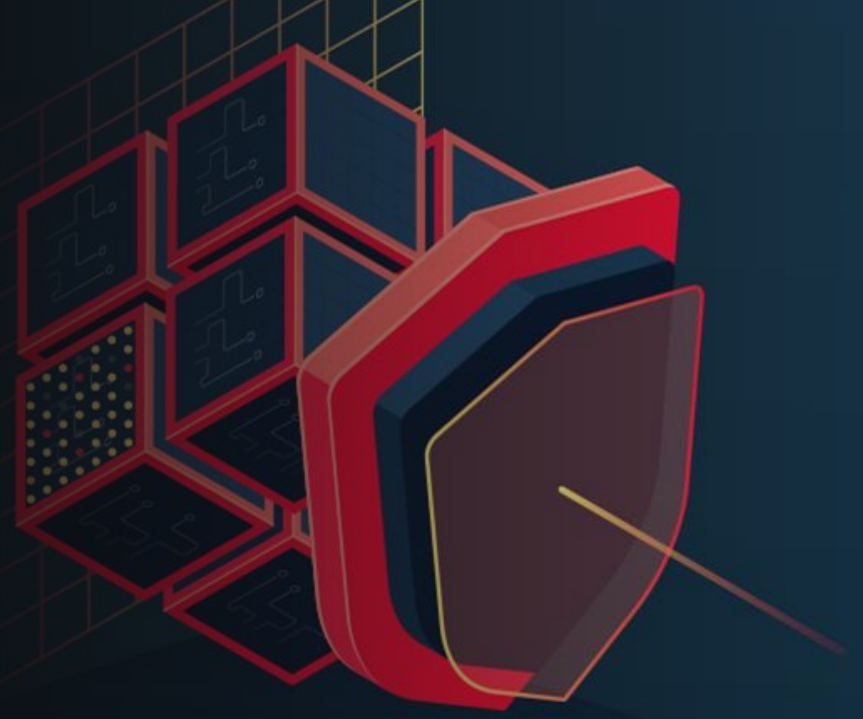
Il perimetro della sicurezza cibernetica

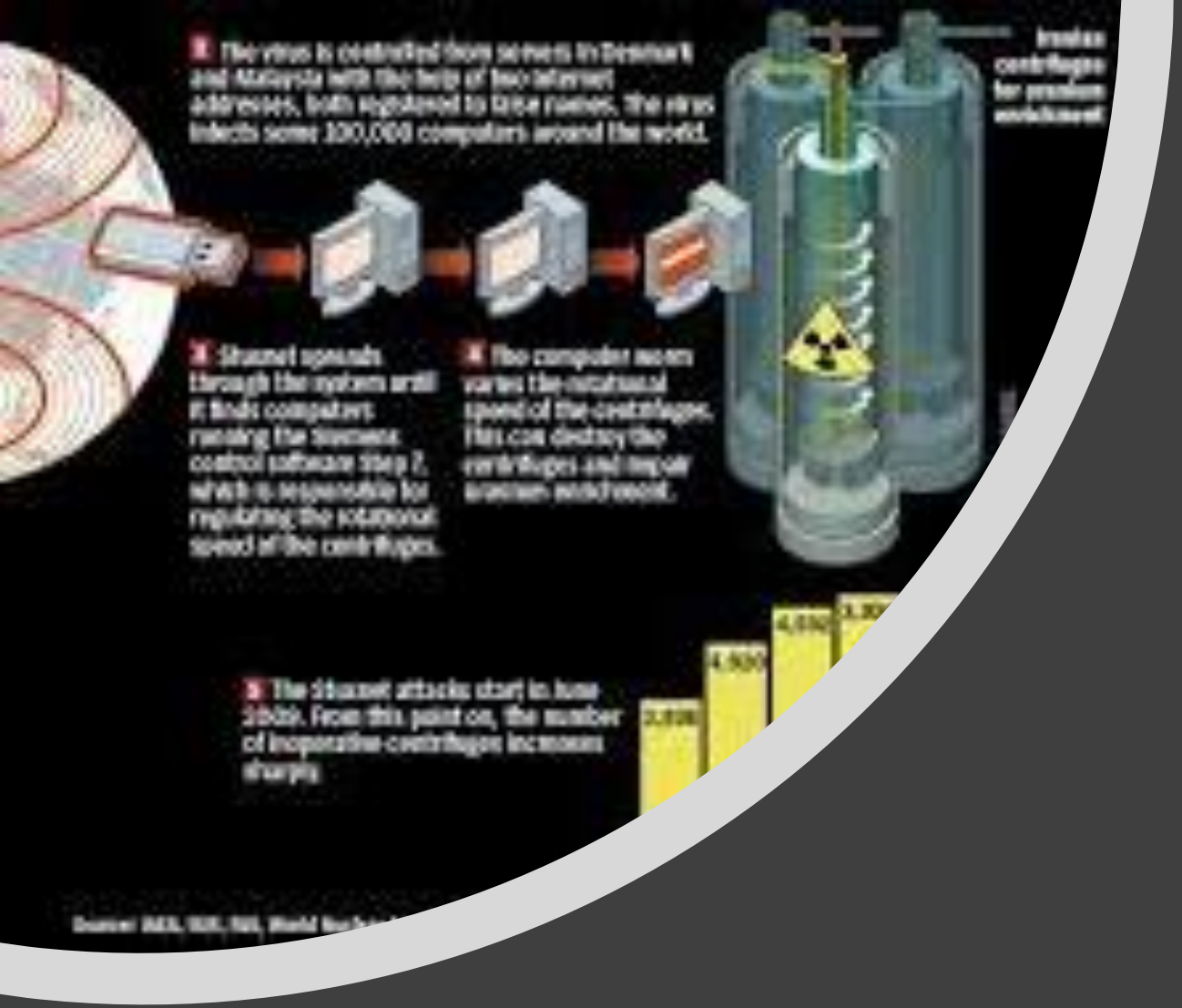


Domenico Ielo

Di cosa parliamo

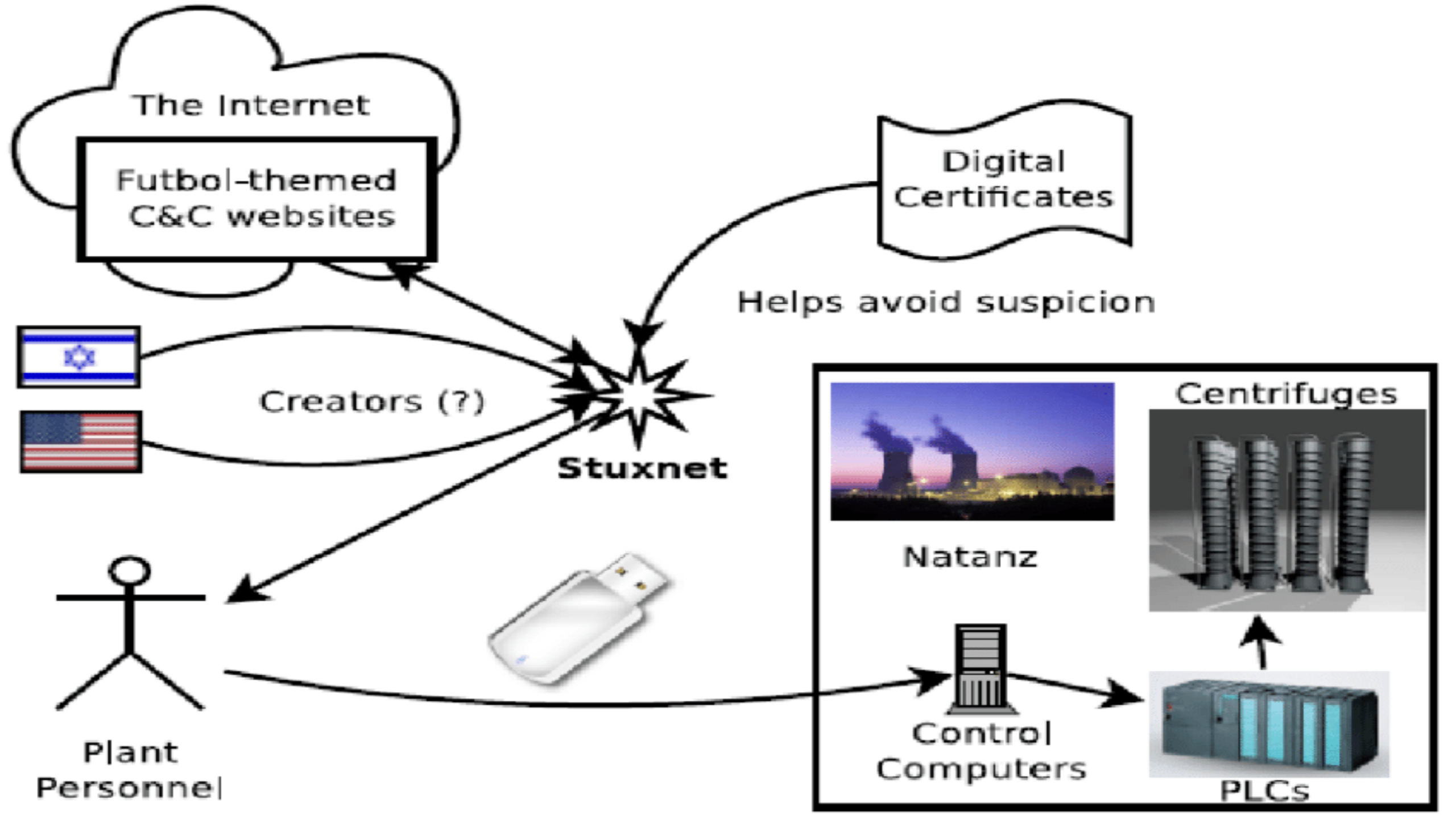
Sicurezza cibernetica funzionale alla sicurezza nazionale

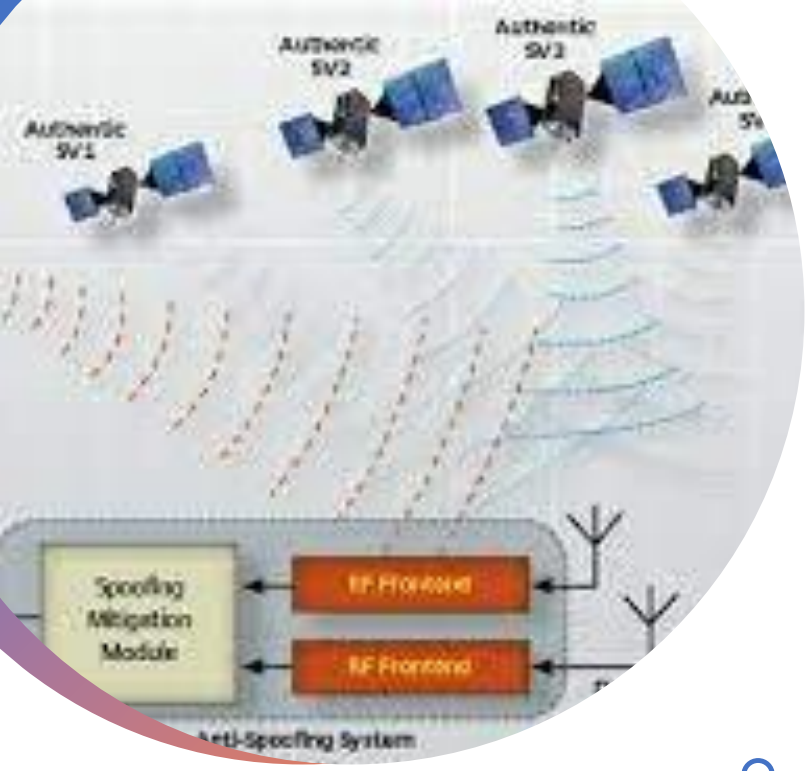
L’attacco all’organizzazione è funzionale ad attaccare le strutture dello Stato

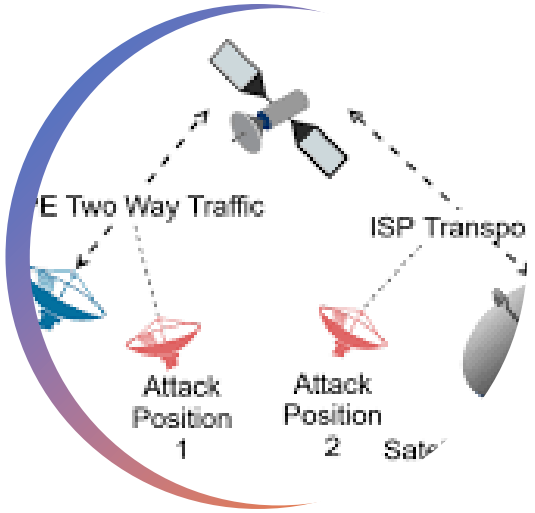


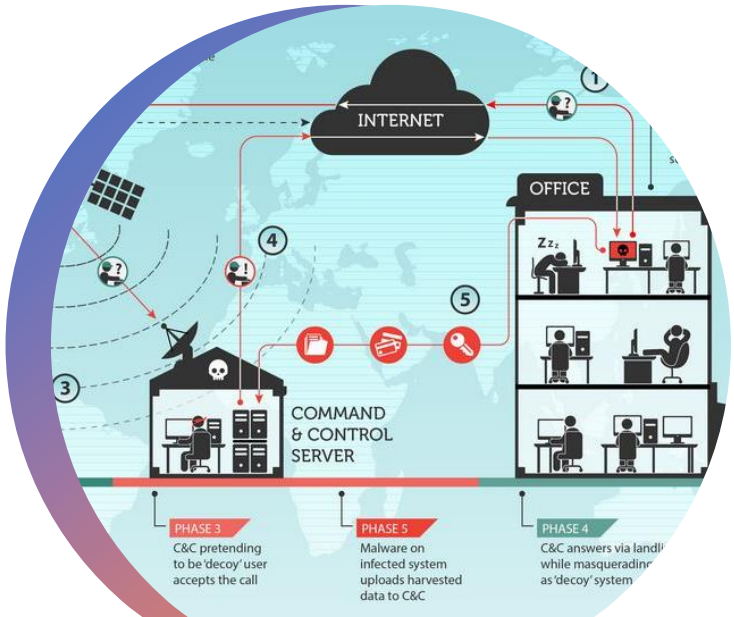
Guerre cibernetiche

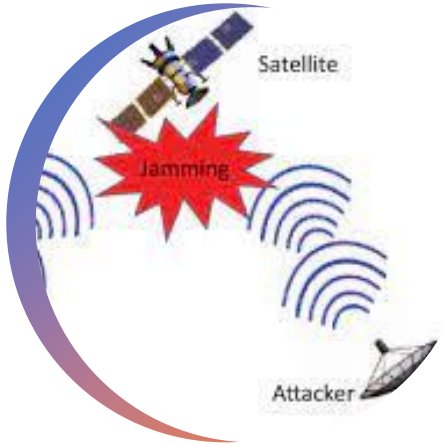
- preparazione e conduzione di operazioni di contrasto nello spazio cibernetico
- intercettazione, alterazione e distruzione informazione e dei sistemi di comunicazione nemici, procedendo a far sì che sul proprio fronte si mantenga un relativo equilibrio dell'informazione


The Internet
Futbol-themed C&C websites
Digital Certificates
Helps avoid suspicion
Creators (?)
Stuxnet
Centrifuges
Natanz
Plant Personnel
Control Computers
PLCs









Attacchi cyber satellitari

- GPS spoofing
- Jamming
- Eavesdropping
- Hijacking
- Accecamento

Criminalità organizzata cyber

Domanda

Con quali pattuglie uno Stato si difende dagli attacchi cibernetici?

Risposta – con lo scudo cibernetico

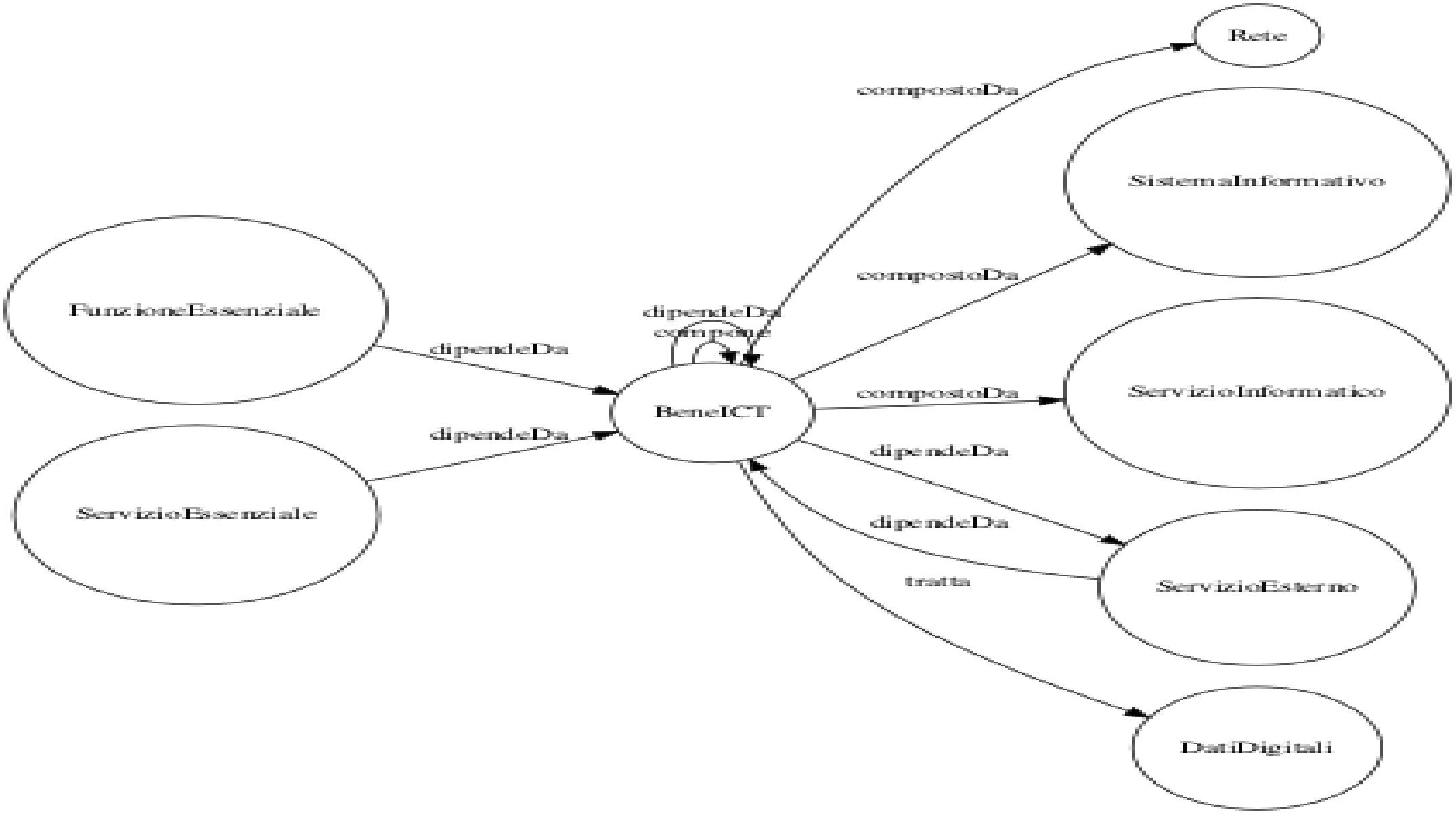
- D.l. 105/2019: assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale
- Reti e sistemi delle p.a., degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende:
  - l'esercizio di una funzione essenziale dello Stato,
  - la prestazione di un servizio essenziale per il mantenimento di attivita' civili, sociali o economiche fondamentali per gli interessi dello Stato

Rischio sicurezza nazionale – DPCM n. 131/2020

- Causa: fatto di natura accidentale o intenzionale
- Effetto: malfunzionamento, interruzione, anche parziali, utilizzo improprio delle reti, dei sistemi informativi e dei servizi informatici
- Nesso: impatto sul bene ICT
  - limitazione della operatività del bene ai fini dello svolgimento della funzione o servizio essenziale
  - compromissione disponibilità, integrità, riservatezza o informazioni trattati dal bene, ai fini dello svolgimento della funzione o servizio essenziale
- Magnitudo: entita' del pregiudizio per la sicurezza nazionale

Da quali mattoni è compost il muro cibernetico?

DPCM 15 giugno 2021


Rete
compostoDa
SistemaInformativo
FunzioneEssenziale
dipendeDa
compostoDa
dipendeDa
compone
BeneICT
compostoDa
ServizioInformatico
dipendeDa
ServizioEssenziale
dipendeDa
dipendeDa
tratta
ServizioEsterno
DatiDigitali

ELENCO DELLE CATEGORIE

Categoria	Bene, sistema, servizio

Componenti hardware e software che svolgono funzionalità e servizi di rete di telecomunicazione (accesso, trasporto, commutazione)	• Router
	• Switch
	• Repeater
	• Bilanciatori di carico
	• Traffic shaper
	• Proxy
	• Ponte radio
	• Access Network per reti radiomobili 2G, 3G, 4G, 5G
	• Gateway Wifi
	• Network Function Virtualization (NFV):
	  ○ vSwitch
	  ○ vRouter
	  ○ Application Function (5G)
	• Optical transmission board
	• Multiservice Provisioning Platform (MSPP)
	• Automotive ECU switch (Ethernet, CAN, LIN)
	• IoT Edge Gateway

Componenti hardware e software che svolgono funzionalità per la sicurezza di reti di telecomunicazione e dei dati da esse trattati	• Firewall
	• Security Gateway
	• Hardware Security Module (HSM)
	• Intrusion Detection System (IDS)
	• Intrusion Prevention System (IPS)
	• Network Function Virtualization (NFV)
	  ○ Authentication Server Function (5G)
	  ○ Whitelisting dei processi
	• Virtual Private Network (VPN)

Domanda preliminare

- Che c’azzecca un legale in temi così tecnici?

Nuovo reato presupposto – 24 bic c. 3 231/2001

- fornire informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti
  - per la predisposizione o l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici impiegati
  - o ai fini delle comunicazioni preventive al CVCN
  - o per lo svolgimento di specifiche attività ispettive e di vigilanza
- omettere di comunicare entro i termini prescritti tali dati, informazioni o elementi di fatto

… e pesanti sanzioni amministrative

- Afflittive
- E ripristinatorie

Condotta sanzionata	Sanzione
mancato adempimento degli obblighi di predisposizione, di aggiornamento e trasmissione dell'elenco delle reti, dei sistemi informativi e dei servizi informatici	sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000
mancata o tardiva notifica degli incidenti	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000
inosservanza delle misure di sicurezza delle reti, dei sistemi informativi e dei servizi informatici	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000
mancata o tardiva comunicazione dell'intenzione di procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici	sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000
impiego di prodotti e servizi sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici, in violazione delle condizioni o in assenza del superamento dei test imposti dal CVCN o dai Centri di valutazione	sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000
mancata collaborazione per l'effettuazione delle attività di test da parte del CVCN e dei Centri accreditati	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000
mancato adempimento delle prescrizioni indicate dal Ministero dello sviluppo economico o dalla Presidenza del Consiglio dei ministri in esito alle attività di ispezione e verifica	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000
mancato rispetto delle prescrizioni di utilizzo dettate al committente da parte del CVCN	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000

Primo francobollo

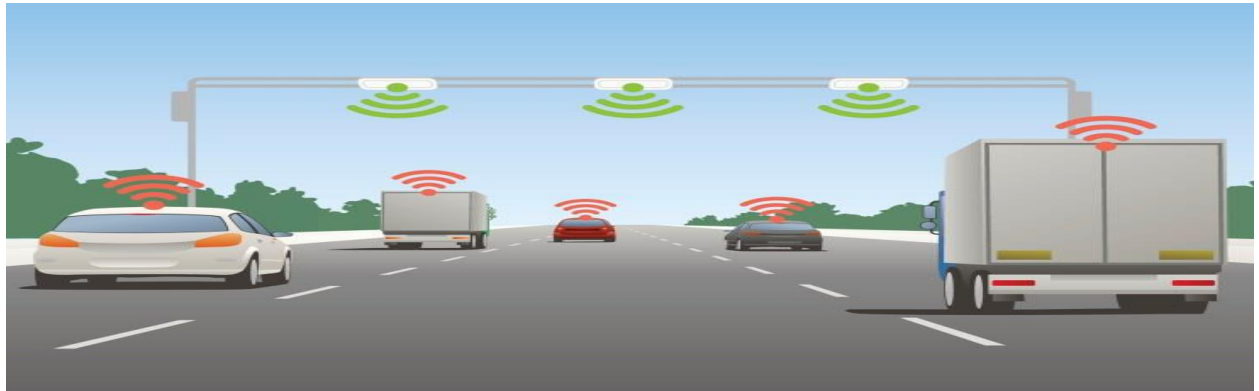
Aumenta il dominio cibernetico

Digitalizzazione sistemi

- Remotizzazione
- Robotizzazione

C - ITS

- progetto lanciato dalla Commissione Europea che prevede la 'comunicazione' tra le autovetture e con le infrastrutture (segnaletica stradale, stazioni di trasmissione/ricezione), scambiandosi informazioni utili alla circolazione
- La piattaforma C-ITS: migliorare la sicurezza stradale, l'efficienza del traffico, il comfort di guida e di ridurre le emissioni inquinanti, aiutando l'automobilista a prendere le decisioni più opportune al verificarsi di determinati eventi esterni (ingorghi, incidenti stradali, condizioni metereologiche, lavori in corso).

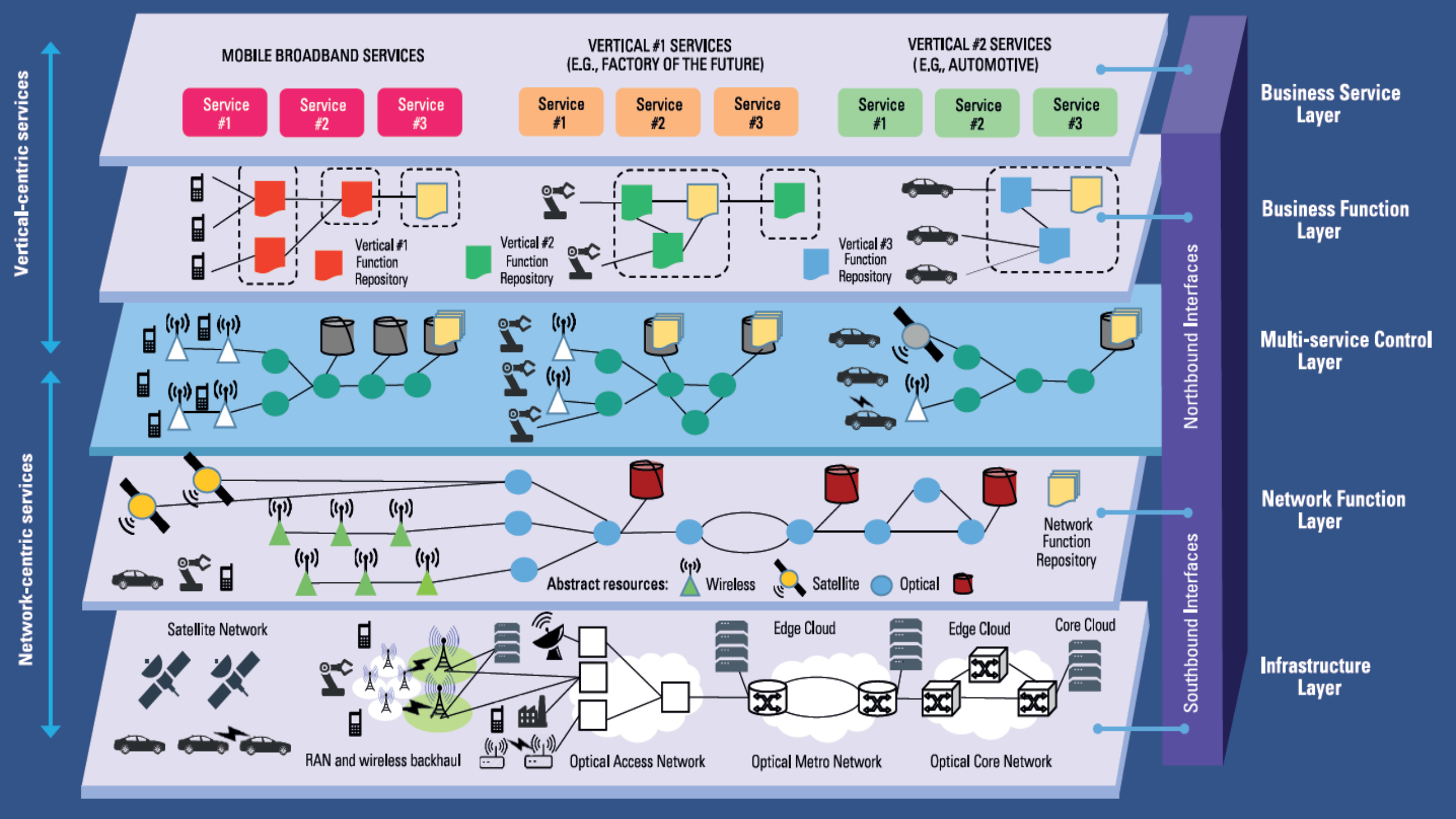


VerificaC19

- Ogni Certificazione viene prodotta digitalmente con una chiave privata dall'ente che rilascia la Certificazione (in Italia il Ministero della Salute).
- Le chiavi private assicurano l'autenticità
- Le corrispondenti chiavi pubbliche vengono poi utilizzate per verificare le Certificazioni attraverso le app di verifica (in Italia VerificaC19).
- sistema di crittografia a doppia chiave assicura che non sia possibile risalire dalla chiave pubblica alla chiave privata e quindi rende impossibile produrre certificazioni non autentiche.

Caso Green Pass

Sottrazione chiavi


Vertical-centric services
Network-centric services
MOBILE BROADBAND SERVICES
Service #1
Service #2
Service #3
VERTICAL #1 SERVICES (E.G., FACTORY OF THE FUTURE)
Service #1
Service #2
Service #3
VERTICAL #2 SERVICES (E.G., AUTOMOTIVE)
Service #1
Service #2
Service #3
Vertical #1 Function Repository
Vertical #2 Function Repository
Vertical #3 Function Repository
Network Function Repository
Abstract resources:
Wireless
Satellite
Optical
Satellite Network
RAN and wireless backhaul
Optical Access Network
Edge Cloud
Edge Cloud
Core Cloud
Optical Metro Network
Optical Core Network
Northbound Interfaces
Southbound Interfaces
Business Service Layer
Business Function Layer
Multi-service Control Layer
Network Function Layer
Infrastructure Layer

	• Trusted Platform Module
Componenti hardware e software per acquisizione dati, monitoraggio, supervisione controllo, attuazione e automazione di reti di telecomunicazione e sistemi industriali e infrastrutturali	• Sistemi SCADA (Supervisory Control And Data Acquisition) • Manufacturing Execution Systems (MES) • Software Defined Network (SDN) Controller • Sistemi Artificial Intelligence (AI) e Machine Learning (ML) per gestione reti/sistemi • 5G Mobile Edge Computing (MEC) • NFV: o Network Slice Selection Function (5G) o Application Function (5G) o Policy Control Function (5G) o Unified Data Management (5G) o Session Management Function (5G) • Management and Orchestration (MANO) • IoT orchestrator
Applicativi software per l'implementazione di meccanismi di sicurezza	• Applicazioni informatiche per la sicurezza o Public Key Infrastructure (PKI) o Single Sign-On (SSO) o Controllo Accessi • Moduli software che implementano Web Service mediante API, per protocolli di comunicazione

ne consegue che …

Secondo francobollo

… aumenta la superficie di attacco

Prima

Attacchi cyber infrastrutture, aerei, centrali nucleari, treni, acquedotti

OGGI!

Attacco ai PLC

- Stuxnet colpiva i PLC: **controllore logico programmabile** specializzato nella gestione o controllo dei processi industriali
- Esegue un programma ed elabora i segnali digitali ed analogici proventianti dai sensori e diretti agli attuatori presenti in un impianto industriale,
- è entrato anche nell'uso domestico

Emerge il concetto di criticità DPCM 179/2020

- «infrastrutture critiche»: essenziali per il mantenimento delle funzioni vitali della societa', della salute, della sicurezza e del benessere economico e sociale della popolazione;
- «tecnologie critiche»: … nonche' per il progresso tecnologico;
- «fattori produttivi critici»: beni e i rapporti essenziali… ;
- «informazioni critiche»: informazioni essenziali …
- «attivita' economiche di rilevanza strategica»: essenziali per il mantenimento delle funzioni vitali della societa', della salute, della sicurezza, del benessere economico e sociale della popolazione, nonche' per il progresso tecnologico.

Tecnologie critiche salute DPCM 179/2020

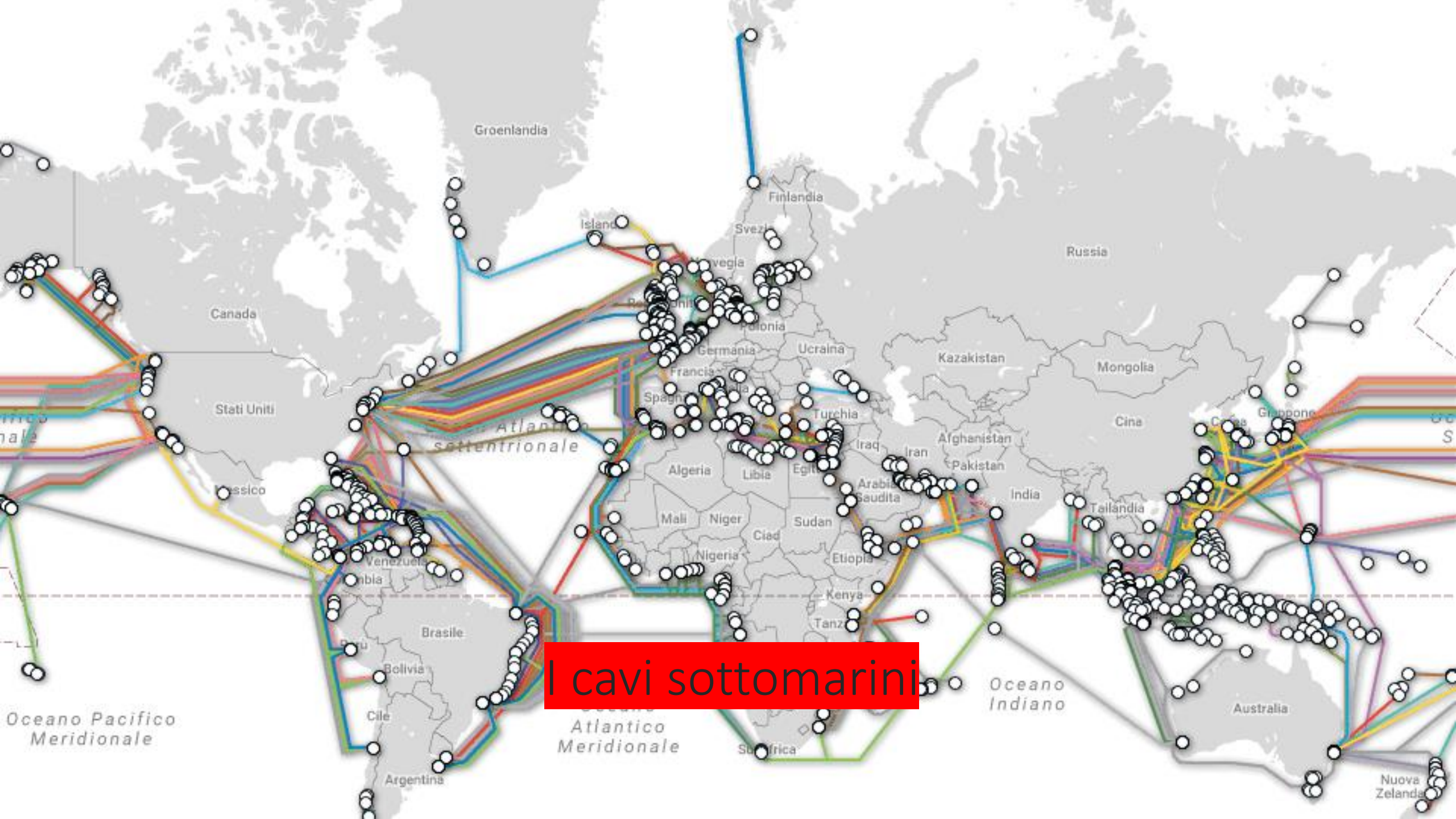
- digitali funzionali all'erogazione, anche da remoto, di servizi in sanita’;
- Finalizzate all'analisi dei dati e l'utilizzo delle conoscenze biologiche per la salute e la diagnostica, la prognostica, la terapia e il relativo follow-up;
- bioingegneristiche e le nanotecnologie critiche utilizzate nel settore farmaceutico e dei dispositivi medici, diagnostica, prognostica e terapia, nei settori chimico e agro-alimentare;

Informazioni critiche trattamento e archiviazione

- censimento e monitoraggio della sicurezza delle opere pubbliche
- dati raccolti tramite sistemi di navigazione satellitare per la tracciatura di campi, di mari e di bacini idrici e per la realizzazione di mappe di produzione e di prescrizione;
- dati raccolti tramite sensori per la rilevazione dello stato del suolo e delle acque o composizione biochimica del suolo agricolo;
- dati raccolti tramite sistemi di auto-guida per una lavorazione precisa, con l'utilizzo di tecniche e strumentazioni tecnologiche e informatiche per la gestione delle variabili spaziali e temporali delle colture, dell'allevamento, della pesca e dell'acquacoltura;
- dati raccolti tramite i sistemi relativi alla gestione e al controllo del trasporto aereo, marittimo, ferroviario, rapido di massa e stradale, che garantiscono i profili di security e safety,
- dati riguardanti la gestione e il monitoraggio dei flussi dei passeggeri e delle merci, che attengono al controllo e all'assistenza delle movimentazioni dei mezzi di trasporto, anche di tipo intelligente, per i sistemi di logistica integrata ed intermodale;
- dati relativi alle attivita' di gestione dei mercati all'ingrosso e del mercato finale del gas naturale dell'energia elettrica e degli idrocarburi;
- dati raccolti e gestiti tramite i sistemi informativi degli uffici giudiziari.

Tecnologie critiche DPCM 179/2020

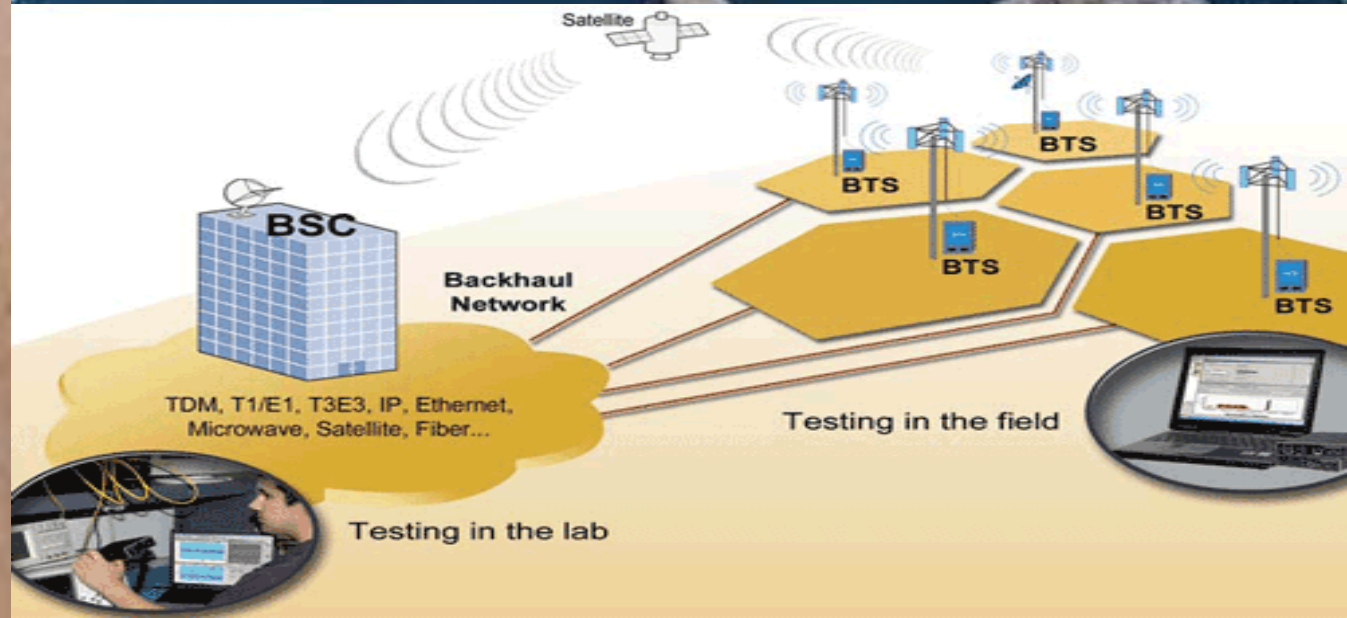
- tecnologie che consentono la geolocalizzazione e la ricostruzione degli spostamenti;
- tecnologie relative a sistemi che consentono la misurazione e trascrizione di informazioni a distanza (telemetria);
- tecnologie nel campo della distribuzione di servizi su richiesta di calcolo (server), archiviazione (database) e analisi (software), configurabili e disponibili da remoto (Cloud Computing);
- tecnologie digitali relative all'erogazione di servizi di assistenza sanitaria, prevenzione delle malattie e promozione della salute, anche da remoto, capaci di acquisire, elaborare, registrare, trasmettere e decodificare le informazioni e i dati clinici;
- tecnologie atte a garantire profili di safety e di security dei sistemi, anche di tipo intelligente, deputati al controllo, alla gestione e all'assistenza alla movimentazione di persone e merci su terra, aria e vie d'acqua, nonche' sistemi di logistica integrata e intermodale.
- Rilevanza strategica per l'interesse nazionale: se trattamento, archiviazione, accesso o controllo abbiano dimensione quantitativa essenziale per il mantenimento delle funzioni vitali della societa', della salute, della sicurezza e del benessere economico e sociale della popolazione, nonche' della liberta' e del pluralismo dei media.
- Ex lege: se riferibili a almeno 300.000 persine o enti

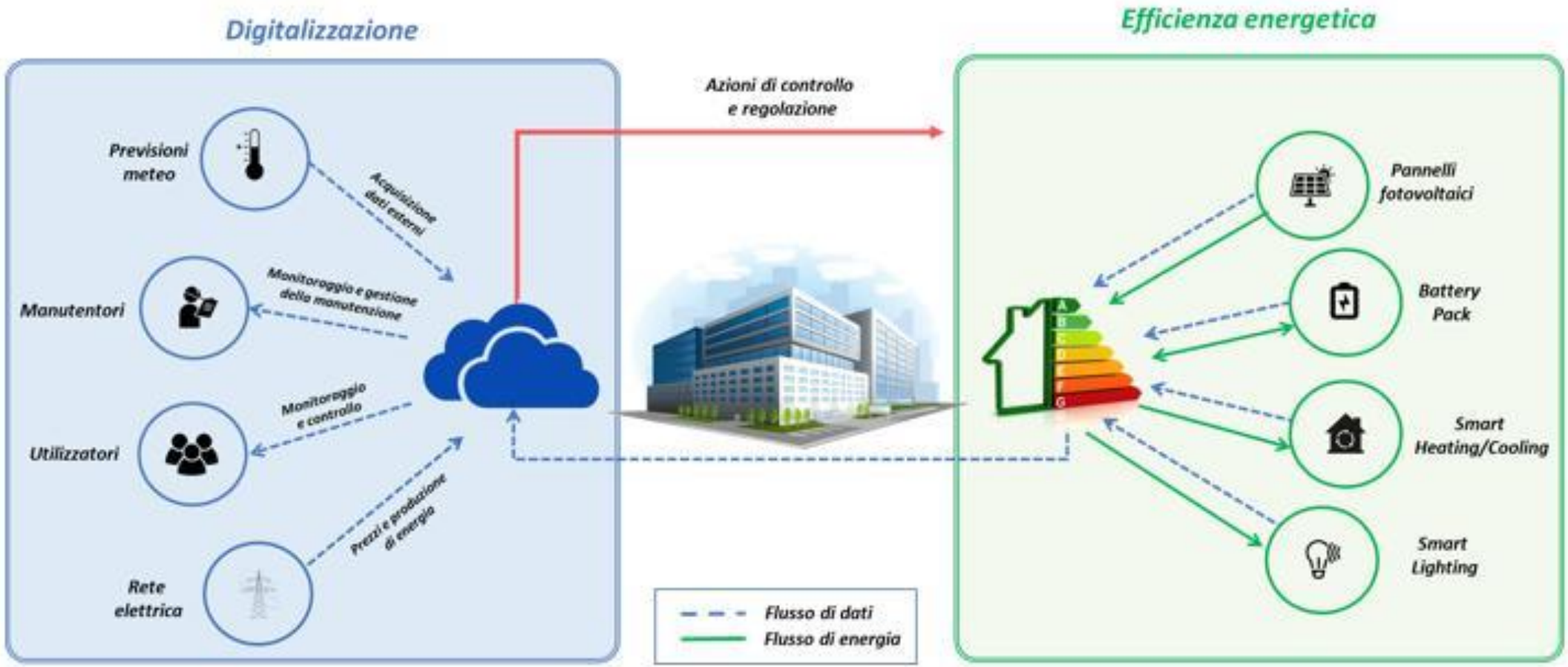


I cavi sottomarini

fronthaul


To metro duct network and alternative data centers
PFE Shelter (Optional)
Landing Man Holes (x6)
6 x Bore Exit Points
Google Earth


Satellite
BSC
Backhaul Network
BTS
BTS
BTS
BTS
BTS
TDM, T1/E1, T3E3, IP, Ethernet, Microwave, Satellite, Fiber...
Testing in the field
Testing in the lab


Digitalizzazione
Efficienza energetica
Azioni di controllo
e regolazione
Previsioni
meteo
Acquisizione
dati esterni
Manutentori
Monitoraggio e gestione
della manutenzione
Utilizzatori
Monitoraggio
e controllo
Rete
elettrica
Prezzi e produzione
di energia
Pannelli
fotovoltaici
Battery
Pack
Smart
Heating/Cooling
Smart
Lighting
Flusso di dati
Flusso di energia

Tecnologie critiche

- tecnologie relative a sistemi digitali che consentono telelettura e telegestione dei contatori di energia elettrica, gas e acqua (Smart Metering);
- tecnologie relative a costruzioni ed edifici dotati di funzionalita' avanzate e sistemi interconnessi per il monitoraggio e la gestione degli impianti e consumi (Smart Building);
- tecnologie digitali per l'ottimizzazione della qualita' delle infrastrutture e dei servizi pubblici (Smart City);

Terzo francobollo

Inevitabili le strategie di difesa

Sugli oggetti - infrastrutture critiche

- D.Lgs n. 61 dell'11 aprile 2011: individuazione e designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione

Settore I. *ENERGIA*[

1. Elettricità - Infrastrutture e impianti per la produzione e la trasmissione di energia elettrica per la fornitura di elettricità

2. Petrolio - Produzione, raffinazione, trattamento, stoccaggio e trasporto di petrolio attraverso oleodotti

3. Gas - Produzione, raffinazione, trattamento, stoccaggio e trasporto di gas attraverso oleodotti - Terminali GNL

Settore II. *TRASPORTI*[

- 4. Trasporto stradale
- 5. Trasporto ferroviario
- 6. Trasporto aereo
- 7. Vie di navigazione interna
- 8. Trasporto oceanico, trasporto marittimo a corto ragg

Sui soggetti: Golden power d.l. 21/2012

NIS- dir. 2016/1148 d.lgs 65/2018

- Ridurre rischio conseguente ad incidenti dei servizi essenziali, dovuto a interoperabilità dei servizi e connessione dispositivi
- **obiettivi** : gestione dei rischi di sicurezza; protezione contro i cyber attacchi; individuazione di incidenti di cyber sicurezza; riduzione dell'impatto degli incidenti di cyber sicurezza.
- Impone: misure di sicurezza comuni ed adeguate; notifica incidenti; istituzione CSIRT (Computer Security Incident Response Team) nazionali, sulla base del CERT-UE, per realizzare un network europeo che si occupi della sicurezza delle reti critiche.
- **Destinatari:**
  - **Operatori di servizi essenziali** (OES) stabiliti nell'Unione europea, i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali;
  - **Digital Service Provide**r (DSP), le persone giuridiche che forniscono servizi della società dell'informazione (e-commerce, social network, cloud computing, motori di ricerca, financial provider, ecc...); le persone giuridiche che forniscono servizi di e-commerce, cloud computing o motori di ricerca, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale.
  Non sono soggetti alla normativa i DSP con meno di 50 dipendenti o con fatturato inferiore ai 10 milioni l'anno (piccole e micro imprese).

obblighi

- - **adozione di misure tecniche e organizzative** adeguate alle gestione dei rischi e a prevenire e minimizzare l'impatto degli incidenti di sicurezza delle reti e dei sistemi informativi, al fine di assicurare la continuità del servizio;
  - **notifica**, senza ingiustificato ritardo, degli incidenti di sicurezza con impatto rilevante, rispettivamante sulla continuità e la fornitura del servizio, al **Computer Security Incident Response Team** (CSIRT) italiano, informandone anche l'Autorità competente NIS di riferimento
- Un incidente è rilevante se si verifica almeno una condizione:
  - indisponibilità del servizio fornito per oltre 5.000.000 di ore utente;
  - perdita di integrità, autenticità o riservatezza dei dati per oltre 100.000 utenti dell'UE;
  - rischio per la sicurezza e/o l'incolumità pubblica, o in termini di perdite di vite umane;
  - danni materiali superiori a 1.000.000 di EUR per almeno un utente nell'UE.

TLC: d.m. 12 dicembre 2018

individuare adeguate misure di natura tecnico - organizzativa per la sicurezza e l'integrita' delle reti e dei servizi di comunicazione elettronica, al fine di conseguire un livello di sicurezza delle reti adeguato al rischio esistente

garantire la disponibilita' e continuita' dei servizi su tali reti, prevenendo e limitando gli impatti di incidenti che possono pregiudicare la sicurezza per gli utenti e per le reti interconnesse;

definire i casi in cui le violazioni della rete o la perdita dell'integrita' sono da considerarsi significative, ai fini della notifica da parte dei fornitori di reti e servizi di comunicazione alle competenti Autorita', nonche' le relative modalita' di tale notifica.

quanto francobollo

Il perimetro

Perimetrati

- Un soggetto, pubblico o privato presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, laddove
  - attività strumentali all'esercizio di funzioni essenziali dello Stato;
  - attività necessarie per l'esercizio e il godimento dei diritti fondamentali;
  - attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica;
  - attività di ricerca;
  - attività relative alle realtà produttive nel campo dell'alta tecnologia e
  - attività in ogni altro settore, (con rilievo economico e sociale), per l'autonomia strategica nazionale, la competitività e lo sviluppo del sistema economico nazionale.

Obblighi

1. Inventario asset
2. Analisi del rischio
3. affidamento beni, sistemi (ICT) con procedura CVCN, anche mediante definizione di caratteristiche e requisiti di carattere generale, di standard e di eventuali limiti
4. Procedura incidenti
5. struttura organizzativa preposta alla gestione della sicurezza;
6. politiche di sicurezza e gestione del rischio;
    1. mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso interventi su apparati o prodotti inadeguati sul piano della sicurezza;
    2. protezione fisica e logica e dei dati;
    3. integrita' delle reti e dei sistemi informativi;
    4. Garanzia gestione operativa, ivi compresa la continuita' del servizio;
    5. monitoraggio, test e controllo;
    6. formazione e consapevolezza;

Elenco asset

predispongono e aggiornano con cadenza almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici inerenti alle reti perimetarte, di rispettiva pertinenza, comprensivo della relativa architettura e componentistica

Aggiornamento con cadenza almeno annuale elenco reti, sistemi informativi e servizi informatici

L’elenco deve comprendere architettura e componentistica

trasmettono tali elenchi all'Agenzia per la cybersicurezza nazionale

Analisi del rischio

- individuare i principali rischi per la sicurezza tenendo conto delle minacce che insistono sugli asset critici;
- definire una metodologia di gestione dei rischi e utilizzare strumenti basati sugli standard di settore;
- verificare l'effettivo utilizzo di tali metodologie e strumenti di gestione del rischio da parte del personale;
- assicurarsi che i rischi residui, anche derivanti da vincoli realizzativi, siano minimizzati rispetto alla probabilita' del verificarsi di incidenti significativi e che siano accettati dalla Direzione;

Appalti – DPR n. 54/2021

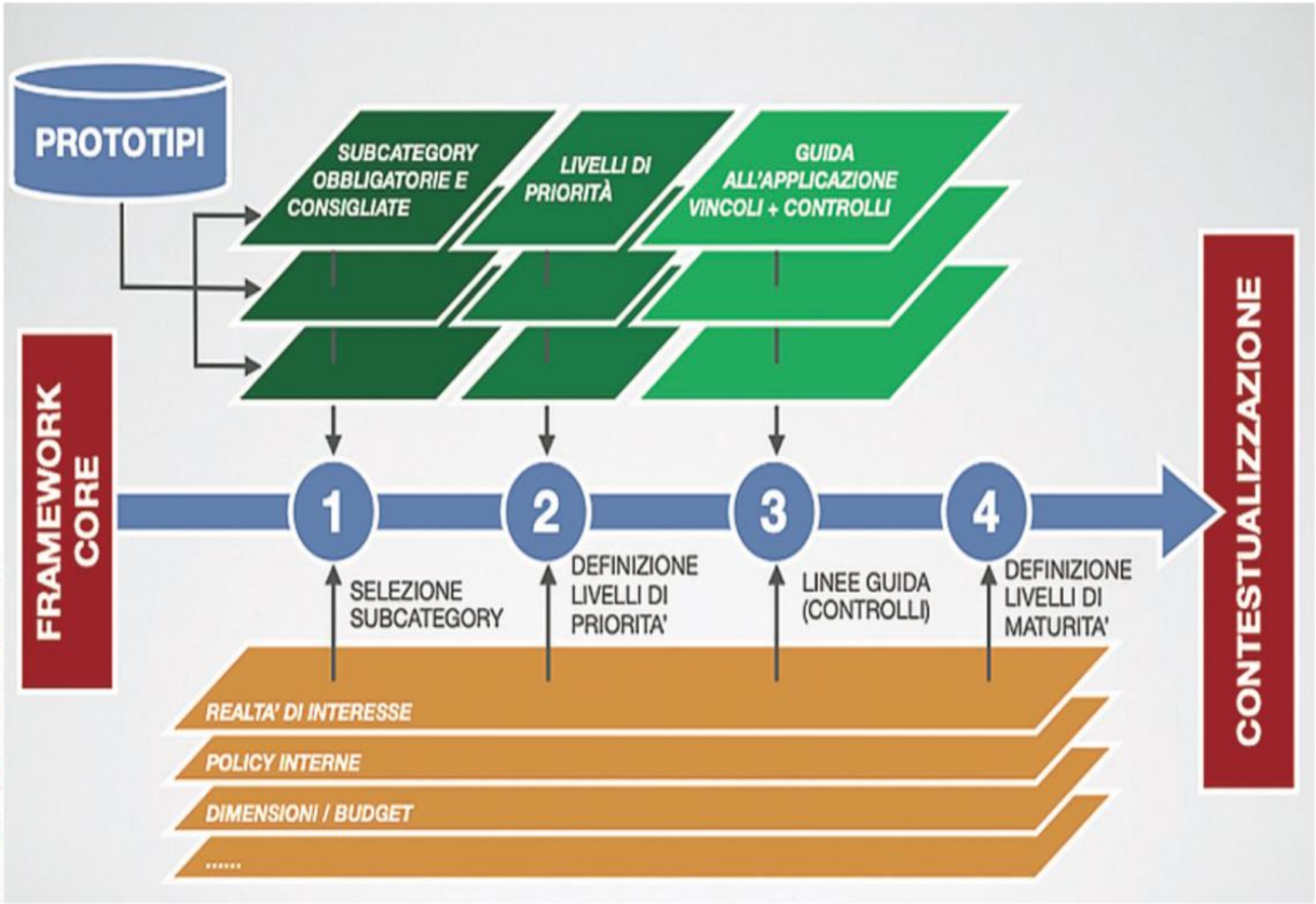
- affidamento sulla base di criteri di natura tecnica,
- preventiva comunicazione CVCN con silenzio assenso
- CVCN: puo' effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da compiere secondo un approccio gradualmente crescente nelle verifiche di sicurezza.
- caso imposizione di condizioni e test di hardware e software:
  - i bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente o risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN.
  - I test devono essere conclusi nel termine di 60 gg, decorsi i quali i oerimetrati possono proseguire nella procedura di affidamento.

Incidenti – DPCM n. 81/2021

- incidenti aventi impatto su reti, sistemi informativi e servizi informatici
- Notifica al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano, che inoltra tali notificheal Dipartimento delle informazioni per la sicurezza anche per le attivita' demandate al Nucleo per la sicurezza cibernetica;
- Piani di rispristino

Misure di sicurezza

- Identificazione
- Protezione
- Rilevamento
- Risposta
- Recupero
- Segretezza



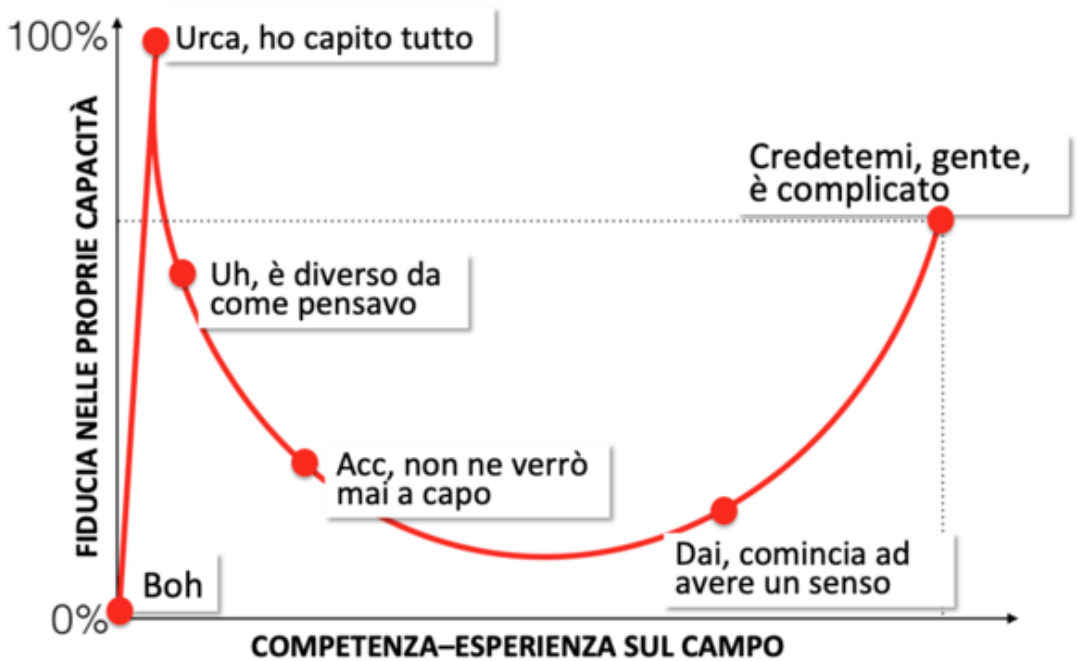
quinto francobollo

Il «foglio del come»

Come iniziare?

- Con una bella terapia d’urto
- Caso:
  - «non abbiamo la policy, ma le cose le facciamo in concreto»
  - «Non scomodiamo il CDA che in questo momento deve fare il budget e non ha tempo; ce ne occupiamo noi»
  - «siamo i migliori del mondo perché abbiamo la 27001»
  - «questa normativa è sostanzialmente la stessa cosa della protezione dati»
  - «… è una questione di competenza del reparto IT»

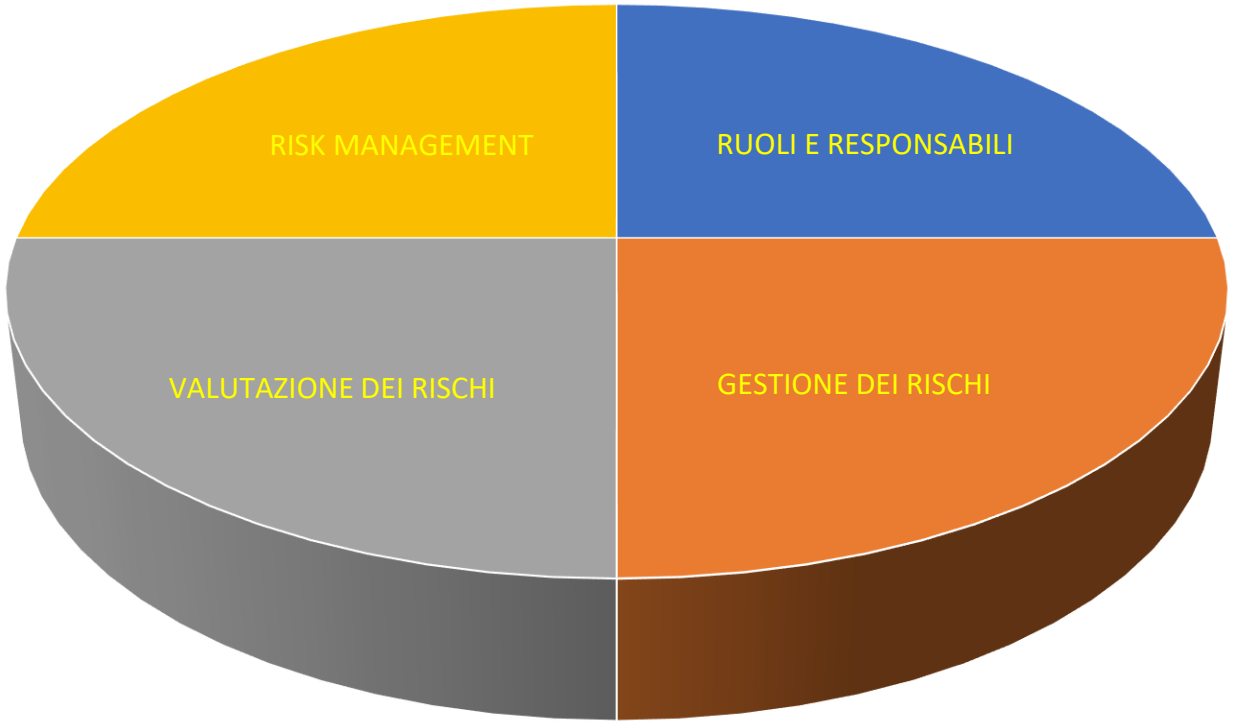
EFFETTO DUNNING-KRUGER



Incontri one to one e questionari

- 1. Le è mai accaduto di riscontrare situazioni di rischi per la sicurezza fisica o cibernetica per l'azienda? Se si, le risulta che tale situazione abbia avuto conseguenze sull'integrità o funzionalità degli apparati informatici?
- 2. Ha mai avuto evidenza di casi di esecuzione non autorizzata di codici o malware veicolati attraverso vettori di infezione o sfruttando le vulnerabiltà di risorse esposte in rete?
- 3. Ha avuto evidenza di casi di malfunzionamenti del sistema cibernetico aziendale?
- 4. È mai accaduto che si verificassero danni quale conseguenza indiretta della mancata o inadeguata predisposizione di presidi di sicurezza fisica o cibernetica?
- 5. Esistono procedure e norme operative rivolte ad assicurare la corretta sicurezza fisica o cibernetica e il pronto intervento in caso di incidenti? Se si, quali misure e quali presidi
- aziendali assicurano la corretta attuazione di tali procedure?
- 6. Ha mai avuto evidenza di casi di perdita o di corruzione irreversibile di dati aziendali?
- 7. Esistono norme operative, procedure o altri strumenti finalizzati a garantire il rispetto e la completa attuazione della sicurezza fisica o cibernetica?
- 8.

Le quattro componenti del sistema di gestione



Oggetto

Modalità di effettuazione

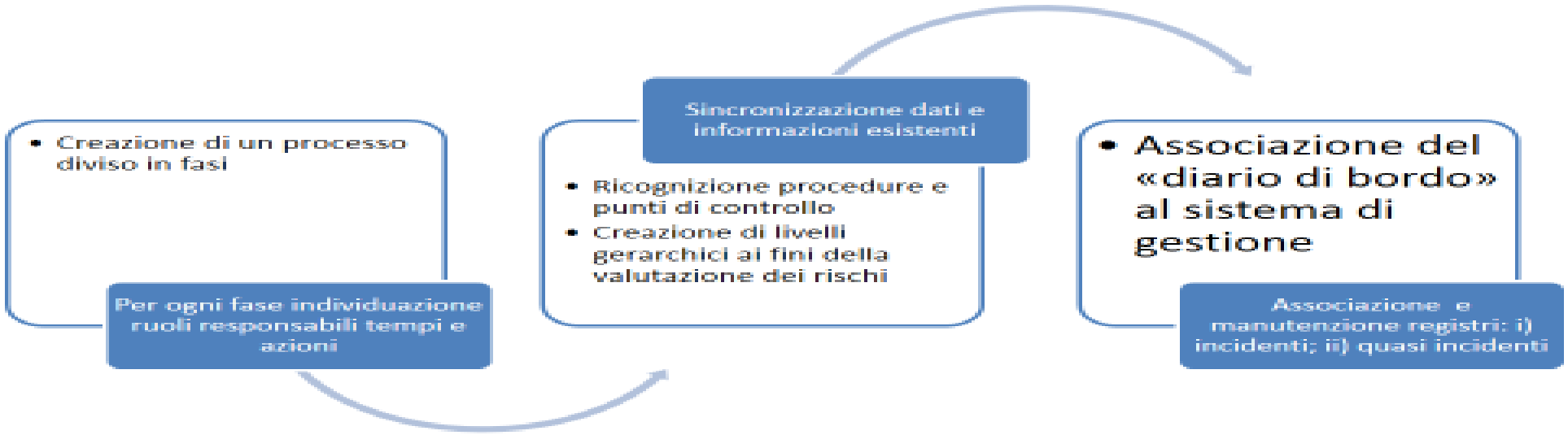
Modelli di organizzazione e gestione

Sistema di gestione: politica di sicurezza approvata dalla Direzione aziendale:

predisporre una documentata politica relativamente alla sicurezza e alla integrita' delle reti e componenti ICT dei servizi forniti;

definire una dettagliata politica di sicurezza per gli asset critici e i processi aziendali;

Creiamo un sistema di gestione



IL PROGRAMMA

Ruoli e reponsabili

La delega

- **Oggetto: proposta di nomina a Referente di Area piattaforme tecnologiche e beni IT rilevanti in materia di sicurezza cibernetica e fisica, e conseguente delega di funzioni in materia di sicurezza fisica e cibernetica**
- in seguito all'inserimento della Società all'interno del perimetro di sicurezza cibernetica, alla luce delle Sue competenze ed esperienze, nonché in ragione del suo ruolo in azienda, dopo un'attenta e approfondita valutazione, è stato identificato come persona più adatta a rivestire il ruolo di "Referente di Area".
- L'Area di cui si propone la nomina a referente riguarda le piattaforme tecnologiche e beni IT rilevanti in materia di sicurezza cibernetica e fisica degli stessi afferenti i sistemi e le infrastrutture Corporate IT.
- Le proponiamo il presente incarico, il cui contenuto è perimetrato dalla delega di funzioni che segue.
- Anche considerata la delicatezza dell'incarico e delle relative responsabilità, non vi è alcun obbligo di accettazione e potrà declinare tale offerta senza che vi sia conseguenza alcuna.
- Laddove dovesse accettare, nella veste di "Referente di Area" per la parte piattaforme tecnologiche e beni IT rilevanti in materia di sicurezza cibernetica e fisica: i) sarà chiamato a svolgere le attività in tale ambito; ii) opererà in stretto contatto e alla luce delle direttive del *compliance officer*; iii) riferirà al *compliance officer*; iv) si adeguerà alle priorità di azione identificate dal *compliance officer.*

Compiti precisi

- **Compiti**
- Per la parte relativa a piattaforme tecnologiche e beni IT rilevanti in materia di sicurezza cibernetica e fisica., sarà responsabile dell'attuazione del Programma di sicurezza fisica e cibernetica allegato per l'area di Sua competenza.
- Il complito principale riguarderà la costituzione di un'organizzazione interna preposta a gestire il rischio, tramite individuazione di personale preposto e incaricato, consolidamento delle capacità tecniche di valutazione e audit della sicurezza dell'hardware e del software e implementazione degli *asset* e delle unità aziendali incaricate della protezione della sicurezza cibernetica
- Rinviando al programma allegato, i compiti e le funzioni che – nel caso di accettazione - sarà chiamato a svolgere saranno i seguenti:
- a) curare la corretta predisposizione del censimento dei beni e rapporti rilevanti inerenti alla Area piattaforme tecnologiche e beni Corporate IT rilevanti in materia di sicurezza cibernetica e fisica, con conseguente redazione di un elenco in cui andranno inseriti i relativi beni;
- b) redigere un un elenco di reti e sistemi sensibili – relativi all'Area piattaforme tecnologiche e beni IT rilevanti in materia di sicurezza cibernetica e fisica – da trasmettere alle Autorità preposte;
- c) svolgere l'analisi – relativa all'Area piattaforme tecnologiche e beni Corporate IT rilevanti in materia di sicurezza cibernetica e fisica. – del rischio *cibersecurity* relativamente a componenti ICT e dei rischi inerenti alla loro sicurezza fisica, secondo una serie di parametri, identificando punti di vulnerabilità, analizzando le potenzialità di attacco e creando sistemi di difesa;
- d) implementare una procedura sugli incidenti (con obblighi di notifica tempestiva e rafforzamento dei presidi di front-line per la gestione degli alert e degli eventi), relativamente all'Area piattaforme tecnologiche e beni Corporate IT rilevanti in materia di sicurezza cibernetica e fisica.;
- e) implementare la parte tecnologica tramite misure quali la creazione di un sistema di automatizzazione delle risposte agli attacchi utilizzando matrici documentate degli attacchi e, se del caso, ricorrendo a soluzioni di tipo Siem (*Security Information and Event Management*, soluzioni di gestione eventi e informazioni di sicurezza) o Soar **(***Security Orchestration Automation and Response*) ecc.
-

Poteri

Relativamente all'Area Risorse umane impiegate e attività connesse e correlate, contribuire:

- alla predisposizione di una documentata e tracciabile politica relativamente alla sicurezza e alla integrità delle reti inserite in perimetro;
- alla individuazione dei principali rischi per la sicurezza e l'integrità delle reti e dei servizi di comunicazione elettronica forniti, tenendo conto delle minacce che insistono sugli *asset* critici desunte da una specifica e mirata analisi del rischio che presupponga l'identificazione del fattori di rischio e dei profili di vulnerabilità, la ricognizione dei presidi esistenti, l'identificazione del rischio lordo, l'identificazione del rischio netto, la previsione di presidi ulteriori e la fissazione di un rischio tollerabile, nel rispetto del principio della riduzione dei rischi alla fonte e della sostituzione di ciò che è pericoloso con ciò che non lo è;
- alla adozione di misure di tracciamento e di eventuale gestione degli incidenti di sicurezza fisica e cibernetica, anche relativi a terze parti, con misurazione e potenziamento della capacità di intervento;
- alla implementazione e attuazione di mirati *stress test* in materia di sicurezza cibernetica;
- alla implementazione di un playbook che predisponga adeguate strategie di risposta contro diverse tipologie di minacce **(**phishing**,** intrusione**,** ransomware, preelaborazione della posta elettronica per estrarre indizi rivelatori, individuazione degli obiettivi coinvolti, azioni di mitigazione e/o prevenzione, ecc.);

Coordinamento 231

- **Poteri**
- Quale delegato avrà i poteri finalizzati e strumentali a:
- a) attuare le prescrizioni contenute nella Guida agli adempimenti e nel Manuale operativo;
- b) attuare le prescrizioni contenute nella policy di sicurezza cibernetica.
- Potrà subdelegare, sotto la propria responsabilità, specifiche attività a soggetti dotati delle competenze per potervi adempiere.
- La presente delega di funzioni sarà incardinata anche nel sistema delle deleghe proprie del *compliance program* adottato ai sensi del d. lgs. n. 231 del 2001.
- Premesso che i reati in materia di sicurezza cibernetica sono reati presupposto ai sensi del d. lgs. n. 231 del 2001, al fine di richiamare l'attenzione sull'importanza e sulla delicatezza delle funzioni delegate, si trasmette uno specchietto riassuntivo delle sanzioni amministrative afflittive previste in materia di sicurezza cibernetica, potenzialmente applicabili alla società, nel caso di inottemperanza dei relativi obblighi di legge

TOP-LEVEL COMMITMENT

- Linee guida
- Obiettivi strategici
- Obiettivi operativi