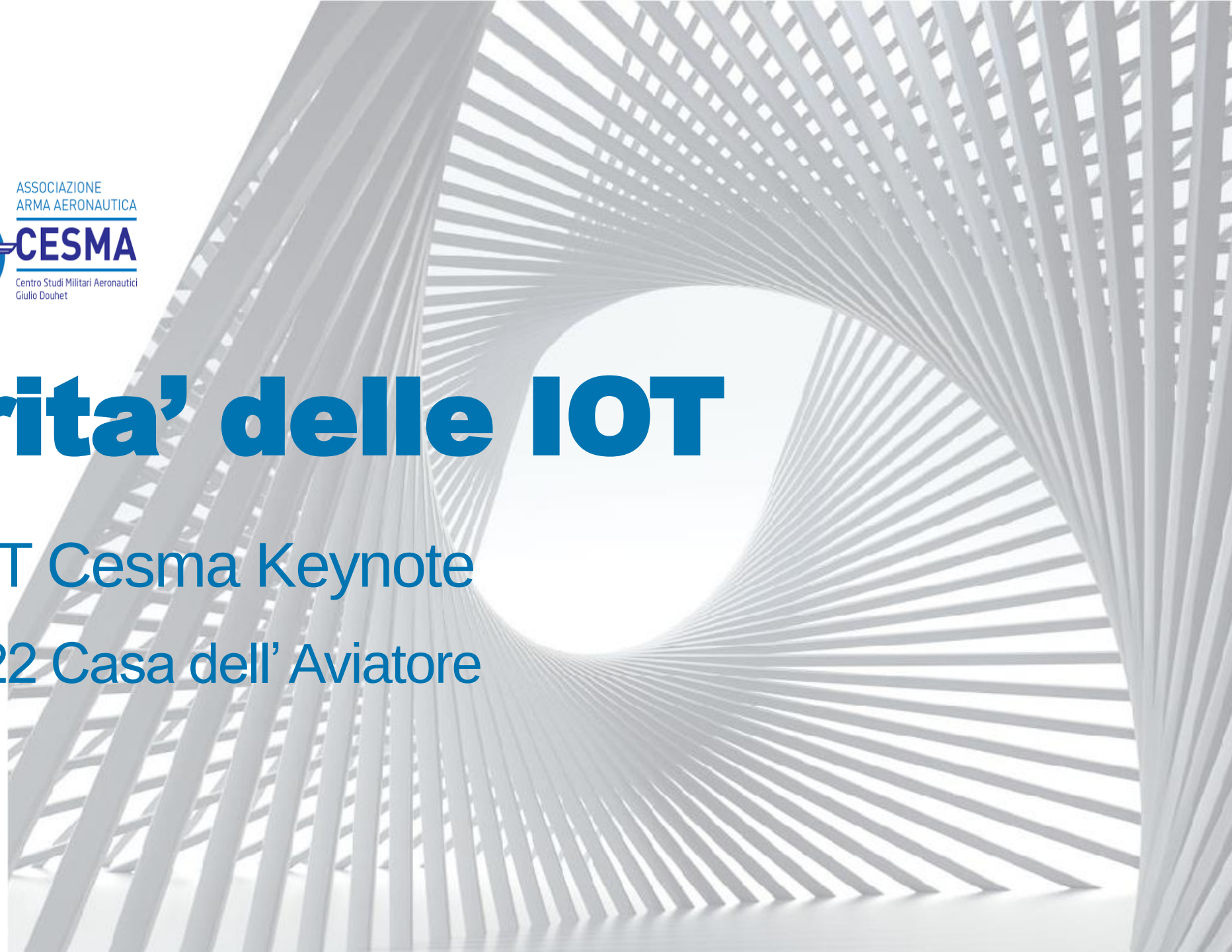


ASSOCIAZIONE ARMA AERONAUTICA
CESMA
Centro Studi Militari Aeronautici Giulio Douhet

Scalarita' delle IOT

IoT, IoBT, OoT Cesma Keynote

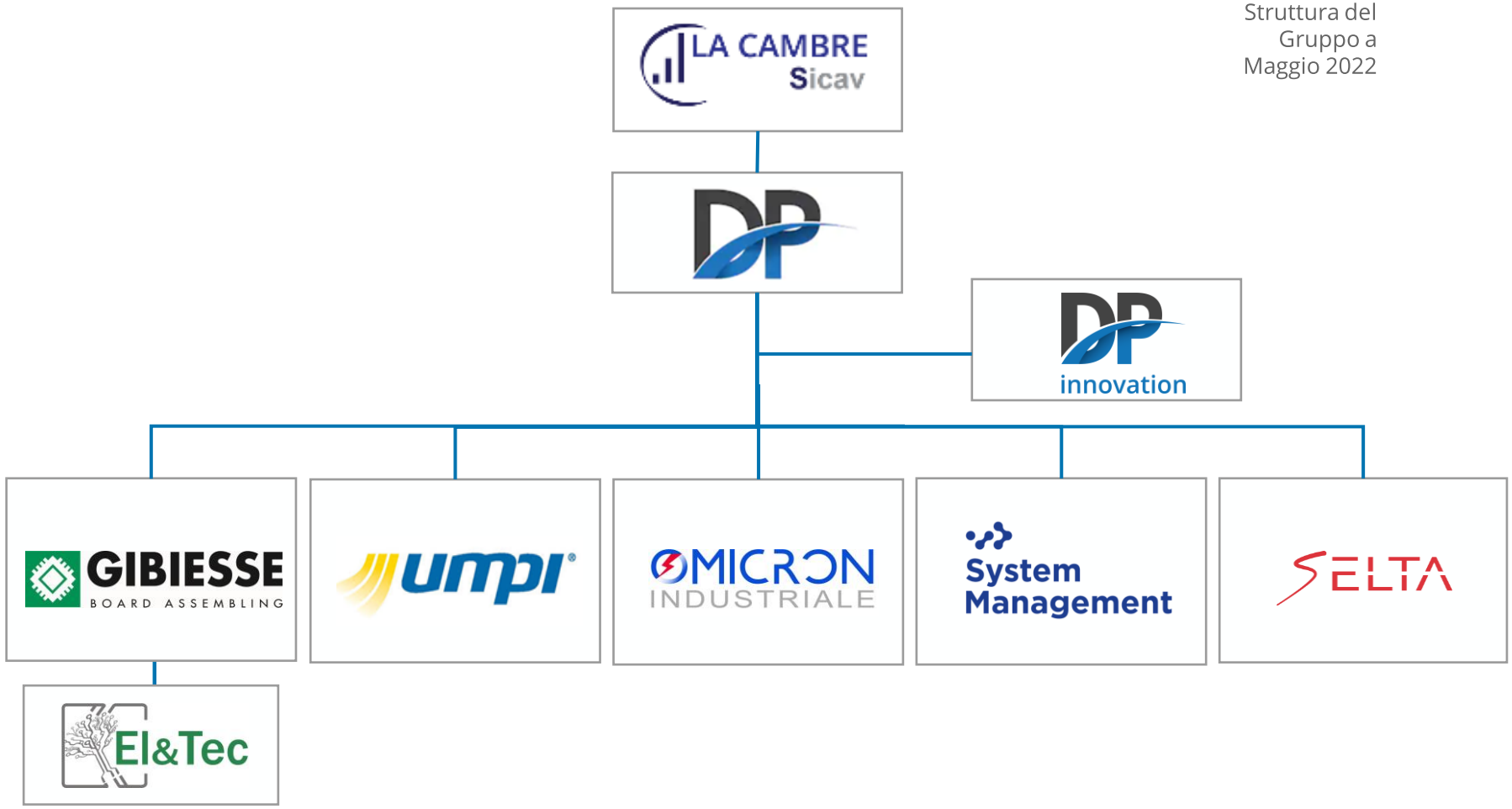
04 Maggio 2022 Casa dell' Aviatore

Il Gruppo DP

- DigitalPlatforms SpA (DP) è un **gruppo industriale italiano** in **rapida crescita** che opera nel settore delle **tecnologie Internet of Things, Cyber e digitali**;
- DP si rivolge primariamente ai **gestori delle infrastrutture critiche** in **Italia** e all'**estero**, nei settori **energia/utilities, telecomunicazioni, trasporti, difesa;**
- **DP è un player full liner**, presente in tutti gli elementi necessari per realizzare **soluzioni IoT end to end**, partendo dallo sviluppo, ideazione e produzione di sensori e prodotti di elettronica industriale, passando per i sistemi e le tecnologie di comando e controllo, fino alle piattaforme IoT, alla system integration per ambienti eterogenei e alla cybersecurity;
- **Il Gruppo DP è oggi costituito da sette aziende/BU**, impiega 400 risorse tra ingegneri, ricercatori, sviluppatori, program manager e addetti alla produzione, esprime un giro d'affari di 70 Ml. di €.

Il Gruppo DP – Organigramma

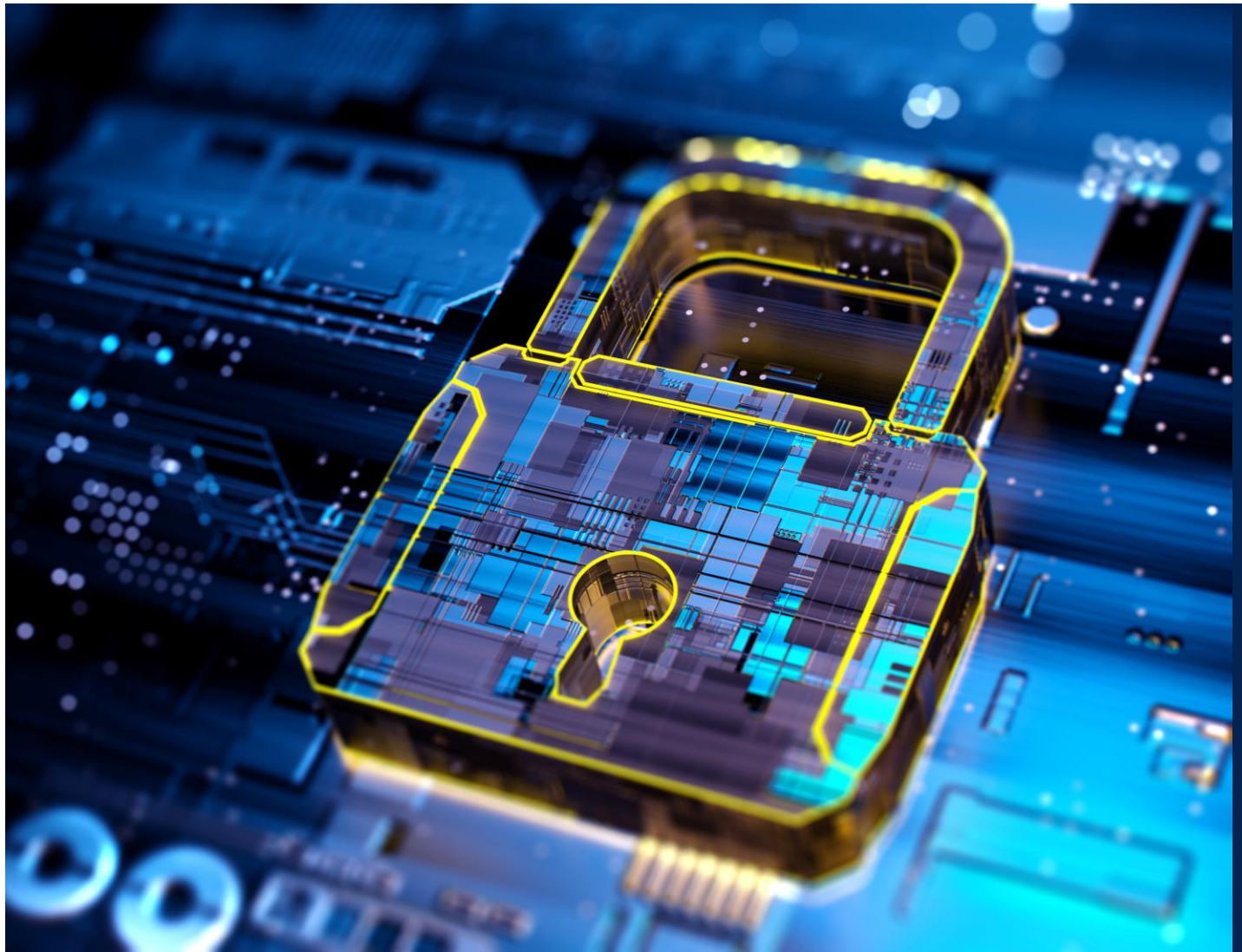
Struttura del Gruppo a Maggio 2022

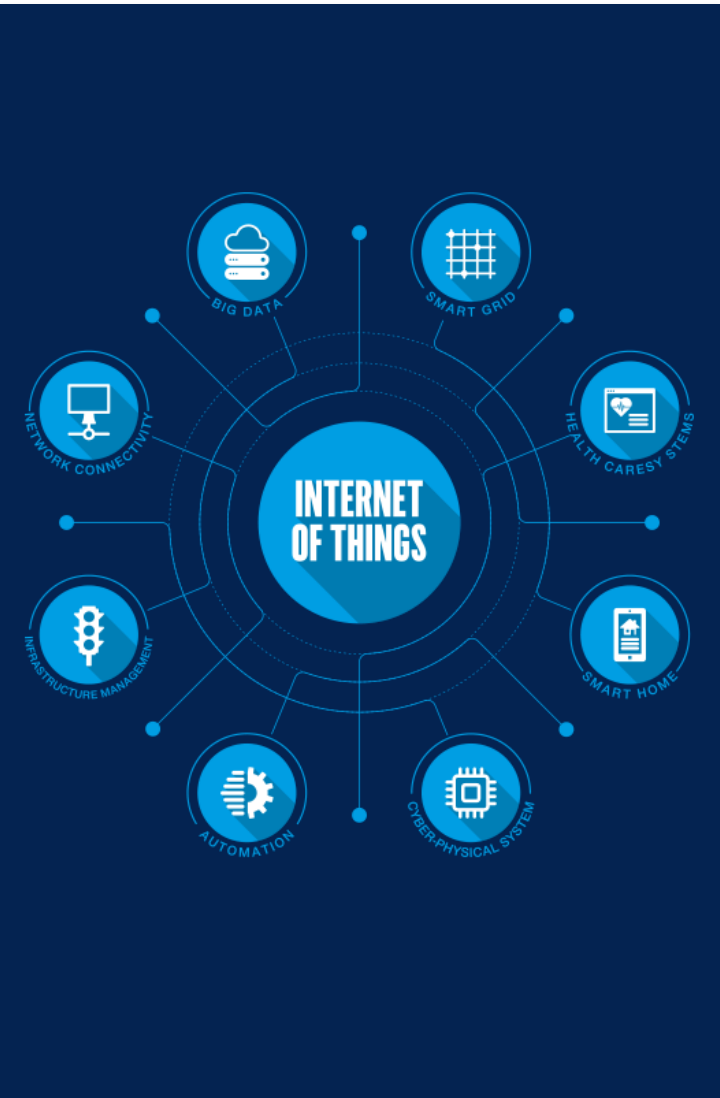


Il mondo IOT:Multisettore

Il mondo IOT:Multi-device

IoT Cyber Security





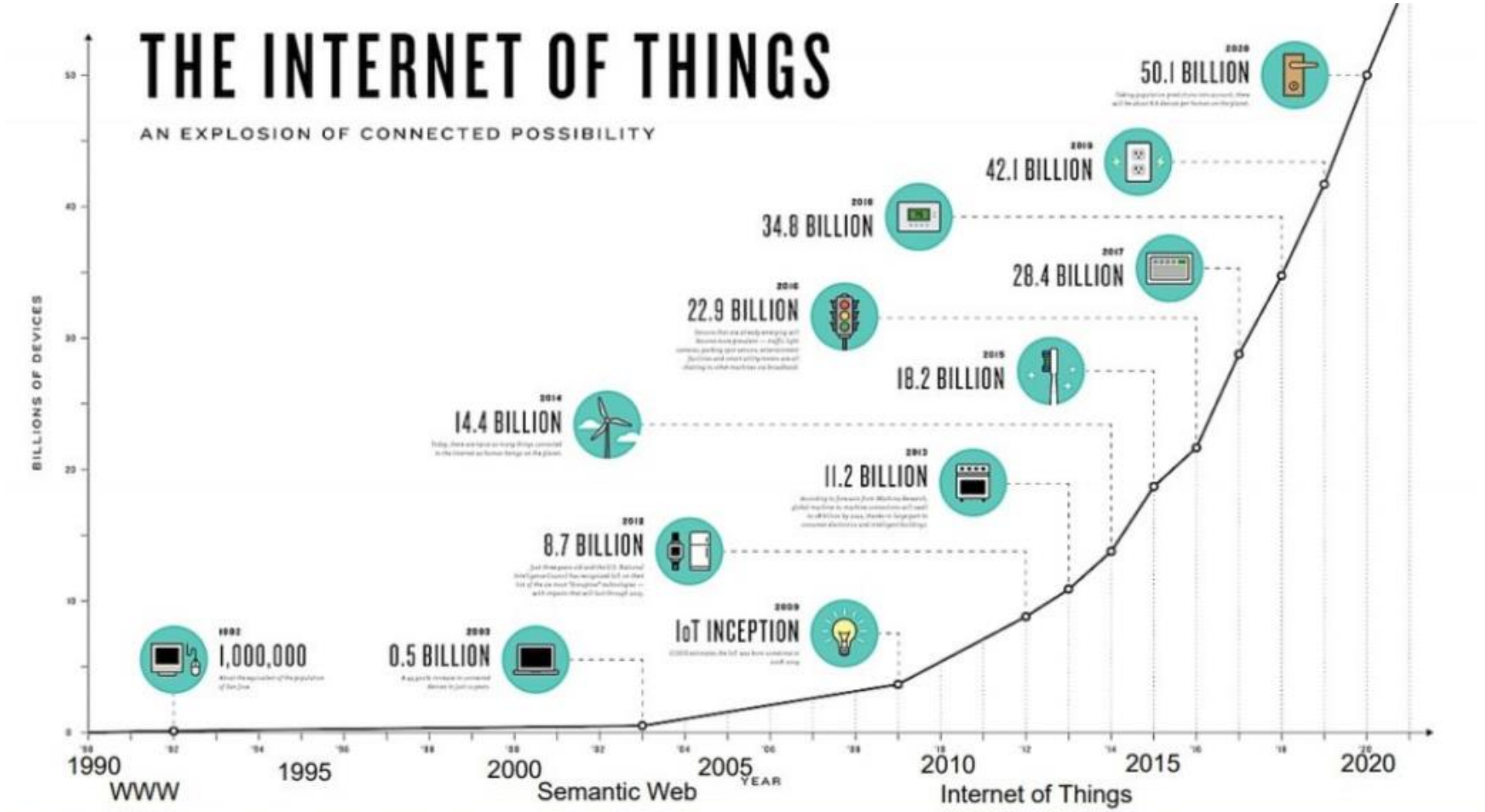
IoT

- Nel 2020 sono stati censiti circa 50 miliardi di device IOT a livello worldwide. I device IOT sono progettati per essere connessi ad una rete e molti di loro sono connessi a Internet.

- Questi device devono essere identificabili, manutenuti e monitorati dai team di sicurezza nelle grandi aziende e nelle grandi organizzazioni.

- Alcuni (pochi) di questi prodotti IOT comunicano una telemetria di base al produttore del device oppure hanno i mezzi per ricevere degli update software; nella gran parte dei casi questo e' impossibile e il Cliente finale IT non sa nemmeno che esse esistano sulla rete.

I numeri dell'IoT



I numeri dell'IoT

EXHIBIT 3

IoT ADOPTION AND VALUE BY COUNTRY

	Global	US	UK	FR	DE	SP	IT	BNLX	CH	JP	AUS
% IoT Adopters	90%	94%	91%	91%	88%	89%	95%	91%	85%	88%	96%
% Projects in Use phase	25%	27%	25%	23%	25%	22%	26%	25%	25%	23%	18%
Time to Use stage (months)	12	11	13	12	14	11	10	12	16	12	16
Plan to use IoT more in 2 years	66%	78%	69%	67%	53%	76%	69%	59%	65%	51%	56%

Principali Applicazioni IoT

- Industria
- Agricoltura
- Automotive e Domotica
- Retail
- Medical
- Military ,Drones ,Soldiers,Sensors
- Energy, Oil and Gas
- Smart Grids
- Smart Cities

Perchè adottare l'IoT

EXHIBIT 7

TOP REASONS FOR IoT ADOPTION BY INDUSTRY

Manufacturing		Power & Utilities		Oil & Gas		Mobility		Smart Places	
Quality and compliance	47%	Smart grid automation	44%	Workplace safety	45%	Inventory tracking and warehousing	48%	Productivity enablement/ workplace analytics	47%
Industrial automation	45%	Grid asset maintenance	43%	Employee safety	43%	Manufacturing operations efficiency	40%	Building safety	42%
Production flow monitoring	43%	Remote infrastructure maintenance	40%	Remote infrastructure maintenance	39%	Surveillance and safety	34%	Predictive maintenance	41%
Production planning and scheduling	38%	Smart metering	37%	Emissions monitoring and reduction	35%	Remote commands	34%	Regulations and compliance mgmt	36%
Supply chain and logistics	38%	Workplace safety	37%	Asset and predictive maintenance	35%	Fleet management	32%	Space mgmt and optimization	34%

IoT Signals aka.ms/IoTsignals

Microsoft | hypothesis

Le sfide dell'IoT

- Cybercrime,Botnet,Shadow IoT,Data Theft;
- Weak authentication (passwords and more);
- Intellectual Property Rights;
- Tech standard spesso inconsistente o non del tutto definite;
- Sicurezza insufficiente per i dati e la loro protezione.

Superficie d’attacco

- Questi device possono essere usati da attori malevoli che possono utilizzarli come porte di ingresso ed, una volta all’interno della rete, possono muoversi alla ricerca di accounts e dati di valore; una volta entrati su ogni IoT device della rete possono, attraverso un “tcpdump”, sniffare tutto il traffico della rete e delle sottoreti locali.
- I device IoT sono usati in molti mondi applicativi dai sistemi di gestione delle citta’, alla sanita’, alle fabbriche, alle imprese fornitrici di servizi di utilita’ come Gas, Acqua, Elettricita’, Trasporto ed in genere nelle infrastrutture critiche.
- Questa espansione allarga in maniera drammatica la base di attacco di attori malevoli.

Difendere

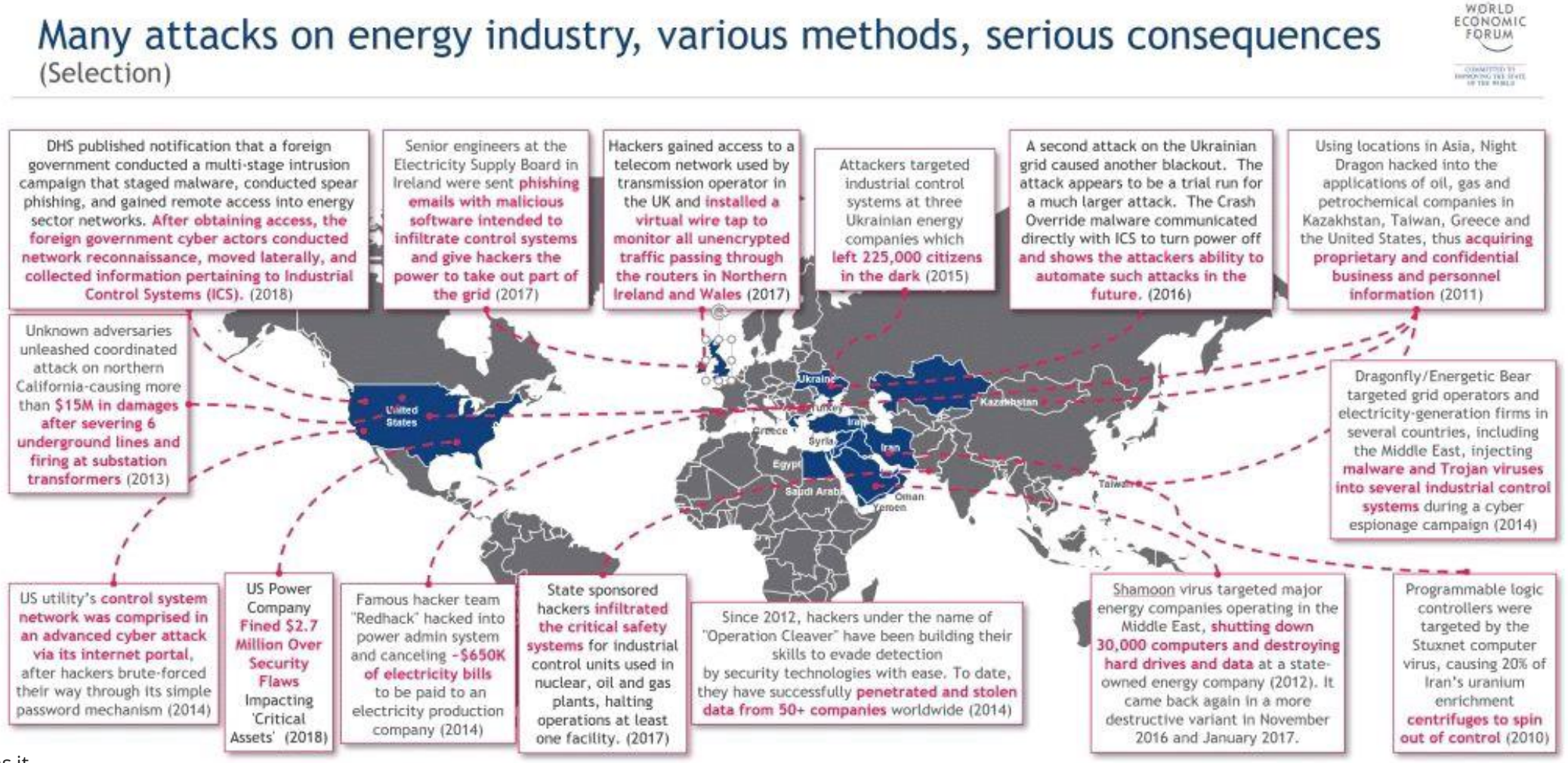
- Questi device embedded non possono essere difesi con la tecnologia basata sugli agent e sono molto spesso non aggiornati o non configurati correttamente e i responsabili della sicurezza necessitano di nuove strategie per mitigare.

- Il Gruppo DP, forte della sua natura di Full Liner sul mondo IoT, intende affrontare il tema della cybersicurezza IOT attraverso un lavaggio del software dei dispositivi IOT cliente con una riscrittura del software per renderli sicuri e affidabili, con una elaborazione di capacita' tutta Italiana.

I 5 step per l'IOT Cybersecurity

1. **Proteggere i processi strategici:** non si può proteggere tutto ma si possono proteggere i più importanti;
2. **Mappare il terreno digitale:** quello della rete interna in prima battuta e poi le terze parti e i manutentori con accesso remoto;
3. **Analizzare il rischio:** valutando vulnerabilità attraverso modelli di threat intelligence o red-team che cercano altri vettori di attacco;
4. **Mitigare e Proteggere:** riducendo il numero degli entry points accessibili della rete usando zero trust policy di accesso e segregando i device IoT e OT dalle altre reti;
5. **Rimuovere tutti i Silos tra IT,OT,IoT e le CPS:** deviando tutti gli alerts verso il Soc e poi verso il Siem e la Soar per rispondere rapidamente agli incidenti OT/IoT.

Un esempio sul mondo energy



IoBT

Per IOBT(Internet of the Batterfield Things) si intende una rete di dispositivi che permettano di aumentare la consapevolezza situazionale degli operatori impegnati sul campo fornendo loro, attraverso una rete di sensori e dispositivi interconnessi in grado di restituire dati e informazioni utili all'operazione, una percezione extrasensoriale dell'ambiente circostante aumentando così le capacità di intelligence, sorveglianza, ricognizione, implementando contestualmente i sistemi IFF (Identification Friend or Foe).

Lo **US Army Research Laboratory** e un consorzio di Universita' americane stanno sviluppando una ricerca denominata IOBT REIGN (Internet of Battlerfield Research on Evolving Intelligent Goal-Driven Networks) il cui scopo è quello di indagare e sfruttare sistemi connessi sul campo di battaglia.

Le applicazioni dell'IoBT

Le reali applicazioni dell'IoBT nell'ambito militare sono diverse:

- Implementazione della capacità C5ISR, al fine di permettere la loro disseminazione a vari livelli della catena di comando e fornire così una **COP (Common Operational Picture)** completa;
- Implementazione di sistemi logistici dove l'impiego di una serie di sensori montati su aerei, UAV, satelliti e navi contribuiranno a monitorare i movimenti ed i traffici marittimi in ampie aree;
- L'Internet of Battlefield Things sarà utile anche per monitorare le condizioni fisiche dei soldati con sensori incorporati nelle uniformi dei militari;
- Svolgere attività di manutenzione predittiva dei vari dispositivi attraverso l'analisi dei big data relativi alle condizioni delle piattaforme, creando così un vantaggio funzionale ed un importante risparmio di costi.

IoBT

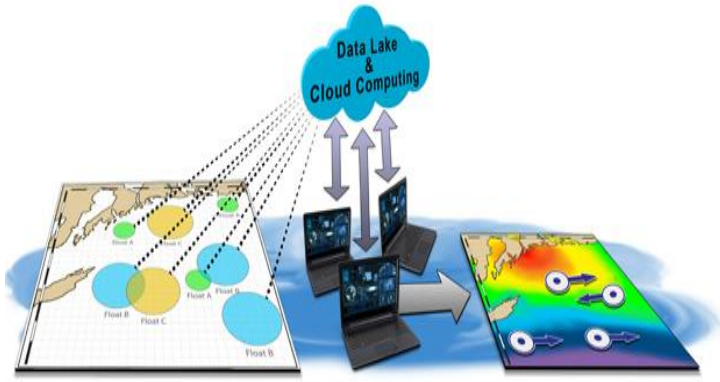
«L'IoBT deve sfruttare adeguatamente tutte le reti: blu, grigia e rossa» ha affermato Stephen Russell, capo del ramo di elaborazione delle informazioni sul campo di battaglia dell'Army Research Lab. In questo costrutto, le reti blu sono sicure e di proprietà militare, le reti grigie sono spesso reti civili dall'affidabilità incerta e le reti rosse sono reti avversarie.

Russell ha sottolineato che lo sforzo di sfruttare le capacità uniche di un campo di battaglia in rete sarà un problema interdisciplinare che riunirà ricercatori in informatica cyber-fisica, teoria dell'informazione, sicurezza, metodi formali, apprendimento automatico, networking, controllo e scienze cognitive.

Un esempio

Ocean of Things mira ad espandere la consapevolezza marittima in mare aperto

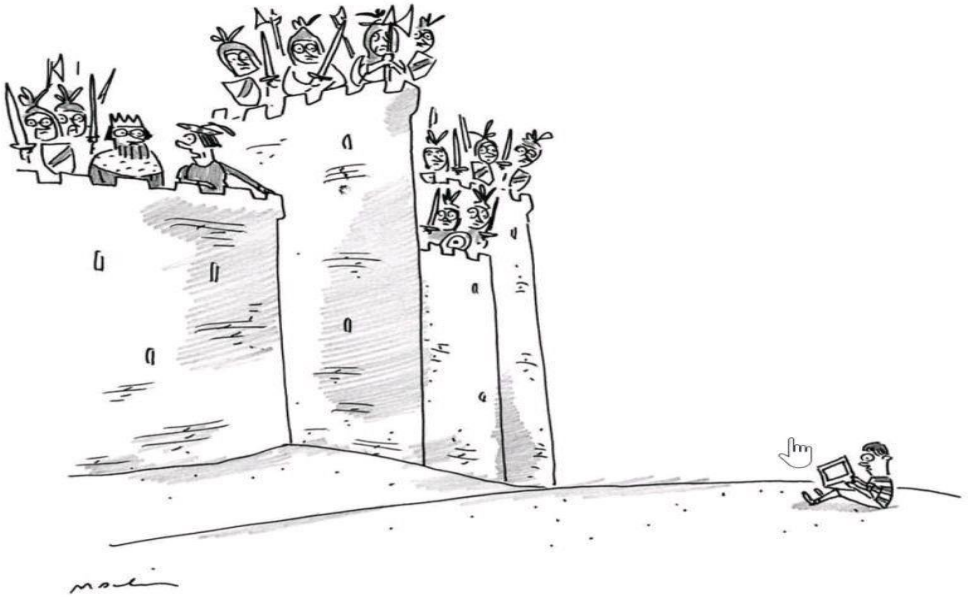
La DARPA ha annunciato il programma Ocean of Things, che mira a consentire una consapevolezza della situazione marittima persistente su vaste aree oceaniche dispiegando migliaia di piccoli galleggianti a basso costo che potrebbero formare una rete di sensori distribuita. Ogni galleggiante intelligente conterrebbe una suite di sensori disponibili in commercio per raccogliere dati ambientali, come la temperatura dell'oceano, lo stato del mare e la posizione, nonché dati sull'attività di navi commerciali, aerei e persino mammiferi marittimi che si spostano nell'area. I galleggianti trasmetterebbero periodicamente i dati via satellite a una rete cloud per l'archiviazione e l'analisi in tempo reale.



Lauren Barrett Knausenberger is the Chief Information Officer for the Department of the Air Force, comprised of the U.S. Air Force and U.S. Space Force.

We are already using more sensors in everything that we deploy, in airplanes, satellites, even airmen.” For the military, the world of Internet of Things, or IoT, has to work across the air, land, space and sea domains. And for the Air Force to enable a greater sensor-based environment, it has to tackle data platforms, cloud storage and capabilities, communication infrastructure and its network.

The key will be the ability to scale such an integrated and connected environment to meet not only the Air Force’s multidomain operations, but also Joint Force operations as well as coalition partner warfighting



"Bad news, Your Majesty—it's a cyberattack."

Grazie per l'attenzione.

marco.braccioli@dplatforms.it

www.dplatforms.it