La minaccia cyber: strumenti di intervento

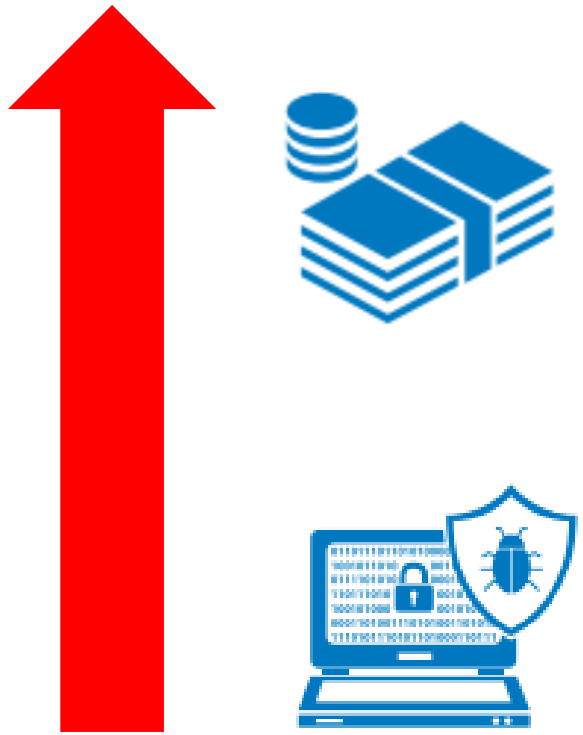
CRISTIANO LEGGERI
Primo Dirigente della P. di S.
Direttore della 3^ Divisione del Servizio Polizia Postale e delle Comunicazioni

Roma, 24 giugno 2024

90° Assemblea Generale Interpol

INTERPOL

“I crimini finanziari e informatici rappresentano le principali minacce criminali a livello globale e sono quelle destinate ad aumentare maggiormente in futuro”



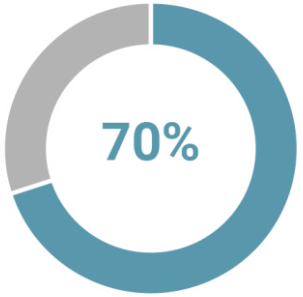
$10.5

Il costo globale della criminalità informatica raggiungerà i 10,5 trilioni di dollari entro il 2025

Interpol Secretary General Jurgen Stock

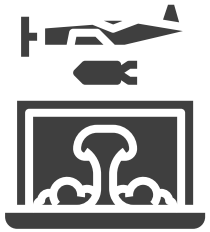
Interpol's 90th General Assembly

Lo scenario globale del cybercrime ha ormai da tempo superato i livelli di guardia, rappresentando oggi una delle principali, se non, ormai, **la principale minaccia** alla tenuta della struttura e del sistema economico del Paese.



Attacchi di matrice CRIMINALE a scopo di lucro

Cyber Warfare



Cyber Hacktivism

Cyber Terrorism

La Sicurezza Cibernetica Nazionale

SICUREZZA CIBERNETICA NAZIONALE

CYBER DEFENCE

CYBER INTELLIGENCE

CYBER RESELIENZA

CYBER INVESTIGATION

POLIZIA POSTALE E DELLE COMUNICAZIONI

INTRODUZIONE

LA POLIZIA POSTALE E DELLE COMUNICAZIONI

- Il 20 gennaio **1984** viene istituito il Compartimento Polizia Postale e delle Comunicazioni «Lazio» (Consegna pacchi a domicilio, assegni rubati, documenti smarriti).
- Nel **1996** viene istituito il NUCLEO OPERATIVO DI POLIZIA DELLE TELECOMUNICAZIONI (N.O.P.T.), un'équipe di investigatori impegnati nell'attività di contrasto ai crimini nel settore delle telecomunicazioni, per fronteggiare le minacce criminali alla sicurezza informatica legate alla evoluzione tecnologica.
- Segue una vasta riorganizzazione di tutta la Specialità che, con decreto del Ministro dell'Interno del 31 marzo **1998** porta all'istituzione del SERVIZIO POLIZIA POSTALE E DELLE COMUNICAZIONI. Al suo interno vengono fatte confluire le risorse del N.O.P.T. e della Divisione Polizia Postale.
- Con Decreto Interministeriale del 19 gennaio **1999**, il SERVIZIO POLIZIA POSTALE E DELLE COMUNICAZIONI viene indicato quale ***'Organo Centrale del Ministero dell'Interno per la Sicurezza e la Regolarità dei Servizi di Telecomunicazioni'***.

Le competenze esclusive della Specialità

- ATTACCHI CYBER E PROTEZIONE DELLE INFRASTRUTTURE CRITICHE
- PEDOPORNOGRAFIA ON-LINE E TUTTI I REATI DI AGGRESSIONE ON-LINE IN DANNO DEI MINORI
- CYBERTERRORISMO
- HACKING E FINANCIAL CYBERCRIME
- SOCIAL NETWORK - REATI POSTALI

Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica - Struttura

Direzione Centrale
per la Polizia Scientifica
e la Sicurezza Cibernetica

- Servizio
  Affari Generali
- Servizio Polizia Postale e
  della Comunicazioni
- Sevizio Polizia Scientifica
- Servizio per la Sicurezza
  Cibernetica del Ministero
  dell'Interno

- **CNAIPIC**
- **CNCPO**
- **Commissariato di P.S. Online**

Polizia Postale e delle Comunicazioni
Attuale organizzazione sul territorio nazionale

SERVIZIO CENTRALE

18 CENTRI OPERATIVI SICUREZZA CIBERNETICA

82 SEZIONI OPERATIVE SICUREZZA CIBERNETICA

Servizio Polizia Postale e per la Sicurezza Cibernetica - Struttura

Servizio
Polizia Postale e per la Sicurezza Cibernetica

1^ DIVISIONE

- **Ufficio analisi e affari giuridici e pianificazione strategica**
- **Gestione risorse umane e formazione**
- **Settore Rapporti internazionali**
- **Settore Rapporti territoriali**
- **Relazioni esterne, istituzionali e Settore scuole**
- **Commissariato di P.S. On-line**

2^ DIVISIONE

- **CNCPO**
- **Reati contro la persona mediante la rete**
- **UACI**

3^ DIVISIONE

- **CNAIPIC**
- **Sezione** informativa-**c**yberterrorismo
- **Sezione** Programmazione finanziaria e acquisizione risorse tecnologiche

4^ DIVISIONE

- **Sezione** Financial cybercrime OF2CEN
- **Sezione** reati contro la persona
- **Sezione** rapporti con Poste Italiane S.p.A.

5^ DIVISIONE

- **Sezione** Sistemi, Reti, Sicurezza e Focal point
- **Sezione** Gestione Servizi Applicativi
- **Sezione** Gestione risorse tecnologiche e digital forensic

Centri Operativi per la Sicurezza Cibernetica di Fascia I-II-III

UFFICIO DI STAFF
(Funz./Isp. ruolo ordinario)

- Ufficio Affari Generali
- URP

DIRIGENTE

VICE DIRIGENTE

SETTORE I
Dir./Funz./Isp. ruolo ordinario

SEZIONE I

- Ufficio denunce
- Contrasto pedopornografia online
- Cyberbullismo

SEZIONE II

- Reati contro la persona mediante socialnetwork

SETTORE II
Dirigente/Funzionario ruolo ordinario

NOSC

- Protezione delle infrastrutture critiche

SEZIONE I

- Informativa-Cyberterrorismo

SEZIONE II

- Contrasto cybercrime
- Frodi on line
- Reati postali

AREA I - IT
Dir./Funz./Isp. ruolo tecnico

COMPETENZE

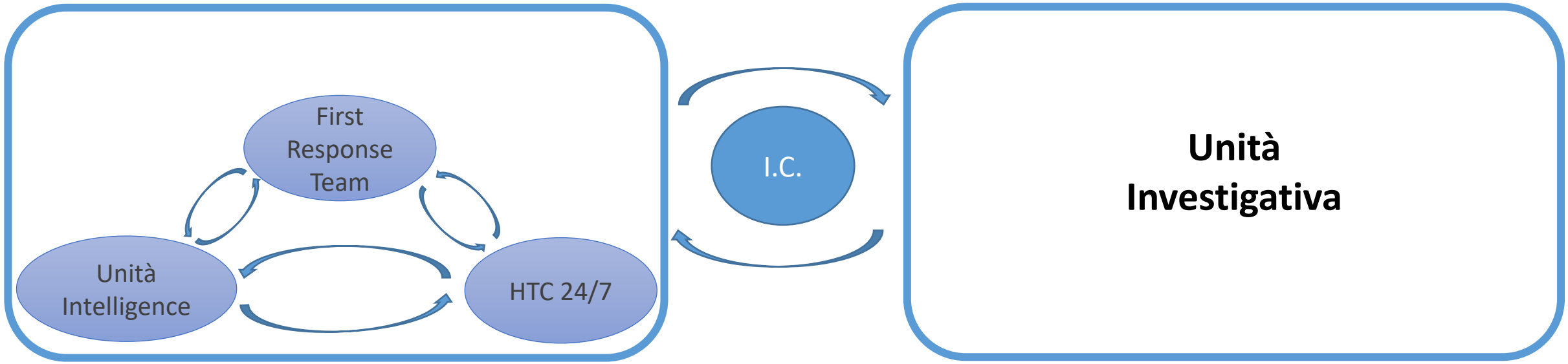
- Assicura la gestione delle infrastrutture e del materiale informatico secondo le direttive impartite dalla 4^ Divisione Servizio Centrale
- Gestione laboratorio forense

Prima normativa CYBER

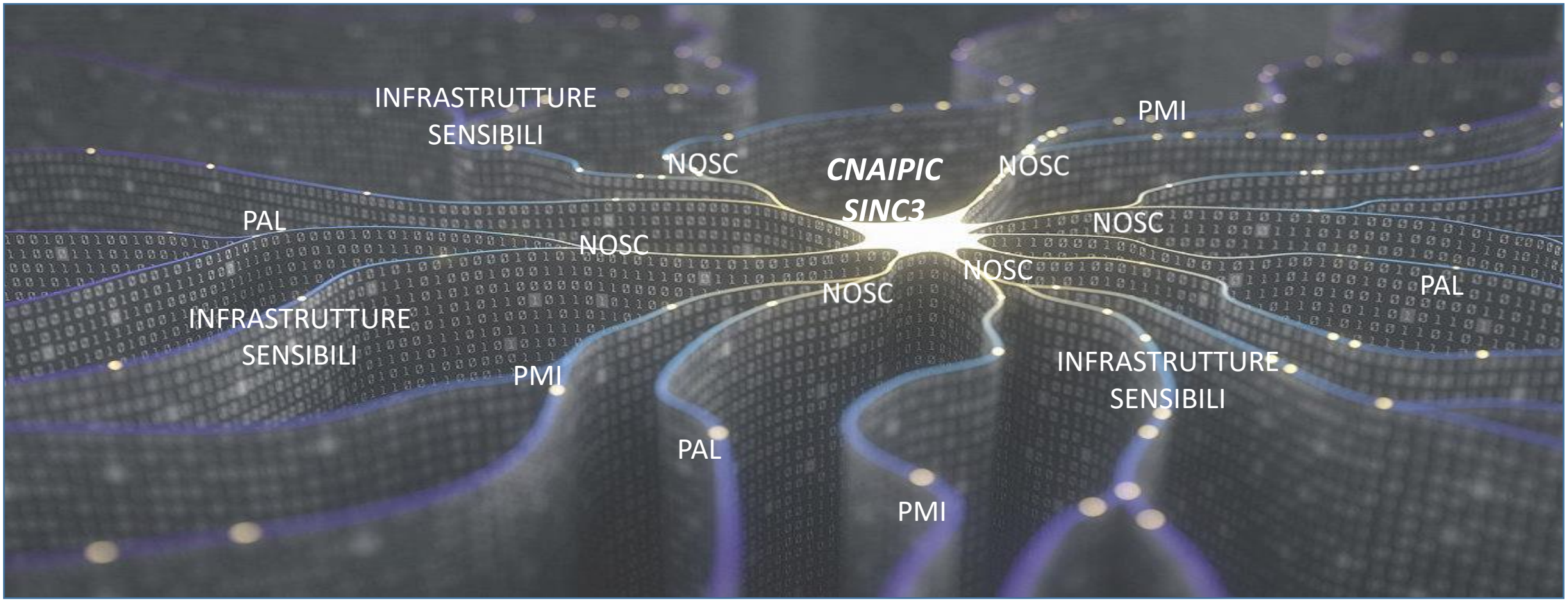
Il CNAIPIC art 7 co 1 DPR 144 2005 è incaricato della prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale. Si avvale di tecnologie di elevato livello e di personale altamente qualificato, specializzato nel contrasto del cyber crime, che ha maturato concreta esperienza anche nei settori del cyber terrorismo e dello spionaggio industriale.

L'operatività del CNAIPIC è soddisfatta attraverso l'esercizio di un Settore Operativo e di un Settore Tecnico. Il Settore Operativo supporta le funzioni di: Sala Operativa, Intelligence e Analisi. Il Settore Tecnico è invece deputato alla gestione ed all'esercizio dell'infrastruttura tecnologica del CNAIPIC e dei collegamenti telematici con le Infrastrutture Critiche convenzionate, ai processi di individuazione, testing ed acquisizione di risorse strumentali ed alla pianificazione di cicli di formazione ed aggiornamento del personale.

C.N.A.I.P.I.C. – Struttura e workflow



SINC3 - Nuclei Operativi per la Sicurezza Cibernetica



Principali tipologie di attacco alle infrastrutture critiche nazionali

Attacchi APT: acronimo di Advanced Persistent Threat, l'espressione indica una tipologia di attacchi mirati e persistenti portati avanti da avversari dotati di notevole expertise tecnico e grandi risorse. Le aziende vittima di questi attacchi vengono scelte con cura dall'hacker e la loro **struttura informatica viene studiata** per mesi prima di essere violata, sfruttando le vulnerabilità esistenti.

Gli **attacchi DDoS** (*Distributed Denial of Service*), si risolvono in tentativi di rendere non disponibile agli utenti legittimi un sito Web o un'applicazione Web, sovraccaricando il sito con un volume enorme di traffico, causandone l'interruzione o il funzionamento estremamente lento.

Gli **attacchi Ransomware** costituiscono una tipologia di malware che blocca l'accesso al sistema o cifra i dati custoditi all'interno dello stesso. A questo punto i cybercriminali richiedono alle loro vittime il pagamento di un riscatto, per poter ottenere nuovamente l'accesso al proprio computer o ai dati.

Il **Defacement** è un attacco consistente nella modifica del contenuto di una pagina o di un sito web mediante l'introduzione illecita di testi o immagini al fine di carpire dati di sistemi di pagamento (cracker), fare propaganda, spamming o cyber-estorsioni.

ALERT diramati dal C.N.A.I.P.I.C.

ANNO 2021	ANNO 2022	ANNO 2023
110.880	**113.420**	**77.012**
Var. % per anno +2%	Var. % per anno -32%	
Var. % nel biennio -30%		

	ANNO 2021	ANNO 2022	ANNO 2023
TOTALE ATTACCHI RILEVATI	**5.509**	**13.099**	**12.101**
Variazione percentuale per anno	+138%	-8%	
Variazione percentuale nel biennio	+120%		

C.N.A.I.P.I.C. e N.O.S.C. – Persone indagate

	ANNO 2021	ANNO 2022	ANNO 2023
TOTALE PERSONE INDAGATE	**201**	**334**	**224**
Variazione percentuale per anno		+66%	-33%
Variazione percentuale nel biennio		+11%	

C.N.A.I.P.I.C. - Convenzioni

Architettura Cybersecurity

Direttiva NIS 2016/1148

Istituzione perimetro sicurezza nazionale cibernetica

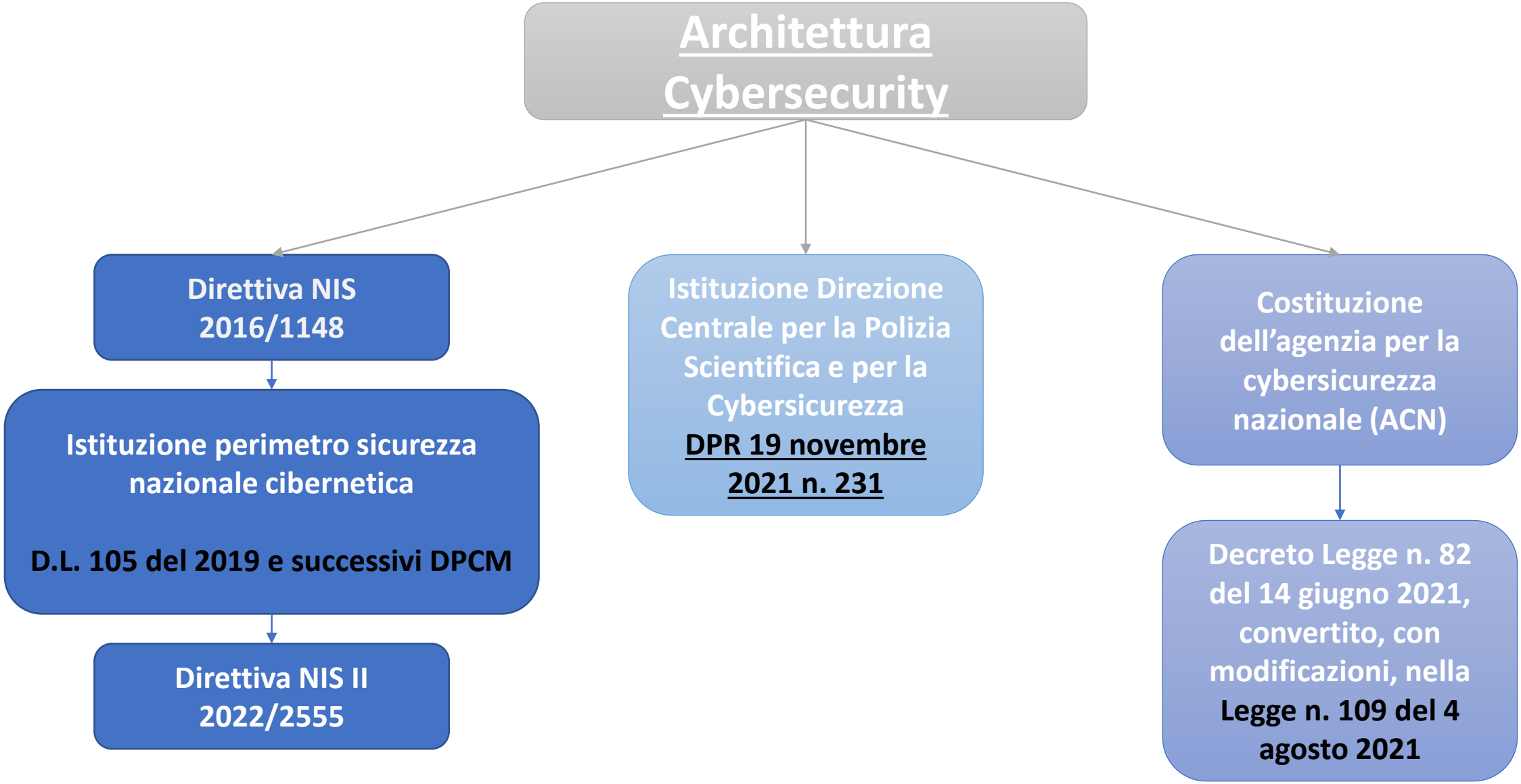
D.L. 105 del 2019 e successivi DPCM

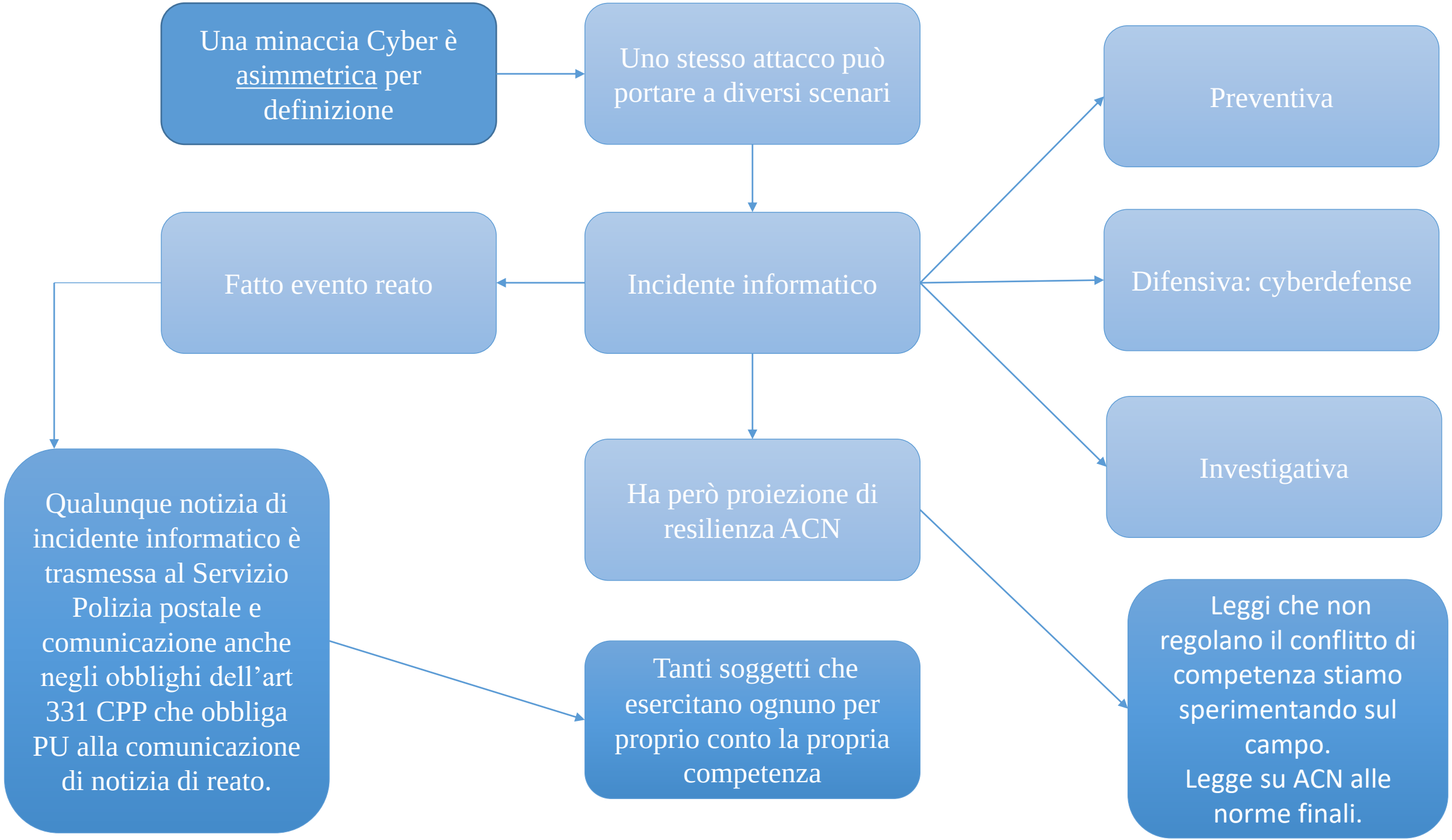
Direttiva NIS II 2022/2555

Istituzione Direzione Centrale per la Polizia Scientifica e per la Cybersicurezza DPR 19 novembre 2021 n. 231

Costituzione dell'agenzia per la cybersicurezza nazionale (ACN)

Decreto Legge n. 82 del 14 giugno 2021, convertito, con modificazioni, nella Legge n. 109 del 4 agosto 2021


Architettura Cybersecurity
Direttiva NIS 2016/1148
Istituzione perimetro sicurezza nazionale cibernetica
D.L. 105 del 2019 e successivi DPCM
Direttiva NIS II 2022/2555
Istituzione Direzione Centrale per la Polizia Scientifica e per la Cybersicurezza
DPR 19 novembre 2021 n. 231
Costituzione dell'agenzia per la cybersicurezza nazionale (ACN)
Decreto Legge n. 82 del 14 giugno 2021, convertito, con modificazioni, nella Legge n. 109 del 4 agosto 2021


Una minaccia Cyber è asimmetrica per definizione
Uno stesso attacco può portare a diversi scenari
Preventiva
Incidente informatico
Difensiva: cyberdefense
Fatto evento reato
Investigativa
Ha però proiezione di resilienza ACN
Qualunque notizia di incidente informatico è trasmessa al Servizio Polizia postale e comunicazione anche negli obblighi dell'art 331 CPP che obbliga PU alla comunicazione di notizia di reato.
Tanti soggetti che esercitano ognuno per proprio conto la propria competenza
Leggi che non regolano il conflitto di competenza stiamo sperimentando sul campo.
Legge su ACN alle norme finali.

Direttiva NIS 2016/1148

Acronimo di
Network Information Security

Decreto Legislativo 18 maggio 2018, n. 65

Adottate per la prima volta misure organiche per la Cybersecurity
Prevede obblighi sia di notifica degli incidenti aventi un impatto rilevante sulla continuità dei servizi forniti, sia di implementazione di misure di sicurezza basate sull'analisi del rischio per gli Operatori di Servizi Essenziali e i Fornitori di Servizi Digitali.

Attiene al concetto di Operatori di Servizi essenziali ed è connesso alla qualità di mantenimento del Sistema Paese

ISTITUZIONE PERIMETRO SICUREZZA NAZIONALE CIBERNETICA

Decreto-legge 21 settembre 2019, n. 105 (di seguito decreto Perimetro), che ha istituito il Perimetro di sicurezza nazionale cibernetica, con l'obiettivo di tutelare gli asset digitalizzati dal cui malfunzionamento, interruzioni, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio **per la sicurezza nazionale**, prevedendo, rispetto **al decreto NIS, più stringenti criteri di notifica degli incidenti e maggiori livelli di sicurezza, estesi anche alla supply chain, nonché specifiche procedure in materia di procurement ICT ad essi destinati;**

Attiene al concetto di Operatori di Servizi Fondamentali ed è connesso alla Sicurezza Nazionale
Legge 124 del 2007

Legge 18 novembre 2019, n. 133 - Gazzetta Ufficiale

Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54

Procedura di Valutazione dei CVCN e dei CV

DPCM 18 maggio 2022 attuato per l'accreditamento dei laboratori centrali e periferici

1

Definizione criteri di individuazione dei soggetti inclusi nel perimetro

(DPCM n. 131 del 30/07/20)

2

Definizioni delle modalità di comunicazione incidenti beni ICT e adozione delle misure di sicurezza

(DPCM n. 81 del 14/04/21)

3

Individuazione delle categorie dei beni ICT alle quali si intende ricorrere anche tramite le centrali di committenza

(DPCM 15/06/21)

Art. 3 → settori:
interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro.

L’accordo convenzionale tra l’Associazione Nazionale Comuni Italiani ed il Dipartimento della Pubblica Sicurezza per la tutela delle reti e dei sistemi informativi della stessa associazione e delle Pubbliche Amministrazioni Locali, stipulato lo scoro luglio, ha rappresentato il primo atto del più ampio “Progetto PRO-C2SI” – Progetto per la Cyber Sicurezza dei Comuni Italiani, strutturato su due pilastri:

- il primo, dedicato alla tutela diretta delle infrastrutture informatiche dei Comuni con più di 20.000 abitanti, per la prevenzione degli attacchi cibernetici che possano comprometterne il regolare funzionamento;
- il secondo, diretto ad innalzare i livelli di competenza tecnica e di *awareness*, mediante iniziative formative rivolte al quadro direttivo e dirigenziale ed ai tecnici specializzati dei Comuni, attività che sarà oggetto di successivi accordi territoriali ad hoc tra gli ANCI regionali, gli stessi Comuni ed i Centri Operativi Sicurezza Cibernetica della Postale competenti su quei territori

Grazie per l’attenzione

Cristiano LEGGERI
Primo Dirigente della Polizia di Stato
Servizio Polizia Postale e delle Comunicazioni
Direttore 3^ Divisione