CESPIS

Centro Studi, Prevenzione, Investigazione e Sicurezza

Relazione sul tema: La cyber security

A cura di Michele Sorrentino

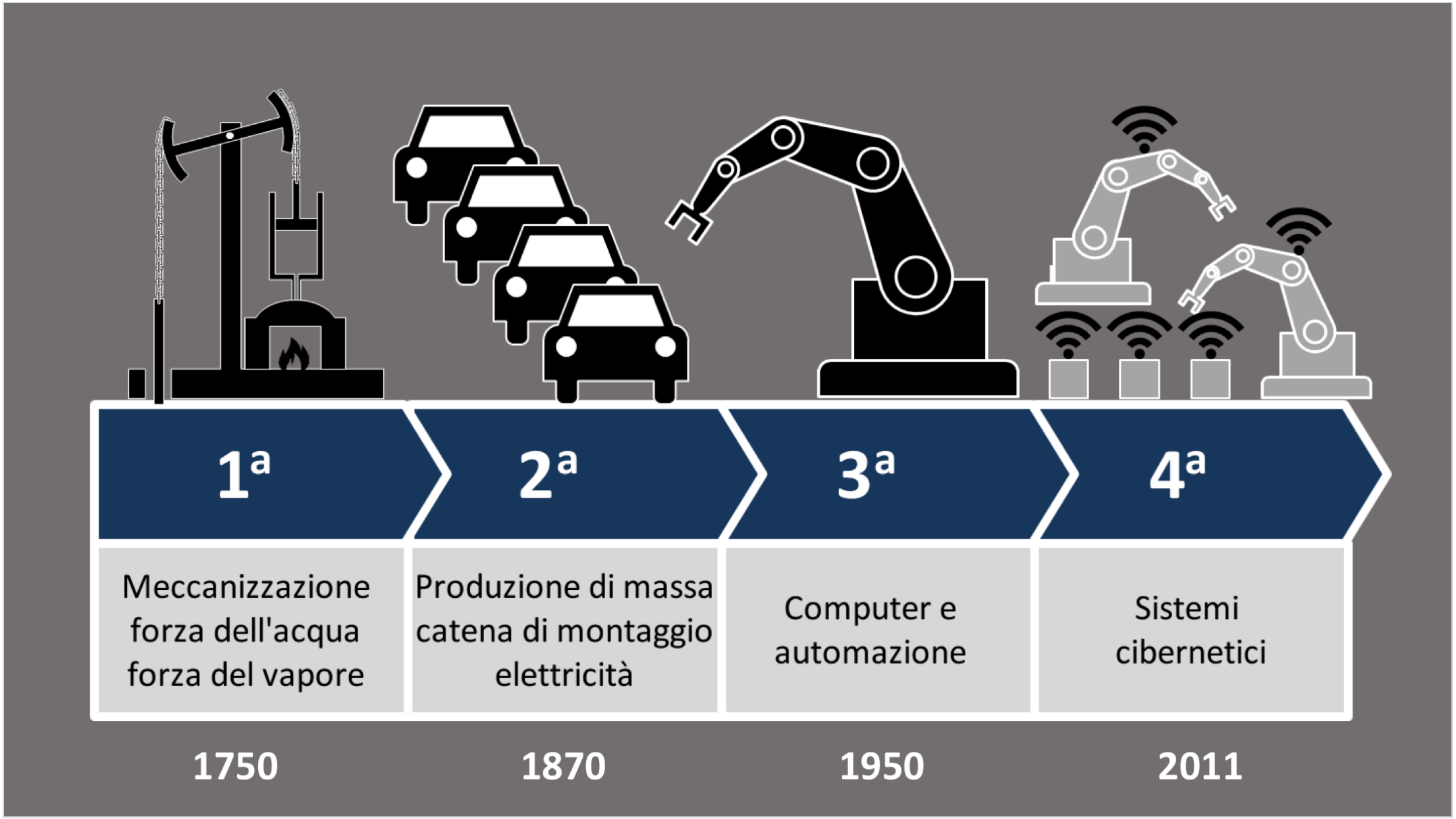
L'UOMO DIPENDENTE DALLA CATENA DI MONTAGGIO

L'UOMO TRAVOLTO DALLA CATENA DI MONTAGGIO

SICUREZZA

L'UOMO DIPENDENTE DAL COMPUTER

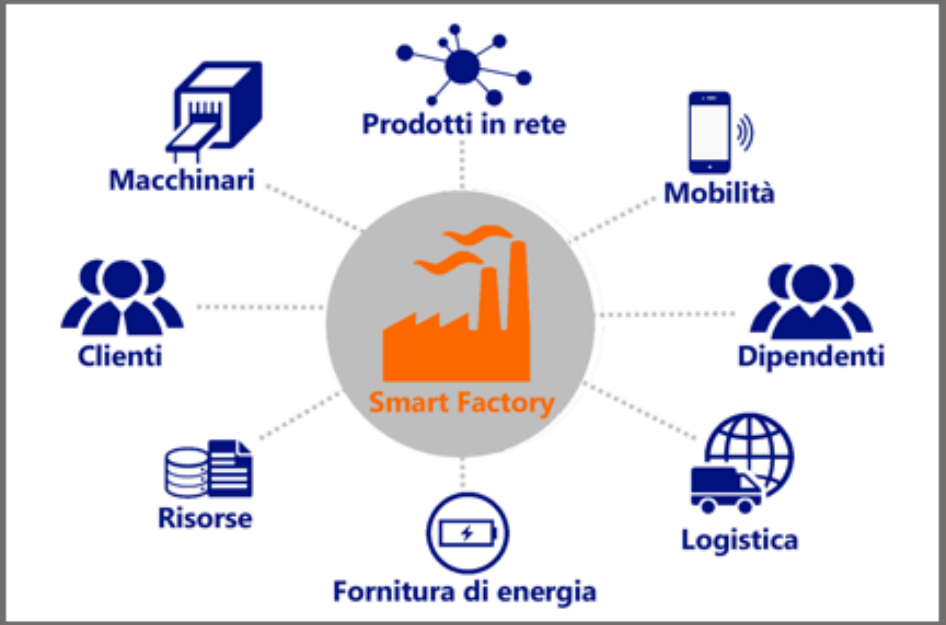
L'UOMO ATTACCATO ATTRAVERSO IL COMPUTER


1ª
2ª
3ª
4ª
Meccanizzazione
forza dell'acqua
forza del vapore
Produzione di massa
catena di montaggio
elettricità
Computer e
automazione
Sistemi
cibernetici
1750
1870
1950
2011

INDUSTRIA 4.0

E' L'ORGANIZZAZIONE INTEGRATA DELL'ATTIVITA' DI PRODUZIONE BASATA SULLA DIGITALIZZAZIONE DI TUTTE LE FASI DEI PROCESSI PRODUTTIVI.

LA CHIAVE DI VOLTA DELL'INDUSTRIA 4.0 SONO I SISTEMI CIBERFISICI (CYBER PHYSICAL SYSTEM-CPS), OVVERO SISTEMI FISICI STRETTAMENTE CONNESSI CON I SISTEMI INFORMATICI, CHE POSSONO INTERAGIRE E COLLABORARE CON ALTRI SISTEMI CPS.



LO SPAZIO CIBERNETICO

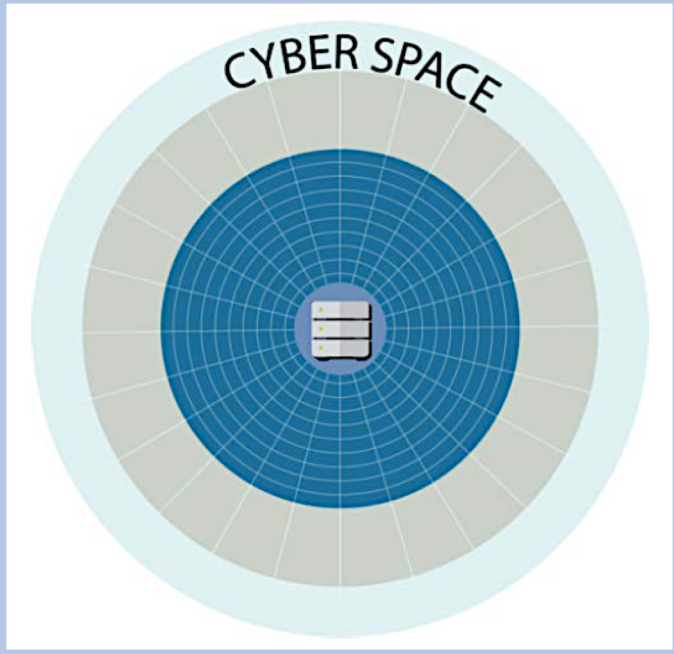
LO "SPAZIO CIBERNETICO" RAPPRESENTA UN NUOVO DOMINIO OPERATIVO DI NATURA ARTIFICIALE, TRASVERSALE AGLI ALTRI QUATTRO DOMINI TRADIZIONALI:

- ✓ **DOMINIO TERRESTRE**
- ✓ **DOMINIO AEREO**
- ✓ **DOMINIO MARITTIMO**
- ✓ **DOMINIO SPAZIALE**

VEROSIMILMENTE NEL PROSSIMO FUTURO GLI ESSERI UMANI E ANCHE LE INTELLIGENZE ARTIFICIALI, POSSONO AGIRE E INTERAGIRE A DISTANZA.

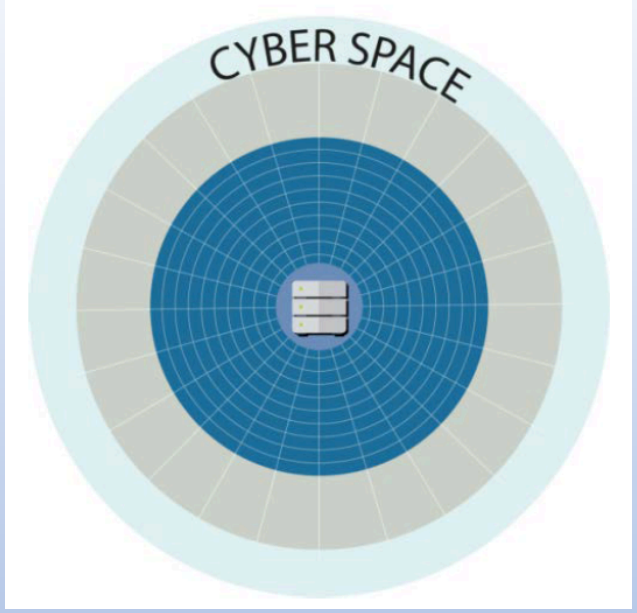
LO SPAZIO CIBERNETICO

ESSO SI PRESENTA COME UN AMBIENTE VIRTUALE, PRIVO DI CONFINI FISICI NEL SENSO TRADIZIONALE DEL TERMINE, COME UNO SPAZIO INDEFINITO NEL CUI AMBITO NON ESISTE DIVISIONE TRA PUBBLICO E PRIVATO, TRA LA SFERA MILITARE E CIVILE.



E' CREATO DALL'UOMO ED È IN CONTINUA EVOLUZIONE E IMPLEMENTAZIONE ATTRAVERSO LE TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE (INFORMATION AND COMMUNICATION TECHNOLOGY) CON LE QUALI VENGONO EROGATI IN MISURA CRESCENTE SERVIZI ESSENZIALI PER LA COLLETTIVITÀ E STRATEGICI PER IL PAESE.

VULNERABILITA’ DELLO SPAZIO CIBERNETICO



PERO’ LO SPAZIO CIBERNETICO PRESENTA DELLE “VULNERABILITÀ” OVVERO DEI PUNTI DI DEBOLEZZA ATTRAVERSO I QUALI È POSSIBILE ACQUISIRE ILLEGALMENTE DATI E INFORMAZIONI CHE “TRANSITANO” IN TALE SPAZIO OVVERO COMPROMETTERE IN TUTTO O IN PARTE IL FUNZIONAMENTO DI SERVIZI E SISTEMI DIGITALI.

DI QUI L’ESIGENZA DI DISPORRE DI MATERIALI TECNOLOGICAMENTE CERTIFICATI PIÙ FACILMENTE CONTROLLABILI E MONITORABILI, CON PARTICOLARE RIFERIMENTO ALLA FORNITURA DI MATERIALE MILITARE.

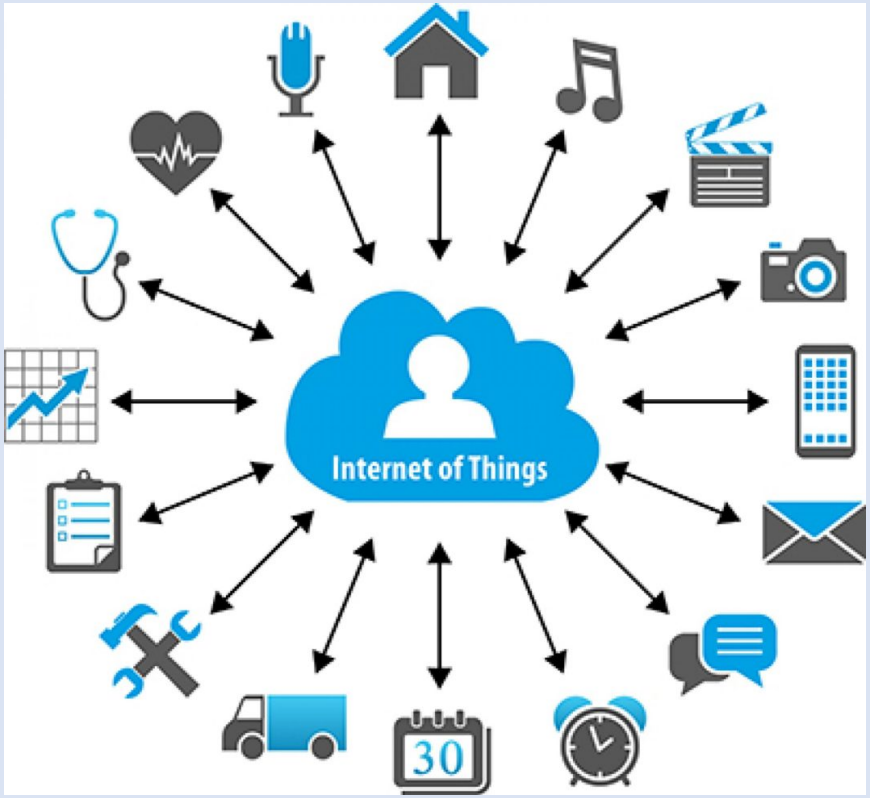
LA MINACCIA CIBERNETICA

LA MINACCIA CIBERNETICA VIENE DA TEMPO CONSIDERATA COME UNA MINACCIA ASSAI SIGNIFICATIVA, MUTEVOLE NEI SUOI TRATTI ESSENZIALI, IN CONTINUA EVOLUZIONE, RAPIDA NEL COLPIRE IL BERSAGLIO DA AGGREDIRE E CAPACE DI PRODURRE EFFETTI A DISTANZE NON RAGGIUNGIBILI CON GLI ORDINARI STRUMENTI DI ATTACCO.

INTERNET OF THINGHS (IOT)

GLI ANALISTI OSSERVANO CHE LE NUOVE TIPOLOGIE DI ATTACCO SARANNO ELABORATE ANCHE IN CONSEGUENZA DEL SEMPRE PIÙ DIFFUSO UTILIZZO DELL'INNOVAZIONE TECNOLOGICA DELL'IOT IN DIVERSI AMBITI DOMESTICI E LAVORATIVI (DAI TELEVISORI DI ULTIMA GENERAZIONE A CERTI GIOCATTOLI PER BAMBINI, PASSANDO PER LE TELECAMERE DI SORVEGLIANZA ATTIVABILI DA REMOTO).

IN QUESTI CONTESTI, SFRUTTANDO I RICHIAMATI DISPOSITIVI COLLEGATI IN RETE, SARÀ POSSIBILE A SOGGETTI OSTILI ACQUISIRE ILLEGALMENTE, CON MAGGIORE FACILITÀ RISPETTO AGLI ATTUALI METODI INTRUSIVI, INFORMAZIONI RIGUARDANTI LA VITA PRIVATA E LAVORATIVA DELLA VITTIMA, OVVERO PRENDERE IL CONTROLLO DI DISPOSITIVI E MACCHINARI ALTRUI, DIROTTANDONE L'AZIONE, VISIONARE DATI RISERVATI (TELEFONICI, DI POSTA ELETTRONICA, ETC.) OPPURE DISTRUGGERE MEMORIE O SEQUESTRARLE A SCOPO DI RICATTO (RENDENDOLE INDISPONIBILI AL LEGITTIMO TITOLARE)



GLI ATTORI

CRACKER

PIRATA INFORMATICO CHE PENETRA O SUPERA LA SICUREZZA DI UN SISTEMA INFORMATICO PER COMPROMETTERNE L'INTEGRITÀ, IL FUNZIONAMENTO O FARNE USO ILLEGALE AL FINE DI RICAVARE PROFITTI ECONOMICI.

SERVIZI DI INTELLIGENCE STRANIERI

USANO STRUMENTI INFORMATICI PER RACCOGLIERE INFORMAZIONI E PER SVOLGERE ATTIVITA' DI SPIONAGGIO

BOT-NETWORK OPERATOR (BOTNET)

PIRATI INFORMATICI CHE UTILIZZANO UN SOFTWARE MALIGNO (MALWARE) PER INFETTARE UN GRAN NUMERO DI MACCHINE E CRPIRE DATI E INFORMAZIONI SENSIBILI (PHISHING), COMPROMETTERNE LA RISERVATEZZA, L'INTEGRITA' O LA DISPONIBILITA'

GRUPPI CRIMINALI

ATTACCANO I SISTEMI INFORMATICI PER COMMETTERE ATTIVITA' DI SPIONAGGIO INDUSTRIALE, FURTI DI IDENTITA' O DI GROSSE ENTITA' DI DENARO, FRODI ONLINE.

TERRORISTI

INDIVIDUI IDEOLOGICAMENTE MOTIVATI, CHE CERCANO DI DISTRUGGERE, DANNEGGIARE O SFRUTTARE LE RETI INFORMATICHE PER MINACCIARE LA SICUREZZA NAZIONALE, CAUSARE VITTIME SU LARGA SCALA, INDEBOLIRE L'ECONOMIA.

TIPOLOGIE DI MINACCE

GUERRA CIBERNETICA (CYBER – WARFARE)

AZIONI EFFETTUATE DAGLI STATI PER PENETRARE I SISTEMI INFORMATICI E I NETWORK DI UN ALTRO STATO, AGENZIA GOVERNATIVA, ORGANIZZAZIONE MILITARE, AL FINE DI CAUSARE DANNI O DISTURBI CONSISTENTI.

SPIONAGGIO CIBERNETICO (CYBER-ESPIONAGE)

ATTIVITA' CHE SFRUTTANO LE POTENZIALITA' DELLA RETE PER SOTTRARRE SEGRETI INDUSTRIALI A FINI DI CONCORRENZA SLEALE (MERCATO DEI BREVETTI CIVILI) O DI SUPERIORITA' STRATEGICA (NEL CASO DI SOTTRAZIONE DI DISEGNI E APPARECCHIATURE MILITARI O DUAL-USE).

CRIMINALITA' CIBERNETICA (CYBER –CRIME)

OPERAZIONI ILLEGALI CHE AVVENGONO ATTRAVERSO LO SPAZIO CIBERNETICO (PER ESEMPIO TRUFFA, FRODE TELEMATICA, FURTO D'IDENTITA', SOTTRAZIONE INDEBITA DI INFORMAZIONI, LA PEDOPORNOGRAFIA ETC.

TERRORISMO CIBERNETICO (CYBER-TERRORISM)

UTILIZZO DELLA RETE DA PARTE DI GRUPPI TERRORISTICI PER EFFETTUARE ATTACCHI INFORMATICI, IDEOLOGICAMENTE MOTIVATI, FINALIZZATI A COLPIRE TARGET SENSIBILI COME IL SETTORE CREDITIZIO, LE INFRASTRUTTURE MILITARI, I SISTEMI DI CONTROLLO DI SERVIZI DI PUBBLICA UTILITA', I MEZZI DI INFORMAZIONE.

LA CYBER SECURITY IN ITALIA

La struttura italiana di cyber security è relativamente recente:

- **2010 RELAZIONE COPASIR** (Comitato parlamentare che controlla i servizi di informazione): necessità di proteggere anche a livello cibernetico **le infrastrutture critiche**.

- **2012 LEGGE DEL 7 AGOSTO N. 133**: si assegna al Dipartimento Informazioni per la Sicurezza (DIS) il coordinamento delle attività informative indirizzate alla protezione delle infrastrutture critiche e dello spazio cibernetico del paese. Tutto ciò per rafforzare la **sicurezza informatica nazionale** e per fronteggiare efficacemente i pericoli della minaccia cibernetica.

- **2013 DPCM DEL 24 GENNAIO** (c.d. decreto Monti): viene delineato un quadro strategico nazionale con l'individuazione di soggetti, sia pubblici che privati, con specifiche funzioni, che mediante un approccio interdisciplinare agiscono in maniera integrata per ridurre le vulnerabilità dello spazio cibernetico, identificare le minacce, prevenire i rischi ed accrescere le capacità di risposta a situazioni di crisi. Il sistema della sicurezza cibernetica viene sviluppato su tre livelli distinti:

DPCM DEL 24 GENNAIO 2013

I LIVELLO **di indirizzo politico** e coordinamento strategico, affidato al Comitato interministeriale per la sicurezza della Repubblica (CISR), per individuare gli obiettivi da conseguire per la protezione cibernetica e la sicurezza informatica nazionale;

II LIVELLO **di supporto**, affidato al Nucleo per la Sicurezza Cibernetica, presieduto dal Consigliere Militare del Presidente del Consiglio, per raccordare tutte le amministrazioni ed enti competenti, programmare l'attività operativa a livello interministeriale ed attivare le procedure di allertamento in caso di crisi;

III LIVELLO **di gestione delle crisi** affidato al Tavolo interministeriale di crisi cibernetica, per coordinare le attività di risposta ed il ripristino delle funzionalità dei sistemi.

DPCM 24 gennaio 2013: Architettura nazionale *cyber*

IL DPCM DEL 17 FEBBRAIO 2017 (C.D. DECRETO GENTILONI)

QUADRO STRATEGICO NAZIONALE (QSN)

INDIRIZZI STRATEGICI

1. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese
2. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati
3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali
4. Promozione e diffusione della cultura della sicurezza cibernetica
5. Rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica
6. Rafforzamento delle capacità di contrasto alle attività e contenuti illegali *on-line*

PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA

PIANO NAZIONALE (PN)

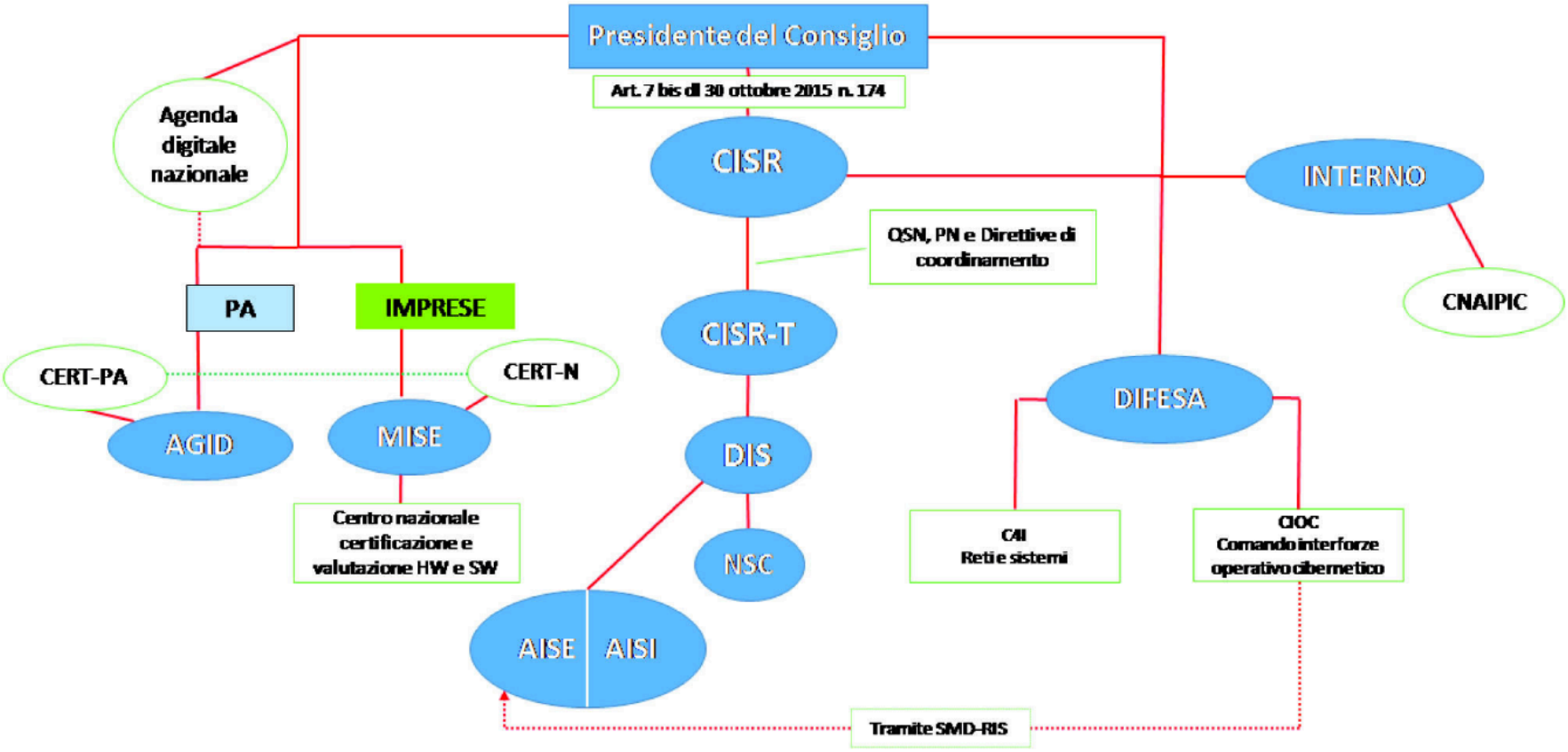
INDIRIZZI OPERATIVI

1. Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento
4. Cooperazione internazionale ed esercitazioni
5. Operatività delle strutture nazionali di *incident prevention*, *response* e *remediation*
6. Interventi legislativi e *compliance* con obblighi internazionali
7. *Compliance* a *standard* e protocolli di sicurezza
8. Supporto allo sviluppo industriale e tecnologico
9. Comunicazione strategica e operativa
10. Risorse
11. Implementazione di un sistema di *cyber risk management* nazionale

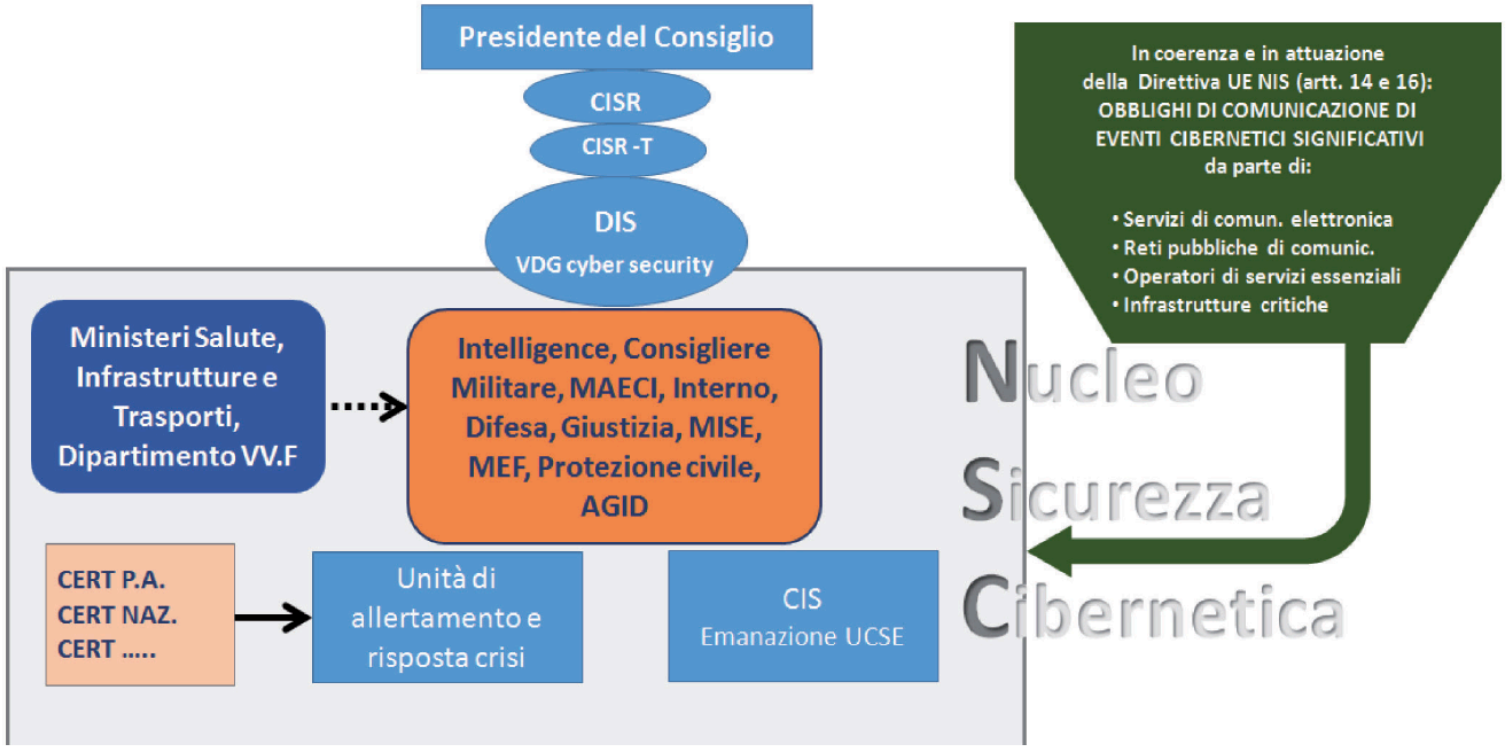
PIANO D'AZIONE

- Revisione del Nucleo per la Sicurezza Cibernetica
- Contrazione della catena di comando per la gestione delle crisi cibernetiche
- Riduzione della complessità dell'architettura nazionale, mediante soppressione/ accorpamento di organi
- Progressiva unificazione dei CERT
- Istituzione di un centro di valutazione e certificazione nazionale ICT
- Fondazione o Fondo di *venture capital*
- Istituzione di un Centro nazionale di ricerca e sviluppo in *cybersecurity*
- Costituzione di un Centro nazionale di crittografia

ARCHITETTURA NAZIONALE *CYBER*



NUOVO SISTEMA DI GESTIONE DELLE CRISI



LA DIRETTIVA NIS

GLI STATI MEMBRI DEVONO ASSICURARE CHE GLI OPERATORI DI SERVIZI ESSENZIALI E I FORNITORI DI SERVIZI DIGITALI ADOTTINO MISURE DI SICUREZZA AL FINE DI:

VALUTARE IL RISCHIO	PREVENIRE IL RISCHIO	GESTIRE GLI INCIDENTI
ORGANIZZAZIONE E STRUMENTI TECNICI PROPORZIONALI AL RISCHIO	GARANTIRE UN LIVELLO DI SICUREZZA ADEGUATO AL RISCHIO	PREVENIRE E MINIMIZZARE L'IMPATTO DEGLI INCIDENTI A CARICO DI RETI USATE PER FORNITURA SERVIZI

GLI STATI MEMBRI PROVVEDONO AFFINCHE' GLI OPERATORI NOTIFICHINO SENZA INDEBITO RITARDO ALLE AUTORITA' COMPETENTI O AL CSIRT:

OPERATORI DI SERVIZI ESSENZIALI	FORNITORI DI SERVIZI ESSENZIALI
INCIDENTI AVENTI UN IMPATTO RILEVANTE SULLA CONTINUITÀ DEI SERVIZI ESSENZIALI PRESTATI	QUALSIASI INCIDENTE AVENTE UN IMPATTO RILEVANTE SULLA FORNITURA DI UN SERVIZIO DI CUI ALL'ALLEGATO III CHE ESSI OFFRONO ALL'INTERNO DELL'UNIONE.

1. Mercato online
2. Motori di ricerca online
3. Servizi di cloud computing

DECRETO LEGGE N.105 DEL 21.09.2019

PUBBLICATO NELLA GAZZETTA UFFICIALE DEL 21 SETTEMBRE 2019 INTRODUCE DISPOSIZIONI URGENTI IN MATERIA DI "PERIMETRO" DI SICUREZZA NAZIONALE CIBERNETICA.

PROVVEDIMENTO LEGISLATIVO FINALIZZATO A STABILIRE MISURE VOLTE A GARANTIRE ELEVATI LIVELLI DI SICUREZZA DELLE RETI, DEI SISTEMI INFORMATIVI E DEI SERVIZI INFORMATICI RELATIVE:

1) ALLE POLITICHE DI SICUREZZA, ALLA STRUTTURA ORGANIZZATIVA E ALLA GESTIONE DEL RISCHIO;
2) ALLA MITIGAZIONE E GESTIONE DEGLI INCIDENTI E ALLA LORO PREVENZIONE, ANCHE ATTRAVERSO LA SOSTITUZIONE DI APPARATI O PRODOTTI CHE RISULTINO GRAVEMENTE INADEGUATI SUL PIANO DELLA SICUREZZA;
3) ALLA PROTEZIONE FISICA E LOGICA E DEI DATI;
4) ALL'INTEGRITA' DELLE RETI E DEI SISTEMI INFORMATIVI;
5) ALLA GESTIONE OPERATIVA, IVI COMPRESA LA CONTINUITA' DEL SERVIZIO;
6) AL MONITORAGGIO, TEST E CONTROLLO;
7) ALLA FORMAZIONE E CONSAPEVOLEZZA;
8) ALL'AFFIDAMENTO DI FORNITURE DI BENI, SISTEMI E SERVIZI DI INFORMATION AND COMMUNICATION TECHNOLOGY (ICT), ANCHE MEDIANTE DEFINIZIONE DI CARATTERISTICHE E REQUISITI DI CARATTERE GENERALE.

LE MISURE DI SICUREZZA

LA PRESIDENZA DEL CONSIGLIO DEI MINISTRI E IL MINISTERO DELLO SVILUPPO ECONOMICO PROVVEDONO, SECONDO GLI AMBITI DI COMPETENZA, ALL'ELABORAZIONE DELLE MISURE DI SICUREZZA, D'INTESA CON IL MINISTERO DELLA DIFESA, IL MINISTERO DELL'INTERNO, IL MINISTERO DELL'ECONOMIA E DELLE FINANZE E IL DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA.

IN PARTICOLARE, IL MINISTERO DELLO SVILUPPO ECONOMICO SI AVVALE DI UN **CENTRO DI VALUTAZIONE E CERTIFICAZIONE NAZIONALE** CHE SVOLGE I SEGUENTI COMPITI:

- ELABORAZIONE DELLE MISURE DI SICUREZZA PER CIÒ CHE CONCERNE L'AFFIDAMENTO DI FORNITURE DI BENI, SISTEMI E SERVIZI ICT;

- VERIFICA ANCHE CON LABORATORI ACCREDITATI E IN RELAZIONE ALL'AMBITO DI IMPIEGO, DELLE CONDIZIONI DI SICUREZZA E DELL'ASSENZA DI VULNERABILITÀ NOTE, DETTANDO, SE DEL CASO, PRESCRIZIONI DI UTILIZZO AL COMMITTENTE;

- ELABORAZIONE E ADOZIONE, PREVIO CONFORME AVVISO DELL'ORGANISMO TECNICO DI SUPPORTO AL CISR, SCHEMI DI CERTIFICAZIONE CIBERNETICA, LADDOVE, PER RAGIONI DI SICUREZZA NAZIONALE, GLI SCHEMI DI CERTIFICAZIONE ESISTENTI NON SIANO RITENUTI ADEGUATI ALLE ESIGENZE DI TUTELA DEL PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA.

Presidenza del Consiglio dei Ministri – Palazzo Chigi

Ministero dello Sviluppo Economico

Ministero della Difesa

Ministero dell'Interno

MEF Ministero dell'Economia e delle Finanze

Sistema di Informazione per la Sicurezza della Repubblica
a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia

GLI ADEMPIMENTI

Secondo quanto previsto dall'art. 1, entro quattro mesi dalla data di entrata in vigore della legge di conversione del decreto legge:

- **individuazione dei soggetti** (amministrazioni pubbliche, enti e operatori nazionali, pubblici e privati) che esercitano una funzione essenziale dello Stato, ovvero assicurano un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;

- **elenco delle reti, sistemi informativi e servizi informatici** utilizzati dai citati soggetti il cui malfunzionamento, interruzione, anche parziale, ovvero l'utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale;

- **il perimetro di sicurezza nazionale cibernetica** è costituito da tali soggetti che sono tenuti al rispetto delle misure e degli obblighi previsti dalla legge;
- (art.1, comma 2, lett. a)

GLI ADEMPIMENTI

Gli stessi soggetti:

- **predispongono e aggiornano con cadenza almeno annuale un elenco delle reti**, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica secondo opportuni moduli organizzativi e criteri previsti dal CISR – Tecnico, integrato con un rappresentante della Presidenza del Consiglio dei Ministri. (art.1, comma 2, lett. b)

- **trasmettono tali elenchi**, entro sei mesi dall'entrata in vigore alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico che, a loro volta, li inoltrano al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

IL CISR

(*art. 4 DPCM del 17 febbraio 2017*)

IL COMITATO INTERMINISTERIALE PER LA SICUREZZA DELLA REPUBBLICA, PRESIEDUTO DAL PRESIDENTE DEL CONSIGLIO O DA UN'AUTORITÀ DELEGATA (SOTTOSEGRETARIO O MINISTRO SENZA PORTAFOGLIO), È UN ORGANISMO DI CONSULENZA, PROPOSTA E DELIBERAZIONE SUGLI INDIRIZZI E LE FINALITÀ GENERALI DELLA POLITICA DELL'INFORMAZIONE PER LA SICUREZZA.

COMPOSIZIONE:

PRESIDENTE DEL CONSIGLIO DEI MINISTRI O AUTORITA' DELEGATA

IL MINISTRO DELL'INTERNO
IL MINISTRO DELLA DIFESA
IL MINISTRO DELLA GIUSTIZIA
IL MINISTRO DELL'ECONOMIA E DELLE FINANZE
IL MINISTRO DELLO SVILUPPO ECONOMICO
IL DIRETTORE GENERALE DEL DIS CON FUNZIONI DI SEGRETARIO

LE PRINCIPALI FUNZIONI DEL CISR

(art. 4 DPCM del 17 febbraio 2017)

Il Comitato interministeriale per la sicurezza della Repubblica (CISR) nella materia della sicurezza dello spazio cibernetico svolge i seguenti compiti:

a) partecipa, in caso di crisi cibernetica, alle determinazioni del Presidente, con funzioni di consulenza e di proposta, nonché di deliberazione nei casi indicati all'art. 7-bis, comma 5, del decreto-legge n. 174 del 2015, convertito con modificazioni dalla legge n. 198 del 2015;

b) propone al Presidente l'adozione del quadro strategico nazionale di cui all'art. 3, comma 1, lettera b);

c) delibera il Piano nazionale per la sicurezza dello spazio cibernetico di cui all'art. 3, comma 1, lettera c), ai fini dell'adozione da parte del Presidente;

d) esprime parere, ai sensi dell'art. 5, comma 2, lettera h), della legge n. 400 del 1988, sulle direttive del Presidente di cui all'art. 3, comma 1, lettera d);

e) è sentito, ai sensi dell'art. 1, comma 3-bis, della legge n. 124 del 2007, ai fini dell'adozione delle direttive del Presidente agli organismi di informazione per la sicurezza;

f) esercita l'alta sorveglianza sull'attuazione del Piano nazionale per la sicurezza dello spazio cibernetico;

g) approva linee di indirizzo per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, nonché per la condivisione delle informazioni e per l'adozione di best pratices e di misure rivolte all'obiettivo della sicurezza cibernetica;

h) elabora, ai sensi dell'art. 5, della legge n. 124 del 2007, gli indirizzi generali e gli obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali da perseguire nel quadro della politica dell'informazione per la sicurezza da parte degli organismi di informazione per la sicurezza, ciascuno per i profili di rispettiva competenza;

i) promuove l'adozione delle iniziative necessarie per assicurare, in forma coordinata, la piena partecipazione dell'Italia ai diversi consessi di cooperazione internazionale, sia in ambito bilaterale e multilaterale, ivi compresa la NATO, e dell'UE, al fine della definizione e adozione di politiche e strategie comuni di prevenzione e risposta;

l) formula le proposte di intervento normativo ed organizzativo ritenute necessarie al fine del potenziamento delle misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle crisi.

CISR TECNICO: ORGANISMO DI SUPPORTO AL CISR

(art. 5 DPCM del 17 febbraio 2017)

L'ORGANISMO COLLEGIALE PRESIEDUTO DAL DIRETTORE GENERALE DEL DIS SVOLGE I SEGUENTI COMPITI:

A) SVOLGE ATTIVITÀ PREPARATORIA DELLE RIUNIONI DEL CISR DEDICATE ALLA MATERIA DELLA SICUREZZA CIBERNETICA;

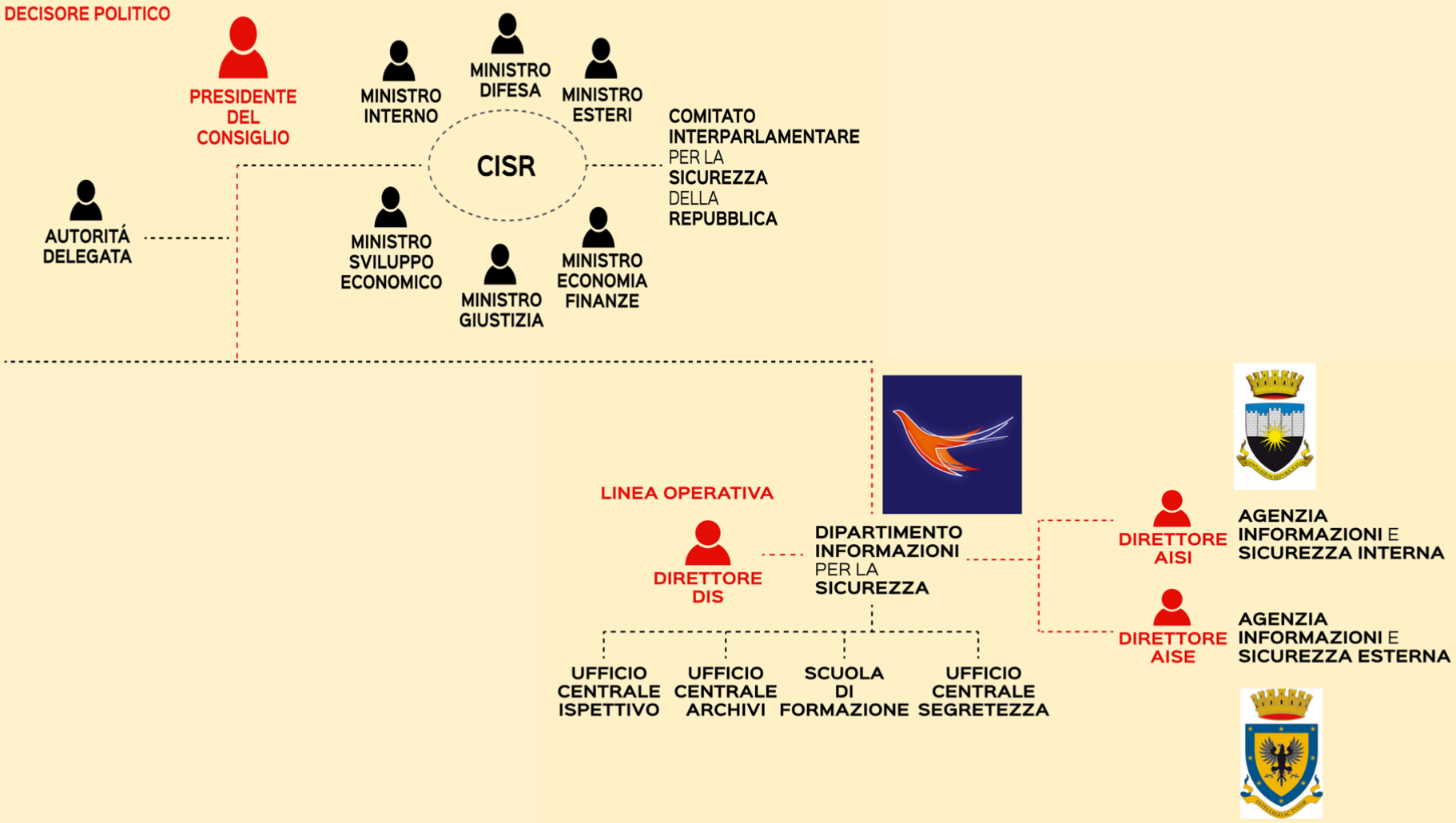
B) ASSICURA L'ISTRUTTORIA PER L'ADOZIONE DEGLI ATTI E PER L'ESPLETAMENTO DELLE ATTIVITÀ, DA PARTE DEL CISR, DI CUI ALL'ART. 4, COMMA 1, DEL PRESENTE DECRETO;

C) ESPLETA LE ATTIVITÀ NECESSARIE A VERIFICARE L'ATTUAZIONE DEGLI INTERVENTI PREVISTI DAL PIANO NAZIONALE PER LA SICUREZZA DELLO SPAZIO CIBERNETICO E L'EFFICACIA DELLE PROCEDURE DI COORDINAMENTO TRA I DIVERSI SOGGETTI, PUBBLICI E PRIVATI, CHIAMATI AD ATTUARLI;

D) COORDINA, IN ATTUAZIONE DEGLI INDIRIZZI APPROVATI DAL CISR E SULLA BASE DEGLI ELEMENTI FORNITI DALLE AMMINISTRAZIONI ED ENTI COMPETENTI, DAGLI ORGANISMI DI INFORMAZIONE PER LA SICUREZZA, DAL NUCLEO PER LA SICUREZZA CIBERNETICA DI CUI ALL'ART. 8 E DAGLI OPERATORI PRIVATI, LA FORMULAZIONE DELLE INDICAZIONI NECESSARIE ALLO SVOLGIMENTO DELLE ATTIVITÀ DI INDIVIDUAZIONE DELLE MINACCE ALLA SICUREZZA DELLO SPAZIO CIBERNETICO, AL RICONOSCIMENTO DELLE VULNERABILITÀ, NONCHÉ PER L'ADOZIONE DI BEST PRACTICES E MISURE DI SICUREZZA;

3. PER LE FINALITÀ DI CUI AL COMMA 2, L'ORGANISMO COLLEGIALE DI COORDINAMENTO COMPIE APPROFONDIMENTI ED ACQUISISCE OGNI UTILE CONTRIBUTO E VALUTAZIONE RITENUTI NECESSARI.

LA LINEA DEL POTERE DEI SERVIZI INFORMATIVI ITALIANI



NOTIFICA DEGLI INCIDENTI

- ENTRO 10 MESI CON DPCM, SENTITO IL PARERE DEL CISR, SONO DEFINITE LE PROCEDURE DI NOTIFICA DEGLI INCIDENTI AVENTI IMPATTO SU RETI, SISTEMI INFORMATIVI E SERVIZI INFORMATICI AL GRUPPO DI INTERVENTO PER LA SICUREZZA INFORMATICA (**CSNRT**) CHE LE INOLTRA TEMPESTIVAMENTE AL DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA ANCHE PER LE ATTIVITÀ DEMANDATE AL NUCLEO PER LA SICUREZZA CIBERNETICA E, A SUA VOLTA, LE TRASMETTE:

  - ALL'ORGANO DEL MINISTERO DELL'INTERNO PER LA SICUREZZA E LA REGOLARITÀ DEI SERVIZI DI TELECOMUNICAZIONE;
  - ALLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI, SE PROVENIENTI DA UN SOGGETTO PUBBLICO O DA AGID;
  - AL MINISTERO DELLO SVILUPPO ECONOMICO, SE EFFETTUATE DA UN SOGGETTO PRIVATO.

IL CSNRT ITALIANO

IL **COMPUTER SECURITY INCIDENT RESPONSE TEAM** (CSIRT ITALIA), ISTITUITO A SEGUITO DELLA DIRETTIVA NIS (D.LGS. 65/2018) PRESSO LA PRESIDENZA DEL CONSIGLIO DEI MINISTRI SVOLGERÀ ALL'INTERNO DELL'ORDINAMENTO NAZIONALE ITALIANO I COMPITI E LE FUNZIONI DEGLI ATTUALI CERT-PA E CERT-N SULLA BASE DI UN MODELLO COOPERATIVO PUBBLICO-PRIVATO, **AVRÀ COMPITI DI NATURA TECNICA FINALIZZATI A SUPPORTARE LA PA, I CITTADINI E LE IMPRESE ATTRAVERSO AZIONI DI SENSIBILIZZAZIONE, PREVENZIONE E COORDINAMENTO DELLA RISPOSTA AD EVENTI CIBERNETICI SU VASTA SCALA, ANCHE IN COOPERAZIONE CON GLI ALTRI CSIRT EUROPEI.**

IN PARTICOLARE, SECONDO QUANTO DISPOSTO DAL DECRETO DI RECEPIMENTO, AVRÀ I SEGUENTI COMPITI:

- DEFINIRE LE PROCEDURE PER LA PREVENZIONE E LA GESTIONE DEGLI INCIDENTI INFORMATICI;
- RICEVERE LE NOTIFICHE DI INCIDENTE, INFORMANDONE IL DIS, QUALE PUNTO DI CONTATTO UNICO E PER LE ATTIVITÀ DI PREVENZIONE E PREPARAZIONE A EVENTUALI SITUAZIONI DI CRISI E DI ATTIVAZIONE DELLE PROCEDURE DI ALLERTAMENTO AFFIDATE AL NSC;
- FORNIRE AL SOGGETTO CHE HA EFFETTUATO LA NOTIFICA LE INFORMAZIONI CHE POSSONO FACILITARE LA GESTIONE EFFICACE DELL'EVENTO;
- INFORMARE GLI ALTRI STATI MEMBRI DELL'UE EVENTUALMENTE COINVOLTI DALL'INCIDENTE, TUTELANDO LA SICUREZZA E GLI INTERESSI COMMERCIALI DELL'OPERATORE DI SERVIZI ESSENZIALI O DEL FORNITORE DI SERVIZI DIGITALI NONCHÉ LA RISERVATEZZA DELLE INFORMAZIONI FORNITE;
- GARANTIRE LA COLLABORAZIONE NELLA RETE DI CSIRT, ATTRAVERSO L'INDIVIDUAZIONE DI FORME DI COOPERAZIONE OPERATIVA, LO SCAMBIO DI INFORMAZIONI E LA CONDIVISIONE DI BEST PRACTICES.

NUCLEO PER LA SICUREZZA CIBERNETICA

(ex Tavolo interministeriale di crisi cibernetica)

COSTITUITO PRESSO IL DIS A SUPPORTO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI E DEL CISR IN MATERIA DI SICUREZZA DELLO SPAZIO CIBERNETICO, SVOLGE I SEGUENTI COMPITI:

- ✓ **PREVENZIONE E PREPARAZIONE AD EVENTUALI SITUAZIONI DI CRISI**
- ✓ **ATTIVAZIONE DELLE PROCEDURE DI ALLERTAMENTO CON FUNZIONI DI RACCORDO TRA LE DIVERSE COMPONENTI DELL'ARCHITETTURA ISTITUZIONALE CYBER.**

È PRESIEDUTO DA UN **VICE DIRETTORE GENERALE DEL DIS** ED È COMPOSTO DAL **CONSIGLIERE MILITARE DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI**, DA **RAPPRESENTANTI DEL DIS**, DELL'AGENZIA INFORMAZIONI E SICUREZZA ESTERNA (**AISE**), DELL'AGENZIA INFORMAZIONI E SICUREZZA INTERNA (**AISI**), DEI **MINISTERI DEGLI AFFARI ESTERI E COOPERAZIONE INTERNAZIONALE**, DELL'**INTERNO**, DELLA **GIUSTIZIA**, DELLA **DIFESA**, **DELL'ECONOMIA E DELLE FINANZE**, **DELLO SVILUPPO ECONOMICO** NONCHÉ DEL **DIPARTIMENTO DELLA PROTEZIONE CIVILE** E **DELL'AGENZIA PER L'ITALIA DIGITALE**;
IN CASO DI CRISI, PARTECIPANO ANCHE RAPPRESENTANTI DEI **MINISTERI DELLA SALUTE**, **DELLE INFRASTRUTTURE E TRASPORTI** NONCHÉ DEL **DIPARTIMENTO DEI VIGILI DEL FUOCO, DEL SOCCORSO PUBBLICO E DELLA DIFESA CIVIL**E E **DELL'UFFICIO DEL CONSIGLIERE MILITARE DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI.**

IL RUOLO DEL CENTRO DI VALUTAZIONE E CERTIFICAZIONE NAZIONALE

I soggetti ricadenti nel perimetro di sicurezza nazionale cibernetica devono comunicare al Centro di Valutazione e Certificazione Nazionale (CVCN), istituito presso il Ministero dello sviluppo economico, l'intenzione di procedere all'affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti e sui sistemi informativi per l'espletamento dei servizi informatici essenziali.

Il CVCN, oltre a contribuire all'elaborazione delle relative misure di sicurezza, sulla base di una valutazione del rischio, anche in relazione all'ambito di impiego e in un'ottica di gradualità, potrà, entro 30 giorni, imporre condizioni e test di hardware e software.

In tale ipotesi, i relativi bandi di gara e contratti sono integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, l'affidamento ovvero il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN;

Ministero dello sviluppo economico

PROVVEDIMENTI URGENTI PER LA SICUREZZA NAZIONALE

E’ RICONOSCIUTA AL PRESIDENTE DEL CONSIGLIO DEI MINISTRI, SU DELIBERAZIONE DEL COMITATO INTERMINISTERIALE PER LA SICUREZZA DELLA REPUBBLICA (CISR), LA FACOLTÀ DI DISATTIVARE, “TOTALMENTE O PARZIALMENTE, UNO O PIÙ APPARATI O PRODOTTI IMPIEGATI NELLE RETI E NEI SISTEMI O PER L’ESPLETAMENTO DEI SERVIZI INTERESSATI” QUALORA VI SIA UN “RISCHIO GRAVE E IMMINENTE PER LA SICUREZZA NAZIONALE”(ART.5)

LE SANZIONI PREVISTE DAL DECRETO LEGGE N.105 DEL 21.09.2019

UNA VOLTA ADOTTATI I PROVVEDIMENTI ATTUATIVI, SCATTERÀ L'OPERATIVITÀ DELLO SPECIALE APPARATO SANZIONATORIO PREVISTO PER LE VIOLAZIONI DI OBBLIGHI E PRESCRIZIONI, COMPRENSIVO DI SANZIONI AMMINISTRATIVE PECUNIARIE DA 200.000 A 1.800.000 EURO E DELLA SANZIONE ACCESSORIA DELLA INCAPACITÀ DI ASSUMERE INCARICHI DI DIREZIONE, AMMINISTRAZIONE E CONTROLLO IN IMPRESE ED ENTI PER UN PERIODO DI TRE ANNI DALL'ACCERTAMENTO DELLA VIOLAZIONE.

COLORO CHE FORNISCONO INFORMAZIONI FALSE OD OMETTONO DI TRASMETTERE I DATI RICHIESTI AL FINE DI OSTACOLARE O CONDIZIONARE I PROCEDIMENTI DI CONTROLLO SONO PUNITI CON LA RECLUSIONE DA UNO A CINQUE ANNI E ALL'ENTE, RESPONSABILE AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231, SI APPLICA LA SANZIONE PECUNIARIA FINO A QUATTROCENTO QUOTE.

a) mancato adempimento degli obblighi di predisposizione e di aggiornamento dell'elenco delle reti, dei sistemi informativi e dei servizi informatici di cui al comma 2, lettera b)	sanzione amministrativa pecuniaria da euro 200.000 a euro 1.200.000
a) mancato adempimento dell'obbligo di notifica nei termini prescritti, di cui al comma 3, lettera a)	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000;
a) inosservanza delle misure di sicurezza di cui al comma 3, lettera b	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000
a) mancata comunicazione nei termini prescritti di cui al comma 6, lettera a)	sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000
a) impiego di prodotti e servizi sulle reti, sui sistemi informativi e l'espletamento dei servizi informatici di cui al comma 2, lettera b), in violazione delle condizioni imposte dal CVCN o in assenza del superamento dei test di cui al comma 6, lettera a),	sanzione amministrativa pecuniaria da euro 300.000 a euro 1.800.000
a) mancata collaborazione per l'effettuazione delle attività di test di cui al comma 6, lettera a), da parte dei soggetti di cui al medesimo comma 6, lettera b)	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000
a) 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 svolte ai sensi del comma 6, lettera c)	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000
a) mancato rispetto delle prescrizioni di cui al comma 7, lettera b)	sanzione amministrativa pecuniaria da euro 250.000 a euro 1.500.000