile Defense Agency, National Reconnaissance Office, CISA

SPACE ISAC

TASK FORCES

- SPD-5
- CMMC
- Table Topic and Exercise TF
- Space ISAC Summit

COLLABORATORS

NASA, Air Force Research Laboratory, NIST, US DoC

GENERAL MEMBERS

(only public members are shown)

Raytheon Technologies, Boeing, Constellation, Synspective, Astroscale U.S., System High, RS21, sophinea, SpaceLink, 14BIS Supply Tracking, KSAT Kongsberg Satellite Services, thinklogical A Belden Brand, FTS International, LLC, CyberInflight

THREAT INTEL PLATFORM

- Threat Intel
- Daily Observations
- Information sharing
- Surveys

CONFERENCES, EVENTS

- VOSS
- Space ISAC Summit
- REX, member discussions, etc.

MEMBERSHIP

National Cybersecurity Center, National Council of ISACs

S-ISAC: Feedback & Observations

1 US approach

- **US mindset**: openness and trust for members & partners
  - No feeling of hierarchy, ability to collaborate to any group
  - Easy to approach other members
  - Big to small members (major to startup)
  - Not political
- **Mostly US centric**
  - Very few EU members
  - Very well connected with the US ecosystem
- **Ambitious group**
  - Many ongoing initiatives
  - Willing to reach more than 100 members by the next year
  - Weekly follow-up and observable progress

2 Nascent ecosystem

- **Early stage** of the ISAC / Creation effective in 2020
- **Definition phases**:
  - Nascent with many initiatives still under construction
  - Focus on the WHY and WHAT before the HOW
- **Not yet entering into more practical/technical** exchanges
- **Time consuming** participation

3 View on RoW

- Strong willing to expand the member base
- Encourage participation of EU members
- The EU point of views seem expected during discussions
- The CN concern is a strong and recurring

4 Legacy - Influence

- ISAC platforms can be seen as "tools" by providers to penetrate specific markets (CTI, others)
- Some founding members brings expertise and vision from other experienced ISACs, avoid common roadblocks and use best practices
- S-ISAC has a different approach than other ISACs

What about an EU equivalent of the Space ISAC ?

Space conferences dedicated to cyber in the last 2 years

Organizers: S-ISAC, NIST, AIAA, DoD, DoC, DHS, USAF, MITRE, CISA, etc.
Supported by : Aerospace Corporation, Lockheed Martin, MITRE, Booz Allen, Kratos, Verizon, etc.

DEFCON

NyanSat

AEROSPACE VILLAGE

Hackasat

"Aviation Village" renamed itself "Aerospace Village"
First Hackasat edition gathered 2,000 teams of hackers

CYBERSAT
CYBERSATGOV
CYBERLEO
CYBERSATCOM

First event of this kind
Started in 2018

By the Defense Strategies Institute
More Intelligence and military than cyber

CYSAT Davos 2021
SECOND EDITION CYSAT PARIS 2022

CYSAT '22 is the only European event entirely dedicated to cybersecurity for **commercial space applications**, taking place online and in Paris, organized by CYSEC.

Cyber and Space Security Conference 10–11 November 2021

Organized by Estonia

COMET cyber

EU events

Space cybersecurity Initiatives & Specific documentation

(not exhaustive)

ACCELERATING SPACE-CYBER INITIATIVES

SPD-4 US Space Force Establishment
Feb. 2019

Commandement de l'espace creation
Sept. 2019

Training range at the EU Space Security Education Center
Sept. 2020

Space Policy Directive SPD-5
Sept. 2020

Space Systems Critical Infrastructure Working Group
May 2021

ESA-EDA cooperation framework
Oct. 2021

Syracuse launch
Oct. 2021

CMMC 2.0
Nov. 2021

A SHIFT TOWARD MORE SPECIFIC GUIDANCE

NIST DOCUMENTATION

- NIST 800-53 Rev5
- CNSSI 1253
- **Space Overlay**
- **NIST IR 8270**
- **NIST IR 8323**
- **OTHERS**

OTHERS

NIS2 Directive

European Parliament

MINISTÈRE DES ARMÉES

CCSDS-SEASEC DOCUMENTATION

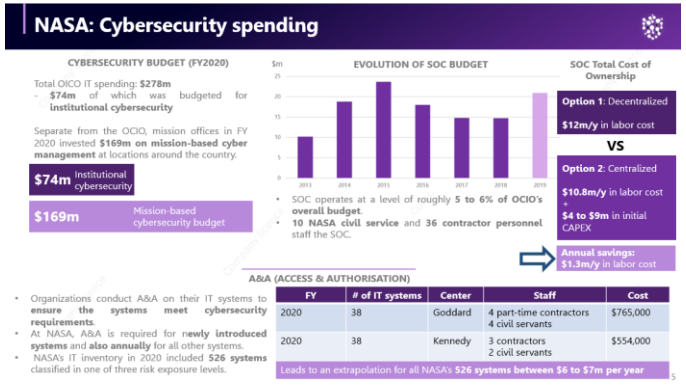
Document	Type	Title	Published
CCSDS 350.0-G-3	Green	The Application of Security to CCSDS Protocols	Mar. 2019
CCSDS 350.1-G-2	Green	Security Threats against Space Missions	Dec. 2015
CCSDS 350.4-G-2	Green	CCSDS Guide for Secure System Interconnection	Apr. 2019
CCSDS 350.6-G-1	Green	Space Missions Key Management Concept	Nov. 2011
CCSDS 350.7-G-2	Green	Security Guide for Mission Planners	Apr. 2019
CCSDS 350.8-M-2	Magenta	Information Security Glossary of Terms	Feb. 2020
CCSDS 350.9-G-1	Green	CCSDS Cryptographic Algorithms	Dec. 2014
CCSDS 351.0-M-1	Magenta	Security Architecture for Space Data Systems	Nov. 2012
CCSDS 352.0-B-2	Blue	CCSDS Cryptographic Algorithms	Aug. 2019
CCSDS 356.0-B-1	Blue	Network Layer Security Adaptation Profile	Jun. 2018
CCSDS 357.0-B-1	Blue	CCSDS Authentication Credentials	Jul. 2019
CCSDS A13.1-Y-1	Yellow	CCSDS Recommended Procedures for Cloud-Based Interoperability Testing	Jun. 2018

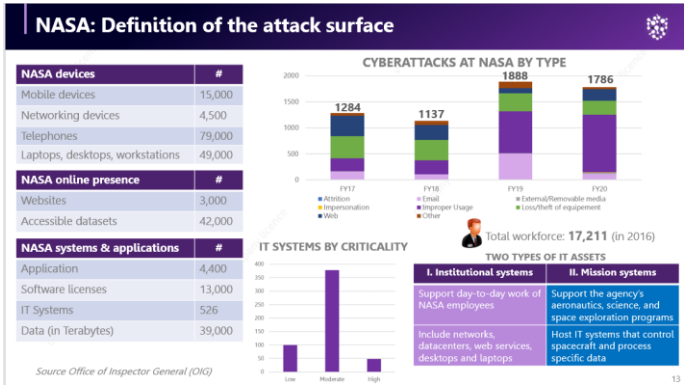
Supporting the industry through market intel. resources

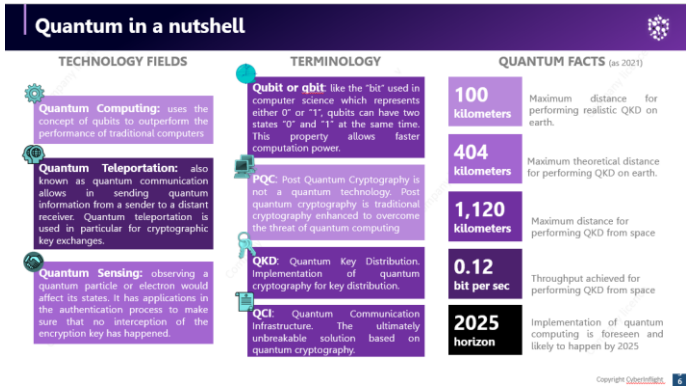
CONTRIBUTE TO THE NEXT EDITION OF OUR STRATEGIC REPORT

Space Cybersecurity Market Intelligence report

- Interview campaign
- Information sharing
- Case studies definition
- Identification of key relevant topics
- Data exchange
- Open to any collaboration and contribution…







florent.rizzo@cyberinflight.com