ALBERTO TRABALLESI E ROBERTO SOMMA

DESTINAZIONI

LA CORSA VERSO NUOVI MONDI

LIBRERIA GEOGRAFICA

Sommario

7. **Nuovi mondi, dalla fantasia alla realtà**
Roberto Somma, Alberto Traballesi

17. **Dalla creazione dell'Universo all'esplorazione umana dello spazio**
Nazzareno Mandolesi, Diego Molinari, Daniela Paoletti

37. **L'economia dello spazio**
Eutimio Tiliacos, Alberto Traballesi

53. **Luna**
Alberto Traballesi, Roberto Somma

77. **Marte**
Enrico Flamini

93. **Giove**
Enrico Flamini

115. **Saturno**
Enrico Flamini

139. **NEO. Near Earth Objects**
Ettore Perozzi, Marco Tantardini

159. **Pianeti Extrasolari**
Roberto Somma

174. **I vincoli giuridici - La disciplina di diritto internazionale e le attività nello spazio**
Maria Beatrice Deli

188. **La situazione internazionale e l'ISECG**
Alberto Traballesi, Roberto Somma, Enrico Ferrone

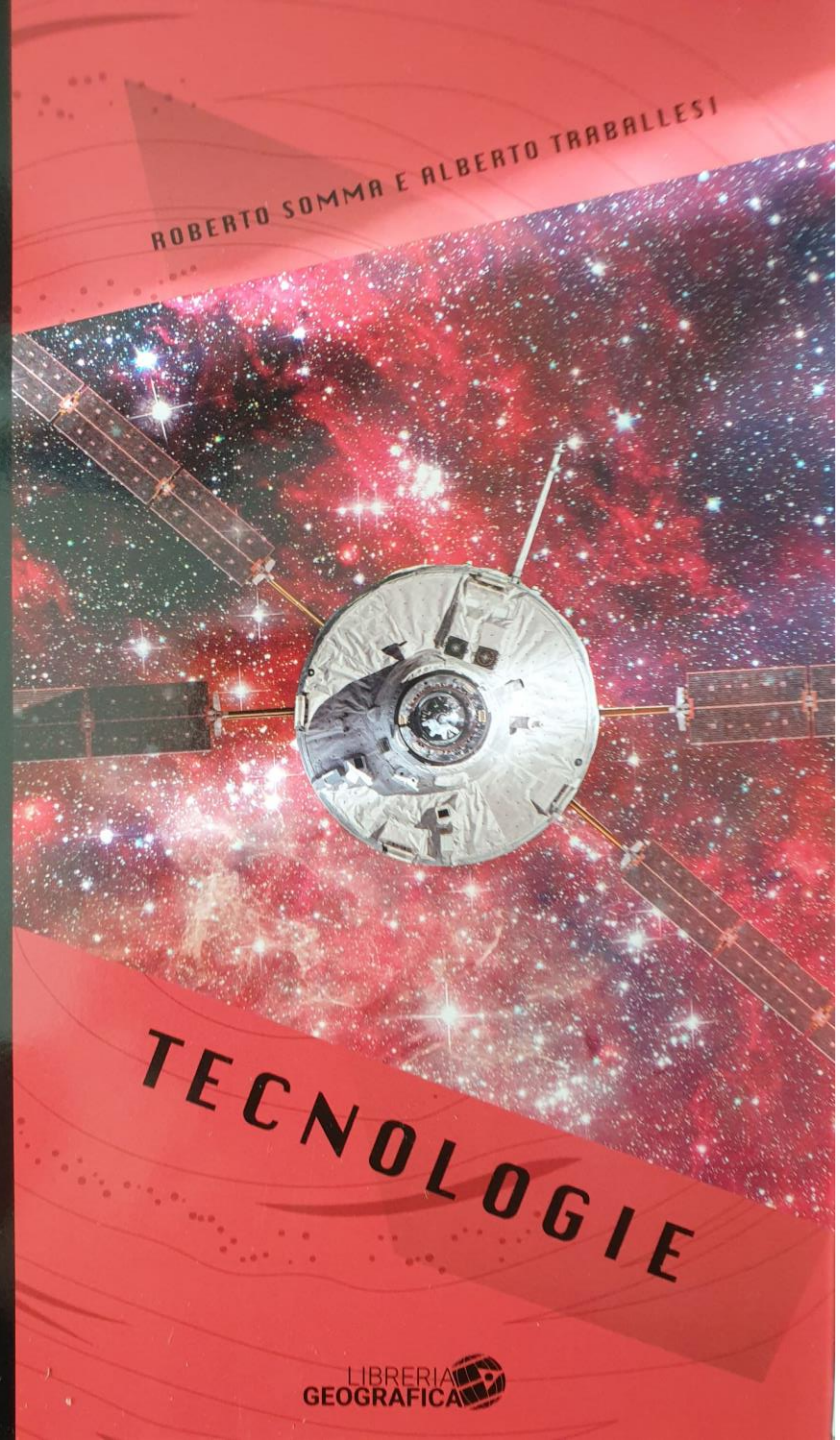
206. **Considerazioni conclusive**
Roberto Somma, Alberto Traballesi

212. **Annotazioni**

237. **Bibliografia**

LA CORSA VERSO NUOVI MONDI

ROBERTO SOMMA E ALBERTO TRABALLESI



TECNOLOGIE

LIBRERIA GEOGRAFICA

Sommario

7. **Tecnologia, dalla geopolitica all'economia**
Roberto Somma, Alberto Traballesi

14. **Traiettorie**
Paolo Teofilatto

30. **L'accesso umano al Sistema Solare e allo spazio Intergalattico**
Francesco Sintoni, Marco Regi, Angelo Fontana, Mike Sintoni

58. **I veicoli spaziali**
Franco Fenoglio, Flavio Bandini

92. **Gli habitat**
Luciano Battoccchio, Cesare Lobascio

108. **La logistica dei Viaggi Spaziali**
Massimo Cicerone, Armando Ciampolini, Rosa Sapone

120. **Le comunicazioni - La connettività come asse portante della esplorazione spaziale**
Marina Ruggieri, Tommaso Rossi, Michele Martino, Armando Ciampolini, Diego Bussi

132. **Cyber Security per le missioni nello spazio**
Pierluigi Paganini, Roberto Somma, Cristiano Nervegna, Alessandro Nepoti

146. **I detriti spaziali**
Claudio Portelli

154. **La protezione fisica nei trasferimenti e sui pianeti**
Cesare Lobascio, Franco Fossati

178. **Effetti fisiologici**
Fabio Morgagni, Angelo Gemignani, Francesca Mastorci, Mario Benassai, Armando Ciampolini, Alberto Traballesi

196. **Aspetti psicologici nei viaggi spaziali e nella permanenza extra-terrestre**
Liliana Ravagnolo, Fabio Morgagni, Angelo Gemignani, Francesca Mastorci, Mario Benassai, Armando Ciampolini

216. **Ritorno alla Luna**
Roberto.Somma

224. **Annotazioni**

236. **Bibliografia**

La sete di sapere e la scoperta di nuove terre

Finita l'esplorazione terrestre verso quella dell'Universo

Futuro dell'umanità:

- **aumento della popolazione (9 Mld nel 2050 e scarsità risorse vitali),**
- **cambiamenti climatici, esplosione del Sole**

Ricerca nuova sede nel sistema solare per poi proseguire oltre il sistema solare

Problematiche connesse con la durata dei trasferimenti (propulsione e durata dei viaggi, nonché difficoltà di vita delle popolazioni)

Esigenze di sicurezza in particolare cibernetica

Riservatezza e *connettività*: *sfide di rete e tecnologie abilitanti*

Roberto Somma

Seminario ISACA, 27 Gennaio 2023

Alberto Traballesi e Roberto Somma: «*La corsa verso Nuovi Mondi e la Cybersecurity*»

Comunicare

Navigare

Colonizzare

Osservare

Oltre 65 anni di spazio ....

4 ottobre 1957

Conoscere

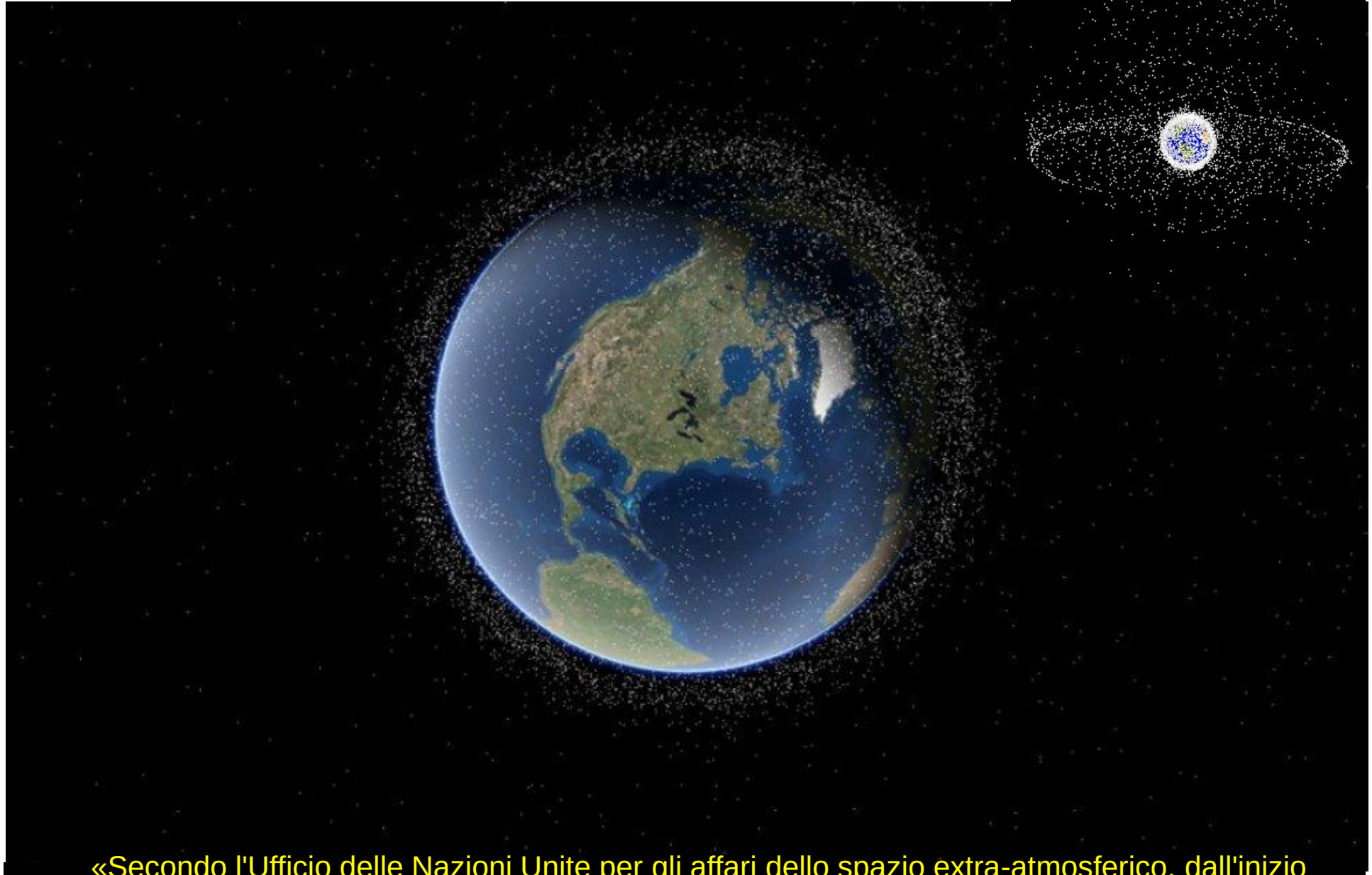
Esplorare

Abitare

Valore strategico del sistema satellitare

Un numero crescente di attività della nostra società dipendono direttamente o indirettamente dai servizi resi possibili dai sistemi satellitari: previsioni meteorologiche, navigazione e posizionamento, distribuzione dell'energia, transazioni bancarie, controllo ambientale, previsione e gestione dei disastri naturali, difesa e sicurezza, etc.

Esso va quindi difeso/protetto contro **attacchi** alla sua integrità per **alterarne il funzionamento** (interruzione del servizio) ovvero per intromettersi in esso allo scopo di **carpirne le informazioni** (intelligence, spionaggio)



«Secondo l'Ufficio delle Nazioni Unite per gli affari dello spazio extra-atmosferico, dall'inizio dell'era spaziale ad aprile 2021 sono stati lanciati 11.139 **satelliti**, 7.289 dei quali sono ancora in orbita. Di questi, **circa quattromila sono attivi**, i restanti sono guasti o spenti». (citato da Scienza in rete, 14 apr 2022)

SATELLITI: Qualche numero

Tipologia

Percentuale degli scopi dei 4.550 satelliti

- **Comunicazioni: 63%**
- **Osservazione della Terra: 22,1%**
- **Sviluppo tecnologico: 7,8%**
- **Navigazione/posizionamento globale: 3,6%**
- **Dimostrazione tecnologica: 0,77%**
- **Scienze della Terra: 0,44%**
- **Osservazione dello spazio: 0,22%**
- **Scienze spaziali: 2,3%**

(Fonte: https://www.truenumbers.it/satelliti-spazio/)

Nazionalità

Quantità per nazionalità

USA	**2.804**	**(174 militari) (1655 SpaceX)**
Cina	**467**	**(68 militari)**
UK	**349**	
Russia	**168**	**(73 militari)**
Giappone	**93**	
India	**61**	
Canada	**57**	
Luxembourg	**40**	
Argentina	**34**	
Francia	**31**	
Spagna	**24**	
Italia	**21**	
Israele	**19**	
Korea Sud	**18**	
Totale	**4186**	

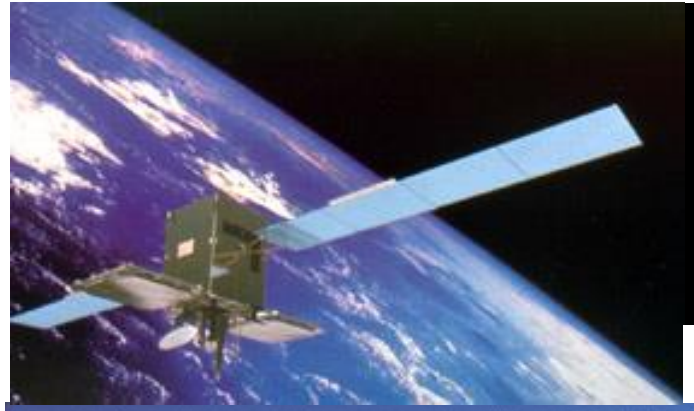
(fonte: Space Foundation - 2021)

Cosa caratterizza i diversi Sistemi Spaziali?

- **Lo scopo: comunicazioni, navigazione, ricerca scientifica, difesa e sicurezza, etc.**
- **Il finanziamento: pubblico, privato, misto**
- **L'utenza: comunità scientifica, ministero della difesa, protezione civile, aziende di servizi commerciali, etc.**

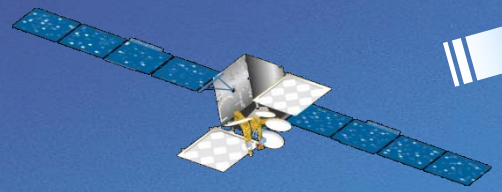
Cosa accomuna tutti i sistemi spaziali?

- La necessità di una connessione affidabile, resiliente e protetta tra essi, dove richiesta, e con il pianeta Terra, dove si concentrano le attività di controllo e gestione del segmento spaziale e di elaborazione ed utilizzazione dei suoi prodotti

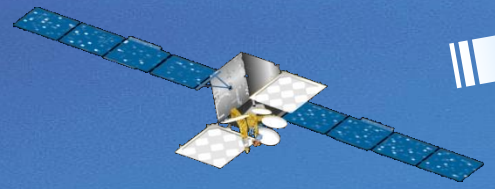


SICRAL

Sistema Italiano di Comunicazioni Riservate ed ALlarmi



- Sicral 1
- Lanciato il 7.2.2001,



- Sicral 1B
- (Versione migliorata di Sicral 1)
- Lanciato il 20 Aprile 2009

- Sicral 2 (con Syracuse 3C)

Progettato come successore di Sicral 1 e scorta in orbita di Sicral 1B.

Lanciato il 26 Aprile 2015

ATHENA FIDUS

Access on THeatres and European Nation for Allied forces – French Italian Dual Use Satellite

Sistema duale di comunicazione satellitare nelle bande EHF e Ka. Cooperazione tra ASI, CNES, DGA, Segredifesa

Opera nelle bande EHF e Ka con velocita fino a 3Gb/sec

Tecniche per la sicurezza delle comunicazioni

Roberto Somma

Alenia Spazio

Giornata di Studio

Echelon e la Sicurezza nel Sistema-Mondo

Milano, 27 Maggio 2004

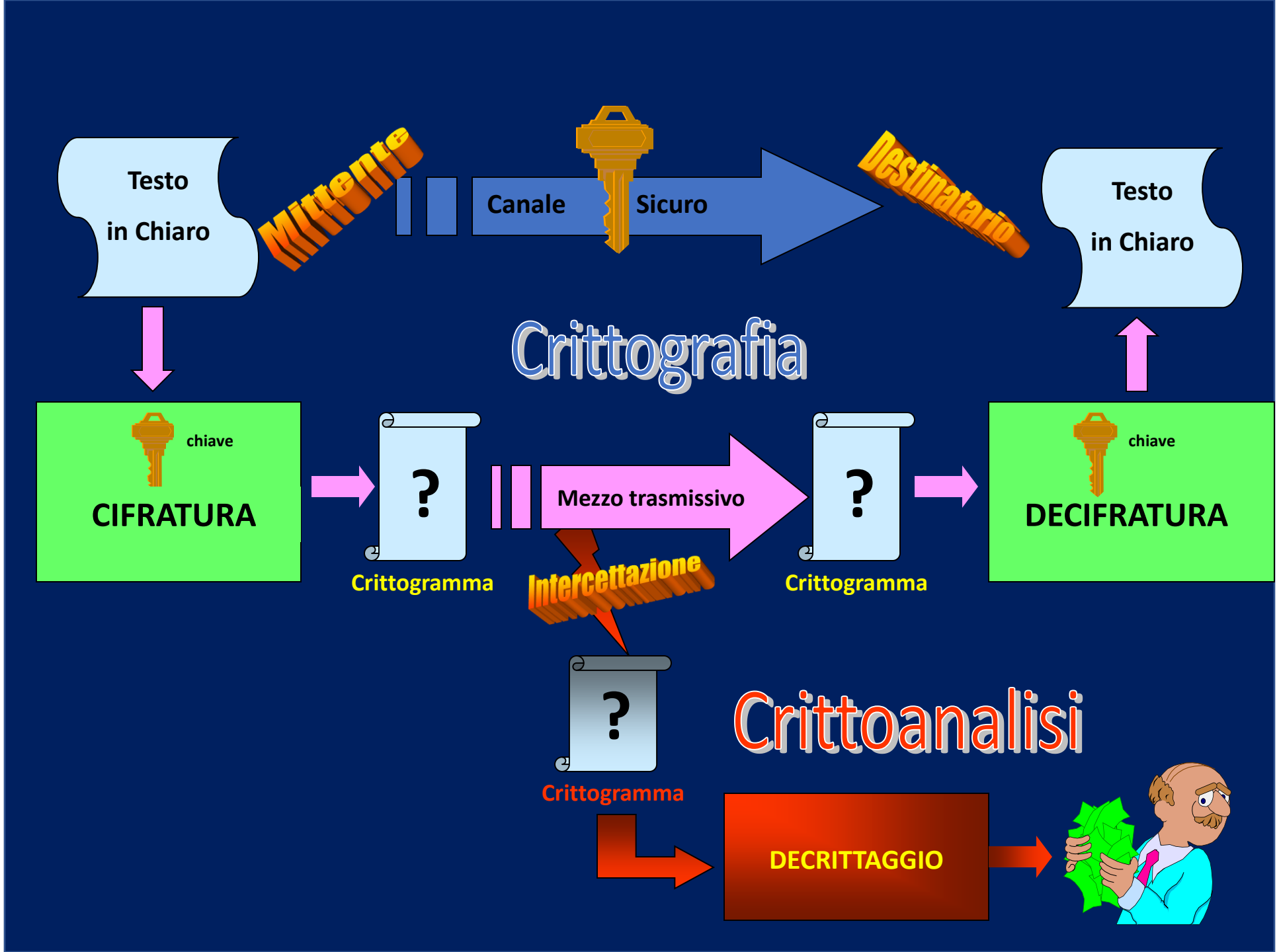
- La "Società dell'Informazione" è caratterizzata dallo scambio di una enorme mole di informazioni/dati tra soggetti in generale distanti tra loro e sovente dislocati sull'intera superficie della Terra.

- Un numero rilevante di informazioni riveste carattere di confidenzialità, per la loro rilevanza politica, economica, strategica.

- Il collegamento tra mittente e destinatario dell'informazione è affidato a mezzi trasmissivi (telefono, fax, onde radio, etc.) per i quali non può essere garantita l'inviolabilità.

- Conseguentemente, lo scenario delle telecomunicazioni deve tener presente la possibilità, tutt'altro che remota, che le informazioni raggiungano ANCHE destinatari diversi da quelli previsti.

- Poiché l'anello più debole della catena è costituito dal transito dell'informazione nel mezzo trasmissivo, lo sforzo di protezione si è concentrato sulla intellegibilità del messaggio, attraverso le tecniche della crittografia.


Testo
in Chiaro
Mittente
Canale
Sicuro
Destinatario
Testo
in Chiaro
Crittografia
chiave
CIFRATURA
?
Crittogramma
Mezzo trasmissivo
?
Crittogramma
chiave
DECIFRATURA
Intercettazione
?
Crittogramma
Crittoanalisi
DECRITTAGGIO

- Un sistema di crittografia “robusto” deve garantire:
  - la trasmissione di informazioni “corrette” tra mittente e destinatario
  - la protezione delle informazioni da intercettazioni/decifrature indesiderate

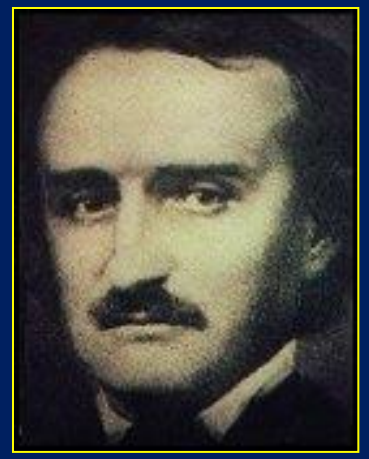
- La progettazione del sistema di crittografia assume che:
  - il mezzo trasmissivo sia violabile all’intercettazione
  - il metodo di cifratura utilizzato sia ricavabile, e quindi disponibile, all’intercettatore

- Anche se vengono adottate tutte le misure possibili per evitare la violazione del mezzo trasmissivo e per proteggere il metodo di cifratura, è evidente che:

la qualità della crittografia adottata risiede principalmente nella chiave e nel modo in cui essa viene scambiata tra mittente e destinatario

Esiste il *Codice Inviolabile*?

"…è veramente da mettere in dubbio che l'intelligenza umana possa creare un cifrario che poi l'ingegno umano non riesca a decifrare con l'applicazione necessaria"



Edgar Allan Poe (1808-1849)

(Citazione tratta da: G.C. Ghirardi- Un'occhiata alle carte di Dio - Il Saggiatore, 1997)

Il Teorema di Shannon

Messaggio: sequenza di numeri corrispondenti ai simboli del messaggio in chiaro secondo una codifica concordata:

m1, m2, m3, m4, …….

Chiave:sequenza di numeri genuinamente casuali :

s1, s2, s3, s4, …….

Crittogramma: sequenza di numeri, c(i) ottenuti sommando m(i) + s(i) (operazione di cifratura):

c1=m1+s1, c2=m2+s2, c3=m3+c3, c4=m4+s4, …….

Decifratura:disponendo della chiave :

m1=c1-s1, m2=c2-s2, m3=c3-s3, m4=c4-s4, …….

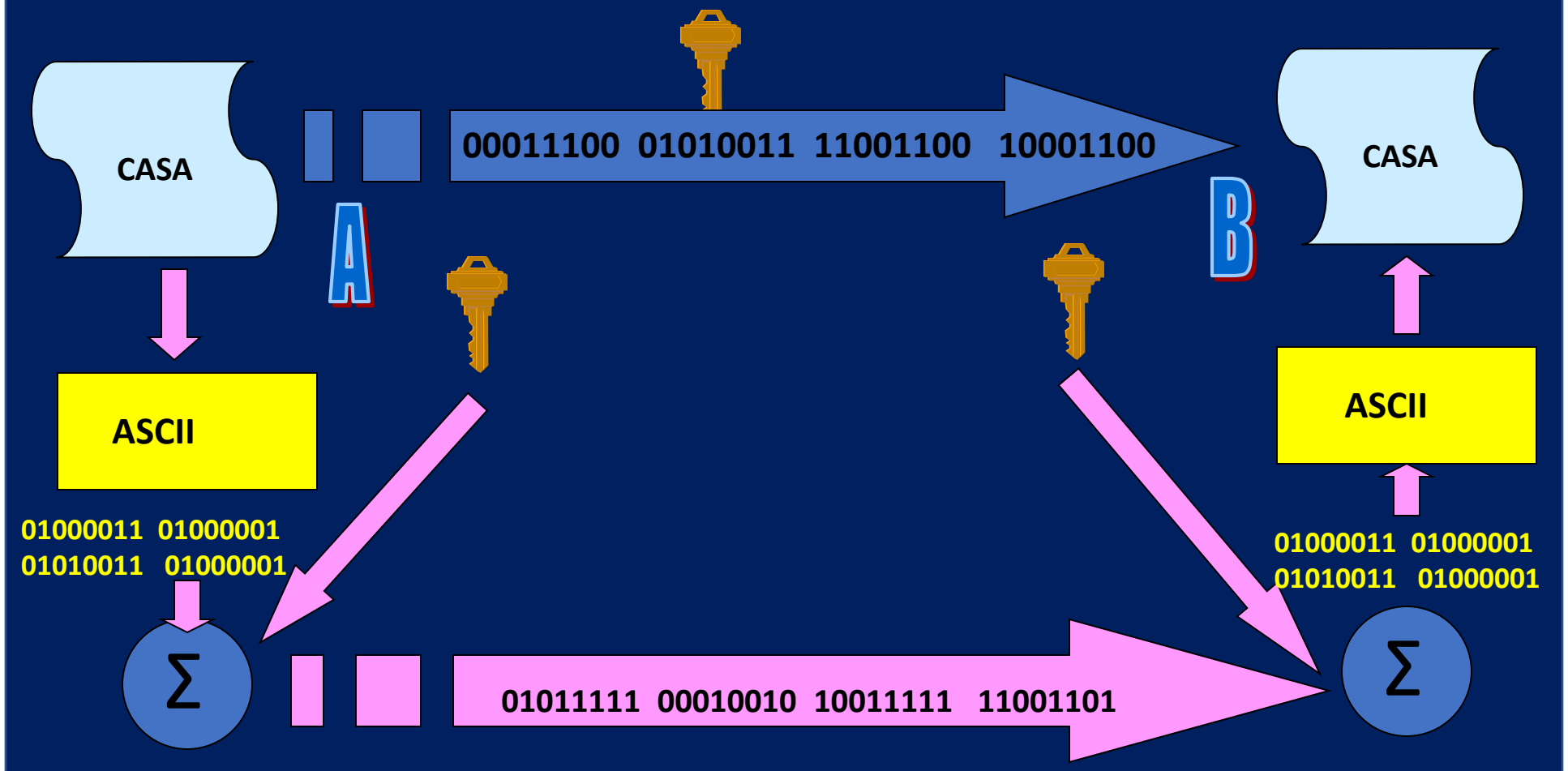
Il teorema afferma che, disponendo del crittogramma, ma non della chiave, tutte le sequenze di messaggio originale sono equiprobabili, cioè la probabilità di interpretazione è la stessa che se non si disponesse del crittogramma.

Le operazioni (cifratura e decifratura) vengono in genere fatte con computers, quindi i simboli del messaggio, così come la chiave, vengono espressi da numeri binari (sequenza di “0” ed “1”), ad es. di 8 cifre (256 simboli).

Somma senza riporto di numeri binari: 0+0=1+1=0; 0+1=1+0=1

Cifratura e Decifratura: Somma senza riporto tra simbolo in chiaro e chiave corrispondente.

Messaggio in chiaro:	C	A	S	A
In numeri (ASCII):	01000011	01000001	01010011	01000001
Chiave (numeri casuali)	00011100	01010011	11001100	10001100
Crittogramma (Σ s.r.)	01011111	00010010	10011111	11001101
Chiave (numeri casuali)	00011100	01010011	11001100	10001100
Messaggio in chiaro (Σ s.r.)	01000011	01000001	01010011	01000001
In lettere (ASCII)	C	A	S	A



PROBLEMA: L'impegno del canale della chiave è della stessa durata di quello del canale del crittogramma. Ciò rende più vulnerabile il sistema

Per risolvere il problema occorrerebbe trovare una maniera inviolabile di trasferire la chiave, cioè la sequenza di numeri casuali

- In linea teorica ciò può farsi ricorrendo alle proprietà della meccanica quantistica ed, in particolare al comportamento di due fotoni generati in maniera *ingarbugliata* (entanglement) ed inviati a mittente e destinatario. La coppia si comporta, complessivamente, come un unico sistema.
- In particolare: se su uno dei fotoni viene effettuata una misura con un filtro polazizzatore, esso lo supererà o no con certe probabilità, la misura effettuata sul secondo fotone darà con certezza lo stesso risultato (superamento o no) nel caso venga utilizzato un filtro di identiche caratteristiche.
- Qualora avvenga una intercettazione non prevista di uno dei fotoni, non è più certo che, a parità di caratteristiche del filtro utilizzato per la misura, il mittente ed il destinatario ottengano lo stesso risultato. Tale evento si verificherà quindi con una certa probabilità valutabile.

come sfruttare questo fenomeno?

Generatore di fotoni *entangled*

Filtro A	Filtro B
0	
	1
0	
	0
	1
1	
	0
	1
1	
0	
1	
	0
	1
0	
1	

Filtro A	Filtro B
	1
1	
0	
	0
1	
1	
	0
1	
1	
0	
	0
	1
	0
1	

Filtro A	Filtro B
0	
	0
1	
	0
1	
0	
	0
	1
1	

Filtro A	Filtro B
0	
	0
1	
	0
1	
0	
	0
	1
1	

A questo punto i due interlocutori sono certi che, a meno che non ci siano state intercettazioni, hanno disponibile la stessa sequenza di "bit"

Filtro A	Filtro B	Filtro A	Filtro B
0		0	
	0		0
1		1	
	0		0
1		1	
0		0	
	0		0
	1		1
1		1	

Per verificare che non ci sono state intercettazioni basta verificare la corrispondenza dei valori in un certo numero di posizioni prese a caso, ed ovviamente scartarle dopo essersele comunicate

Se p è la probabiltà di avere un identico risultato malgrado l'intercettazione, la probabilità che verificando i risultati di n posizioni qualunque essi risultino uguali malgrado l'intercettazione è p^n.

Se p=75% (valore tipico nel caso considerato) ed n=100, si ottiene che la probabilità di una violazione non rilevata vale $(0,75)^{100} = 10^{-13}$, un valore di assoluta garanzia.

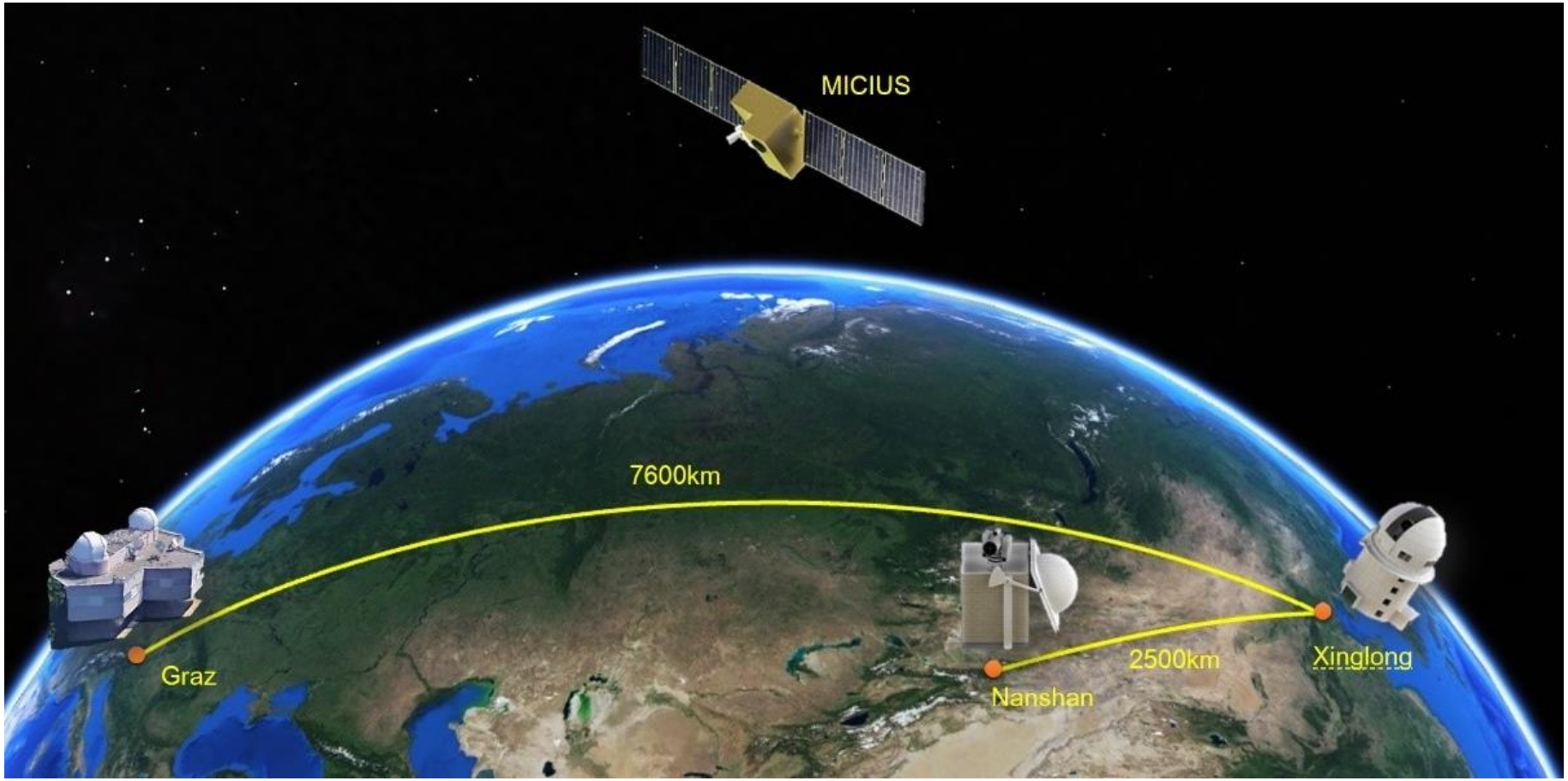
A questo punto i due interlocutori possono inviarsi il crittogramma con certezza più che ragionevole sulla sua inviolabilità (decifrazione).

La “crittografia quantistica”, della quale si è compreso appieno il funzionamento concettuale è attualmente (2004) in fase di “ricerca e sviluppo”, soprattutto per quanto concerne :

- le tecnologie per la sua realizzazione pratica (es: generazione di fotoni entangled, rivelatori, etc.)
- la sperimentazione di eventuali effetti determinati dall’interazione tra il fotone ed il mezzo trasmissivo nel percorso generatore-utente.

La “crittografia quantistica” appare essere un approccio promettente (2004) ed è comunque una ulteriore dimostrazione dello sforzo verso comunicazioni sicure nella ormai millenaria battaglia contro le intercettazioni indesiderate.

E dopo il 2004 ?



15 Agosto 2016
QSS (**Quantum Science Satellite**) o **Mozi** o **Micius**, anche noto come **QUESS** (**Quantum Experiments at Space Scale**),
Realizzato da CAS (Chinese Academy of Sciences)
Accordo con l'Accademia delle Scienze dell'Austria e l'Universita di Graz (Prof Anton Zeilinger, nobel 2022).
Sperimentazione tra Università di Graz e 2 siti cinesi (Xinglong e Nanshan)

Il notiziario online dell'Istituto Nazionale di Astrofisica
19/1/2018

STREAMING SICURO VIA SATELLITE CON L'AUSTRIA

La Cina è quantisticamente vicina

Il satellite cinese Micius ha permesso di dimostrare la fattibilità concreta di un collegamento internet intercontinentale ultra-sicuro facendo comunicare Pechino con Graz, in Austria, attraverso un sistema di crittografia quantistica basato sulla trasmissione di un singolo fotone

LE SCIENZE
6/7/2020

Nuovo successo cinese nelle comunicazioni quantistiche sicure di Karen Kwon/Scientiifiic American

Usando il suo satellite Micius, la Cina è riuscita a stabilire una comunicazione ultra sicura tra due stazioni a terra distanti tra loro più di mille chilometri grazie all"entanglement, uno dei fenomeni più peculiari della meccanica quantistica. Il risultato avvantaggia Pechino nella corsa internazionale verso comunicazioni quantistiche invulnerabili agli attacchi

STARTMAG
11/12/2021

La Cina ha creato una rete di comunicazione quantistica nello spazio per proteggere la sua rete elettrica da eventuali attacchi.

SCIENZA E RICERCA14 OTTOBRE 2022

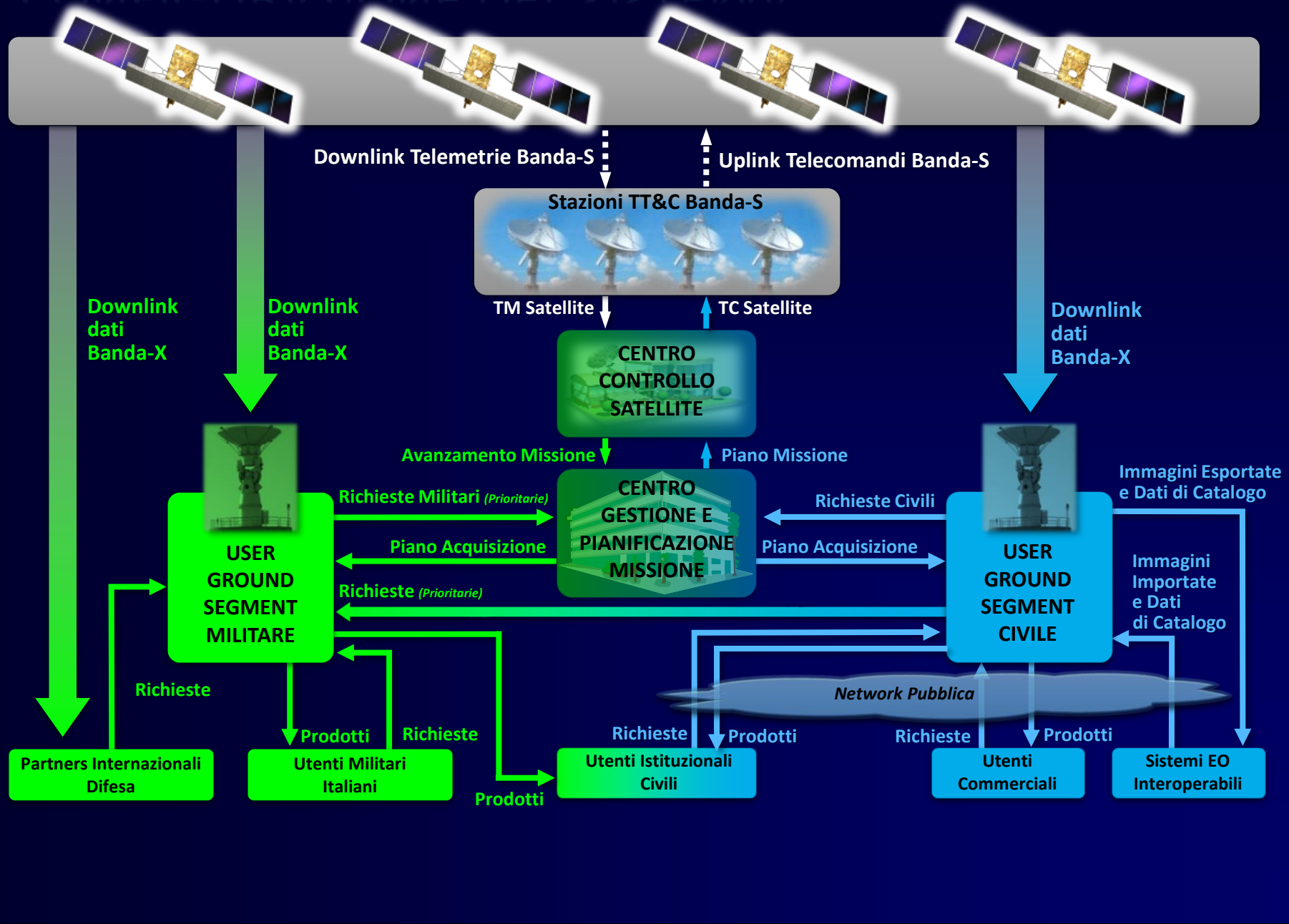
Comunicazioni quantistiche tra Terra e spazio: la Cina si è mossa prima dell'Europa
(https://ilbolive.unipd.it/it/news/comunicazioni-quantistiche-terra-spazio-cina-si ...)

Observo ut Terra custodiatur

Sistema duale

- Il più ingente investimento spaziale italiano in ambito Osservazione della Terra
- Un programma nazionale specificato dall'Agenzia Spaziale Italiana (ASI) e dal Ministero della Difesa
- Finanziato dal Ministero dell'Istruzione, Università e Ricerca e dal Ministero della Difesa con il supporto del Ministero per lo Sviluppo Economico
- Gestito in coperazione da ASI ed Amministrazione Difesa (AD)
- Sviluppato dall' Industria Nazionale Italiana

CONFIGURAZIONE DEL SISTEMA



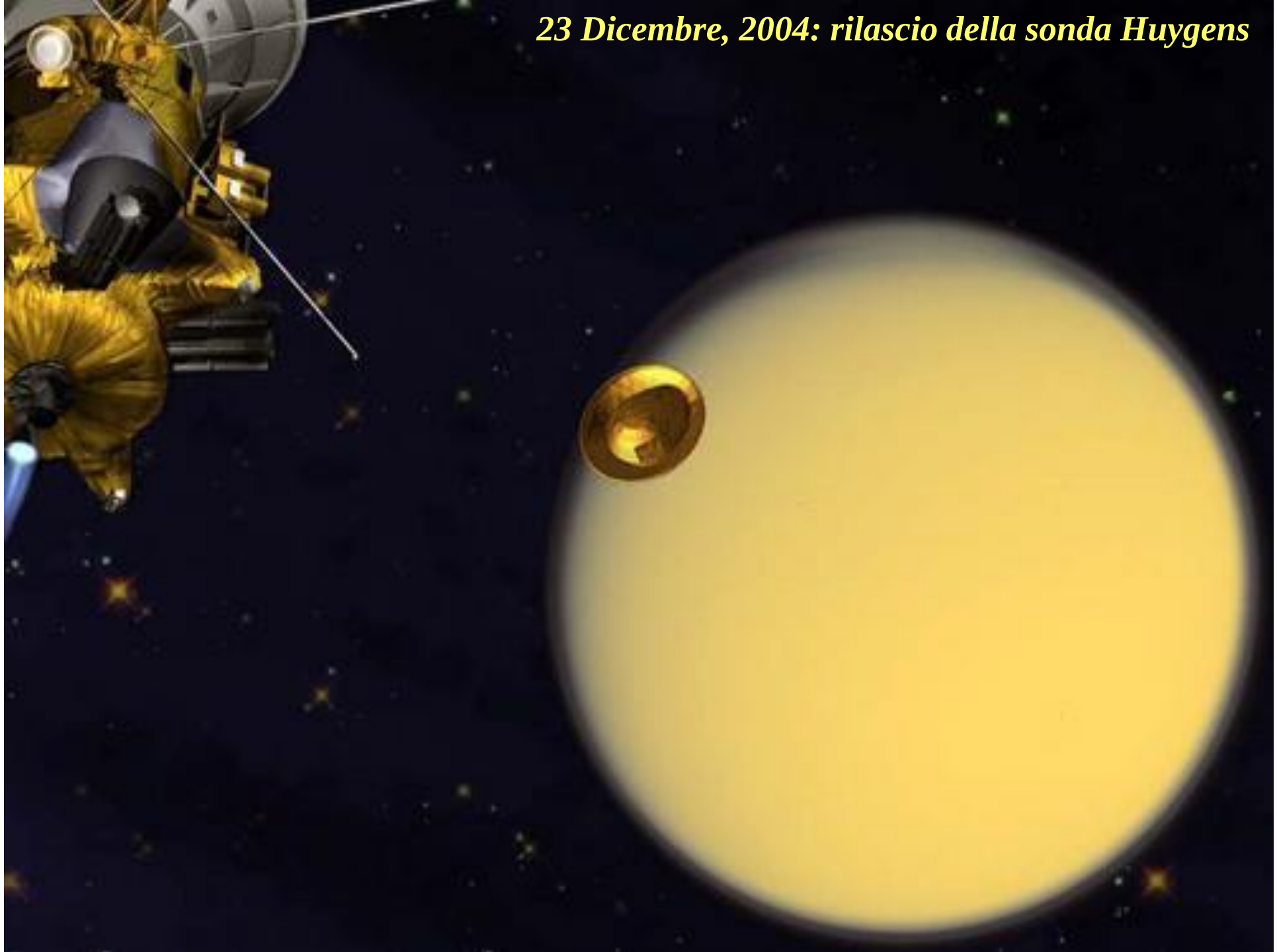
DISTRIBUZIONE GEOGRAFICA

GROUND SEGMENT

Accesso al servizio	USO DUALE
Centro di controllo e pianificazione	FUCINO
Centro di processamento civile	MATERA
Centro di processamento militare	PRATICA DI MARE
TT&C	BANDA S
Link bordo-suolo	BANDA X

DISTRIBUZIONE GEOGRAFICA

DISTRIBUZIONE GEOGRAFICA



23 Dicembre, 2004: rilascio della sonda Huygens

Rosetta

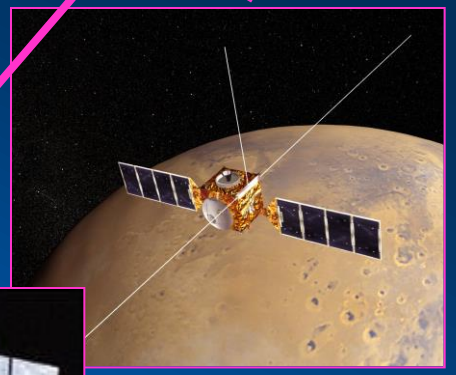
2.3.2004: Lancio
3.2005: FB -1Terra
2 2007: FB Marte
11.2007: FB -2 Terra
5.9.2008: Asteroide Steins
11.2009: FB 3 Terra
10.7.2010: Asteroide Lutetia
7.2011-1.2014: Ibernazione
1-5.2014: verso la cometa
8.2014: studio e caratterizzazione della cometa
12.11.2014:Philae sulla Churyumov-Gerasimenko
11.2014-12.2015: insegimento della cometa
13.8.2015 Rosetta al Perielio
30.9.2016 Fine della missione con discesa sulla cometa

© ESA

Rosetta 2004

TLC

Deep Space



© ESA MEX 2003

© ESA VEX 2005

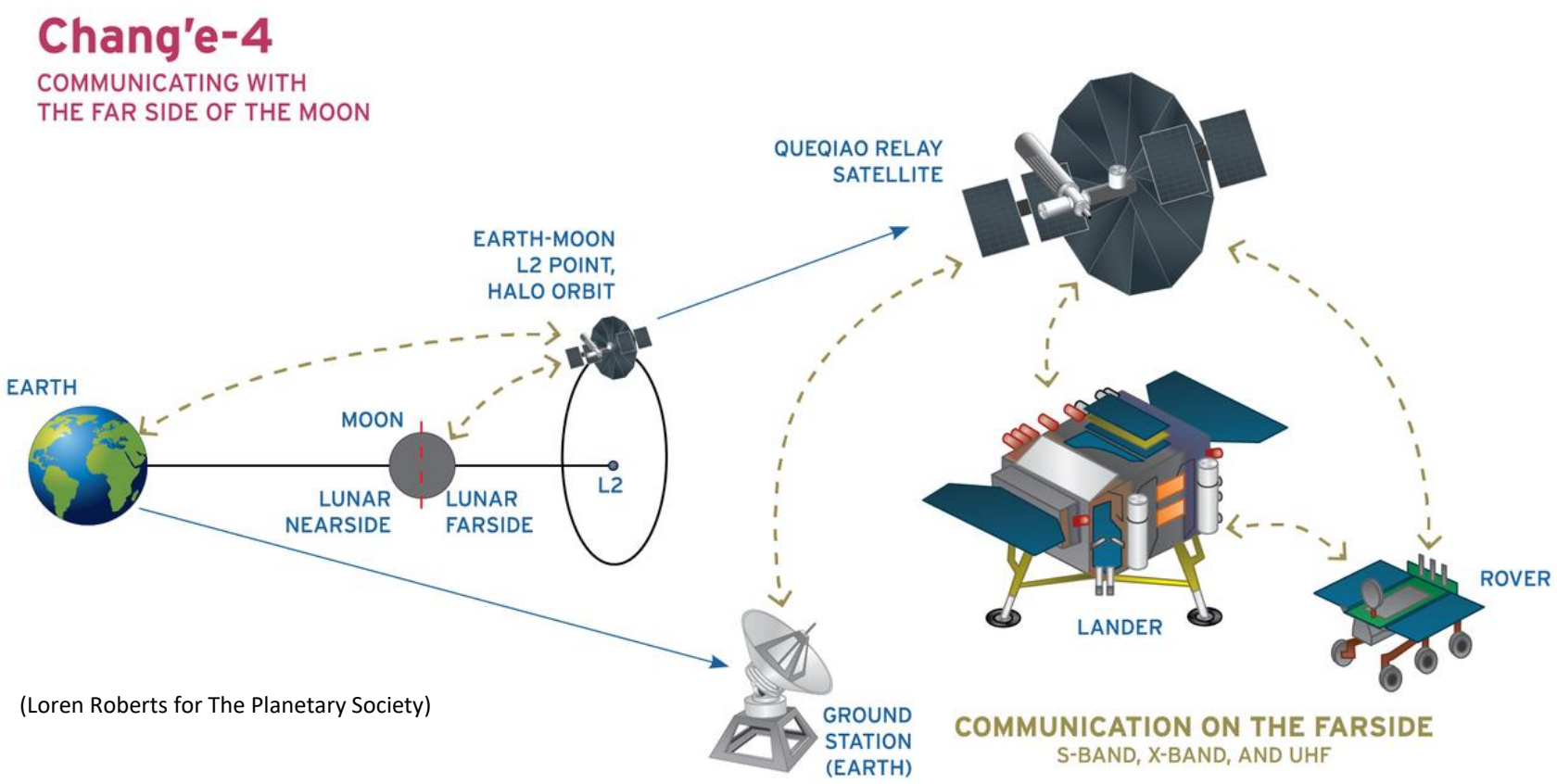
DST: FM

- **Apparato allo stato dell'arte di concezione originale, operante nelle bande S ed X ed in grado di ricevere segnali debolissimi (-150 dBm)**

2013: Bepi Colombo

nelle bande X e Ka

Chang'e 4, atterraggio nella faccia nascosta della Luna (2018)



(Loren Roberts for The Planetary Society)

Componenti: Queqiao – microsatellti Longjiang-1 e **Longjiang-2 – Chang'e 4 – Yutu 2**

Collaborazioni internazionali:

***OLANDA*: ASTRON (strumento per osservazioni astronomiche a frequenze schermate dall'atmosfera)**
***ARABIA SAUDITA*: microcamera sviluppata al King Abdulaziz City for Science and Technology (KACST)**
ALTRI: ad es. Francia, nelle attività di ricerca sui dati dalla Luna

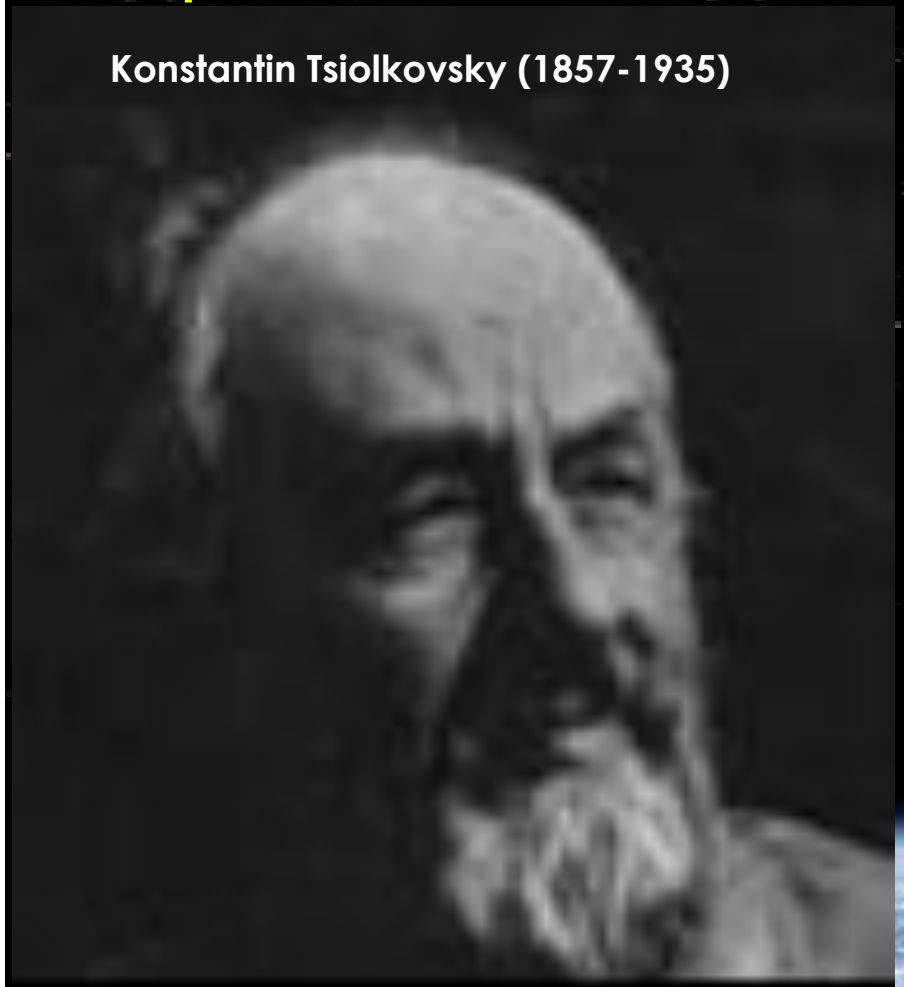
Il prossimo passo dell'umanità verso lo spazio è rappresentato dal ritorno alla Luna, non più inteso come competizione per il primato politico come negli anno '60, ma motivato da ragioni economiche (e quindi anche politiche) legate al reperimento di elementi di interesse strategico (es. Elio-3 e terre rare, presenti sulla Luna).
Il programma prevede stazioni spaziali attorno alla Luna ed insediamenti abitabili sulla sua superficie e si sta configurando una competizione tra gli USA ed alcuni paesi che hanno aderito al suo programma Artemis e la Cina in accordo con la Russia ed altri paesi.
Già si elaborano programmi per missioni umane sul passo successivo, Marte.

Condizione necessaria per l'espansione dell'umanità nel sistema solare è la realizzazione di un sistema di comunicazioni che assicuri la connessione ad elevatissima copertura, affidabile, flessibile e sicura tra tutte le persone ed i mezzi impegnati nell'impresa, ovunque dislocati (in orbita, in infrastrutture spaziali, in insediamenti sulla superficie dei corpi celesti, etc.)

T. Rossi, M. De Sanctis, E. Cianca, C. Fragale, M. Ruggieri, H. Fenech, "Future space-based communications infrastructures based on High Throughput Satellites and Software Defined Networking", 2015 IEEE ISSE, pp.332 - 337, DOI: 10.1109/SysEng.2015.7302778.

E. Cianca, T. Rossi, M. Ruggieri, M. Presi, E. Ciaramella, L. Luini, C. Sacchi, G. Parca, G. Codispoti, "Softwarization and Virtualization as enablers for Future EHF/FSO High Throughput Satellites", IEEE GLOBECOM 2018, pp. 1-6, 9-13, DOI: 10.1109/GLOCOM.2018.8647698

“La Terra è la culla dell’umanità, ma non si può vivere nella culla per sempre”



Konstantin Tsiolkovsky (1857-1935)

«L'esplorazione dello spazio cosmico per mezzo di motori a reazione» 1903