La protezione delle infrastrutture critiche

Luigi Ballarano
Responsabile Cybersecurity & Data Protection di Terna

MILANO, 23 Gennaio 2020

Agenda

- Introduzione Terna
- Lo scenario di rischio Cyber e Terna
- L’organizzazione di Cybersecurity di Terna
- Il TERNA-CERT
- Wrap-up

Chi sono

Luigi Ballarano

Attualmente ricopre il ruolo di **Responsabile Cybersecurity & Data Protection del Gruppo Terna** e coordina le attività di Information Security, Computer Emergency Readiness Team (CERT), Cybersecurity Engineering, Cybersecurity Assessment e Data Protection & Privacy.

Ha maturato una consolidata esperienza nelle aree di Information Risk Management, Information Security Governance, Information Security Program Development & Management, Information Security Incident Management, Physical Intrusion Surveillance, Crisis Management & Situational Awareness nell'ambito delle Infrastrutture Critiche.

Ha iniziato la sua carriera professionale partecipando a progetti tecnologici complessi in ambito Aerospazio e Difesa in società del Gruppo Finmeccanica. Dal 2004 ha fatto parte dello Staff della Direzione Sistemi e Tecnologie del Gestore Rete Trasmissione Nazionale (GRTN). Dal 2011 è stato responsabile in Terna dell'Information Security Competence Center, definendo le strategie del Gruppo Terna in ambito Information Risk Management, Compliance e Cybersecurity nei contesti IT e OT. Dal 2015 al 2017 è stato responsabile del Security Operations Center di Terna, centro nevralgico operativo della sicurezza integrata della Direzione Tutela Aziendale con coordinamento delle sale di Monitoring & Respond Physical e Cyber (h24 – 7/7).

Pubblicazioni:

- L. Ballarano & M. Macina (2019). **Evolving from SOC to CERT** in A. Armando, M. Henauer & A. Rigoni Next Generation CERTs (pp 82 - 87). NATO Science for Peace and Security Series - D: Information and Communication Security

Chi siamo

- Il Gruppo Terna è **Gestore Unico e proprietario della Rete di Trasmissione Nazionale in Alta Tensione (RTN) italiana**. È titolare di una concessione governativa in regime di monopolio regolato

- Tra i **principali gestori di rete in Europa e al mondo** con oltre 74.000 km di linee gestite

- Gestisce la **trasmissione** dell'energia elettrica sul territorio italiano e **i flussi elettrici** 365 giorni l'anno, 24 ore su 24

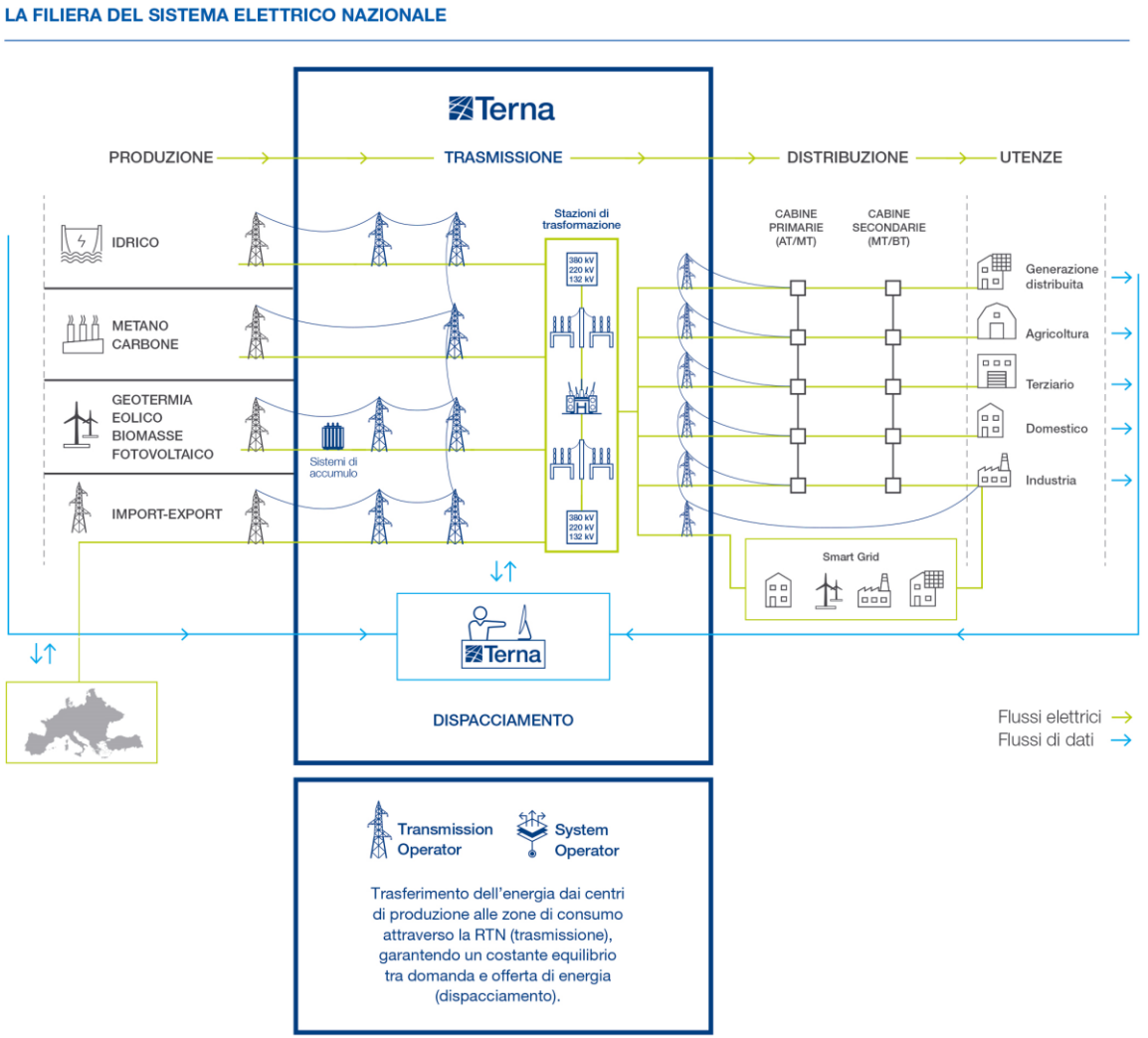
- Quotato in Borsa dal 2004, è **tra le prime società industriali** del FTSE-MIB

- È una realtà d'eccellenza formata da 4.252 **professionisti**

- Ruolo guida per una **transizione energetica sostenibile**

- **Innovazione, Qualità del servizio e minimizzazione dell'impatto ambientale** sono i driver fondamentali che guidano le attività nella generazione dei risultati del Gruppo Terna

Overview

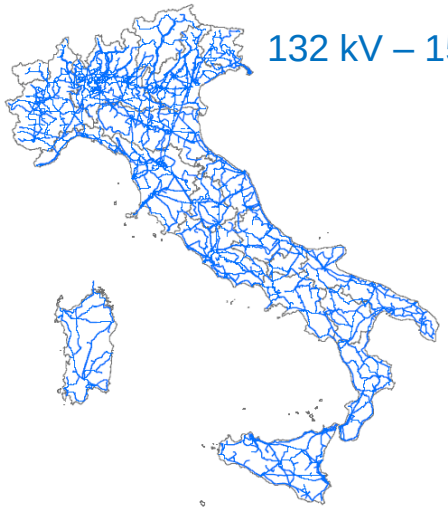


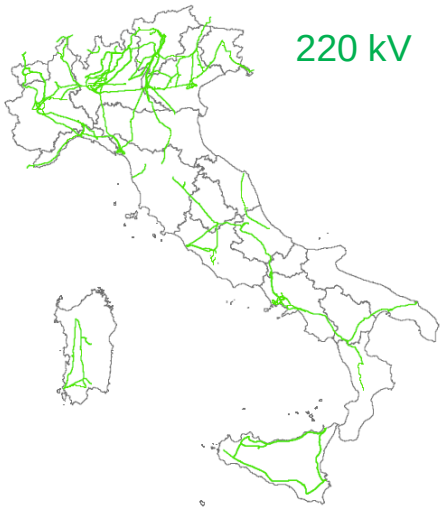
Terna trasmette Energia

La filiera del sistema elettrico nazionale si compone di quattro segmenti:

- Produzione
- Trasmissione
- Distribuzione/vendita di energia elettrica.

Chi siamo – I nostri asset

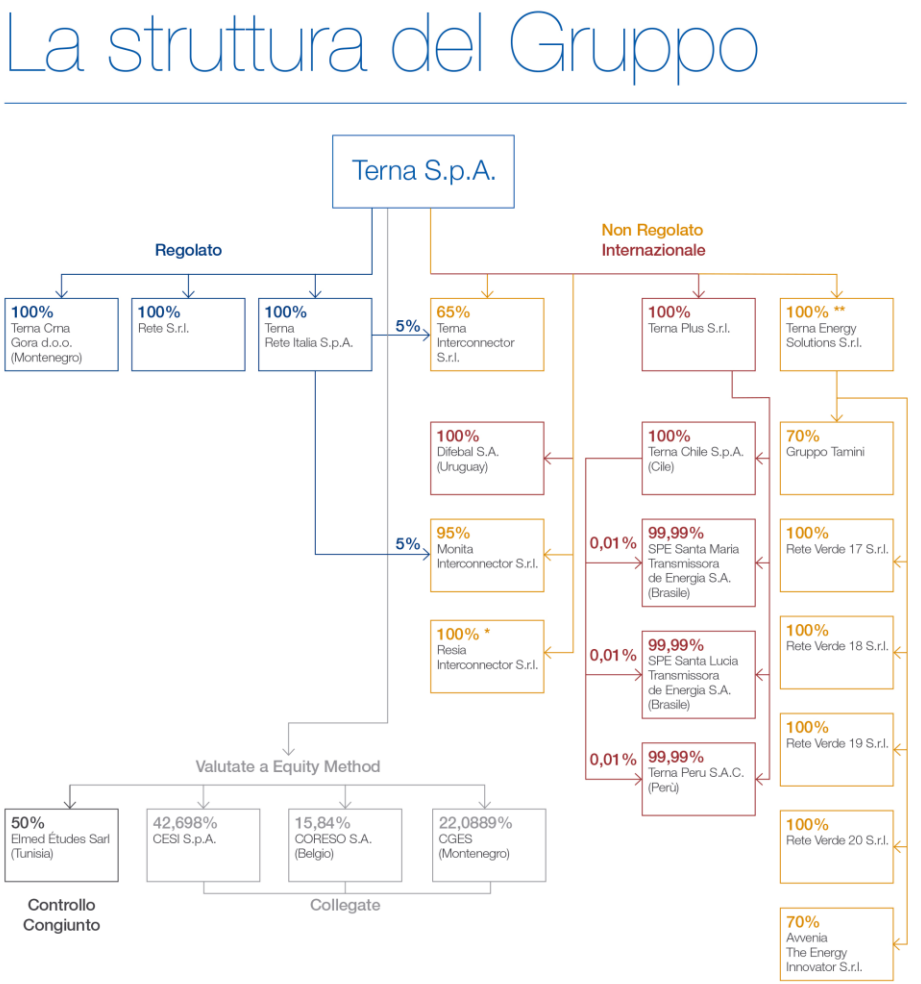




- **oltre 74.000 km di linee elettriche** in Alta e Altissima Tensione (123/150 kV, 220 kV, 380 kV)
- **881 stazioni** di trasformazione e smistamento
- **723 trasformatori**
- **25 linee di interconnessione** con l'estero
- **1 Centro Nazionale di Controllo**
- **5 siti di accumulo**

Chi siamo – La struttura del Gruppo Terna

- **Terna S.p.A., la Capogruppo**, elabora gli orientamenti strategici per lo sviluppo della Rete e per i nuovi business.
- **Terna Rete Italia** è la Società operativa che gestisce la Rete elettrica italiana: esercizio, manutenzione e sviluppo.
- **Terna Plus** è la società del Gruppo responsabile dello sviluppo di nuovi business nel mondo.
- **Tamini Trasformatori S.r.l.** eccellenza italiana riconosciuta nel mondo, produce e commercializza trasformatori elettrici industriali di potenza.
- **Avvenia The Energy Innovator S.r.l.** società di consulenza strategica leader nel settore dell'efficienza energetica.



Cosa facciamo – Gestione e sviluppo della RTN

- Nel rispetto del territorio e delle comunità, Terna **sviluppa e potenzia la RTN** adeguandola costantemente ai più avanzati standard tecnologici.

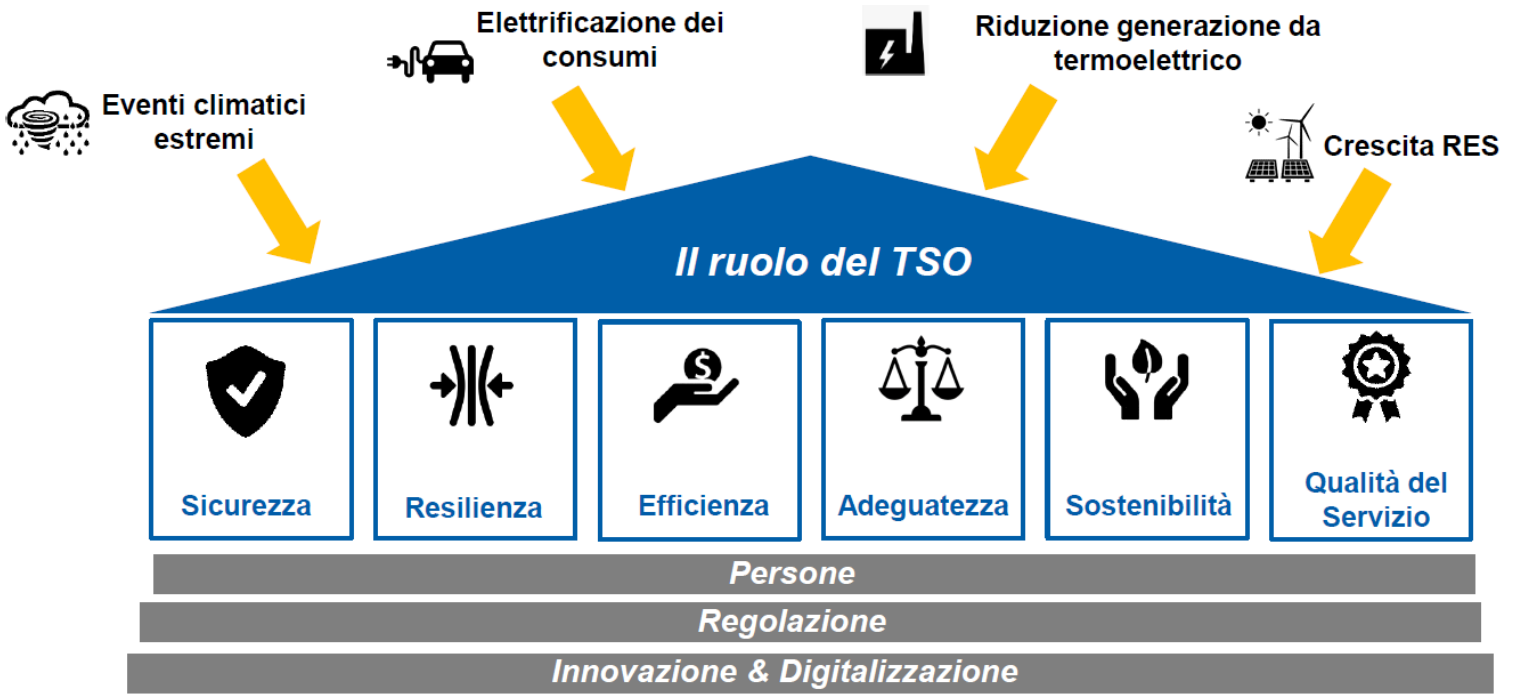
- Istante per istante, 24 ore al giorno, 365 giorni l'anno, Terna assicura **l'equilibrio dei flussi elettrici** all'interno della RTN.

- Terna garantisce la **sicurezza della RTN** attraverso standard operativi d'eccellenza e modelli innovativi nella gestione integrata dei rischi.

- A ulteriore protezione della Rete, Terna ha stipulato **protocolli istituzionali** con Ministero dell'Interno (sicurezza fisica e informatica), Guardia di Finanza (trasparenza nella gestione degli appalti) e Vigili del fuoco (pronto intervento in casi di criticità).

- Il business è gestito con un **approccio sostenibile** che riguarda tutte le attività aziendali. Lo sviluppo della rete comporta, in particolare, un'intensa attività di **concertazione** con gli Enti locali per individuare soluzioni che riducano gli impatti visivi e ambientali di linee e stazioni.

Terna e la transizione energetica



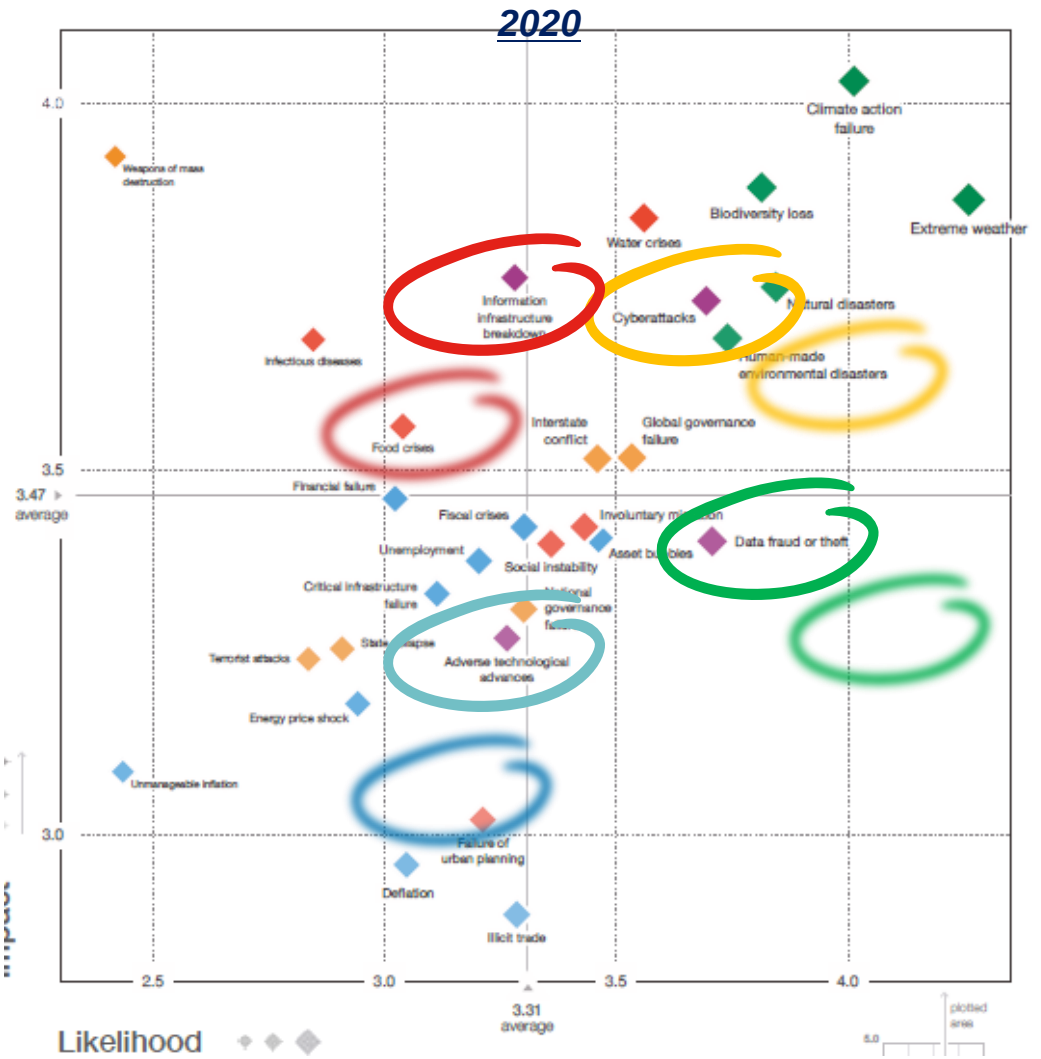
Esercitare un ruolo guida nella transizione energetica

Rif. Terna - 2019-2023 Strategic Plan

I nuovi scenari di rischio

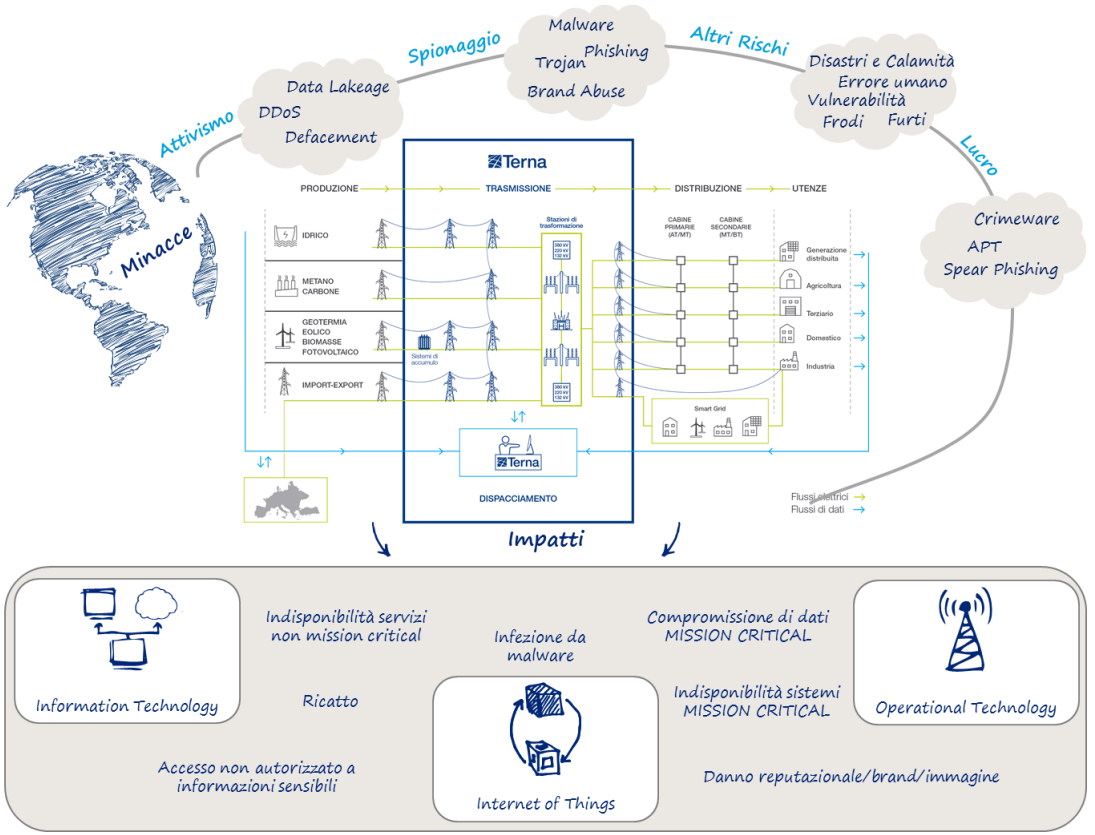
WEF – The Global Risk Report
Variazione Probabilità (P)-Impatto (I) tra 2019 e 2020

	P	I
Cyberattacks	↓	↓
Information information breakdown	↓	→
Data fraud or theft	↓	↓
Adverse technological advances	↑	↑



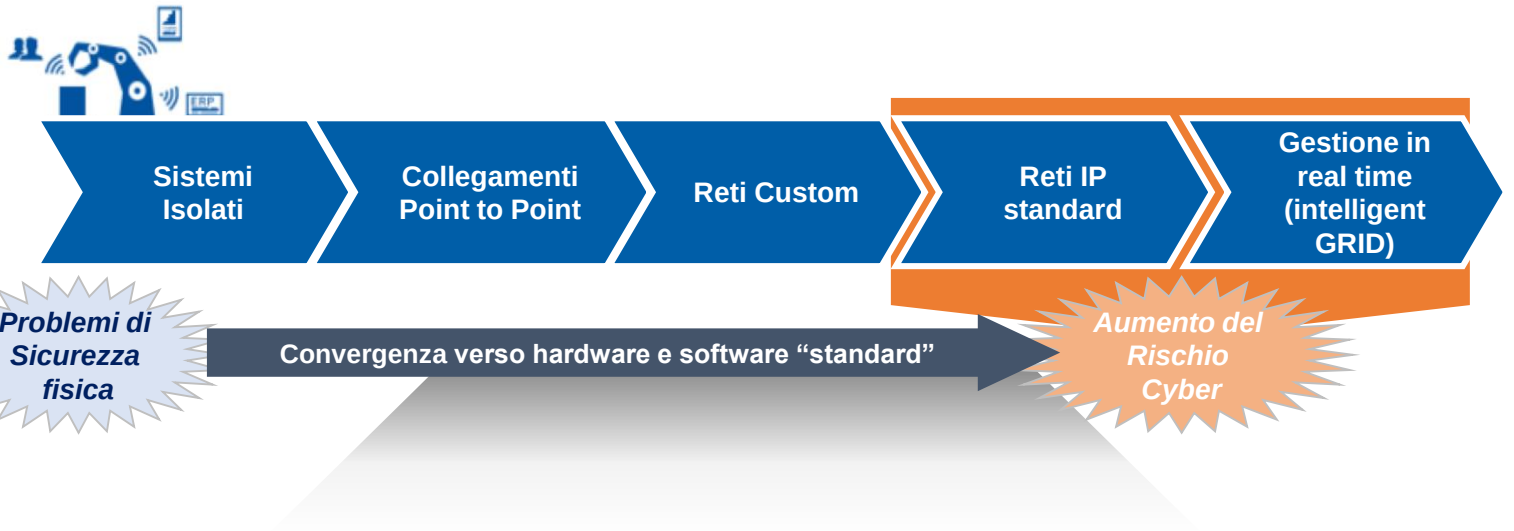
Terna e il contesto di minaccia Cyber

Per effetto di uno scenario di crescente pericolosità delle minacce di origine Cyber che interessano il parco delle tecnologie IT&OT, si impone l'attuazione di meccanismi di difesa avanzati, con misure di contenimento del rischio sempre più sofisticate con ambiti di applicazione su vari livelli.



Evoluzione dei Sistemi di Controllo Industriale e Rischi

L'evoluzione dei sistemi nel settore elettrico, implicando una maggiore integrazione fra sistemi IT e OT, introduce un nuovo livello di rischio Cyber



Conseguenze dei rischi cyber per le Infrastrutture Critiche

Business

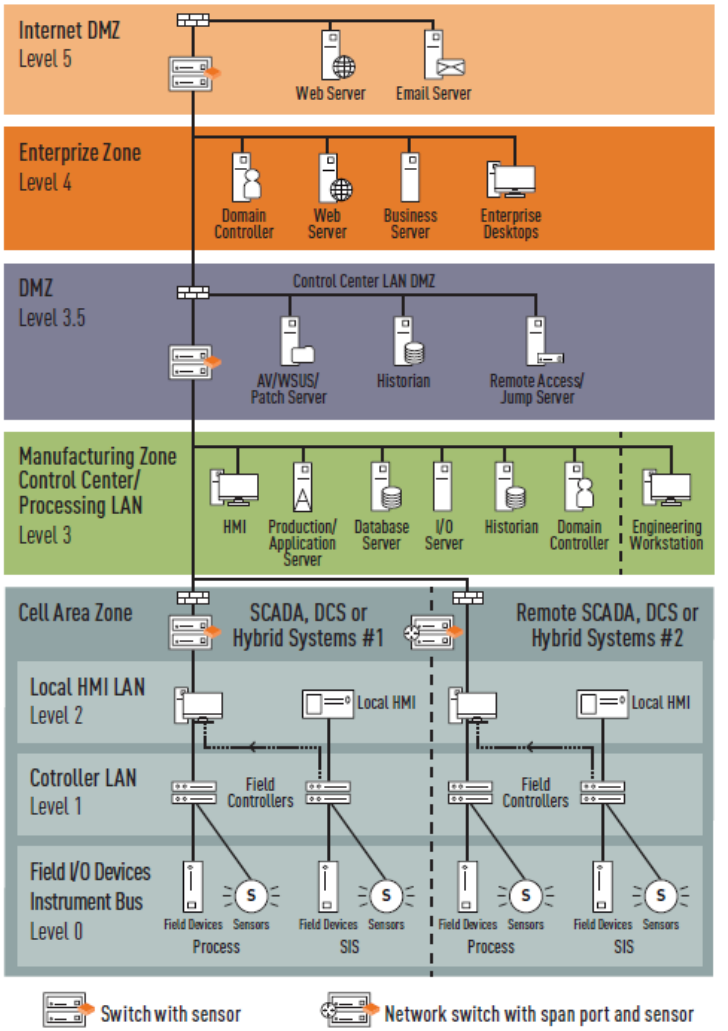
- Blackout, infortuni, fermo macchina, danni di reputazione, violazione normative, perdita proprietà intellettuale

Sicurezza nazionale

- Interruzione servizi critici, perdita vite umane, danni ambientali, perdita informazioni confidenziali

Modello di riferimento di architettura di rete industriale

La rappresentazione a lato presenta una architettura di alto livello di rete industriale, dalle componenti di campo nelle stazioni alle componenti gestionali della organizzazione e di connettività esterna verso Internet.



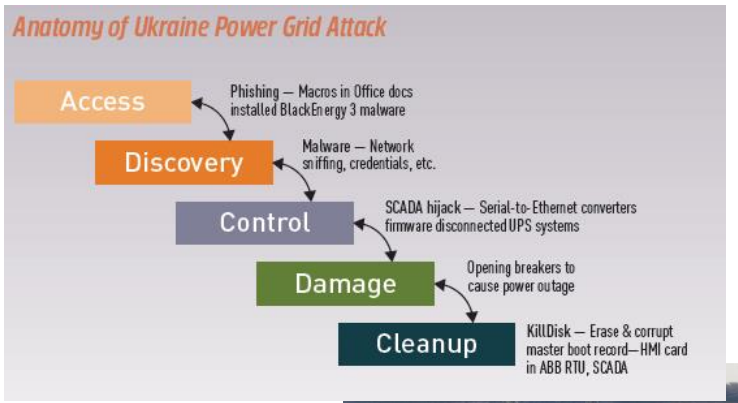
Il caso ucraino

Il 23 dicembre 2015 il sistema elettrico ucraino subisce un cyber attack.

L'attacco al gestore della rete di distribuzione Ukrenergo ha causato la disconnessione di una sottostazione di trasmissione provocando **un blackout di circa 6 ore per circa 230.000 di utenti a Kiev con circa 73MWh di energia non distribuita**.

L'attacco è stato complesso, l'infezione della rete è stata avviata tramite file malevolo con **macro Office** e accesso ai componenti SCADA e ha preso di mira diversi target come riassunto nella figura.

Sono state evidenziate **azioni manuali** che hanno sfruttato le componenti vulnerabili della rete ICS e tali da necessitare di **specifiche competenze** per un attacco completo



Principali differenze fra sistemi IT e OT

Differenze importanti in termini di obiettivi, contesto e gestione del Rischio

Operational Technology	differenze	Information Technology
Bassa tolleranza ai ritardi	**Prestazioni**	Richiede rendimento elevato
Alta affidabilità, sistemi ridondanti	**Disponibilità**	Reeboot e affidabilità variabile sono tollerati
Focus su sicurezza delle persone e tolleranza agli errori per prevenire perdita di vite o rischi per sicurezza pubblica	**Risk Management**	Focus su confidenzialità e integrità dei dati
Sistemi Operativi differenti con misure di sicurezza spesso non adeguate e minacce difficili da prevedere	**Operatività**	Sistemi progettati per essere utilizzati con sistemi operativi tipici con funzioni di sicurezza integrate
Durata compresa fra 10 e 15 anni	**Ciclo di Vita**	Durata compresa fra 3 e 5 anni
Diversi protocolli standard e proprietari obsoleti, diversi tipi di dispositivi e reti complesse	**Comunicazione**	Protocolli standard, reti cablate e configurazioni standard
Cambiamenti software testati e implementati in modo incrementale per garantire l'integrità dei sistemi	**Aggiornamento**	Le modifiche apportate rapidamente se presenti valide procedure di sicurezza. Spesso sono automatizzate

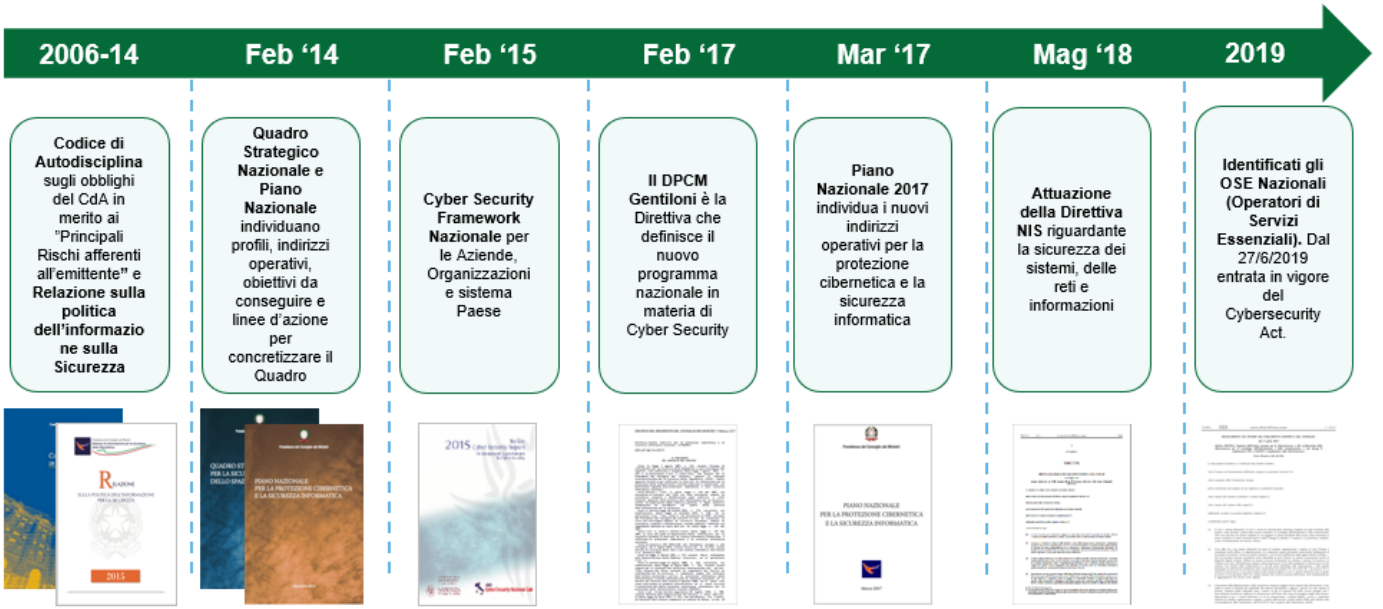
L’integrazione IT-OT: differenti priorità

Nel mondo IT l’obiettivo principale è garantire la confidenzialità del dato, ovvero l’impossibilità da parte di chi non ne possiede i privilegi di avere accesso ai dati

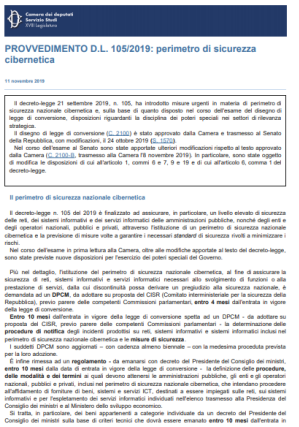
Nel mondo dell’Operation Tecnology risulta invece fondamentale garantire la disponibilità degli impianti, in quanto possibili indisponibilità degli impianti di regolazione e sicurezza potrebbe determinare disservizi importanti (ad es. all’interno delle cabine elettriche potrebbero creare dei blackout)

Le differenti priorità dei due mondi determinano l’impossibilità di applicare fedelmente le logiche di sicurezza del mondo IT (quali ad esempio l’aggiornamento/patching del software) all’interno del contesto OT

L'Evoluzione della Cyber Security in Italia



PROVVEDIMENTO D.L. 105/2019: perimetro di sicurezza cibernetica


PROVVEDIMENTO D.L. 105/2019: perimetro di sicurezza cibernetica

11 novembre 2019

Il decreto-legge 21 settembre 2019, n. 105, ha introdotto misure urgenti in materia di perimetro di sicurezza nazionale cibernetica e, sulla base di quanto disposto nel corso dell'esame del disegno di legge di conversione, disposizioni riguardanti la disciplina dei poteri speciali nei settori di rilevanza strategica.

Il disegno di legge di conversione (C. 2100) è stato approvato dalla Camera e trasmesso al Senato della Repubblica, con modificazioni, il 24 ottobre 2019 (S. 1629).

Nel corso dell'esame al Senato sono state apportate ulteriori modificazioni rispetto al testo approvato dalla Camera (C. 2100-B), trasmesso alla Camera (6 novembre 2019). In particolare, sono state oggetto di modifica le disposizioni di cui all'articolo 1, commi 6 e 7, 9 e 19 e di cui all'articolo 6, comma 1 del decreto-legge.

Il perimetro di sicurezza nazionale cibernetica

Il decreto-legge n. 105 del 2019 è finalizzato ad assicurare, in particolare, un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi.

Nel corso dell'esame in prima lettura alla Camera, oltre alle modifiche apportate al testo del decreto-legge, sono state previste nuove disposizioni per l'esercizio dei poteri speciali del Governo.

Più nel dettaglio, l'istituzione del perimetro di sicurezza nazionale cibernetica, al fine di assicurare la sicurezza di reti, sistemi informativi e servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi, dalla cui discontinuità possa derivare un pregiudizio alla sicurezza nazionale, è demandata ad un **DPCM**, da adottare su proposta del CISR (Comitato interministeriale per la sicurezza della Repubblica), previo parere delle competenti Commissioni parlamentari, **entro 4 mesi** dall'entrata in vigore della legge di conversione.

Entro 10 mesi dall'entrata in vigore della legge di conversione spetta ad un DPCM - da adottare su proposta del CISR, previo parere delle competenti Commissioni parlamentari - la determinazione delle **procedure di notifica** degli incidenti prodottisi su reti, sistemi informativi e sistemi informatici inclusi nel perimetro di sicurezza nazionale cibernetica e le **misure di sicurezza**.

I suddetti DPCM sono aggiornati – con cadenza almeno biennale – con la medesima procedura prevista per la loro adozione.

È infine rimessa ad un **regolamento** - da emanarsi con decreto del Presidente del Consiglio dei ministri, **entro 10 mesi** dalla data di entrata in vigore della legge di conversione - la definizione delle **procedure, delle modalità e dei termini** ai quali devono attenersi le amministrazioni pubbliche, gli enti e gli operatori nazionali, pubblici e privati, inclusi nel perimetro di sicurezza nazionale cibernetica, che intendano 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 individuati nell'elenco trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico.

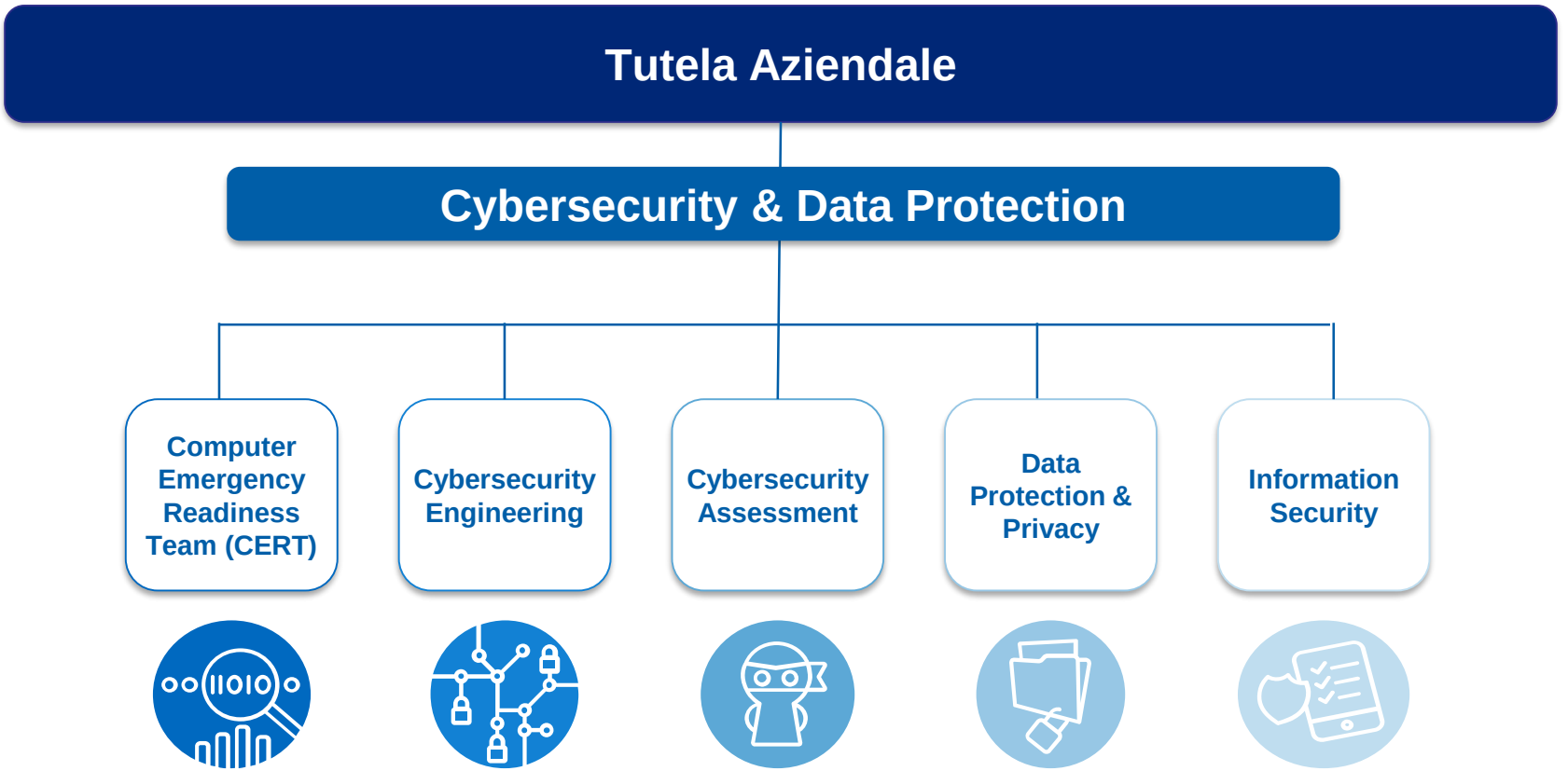
Si tratta, in particolare, dei beni appartenenti a categorie individuate da un decreto del Presidente del Consiglio dei ministri sulla base di criteri tecnici che dovrà essere emanato **entro 10 mesi** dall'entrata in

Focus

Ordinamenti Giuridici		Obblighi normativi
Europeo	**Direttiva NIS (Network and Information Security – EU 2016/1148)**	Implementazione di piani strutturali per impedire che reti e sistemi informativi possano diventare bersagli di azioni tese ad interrompere la loro operatività
Italiano	**Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico**	Potenziamento delle capacità di difesa delle infrastrutture critiche nazionali
	DPCM 17 febbraio 2017	Coinvolgimento degli operatori privati per garantire la diffusione delle best practice da adottare al fine di minimizzare gli impatti di eventuali crisi di natura cibernetica

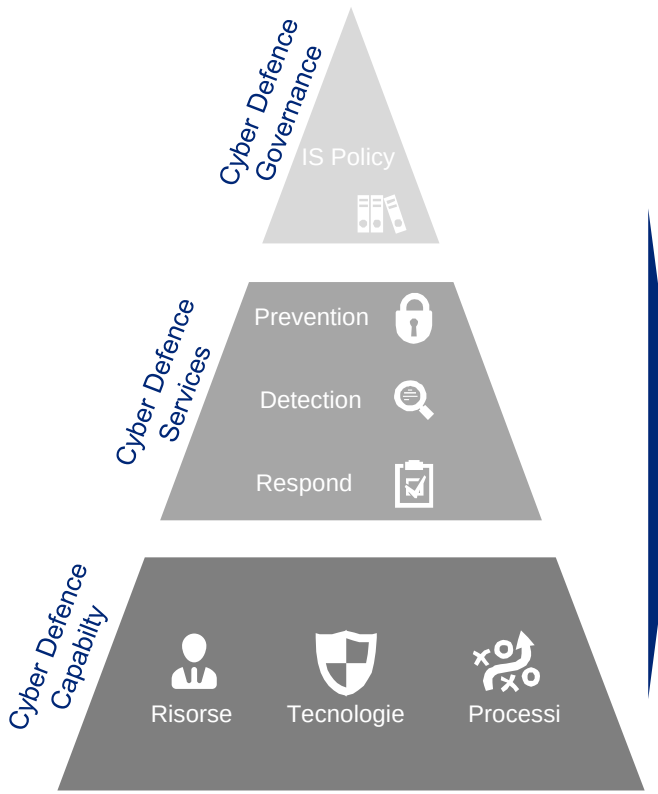
La nostra «organizzazione»

Dal punto di vista organizzativo, il TERNA-CERT fa parte della micro struttura **Cybersecurity & Data Protection**, all'interno della macro struttura **Tutela Aziendale**.



La Cyber Defence realizzata da Terna

Attraverso l'attuazione di Information Security Program Development & Management, Terna ha implementato una soluzione integrata a presidio dei principali Cyber Risk.

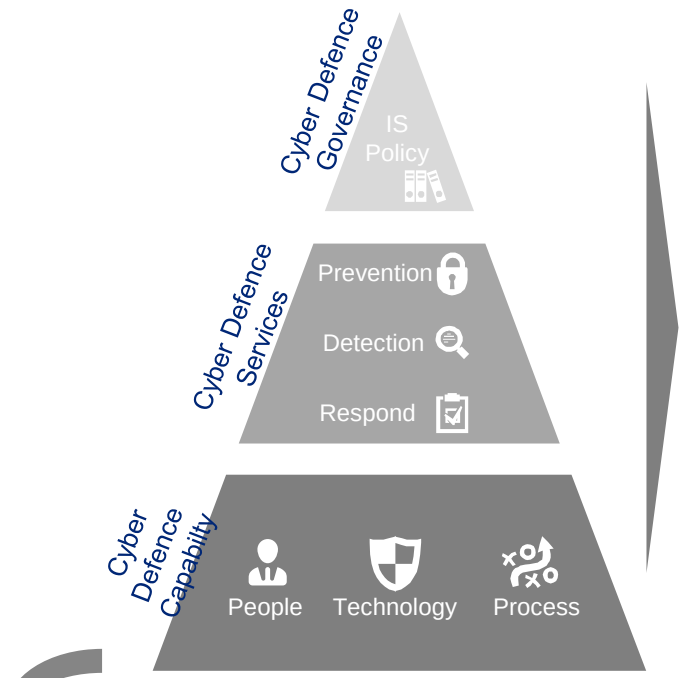


- Politiche e Information Security Framework
- Security by Design sistemi IT e OT
- Servizi digitali
- Sicurezza canale email
- Sicurezza navigazione
- Vuln. Assessment e Penetration Test
- Sicurezza end point
- Controllo Accessi logici
- Monitoraggio e Risposta Eventi Sicurezza Logica
- Sicurezza logica perimetrale

Information Technology	Operational Technology
Business Asset	Critical Business Asset

Le interazioni con il processo di Security Incident Management

Il processo di Security Incident Management è completamente integrato nel framework di Information Security Program Development & Management



- Comprensione del contesto
- Approccio Risk Based By Design
- Information Risk Framework (IRM)
- Classificazione dei sistemi
- Piano della Sicurezza
- Formazione (table top exercise for top management)
- Visibilità sul perimetro e sulle reti interne
- Evoluzione delle infrastrutture
- Clausole contrattuali specifiche
- Infosharing con soggetti trust
- Intelligence

Security Incident Management

Modello Operativo e Processi Cybersecurity

Il Modello Operativo di Cybersecurity & Data Protection supporta i principali processi in ambito ICT garantendo principi di separazione dei compiti e associando responsabilità di governance a responsabilità di indirizzo operativo e di gestione degli eventi di Cybersecurity.

PROGETTAZIONE → ***INGEGNERIZZAZIONE E DELIVERY*** → ***ESERCIZIO***

Cybersecurity Governance

- Definizione Strategie e Policy
- Supporto all'Information System Owner (ISO) attraverso indirizzi per la sicurezza dei progetti ICT

Security by Design

- Cybersecurity assurance
- Definizione Standard tecnici di Cybersecurity
- Progettazione e implementazione infrastrutture di Cybersecurity

Cybersecurity Operations

- Cybersecurity monitoring
- Incident Management
- Cybersecurity awareness
- Security Assessment (VA/PT)

Information Risk Management & Compliance

- Information Risk Analysis
- Supporto attuazione Framework IRM
- Compliance Information Security Framework
- Compliance Privacy (GDPR, etc.)
- Compliance IS (NIS, etc.)

Descrizione dei servizi offerti dal CERT

Il TERNA-CERT fornisce alla propria Constituency il **Services Portfolio** illustrato precedentemente, focalizzando l'attenzione su due servizi, **Incident Management** e **Threat Intelligence**, alla base dei quali vi è l'**Information Sharing** che permette di mantenere un adeguato livello di classificazione delle informazioni.

1 Incident Management

Questo servizio è fondamentale nella **prevenzione, rilevamento e risposta agli incidenti di sicurezza** che si verificano o che minacciano di verificarsi all'interno della Constituency del CERT.

Le **fasi** che governano questo servizio sono:

- **Identificazione** degli incidenti di sicurezza e il **rilevamento** di **attività sospette**;
- **Valutazione** e la **classificazione** degli incidenti di sicurezza **per rilevanza, urgenza e impatto**;
- Gestione delle **comunicazioni** relative all'identificazione di **eventi rilevati verso le Strutture Organizzative interessate**;
- **Identificazione** di appropriate **strategie di remediation** volte a ridurre gli impatti di un incidente di sicurezza;
- **Attuazione di azioni di Remediation** e rispettive verifiche finali atte a convalidare il corretto ripristino del servizio;

2 Threat Intelligence

È un servizio di **generazione**, **condivisione** e **raccolta** delle **informazioni da e verso l'esterno** atto a **prevenire e proteggere** l'infrastruttura e le informazioni, di proprietà della Constituency, dall'esposizione a minacce informatiche.

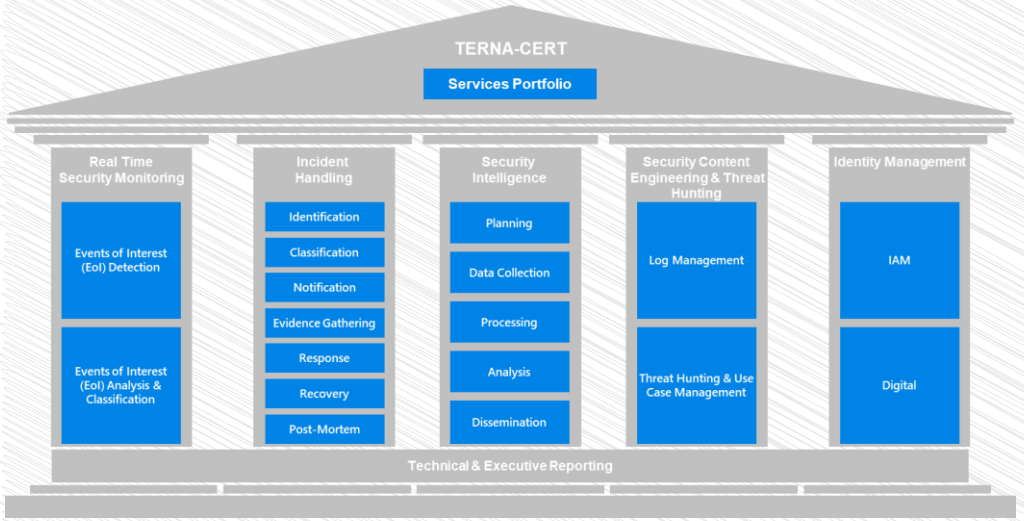
Le **principali attività** che governano questo servizio sono:

- **Monitoraggio in tempo reale dei feed** relativi ad eventi di sicurezza esterni;
- **Analisi** di eventuali dati aggregati o **alert provenienti dall'esterno dell'organizzazione**;
- **Arricchimento del dato** attraverso la raccolta delle informazioni rilevate sulla tipologia, sulla fonte, sulla mitigazione e sulla remediation della minaccia.
- **Comunicazioni verso la Constituency** sulle azioni da intraprendere nella prevenzione alla risposta di tali minacce;
- **Raccolta e analisi dei feedback** ricevuti dalla Constituency al fine di **evidenziare e definire attività di miglioramento** nell'ambito della security awareness e nella comunicazione delle segnalazioni.

Information Sharing

Modello Operativo

Il Gruppo Terna ha adottato un modello co-managed, prevedendo che il Computer Emergency Readiness Team (**CERT**) sia coadiuvato da un **SOC** esterno **H24**, al fine di garantire, attraverso il **Services Portfolio**, il **governo del processo di Cyber Security** grazie allo sviluppo di strumenti e standard, la verifica di vulnerabilità dei sistemi e un monitoraggio in tempo reale.



Il **TERNA-CERT** opera garantendo:

- il **monitoraggio** centralizzato in tempo reale **della postura di sicurezza** del Gruppo Terna;
- ➢ *il **monitoraggio preventivo e reattivo** delle potenziali minacce, attraverso lo sviluppo di **use case** e aggiornamento delle relative **regole di correlazione**;*
- lo sviluppo e la gestione di **strumenti di monitoraggio**, la **risposta** agli incidenti informatici e lo sviluppo di analisi predittive attraverso la "**Threat Intelligence**";
- ➢ ***l'ottimizzazione** continua dei criteri operativi per la **gestione degli incidenti**.*
- la **cooperazione e la condivisione delle informazioni** tra CERT/CSIRT, SOC e/o organismi simili al fine di assicurare una **prevention** delle minacce informatiche che possano minare la riservatezza delle informazioni e l'operatività della propria Constituency.

➢ *Il TERNA-CERT garantisce l'espletamento di tali servizi attraverso una collaborazione con un SOC esterno H24.*

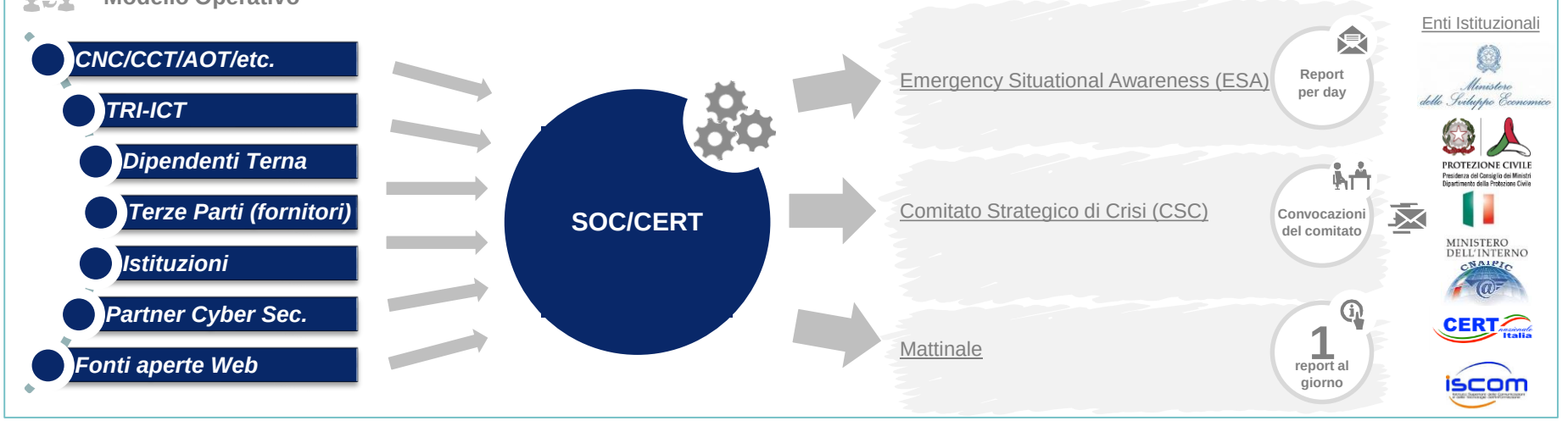
Emergency Situational Awareness

Il processo di gestione degli eventi di sicurezza in Terna vede come Security Contact Points il SOC e il CERT in funzione della tipologia di evento da gestire

Timeframe main events

- T_1: •Identificazione eventi di sicurezza •Identificazione impatti per Terna
- T_2: •Monitoraggio della situazione da parte delle strutture preposte
- T_3: •Impatti rilevanti per il business di Terna •**Attivazione** Comitato di Crisi evento critico C_x
- T_4: •Convocazione giornaliera Comitato Strategico di Crisi e reportistica periodica (max. 3 per day)
- T_5, T_6
- T_7: •**Chiusura Comitato di Crisi**

Modello Operativo



Tipico processo di comunicazione

- Scambio prime email vs. i vertici Terna
- Report CSC → Comunicazione Enti Istituzionali
- Report CSC → Comunicazione Enti Istituzionali
- Report CSC → Comunicazione Enti Istituzionali
- Report CSC → Comunicazione Enti Istituzionali
- Report CSC → Comunicazione Enti Istituzionali
- Invio mattinale di Tutela Aziendale con la comunicazione degli eventi rilevanti di sicurezza del Gruppo Terna riferiti alle ultime 24h

Wrap-up

- Da soli, questa “guerra” è impari…
- Fondamentale comprendere che cosa è un incidente (ad es. rilevante ai fini NIS, …)
- Gestione dei rischi emergenti derivanti dalle crescenti sinergie del mondo IT e del mondo OT (reti fortemente interconnesse)
- Definizione di relazioni prima che si verifichi un evento (o un incidente) di sicurezza
- Accordi bilaterali e MoU in ottica infosharing con soggetti trust
- Information sharing e Experience sharing che possa essere cross sector/industry (e cross country)
- Supply Chain

*“L’Arte della Guerra ci insegna a confidare non sulla probabilità che il nemico non arrivi, ma sulla nostra **prontezza** nel riceverlo; non sul fatto che non attacchi, ma piuttosto sul fatto che abbiamo reso la nostra posizione **inattaccabile**.”*

L’Arte della Guerra (Sun Tzu)

Grazie

luigi.ballarano@terna.it