POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

REPORT ANNUALE 2025

A TUTELA

dei dati

dei diritti

dell'identità

#essercisempre

POLIZIA

Maggiori Informazioni:
www.commissariatodips.it

Dati aggiornati al 21 dicembre 2025

C3 Combating Cyber Crime

POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

REPORT ANNUALE 2025

A TUTELA

dei dati

dei diritti

dell'identità

#essercisempre

POLIZIA

Maggiori Informazioni:
www.commissariatodips.it

Dati aggiornati al 21 dicembre 2025

C³ *Combating Cyber Crime*

Sommario

Analisi statistica e rielaborazione dati a cura di: Ispettore della Polizia di Stato Gaetano Martucci, Assistente Capo della Polizia di Stato Luigi Ummaro e Agente della Polizia di Stato Valeria Pettirossi

Raccolta dati statistici a cura di: Ispettore della Polizia Gaetano Martucci, Assistente Capo della Polizia di Stato Luigi Ummaro e Agente della Polizia di Stato Valeria Pettirossi

Editing & Grafica a cura di: Ispettore della Polizia di Stato Gaetano Martucci

Copertina a cura di: Ispettore della Polizia di Stato Gaetano Martucci

Coordinatori delle attività: Primo Dirigente della Polizia di Stato Barbara Strappato, Vice Questore della Polizia di Stato Roberta Mestichella, Vice Questore Aggiunto della Polizia di Stato Alessandro Tundo

PREMESSA

***Ivano Gabrielli**, Dirigente Superiore della Polizia di Stato, Direttore del Servizio Polizia Postale e per la sicurezza cibernetica*

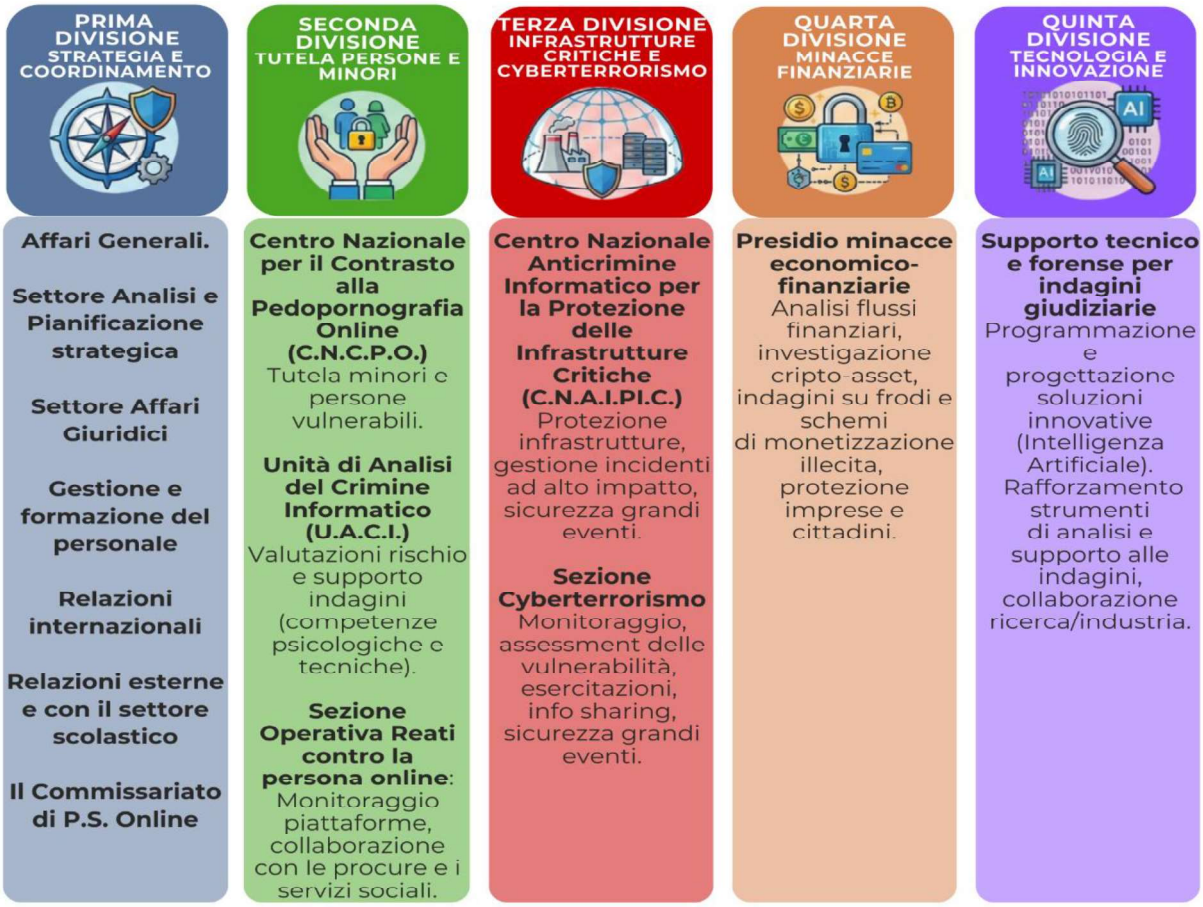
Nel 2025 il panorama della sicurezza cibernetica ha mostrato una crescente complessità: attacchi sofisticati alle infrastrutture critiche, campagne *ransomware*, frodi economico-finanziarie, fenomeni di sfruttamento dei minori e reati contro la persona commessi online che hanno inciso in modo diretto sulla vita dei cittadini e sulla continuità dei servizi essenziali. La rapidità di propagazione degli incidenti e la molteplicità dei vettori d'attacco hanno reso indispensabile un presidio costante, capace di coniugare innovazione tecnologica, competenze investigative e attenzione alla dimensione umana delle vittime.

In questo quadro, la Polizia Postale ha adottato un approccio integrato, articolato su tre direttrici complementari: prevenzione, per ridurre i rischi e diffondere consapevolezza; contrasto investigativo, per interrompere circuiti criminali e assicurare i responsabili alla giustizia; costruzione di competenze, per formare personale altamente qualificato e rafforzare la resilienza collettiva. Ogni intervento è stato concepito non solo per contenere l'emergenza, ma per trasformare l'esperienza operativa in apprendimento e contribuire, insieme agli altri partner istituzionali, al consolidamento della capacità di risposta del sistema Paese.

Il Servizio Polizia Postale e per la Sicurezza Cibernetica, parte integrante della Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica del Dipartimento della Pubblica Sicurezza, è articolato in cinque Divisioni e coordina le attività degli uffici territoriali, costituiti dai Centri

Operativi per la Sicurezza Cibernetica e dalle Sezioni Operative per la Sicurezza Cibernetica con competenza provinciale. Accanto alle funzioni di prevenzione, contrasto e supporto tecnico-scientifico, il Servizio assicura anche il supporto tecnico-logistico, indispensabile per garantire continuità operativa, gestione delle risorse e tempestività di intervento su tutto il territorio nazionale.

ORGANIZZAZIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA



La Prima Divisione svolge un ruolo di governance strategica e di raccordo, coordinando linee operative, programmi formativi e funzioni di presidio. Al suo interno è incardinato il Commissariato di P.S. Online, punto di contatto diretto con i cittadini per segnalazioni, orientamento delle vittime e diffusione di alert. La Divisione si avvale del Settore personale, del Settore rapporti con gli uffici territoriali della specialità, Settore Formazione del Personale, del Settore Affari Giuridici, del Settore Relazioni Internazionali e del Settore Analisi e Pianificazione Strategica. Anche nel 2025 ha promosso campagne di sensibilizzazione, rafforzato la cooperazione con enti pubblici e privati e sviluppato strumenti di analisi strategica a supporto delle decisioni operative.

La Seconda Divisione, attraverso il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.), ha mantenuto un impegno costante nella tutela dei minori e delle persone vulnerabili. Il Settore dedicato ai reati contro la persona commessi online ha intensificato il monitoraggio delle piattaforme digitali e consolidato protocolli di collaborazione con procure e servizi sociali, mentre l'Unità di Analisi del Crimine Informatico ha integrato competenze psicologiche e tecniche per fornire valutazioni di rischio e supporto alle indagini per un'efficace azione di contrasto strategico.

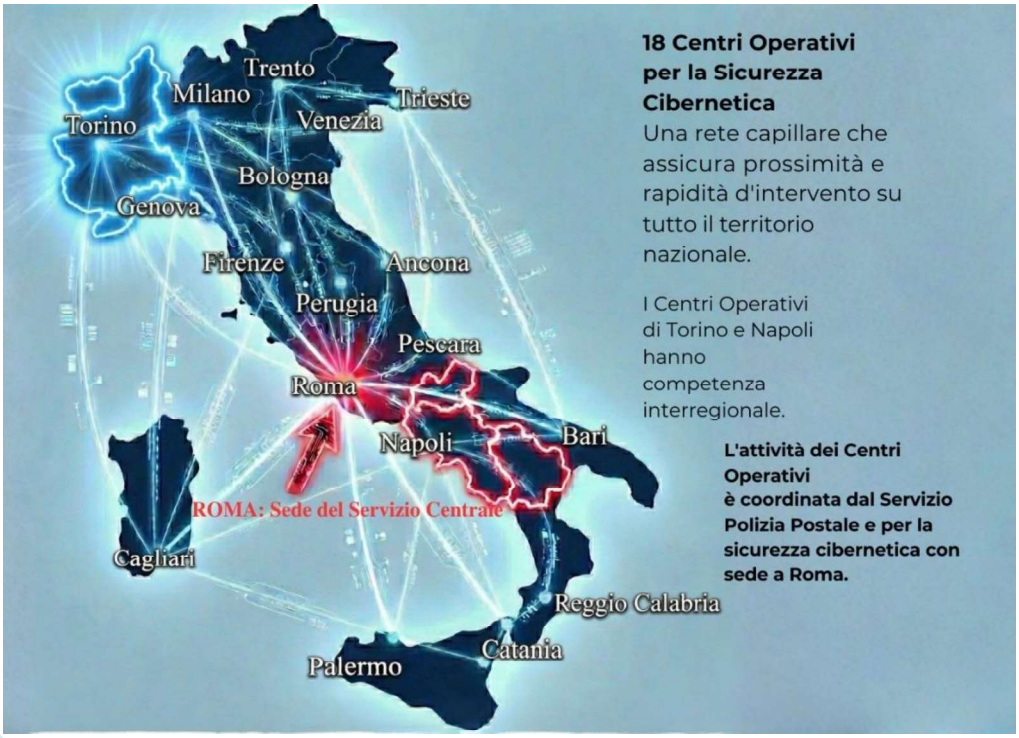
La Terza Divisione ha garantito un presidio essenziale per la sicurezza degli asset nazionali. Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), di cui quest'anno si è celebrato il ventennale dalla sua istituzione, ha operato per assicurare la resilienza delle infrastrutture critiche e la protezione dei grandi eventi, mentre la Sezione Cyberterrorismo ha fronteggiato le sfide poste dalle moderne minacce ibride: in un contesto segnato da forti tensioni geopolitiche, l'attività di intelligence ha permesso di intercettare le derive del radicalismo digitale e dell'hacktivismo ideologico attraverso un lavoro di anticipazione che ha consentito di individuare percorsi eversivi e neutralizzare campagne ostili prima che potessero tradursi in azioni violente.

La Quarta Divisione ha presidiato le minacce economico-finanziarie, sviluppando competenze di analisi dei flussi e investigazione su cripto-asset. Nel 2025 ha condotto indagini su circuiti di frode e schemi di monetizzazione illecita, supportando procure e proteggendo imprese e cittadini.

La Quinta Divisione ha garantito il supporto tecnico e forense indispensabile per rendere le indagini efficaci e utilizzabili in sede giudiziaria. Nel 2025 ha orientato la propria attività verso la programmazione e la progettazione di soluzioni innovative, con particolare attenzione alle tecnologie

di intelligenza artificiale, rafforzando gli strumenti di analisi e di supporto alle indagini in collaborazione con centri di ricerca e partner industriali.

Un ulteriore tassello strategico nel 2025 è stato l'avvio del corso di formazione tecnico-professionale per la nomina alla qualifica di Vice Ispettore Tecnico della Polizia di Stato – settore sicurezza cibernetica, inaugurato a settembre presso il Centro Addestramento della Polizia di Stato di Cesena alla presenza del Capo della Polizia – Direttore Generale della Pubblica Sicurezza. Il percorso, che si concluderà nel giugno 2026, rappresenta un momento qualificante per la formazione specialistica del personale, fornendo competenze avanzate in materia di investigazioni digitali, analisi forense e protezione delle infrastrutture critiche. L'investimento nella formazione degli ispettori tecnici cyber contribuisce a consolidare il presidio istituzionale e a garantire un livello elevato di professionalità nelle attività di prevenzione e contrasto, favorendo al contempo uniformità di metodo e coerenza operativa su tutto il territorio nazionale.



La rete territoriale, composta dai 18 Centri Operativi per la Sicurezza Cibernetica e dalle 82 Sezioni Operative per la Sicurezza Cibernetica, ha assicurato prossimità e rapidità d'intervento.

Anche nel 2025 gli uffici territoriali hanno intercettato segnali deboli,

intesi come indicatori precoci e frammentari di possibili minacce informatiche – accessi anomali, comportamenti sospetti o variazioni nei flussi di rete – che hanno permesso di anticipare l'evoluzione degli attacchi e attivato la prima risposta agli incidenti, trasformando le strategie nazionali in interventi concreti e tempestivi.

La cooperazione internazionale e il partenariato pubblico–privato hanno ampliato la capacità di prevenire, contenere e ripristinare, attraverso lo scambio di indicatori e la conduzione di operazioni congiunte, gli eventi cyber ostili.

Nel 2025, con riferimento ai dati consolidati al 21 dicembre, l'attività della Polizia Postale e per la Sicurezza Cibernetica si è sviluppata su scala nazionale con un impegno operativo continuo e ad alta intensità. Nel periodo di riferimento sono stati trattati 51.560 casi, con 293 arresti, 7.590 persone denunciate e 2.157 perquisizioni, delineando un'azione investigativa strutturata, capillare e costantemente orientata alla gestione di fenomeni complessi.

Il cybercrime di matrice economico-finanziaria ha confermato il proprio ruolo centrale in termini di volumi operativi, con 27.085 procedimenti trattati e somme sottratte superiori a 269 milioni di euro, evidenziando la capacità delle organizzazioni criminali di operare attraverso ecosistemi digitali articolati e dinamiche transnazionali. In parallelo, sono stati gestiti 9.250 eventi di computer crime rivolti a infrastrutture critiche, soggetti pubblici, aziende e privati, a testimonianza di una pressione costante sul perimetro cibernetico nazionale.

Resta elevata l'attenzione verso i reati contro la persona commessi online, che hanno fatto registrare 9.564 casi, così come l'impegno nel contrasto alla pedopornografia e all'adescamento di minori, ambito nel quale sono stati trattati 2.574 procedimenti, con un numero particolarmente significativo di arresti e perquisizioni.

Le attività condotte nel corso dell'anno hanno prodotto risultati rilevanti in termini di contrasto operativo e tutela delle vittime: indagini complesse su reti criminali transnazionali, interventi mirati su fenomeni di frode e monetizzazione illecita, azioni di rimozione e oscuramento di contenuti illegali. Ogni intervento ha richiesto l'integrazione di competenze investigative, capacità tecnico-forensi e cooperazione internazionale, confermando la centralità di un approccio multidisciplinare nella gestione delle minacce cibernetiche.

Accanto alle attività di contrasto, il Servizio ha rafforzato il proprio ruolo sul versante preventivo e formativo, promuovendo iniziative di sensibilizzazione che hanno coinvolto migliaia di istituti scolastici e centinaia di migliaia di studenti, docenti e genitori, confermando la prevenzione come leva strategica per accrescere la consapevolezza digitale della collettività.

Per il futuro le priorità restano il rafforzamento della formazione specialistica, lo studio di quadri normativi anche in chiave di presidio di pubblica sicurezza, il potenziamento delle capacità di analisi e l'uso efficace e responsabile delle potenzialità offerte dall'intelligenza artificiale. Consolidare le alleanze internazionali e investire in ricerca e sviluppo sono condizioni necessarie per anticipare le evoluzioni della minaccia e garantire la tutela dei diritti fondamentali.

LA PRIMA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Barbara Strappato, *Primo Dirigente della Polizia di Stato, Direttore*

Il 2025 ha confermato la Prima Divisione come cuore strategico della Specialità, orientando le risorse per rendere l'azione della Polizia Postale incisiva e coerente su tutto il territorio nazionale. La linea di indirizzo seguita ha avuto risultati tangibili, rafforzando allo stesso tempo la continuità di visione strategica e la capacità di risposta delle articolazioni territoriali.

© Polizia Postale – Report annuale 2025 – Aggiornamento 21/12/2025

Al 21 dicembre 2025, l'attività del Commissariato di P.S. online ha confermato il suo ruolo fondamentale quale presidio quotidiano della rete, agendo come uno dei punti di contatto privilegiato tra istituzioni e cittadinanza. La dimensione dell'impegno profuso emerge con chiarezza dai dati raccolti tramite il portale istituzionale www.commissariatodips.it, che ha gestito un flusso di oltre trentaduemila segnalazioni di phishing e un volume pressoché identico di denunce relative all'area dei social network, affiancate da più di trentamila segnalazioni di attacchi informatici. In ambiti di estrema criticità per la sicurezza pubblica, l'azione del Commissariato ha permesso di istruire oltre duemilacinquecento casi legati alla pedopornografia online e più di mille segnalazioni riconducibili all'area antiterrorismo. Ogni istanza pervenuta è stata sottoposta a un processo di analisi che ha consentito di gestire le emergenze o di inoltrare le pratiche verso i settori investigativi competenti, garantendo una risposta tempestiva e un raccordo costante con le articolazioni specializzate della Specialità. A questa attività di analisi si affianca un'importante presenza digitale, testimoniata da 5,2 milioni di visite al sito con quasi 76 milioni di pagine consultate, che hanno generato oltre venticinquemila richieste di informazioni e reso necessari 232 interventi diretti di soccorso pubblico. L'efficacia della prevenzione è stata inoltre supportata dalla diramazione di 26 alert a tutela della collettività, trasformando il dialogo continuo con l'utenza in un patrimonio di informazioni operative essenziale per intercettare tempestivamente le nuove tendenze del cybercrime e consolidare il legame di fiducia con il cittadino.

La gestione del capitale umano, curata dal settore personale e servizi, ha rappresentato un elemento essenziale per la tenuta organizzativa dell'intera struttura, consentendo di valorizzare competenze e garantire equilibrio tra stabilità e flessibilità operativa.

Su un piano complementare, il settore archivio ha assicurato la conservazione e la valorizzazione della memoria documentale: la digitalizzazione progressiva e l'aggiornamento degli archivi hanno trasformato un patrimonio di atti e informazioni in un supporto concreto alle attività investigative e alla pianificazione strategica.

In un'ottica di costante aggiornamento professionale, il settore formazione ha proseguito nella predisposizione di corsi specialistici in ambito OSINT, cyber security e tutela dei minori online, contribuendo in modo significativo all'elevazione del livello tecnico-operativo del personale. In particolare, sono attivi i percorsi "Analista di fonti aperte (OSINT e SOCMINT)", "Incident Responder" e "Child Sexual Exploitation Operator", strutturati per rispondere alle esigenze emergenti

del contrasto al crimine informatico e alla protezione dei minori in rete. Particolarmente significativo è stato l'avvio, a settembre 2025, del corso per vice ispettori tecnici nel settore d'impiego della sicurezza cibernetica, che si completerà a giugno 2026. Un momento storico, che ha segnato l'ingresso di nuove figure professionali nella Polizia di Stato, capaci di sviluppare competenze specialistiche e di lavorare in squadra su indagini digitali sempre più complesse.

Il settore affari giuridici ha accompagnato ogni scelta operativa con pareri puntuali, assicurando la piena conformità alle normative nazionali ed europee e consolidando la credibilità istituzionale del Servizio. Sul piano internazionale, i rapporti con Europol e con le altre forze di polizia estere si sono ulteriormente rafforzati. La partecipazione a progetti innovativi, come STARLIGHT, dedicati al ruolo dell'intelligenza artificiale nella prevenzione e nel contrasto del crimine informatico, ha dato nuova linfa alla cooperazione. A questo si sono aggiunti momenti di confronto con delegazioni straniere incontrate presso gli uffici centrali e territoriali della Specialità, che hanno sancito il riconoscimento del modello italiano come punto di riferimento nella lotta al cybercrime.

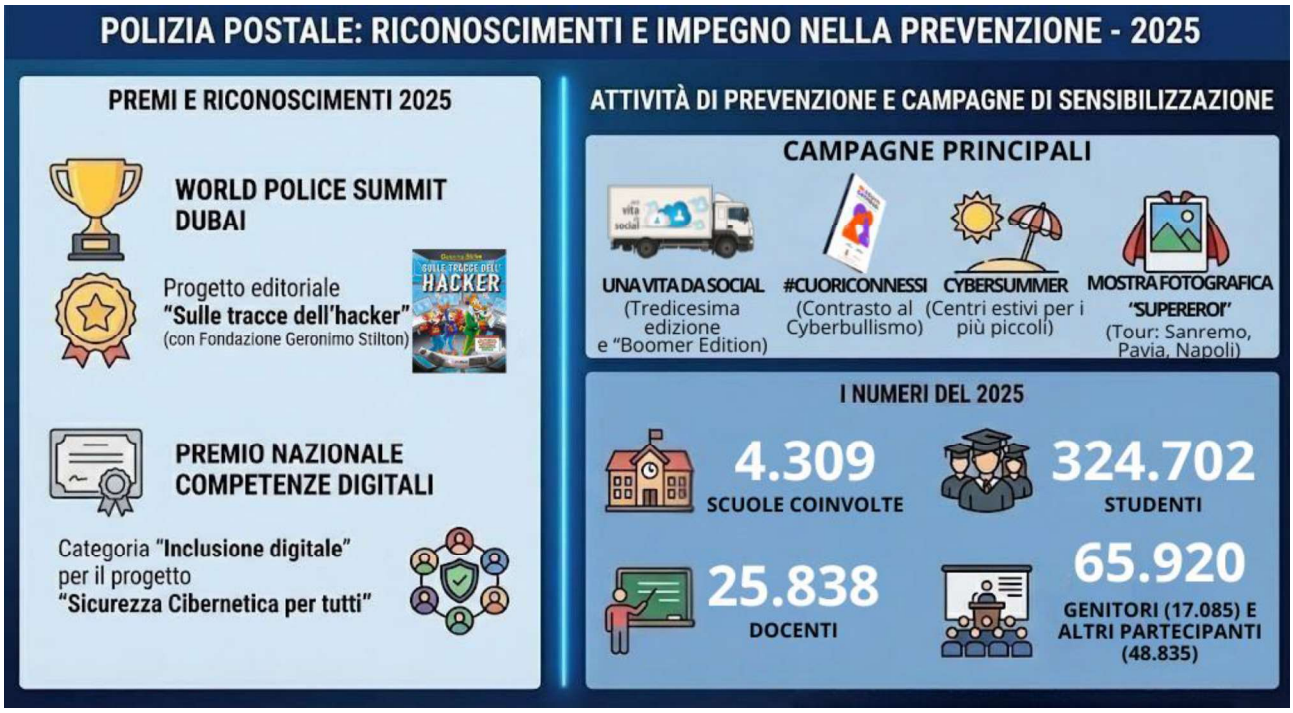
La prevenzione ha trovato voce attraverso campagne di sensibilizzazione di vasta portata, coordinate dal settore Relazioni Esterne e capaci di raggiungere minori e adulti con iniziative diversificate. Tra queste, "Una Vita da Social", giunta alla tredicesima edizione, ha portato il messaggio della sicurezza digitale nelle scuole e a bordo del truck istituzionale, affiancata dalla versione *boomer edition* che ha coinvolto genitori, insegnanti e adulti.

All'iniziativa #Cuoriconnessi, che dal 2016 affronta il tema del cyberbullismo con contenuti dedicati e riflessioni sul valore delle parole online, si è aggiunta Cybersummer, in cui gli operatori hanno incontrato i bambini nei centri estivi, preparandoli a navigare in sicurezza. Nel 2025 è proseguito anche il viaggio della mostra fotografica "Supereroi – Proteggiamo i bambini insieme", con tappe a Sanremo, Pavia e Napoli, arricchite da momenti di approfondimento per studenti e visitatori.

A conferma dell'impegno, la Polizia Postale ha ottenuto due importanti riconoscimenti: al World Police Summit di Dubai per il progetto editoriale *"Sulle tracce dell'hacker"*, realizzato con la Fondazione Geronimo Stilton, e il Premio Nazionale per le Competenze Digitali nella categoria "Inclusione digitale" con il progetto *"Sicurezza Cibernetica per tutti"*.

Complessivamente, le attività di prevenzione hanno coinvolto 4.309 scuole, 324.702 studenti, 25.838 docenti, 17.085 genitori e altri 31.858 partecipanti in incontri scolastici, seminari e convegni dedicati alla cultura della sicurezza online.

Parallelamente, il settore analisi e pianificazione strategica ha elaborato indicatori e scenari previsionali che hanno guidato le priorità investigative, trasformando i dati in insight capaci di anticipare minacce emergenti.



L'azione del settore rapporti con le articolazioni territoriali della Polizia Postale, sostenuta dalla storica ed efficace collaborazione con Poste Italiane, ha assicurato un legame costante con le realtà locali. Questo collegamento diretto ha permesso di cogliere tempestivamente i bisogni quotidiani, dalle risorse umane alle infrastrutture, e di trasformarli in interventi concreti, fondamentali per garantire la continuità e la solidità dell'azione della Specialità su scala nazionale.

ln questo quadro, il settore automezzi ha assicurato la piena efficienza delle autovetture in dotazione, curando manutenzione e rinnovo dei veicoli. Questo presidio logistico ha consentito agli operatori di raggiungere con tempestività ogni realtà locale, rafforzando la continuità operativa e garantendo una risposta pronta e adeguata alle esigenze del territorio.

Il bilancio del 2025 dimostra come la Prima Divisione abbia saputo integrare competenze diversificate in un sistema coeso. Ogni settore è riuscito a operare, in perfetta complementarità con gli altri, conservando la propria specificità. Le analisi strategiche hanno fornito la mappa per orientare gli interventi; la formazione ha preparato le persone a leggerla e tradurla in azione; la comunicazione ne ha amplificato il messaggio preventivo; il supporto giuridico ne ha consolidato le fondamenta. Il Commissariato online e i rapporti territoriali hanno fatto confluire le diverse segnalazioni nel circuito dell'analisi, implementando nuovi cicli di formazione e prevenzione. La dimensione internazionale ha arricchito questo ecosistema, importando ed esportando best practices che hanno costantemente raffinato il modello operativo.

Il vero valore aggiunto del 2025 è stata la collaborazione tra i settori che ha permesso di trasformare le differenze in ricchezza operativa, dimostrando come la forza di un'organizzazione complessa risieda nella capacità di unire le diverse componenti attraverso una visione condivisa e una responsabilità diffusa, consentendo la creazione di un presidio di sicurezza nazionale capace di trasformare le sfide in opportunità.

IL CASO: ALLARME ALL'ALBA - SALVATO UN MINORE VITTIMA DI ESTORSIONE SESSUALE ONLINE

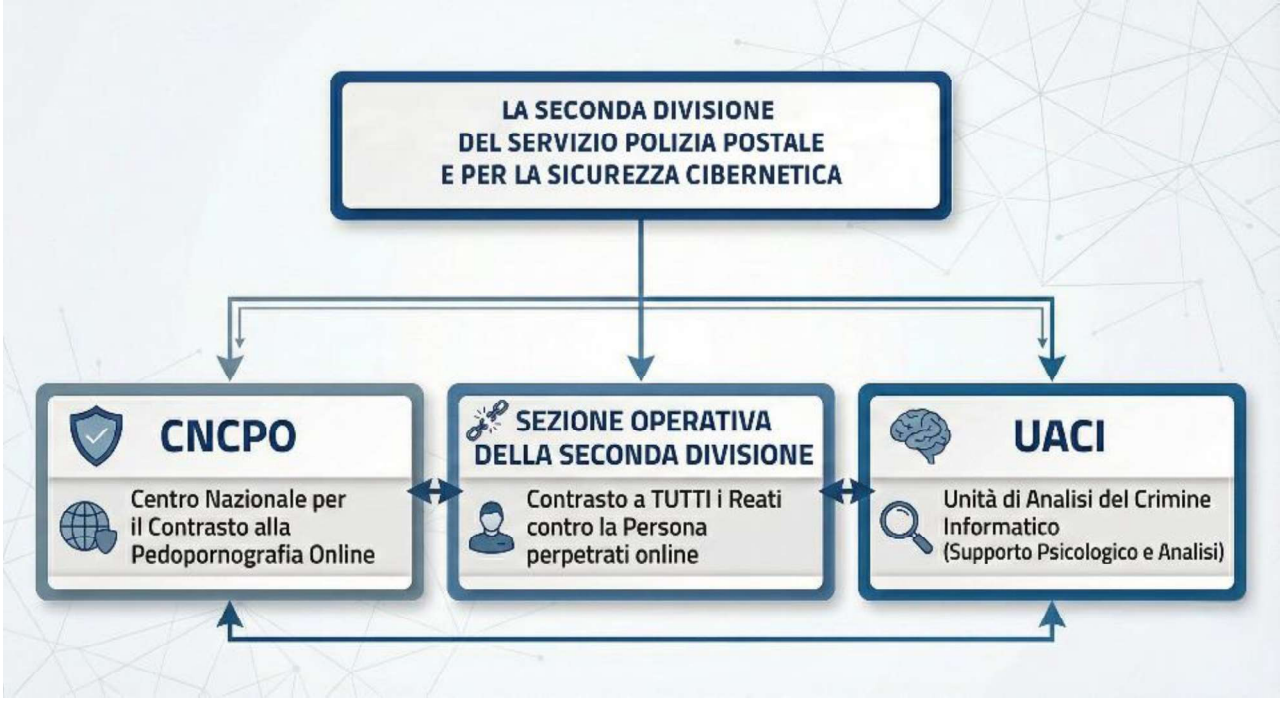
All'alba di una mattina di novembre 2025, una richiesta di aiuto arrivata sul portale del Commissariato di PS Online ha fatto scattare un intervento urgente per soccorrere un minore vittima di estorsione sessuale online. Il giovane, in forte agitazione, riferiva che un soggetto lo minacciava di diffondere le sue immagini intime in cambio di denaro. Il tono dei messaggi e la crescente disperazione del minore hanno immediatamente fatto temere agli operatori la possibilità di un gesto che potesse mettere a rischio la sua incolumità. Il personale del Commissariato ha stabilito un contatto diretto e continuativo con il giovane, attivando l'Unità di Analisi del Crimine Informatico per garantire il supporto specialistico nella gestione emotiva e operativa del caso. Le comunicazioni, mantenute senza interruzioni, hanno permesso di monitorare lo stato d'animo del minore e valutare l'urgenza della situazione. Quando il minore ha riferito di volersi spostare verso una struttura pubblica, gli operatori hanno avviato una rapida attività di analisi su fonti aperte per individuare il

luogo indicato e predisporre l'invio di personale. L'intervento, coordinato dal Commissariato di PS Online, si è svolto con particolare attenzione alla salvaguardia del giovane, che è stato raggiunto e messo in sicurezza. Poco dopo un familiare giunto sul posto, ha contribuito a rasserenarlo e riportarlo in un contesto protetto. L'episodio, gestito fino al primo pomeriggio, conferma l'impegno quotidiano del Commissariato di PS Online nella tutela delle persone più vulnerabili e nella gestione dei reati digitali, rappresentando solo uno dei tantissimi casi che ogni giorno l'ufficio si trova ad affrontare e gestire con professionalità e tempestività.

LA SECONDA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Maria Rosaria Romano, *Primo Dirigente della Polizia di Stato, Direttore*

La Seconda Divisione costituisce il fulcro strategico della Polizia Postale dedicato alla protezione delle vittime più vulnerabili e alla salvaguardia dei diritti fondamentali nel cyberspazio. In uno scenario in cui l'evoluzione tecnologica ridefinisce costantemente le modalità di interazione sociale, la Divisione adotta un approccio olistico che non si limita alla repressione, ma integra investigazione tecnologica, cooperazione internazionale e analisi criminologica. La missione di garantire una risposta istituzionale adeguata alla complessità delle minacce online si realizza attraverso la sinergia di tre articolazioni specialistiche.



Il C.N.C.P.O. rappresenta l'anima istituzionale e di coordinamento nella lotta globale allo sfruttamento sessuale dei minori, mentre la Sezione Operativa funge da presidio investigativo trasversale per l'intero spettro dei reati contro la persona; quest'ultima non si limita a singole

fattispecie, ma interviene su ogni forma di aggressione alla sfera individuale, dal cyberstalking alla sostituzione di persona, fino alle minacce e alla diffusione illecita di immagini intime. A completare il quadro interviene l'U.A.C.I., che fornisce il supporto scientifico, psicologico e analitico indispensabile per tutelare le vittime e gli operatori coinvolti in indagini ad alto impatto emotivo, coniugando così l'elevata specializzazione tecnica con una profonda attenzione al fattore umano.

Il Centro Nazionale per il Contrasto alla Pedopornografia Online

Il contrasto allo sfruttamento online dei minori in tutte le sue forme costituisce una priorità strategica per la Polizia di Stato e impone una costante analisi delle nuove minacce, l'adozione di strumenti tecnologici avanzati e un approccio operativo coerente con l'evoluzione dei mezzi di comunicazione, al fine di favorire nuove modalità di conoscenza e di interazione sociale.

Nel tempo, le competenze della Specialità in materia di protezione dei minori si sono progressivamente ampliate grazie all'introduzione di specifiche disposizioni normative volte a

rafforzare il sistema di tutela, estendendo l'azione anche a nuovi ambienti digitali e servizi online, nei quali si registra una presenza sempre più precoce di minori, spesso in assenza di un'adeguata supervisione adulta.

Il Servizio Polizia Postale e per la Sicurezza Cibernetica, quale articolazione del Ministero dell'Interno, esercita competenze istituzionali esclusive sancite dalla normativa istitutiva del Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO), organismo deputato alla prevenzione e repressione dei reati connessi allo sfruttamento sessuale dei minori in rete (legge 6 febbraio 2006, n. 38). Tali attribuzioni sono state ulteriormente estese dal decreto del Ministro dell'Interno del 15 agosto 2017, recante la Direttiva sui comparti di specialità delle Forze di Polizia e sulla razionalizzazione dei presidi di polizia. In un'ottica di prevenzione e contrasto alle molteplici forme di abuso online, il legislatore è intervenuto con ulteriori provvedimenti a tutela dei minori (come la legge 29 maggio 2017, n. 71 sul cyberbullismo, successivamente modificata dalla legge 17 maggio 2024, n. 70), finalizzati alla creazione di una rete coordinata di interventi in grado di offrire un sostegno rapido ed efficace alle vittime.

Per l'espletamento di tali funzioni, il Servizio si avvale di sofisticate metodologie investigative, assicurando al contempo il coordinamento internazionale con le polizie straniere, oltre al supporto operativo e al coordinamento dei 18 Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.) e delle 82 Sezioni Operative (S.O.S.C.) presenti sul territorio nazionale. In attuazione dell'art. 19 della legge n. 38/2006, che attribuisce al CNCPO la competenza esclusiva nella raccolta di tutte le segnalazioni – provenienti anche da autorità estere e da soggetti pubblici e privati – relative alla presenza di contenuti pedopornografici online, nel corso del 2025 sono state rafforzate le collaborazioni con numerose associazioni impegnate nella tutela dei minori, secondo una logica di partenariato pubblico-privato. Tra queste figurano *Telefono Azzurro*, *Save The Children, Terres Des Hommes, Operation Underground Railroad Rescue*, *National Centre for Missing and Exploited Children, Child Rescue Coalition (C.R.C.),* l'*Associazione Meter* di don Fortunato Di Noto e la *Comunità di Sant'Egidio*.

La Polizia Postale partecipa inoltre a numerosi tavoli interistituzionali dedicati alla protezione dell'infanzia, tra cui *l'Osservatorio Nazionale per l'Infanzia e l'Adolescenza* e l'*Osservatorio per il Contrasto della Pedofilia e della Pornografia Minorile*, presso il Dipartimento per le politiche della

Famiglia, il *Comitato Interministeriale per l'Alfabetizzazione Mediatica e Digitale*, presso il Ministero delle Imprese e Made in Italy nonché al Tavolo Tecnico per la prevenzione e il contrasto del bullismo e del cyberbullismo ai sensi della legge 29 maggio 2017, n. 71 sul cyberbullismo, successivamente modificata dalla legge 17 maggio 2024, n. 70 confermando la necessità di un approccio integrato per affrontare fenomeni caratterizzati da elevata complessità.

Tenuto conto della dimensione transnazionale dei reati in esame, è stato potenziato lo scambio informativo attraverso i canali di Europol e Interpol, al fine di favorire un'azione coordinata a livello nazionale tra gli Uffici della Polizia Postale e per la Sicurezza Cibernetica volta all'individuazione degli autori dei reati e alla protezione delle vittime.

Nel corso del 2025, il Centro ha fornito un contributo attivo, per conto del Ministero dell'Interno, alla definizione della proposta di Regolamento europeo in materia di prevenzione e contrasto dell'abuso sessuale sui minori, che prevede, tra l'altro, un rafforzamento delle misure nell'attività di rilevazione dei contenuti per i fornitori di servizi di connettività nella rilevazione dei contenuti pedopornografici. Il CNCPO ha fornito contributi tecnici fondati anche sull'esperienza operativa maturata nella gestione delle attività operative al fine di orientare la predisposizione di un testo normativo adeguato al raggiungimento degli obiettivi di prevenzione e contrasto in un'ottica di equilibrio tra la tutela della riservatezza delle comunicazioni e le esigenze investigative delle forze dell'ordine.

Il Centro ha inoltre preso parte a molteplici tavoli di lavoro di carattere internazionale, tra cui il gruppo G7 per il contrasto alla pedopornografia nell'ambito dell'*High Tech Crimes* Sub-Group e il sottogruppo *G7 Law Enforcement Practitioners*, promuovendo iniziative volte al rafforzamento dei canali di cooperazione di polizia per la protezione dei minori.

Nell'ambito della cooperazione operativa internazionale, il CNCPO ha partecipato a rilevanti meeting e task force, quali la *Victim Identification Task Force*, finalizzata all'identificazione delle vittime e degli autori di abusi, la *High Value Targets Task Force*, orientata alla deanonimizzazione delle comunità pedofile attive nel dark web e il *Global Covert Internet Investigations Meeting,* occasione di confronto tra investigatori di diversi Paesi sulle tecniche investigative sotto copertura e sulle migliori prassi operative.

Nel 2025, l'azione di contrasto alla diffusione di contenuti illeciti online si è concentrata sul rafforzamento delle attività di monitoraggio dei siti web che veicolano materiale CSAM, tramite l'Area Operativa "Black List" del CNCPO. Tale attività ha consentito la sorveglianza di **16.549 siti segnalati** e l'**inserimento di 2.876** di essi nella relativa lista di blocco.

L'individuazione delle vittime rappresenta un obiettivo prioritario ed è affidata a una specifica unità investigativa che, in conformità agli standard internazionali, analizza e gestisce i file multimediali illeciti mediante l'accesso alla banca dati I.C.S.E. (International Child Sexual Exploitation Database) di Interpol, alimentata dalle segnalazioni delle forze di polizia di tutto il mondo.

A tale comparto confluiscono anche le informazioni trasmesse dall'Unità di Informazione Finanziaria (U.I.F.) della Banca d'Italia, relative a operazioni sospette riconducibili al commercio di materiale pedopornografico online, utili per finalità di approfondimento investigativo.

Grazie agli strumenti normativi che consentono lo svolgimento di attività sotto copertura sul web, sono state realizzate operazioni nel Deep Web e nel Dark Web per contrastare lo sfruttamento sessuale dei minori attraverso i sistemi informatici. Gli uffici territoriali hanno beneficiato del supporto tecnico-investigativo del CNCPO, che ha operato in stretta collaborazione con le agenzie estere per lo scambio di informazioni, buone prassi e la gestione di operazioni internazionali sotto copertura.

Il contrasto ai reati di pedopornografia e di adescamento di minorenni online si colloca in un contesto caratterizzato da una costante evoluzione delle modalità di commissione dei reati, favorita dalla diffusione capillare delle piattaforme digitali, dei sistemi di messaggistica istantanea e, in taluni casi, dall'utilizzo di ambienti tecnologici più opachi, quali le *darknet*. In tale scenario, l'azione della Polizia Postale è chiamata a coniugare capacità di prevenzione, attività di intelligence e incisività repressiva.

Alla data del 21 dicembre 2025, l'attività di contrasto ai reati informatici a danno di minori si inserisce in un contesto digitale caratterizzato da elevata complessità operativa e da modalità criminali sempre più strutturate, che richiedono interventi specialistici e mirati.

Nel periodo considerato, i casi trattati in materia di pedopornografia e adescamento online risultano pari a 2.574. L'azione repressiva ha condotto all'arresto di 222 soggetti, nell'ambito di procedimenti investigativi che hanno previsto anche numerose perquisizioni e la denuncia di ulteriori persone coinvolte.

L'attività di monitoraggio dei contenuti illeciti ha interessato circa 16.500 siti presenti nel web in chiaro. Le indagini si sono inoltre concentrate su ambienti digitali complessi, comprendenti aree della rete non indicizzate e piattaforme caratterizzate dall'utilizzo di sistemi di cifratura, che richiedono specifiche competenze tecniche e investigative.

Nel complesso, i dati rilevati al 21 dicembre 2025 delineano un quadro operativo in cui l'azione di prevenzione e contrasto si sviluppa attraverso interventi mirati, fondati su attività investigative specialistiche e su un costante adattamento alle caratteristiche del contesto digitale.

ADESCAMENTO ONLINE

Nell'anno 2025, l'adescamento online si conferma un fenomeno di preoccupante vitalità, con un totale di 428 casi trattati.

L'analisi demografica delle vittime delinea uno scenario netto: il rischio si concentra in modo massiccio sulla fascia adolescenziale. I dati indicano che i predatori digitali focalizzano i propri sforzi principalmente sui minori di età compresa tra i 14 e i 16 anni, che con 237 casi rappresentano la maggioranza assoluta delle vittime (55% del totale).

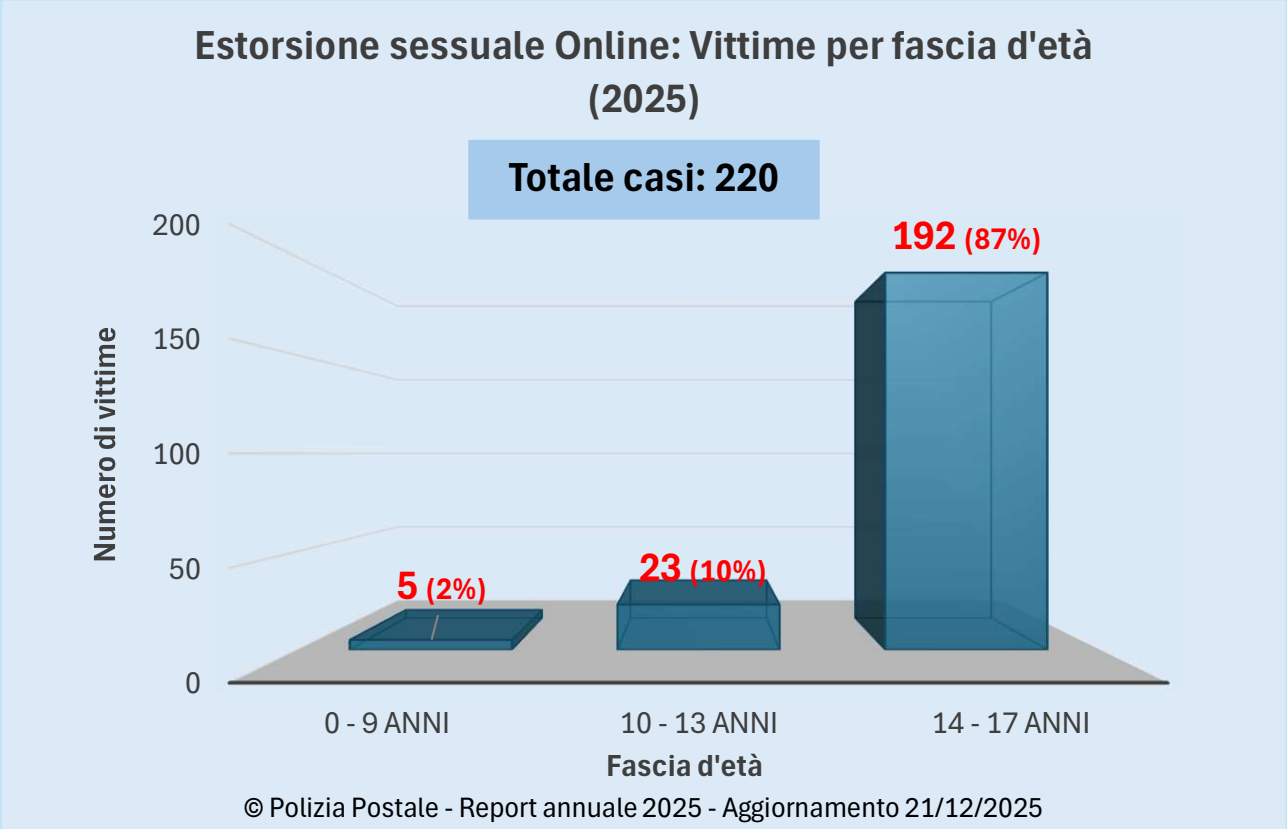
Seguono i preadolescenti (10-13 anni) con 174 casi, mentre la fascia dei più piccoli (0-9 anni) registra 17 episodi. Questo quadro evidenzia come gli adolescenti, sebbene spesso considerati più autonomi nell'uso della rete, si rivelino il target primario di manipolazioni emotive complesse da parte degli adescatori

ESTORSIONE SESSUALE

Nel 2025, l'estorsione sessuale online con vittime minorenni si è imposta come una delle minacce più gravi nel panorama dei reati digitali contro i minori, con 220 casi trattati. Il fenomeno si manifesta attraverso dinamiche di ricatto emotivo e coercizione, spesso innescate dalla condivisione di contenuti intimi in ambienti digitali apparentemente protetti.

La fascia d'età più colpita è quella degli adolescenti tra i 14 e i 17 anni, che rappresentano 192 vittime, pari all'87% del totale. Questo dato evidenzia una vulnerabilità specifica legata all'autonomia digitale, alla ricerca di relazioni online e alla difficoltà nel riconoscere situazioni manipolatorie.

Anche i minori più giovani non sono immuni: si registrano 23 casi tra i preadolescenti (10–13 anni) e 5 casi nella fascia 0–9 anni. Questi numeri, pur contenuti, indicano un abbassamento della soglia di età del rischio, che impone una vigilanza costante e interventi educativi precoci.



L'estorsione sessuale online non è solo un reato: è una forma di violenza invisibile che agisce nel silenzio delle relazioni digitali, sfruttando fragilità emotive e meccanismi di fiducia.

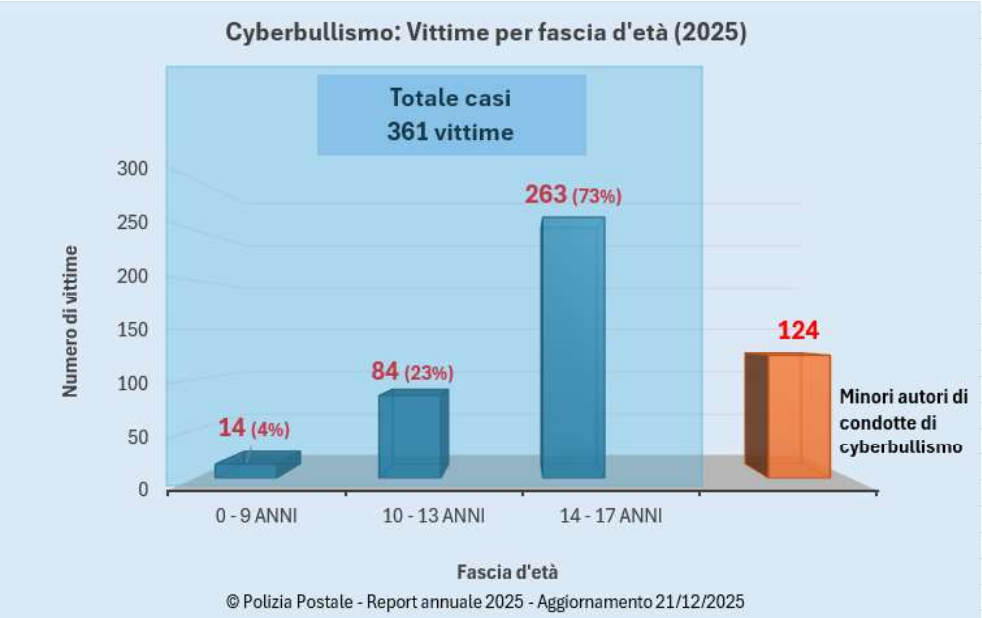
CYBERBULLISMO

Nel 2025, il cyberbullismo ha rappresentato una componente rilevante delle condotte illecite commesse in ambiente digitale da e contro minori, con 361 casi trattati.

Il fenomeno comprende una varietà di comportamenti ostili veicolati attraverso piattaforme online, caratterizzati da continuità, ripetitività e impatto sulla sfera relazionale dei giovani utenti.

L’analisi delle fasce d’età coinvolte mostra una prevalenza significativa tra gli adolescenti tra i 14 e i 17 anni, che risultano maggiormente esposti a dinamiche di conflitto, imitazione e pressione del gruppo dei pari. Una quota rilevante di episodi riguarda anche i preadolescenti tra i 10 e i 13 anni, fascia in cui le interazioni digitali si intrecciano con dinamiche scolastiche e di gruppo.

Più contenuti, ma comunque presenti, i casi che coinvolgono minori sotto i 10 anni, indicativi di un’esposizione precoce agli ambienti digitali e della necessità di un accompagnamento educativo adeguato. Un elemento di rilievo riguarda il ruolo attivo dei minori come autori delle condotte: nel 2025 sono state registrate 124 denunce a carico di minorenni per episodi di cyberbullismo. Questo dato conferma la natura relazionale del fenomeno, che si sviluppa all’interno dei gruppi dei pari e richiede interventi educativi mirati alla responsabilità digitale.



Il quadro complessivo evidenzia un fenomeno articolato, che intreccia dinamiche emotive, sociali e tecnologiche. La tutela dei minori nello spazio digitale richiede un approccio integrato, fondato sulla protezione delle vittime, sulla responsabilizzazione degli autori e sulla promozione di una cultura della cittadinanza digitale consapevole.

IL CASO: OPERAZIONE 'STREAM'

La Procura Distrettuale di Napoli ha coordinato una vasta operazione nazionale contro lo sfruttamento sessuale dei minori online avviata dal CNCPO con la collaborazione del COSC Campania. Sono state tratte in arresto 4 persone e indagate 15 per detenzione di ingente materiale pedopornografico, con il sequestro di numerosi *wallet* di criptovalute, nonché dispositivi informatici contenenti decine di migliaia di *file* illegali. L'operazione ha visto il coinvolgimento nella fase esecutiva dei C.O.S.C. della Lombardia, Lazio, Piemonte, Toscana, Emilia-Romagna, Puglia, Veneto e Sardegna nell'esecuzione di 15 decreti di perquisizione delegati dalla Procura della Repubblica di Napoli. La cooperazione con il collaterale tedesco nell'ambito di una più ampia operazione coordinata da Europol e le complesse analisi delle *blockchain* hanno permesso di identificare i soggetti che hanno effettuato diversi pagamenti in *criptovaluta* per accedere alla piattaforma nel *Dark web* denominata "KidFlix" - nome che si ispira alla nota piattaforma di contenuti *on-demand Netflix* - utilizzata per la riproduzione *on-demand* di contenuti multimediali a carattere pedopornografico raggruppati per categorie. Grazie al coordinamento di Europol, l'operazione ha potuto garantire un'efficace cooperazione transfrontaliera tra le forze dell'ordine di oltre 35 Paesi tra cui Germania, Italia, Stati Uniti, Regno Unito, Francia, Spagna, Canada con la chiusura della piattaforma e l'identificazione di quasi 1.400 sospettati a livello globale.

La Sezione Operativa della Seconda Divisione

Negli ultimi anni, la rivoluzione digitale ha profondamente trasformato la morfologia dei reati contro la persona. Lo spazio virtuale non è più soltanto un mezzo di comunicazione: è diventato un vero e proprio teatro di conflittualità, dove la violenza fisica cede il passo a forme di aggressione psicologica e sociale altrettanto pervasive e devastanti.

Il fenomeno dei cosiddetti "reati spia" e della violenza di genere ha trovato nel web un pericoloso moltiplicatore. Condotte come lo stalking, le molestie, la diffusione non consensuale di materiale intimo si sono evolute in pratiche di violenza digitale organizzata, spesso reiterata e amplificata da dinamiche collettive. In risposta a questa escalation, l'ordinamento italiano ha introdotto il "Codice Rosso" (Legge 69/2019), che prevede corsie accelerate per la tutela delle vittime e nuove fattispecie di reato, come l'art. 612-ter c.p. sul cosiddetto revenge porn. La sfida per le forze di polizia, oggi, non è più soltanto quantitativa: è qualitativa. Occorre agire con tempestività e precisione chirurgica, per interrompere la catena della vittimizzazione prima che la viralità della rete renda il danno irreversibile.

In questo scenario, la Sezione Operativa della Seconda Divisione ha affrontato mesi di intensa attività, gestendo migliaia di segnalazioni relative alla diffusione illecita di contenuti sessualmente espliciti. Tali condotte si manifestano prevalentemente su forum e piattaforme multimediali, dove l'illecito iniziale viene spesso rilanciato da terzi attraverso linguaggi denigratori e sessualizzati. Si configura così una forma di violenza digitale che impone un'applicazione rigorosa delle tutele previste dal Codice Rosso, per salvaguardare la dignità e la riservatezza delle vittime.

Questi numeri non sono solo statistiche: sono il riflesso di una società che cambia, di nuove forme di violenza che si insinuano nei linguaggi digitali, nei rapporti affettivi, negli spazi della quotidianità online. È nella varietà dei fenomeni – dalle molestie online al cyberstalking, dalla sextortion alla diffamazione digitale – che si coglie la portata del mutamento nei comportamenti umani mediati dalle tecnologie dell'informazione.

L’azione della Divisione si è tradotta in 1.298 persone indagate e 245 perquisizioni, a testimonianza di un impegno operativo costante, multidisciplinare e orientato alla tutela concreta delle persone. In un contesto in cui la violenza assume forme sempre più sofisticate e pervasive, la risposta istituzionale deve essere altrettanto evoluta, fondata su competenze tecniche, sensibilità investigativa e una profonda consapevolezza del valore della persona.

Proprio l'estrema delicatezza di questi reati ha richiesto l’introduzione di una cornice normativa dedicata, concepita per garantire una corsia preferenziale di protezione a chi subisce le forme più odiose di violenza digitale.

STALKING ONLINE

Il reato di stalking (dall'inglese to stalk, letteralmente "fare la posta") è stato introdotto nell'ordinamento penale italiano con il d.l. n. 11/2009 (convertito, con modificazioni, dalla l. n. 38/2009) che ha inserito all'art. 612-bis c.p., il reato di "atti persecutori". Tale disposizione punisce chiunque "con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.

Nel 2025, lo stalking online si è confermato come una delle forme più insidiose di violenza relazionale e digitale, con 201 casi trattati nel corso dell'anno. Si tratta di un fenomeno trasversale, che si manifesta soprattutto attraverso piattaforme di messaggistica, social network e ambienti digitali scarsamente regolamentati, dove i confini tra pubblico e privato si fanno sempre più labili.

La distribuzione delle vittime evidenzia un marcato squilibrio di genere: il 75% è costituito da donne (151 casi), mentre il restante 25% riguarda uomini (50 casi). Questa asimmetria riflette dinamiche di controllo e intimidazione che si inseriscono nel più ampio contesto della violenza di genere, spesso agita attraverso strumenti digitali con modalità reiterate e pervasive.

Sul fronte operativo, la risposta investigativa è stata tempestiva e mirata: 90 persone sono state indagate per questo reato, grazie a un'attività di analisi e intervento che ha saputo coniugare competenze tecnologiche, ascolto delle vittime e capacità di lettura dei contesti digitali. L'esperienza maturata negli ultimi anni ha permesso di affinare gli strumenti di tracciamento e attribuzione, anche in ambienti dove l'anonimato e la volatilità delle prove rappresentano una sfida costante.

I dati del 2025 confermano la necessità di mantenere alta l'attenzione su questo tipo di condotte, rafforzando un approccio integrato che unisca prevenzione, educazione digitale, protezione delle vittime e azione investigativa specializzata. Lo stalking online non è un episodio isolato, ma una forma di violenza che si nutre di silenzi e invisibilità.

MOLESTIE ONLINE

Il reato di molestie realizzato mediante l'utilizzo della rete Internet, e in particolare attraverso i social network, si inquadra nella più ampia fattispecie astratta prevista dall'art.660 del Codice Penale, rubricato "Molestia o disturbo alle persone". Ai sensi di tale disposizione, chiunque, in un luogo pubblico o aperto al pubblico, ovvero per mezzo del telefono, reca a taluno molestia o disturbo, è punito con la pena dell'arresto fino a sei mesi o con l'ammenda fino a 516 euro.

Nel 2025, le **molestie online** hanno rappresentato una delle forme più frequenti di aggressione digitale, con **552 casi trattati** nel corso dell'anno. Il dato conferma la persistenza del fenomeno, che si manifesta attraverso comportamenti reiterati di disturbo, intimidazione o invasione della sfera privata, spesso veicolati da piattaforme digitali che amplificano la portata e la durata dell'offesa.

Anche in questo ambito, la distribuzione delle vittime evidenzia un marcato squilibrio di genere: **il 66% delle vittime è di sesso femminile (366 donne)**, mentre **il 34% riguarda uomini (186 casi)**. Questa asimmetria riflette dinamiche relazionali in cui la rete viene utilizzata come strumento di pressione psicologica, controllo o umiliazione, con effetti che possono protrarsi nel tempo e compromettere il benessere psico-sociale delle persone coinvolte.

Dal punto di vista operativo, l'attività investigativa ha portato all'identificazione e all'iscrizione nel registro degli indagati di **75 persone**, a testimonianza di un'azione costante e mirata da parte delle forze dell'ordine. L'approccio adottato ha privilegiato l'intervento tempestivo, la raccolta strutturata delle evidenze digitali e il supporto diretto alle vittime, in un'ottica di tutela integrata e multidisciplinare.

I dati del 2025 confermano che le molestie online non sono episodi isolati, ma parte di un fenomeno più ampio che richiede attenzione, competenze aggiornate e una rete di protezione efficace.

DIFFUSIONE ILLECITA DI IMMAGINI O VIDEO SESSUALMENTE ESPLICITI, DESTINATI A RIMANERE PRIVATI, SENZA IL CONSENSO DELLE PERSONE RAPPRESENTATE (REVENGE PORN)

Il reato di diffusione illecita di immagini o video sessualmente espliciti, destinati a rimanere privati (c.d. revenge porn) consiste nella divulgazione, senza il consenso delle persone rappresentate, di contenuti a carattere sessualmente esplicito, spesso effettuata con finalità ritorsive nei confronti di un ex partner o di un soggetto con cui si è intrattenuta una relazione sentimentale o sessuale.

Tale fattispecie è disciplinata dall'art 612-ter del Codice Penale, rubricato "Diffusione illecita di immagini o video sessualmente espliciti". La norma prevede una pena che va da un anno a sei anni di reclusione e multe che variano in base alla gravità del reato. L'articolo mira a tutelare la privacy e la dignità delle persone, prevedendo anche specifiche circostanze aggravanti in caso di diffusione su larga scala o qualora i fatti riguardino minori o persone in condizioni di inferiorità fisica o psichica.

Nel 2025, la diffusione non consensuale di contenuti intimi – conosciuta come *revenge porn* – ha continuato a rappresentare una delle forme più crudeli e invasive di violenza digitale. In 255 casi trattati, la rete si è trasformata in un'arma, capace di colpire la sfera più privata delle persone, esponendole a umiliazioni pubbliche, isolamento e danni psicologici profondi.
Le vittime sono in larga parte donne: 188 su 255, pari al 74%. Una prevalenza netta, che conferma quanto questo reato sia spesso l'esito di dinamiche di potere, vendetta o controllo esercitate in modo mirato e sistematico. Ma non si tratta solo di numeri: dietro ogni caso c'è una storia di fiducia tradita, di intimità violata, di identità esposta senza consenso.

L’attività investigativa ha portato all’individuazione di 106 autori, grazie a un lavoro meticoloso che ha combinato competenze digitali, tempestività operativa e ascolto attento delle vittime. La risposta della Seconda Divisione si è articolata in interventi rapidi, sequestri mirati e un dialogo costante con le piattaforme online, per fermare la circolazione dei contenuti e contenere il danno.

Il revenge porn non è un episodio isolato, ma un fenomeno che si alimenta del silenzio, della velocità della rete e della difficoltà di rimuovere ciò che è già stato condiviso. Per questo, accanto all’azione repressiva, è fondamentale continuare a investire in educazione affettiva, consapevolezza digitale e protezione attiva delle vittime, affinché nessuno si senta più solo di fronte a questa forma di violenza.

ESTORSIONE SESSUALE ONLINE

L'**estorsione sessuale** (c.d. *sextortion*) consiste nel ricattare una persona mediante la minaccia di divulgare immagini o video a contenuto sessualmente esplicito, ottenuti senza il consenso della vittima o tramite manipolazione, al fine di ottenere denaro, prestazioni di natura sessuale, favori o altri vantaggi. Tale condotta si manifesta prevalentemente in ambito digitale, sfruttando la vulnerabilità psicologica della vittima, la quale teme la diffusione di contenuti intimi.

In Italia, la *sextortion* trova inquadramento nell'ambito dell'**art.629** del Codice penale, che disciplina il delitto di estorsione, punito con la reclusione da tre a dieci anni e con la multa da 516 a 2.065 euro. La norma prevede circostanze aggravanti qualora la minaccia comporti un danno alla persona, alla sua libertà o alla reputazione.

Nel 2025, l'estorsione sessuale online si è confermata come una delle minacce digitali più aggressive e strutturate, con 1.225 casi trattati su tutto il territorio nazionale. Questo reato si manifesta attraverso la richiesta di denaro o altre utilità in cambio della non diffusione di immagini intime, spesso ottenute con l'inganno o attraverso relazioni simulate. La dinamica è rapida, predatoria e quasi sempre seriale.

Il profilo delle vittime mostra una prevalenza marcata di soggetti maschili, che rappresentano l'89% dei casi (1.092 uomini), a fronte di 133 donne (11%). Questo dato, in controtendenza rispetto ad altri reati digitali, evidenzia una strategia criminale mirata, che sfrutta la vulnerabilità emotiva e l'esposizione online, in particolare tra adolescenti e giovani adulti.

L’azione investigativa ha portato all’identificazione di 107 persone indagate, grazie a un lavoro congiunto tra la Seconda Divisione e le articolazioni territoriali della Specialità della Polizia Postale, che hanno operato in stretta sinergia. L’attività si è articolata attraverso operazioni di intelligence digitale, tracciamento delle transazioni, cooperazione internazionale e interventi tempestivi per interrompere le richieste estorsive, sequestrare i dispositivi utilizzati e oscurare i contenuti illeciti.

L’estorsione sessuale online è un reato che si alimenta della fiducia mal riposta, della solitudine e della pressione sociale. Per questo, oltre all’intervento repressivo, è fondamentale rafforzare le attività di prevenzione, educazione digitale e sensibilizzazione, soprattutto tra i più giovani.

MINACCE ONLINE

Il reato di minaccia è disciplinato dall'art. 612 del codice penale, che punisce chiunque "minaccia ad altri un ingiusto danno" con la multa fino a 1.032 euro, salvo che il fatto costituisca un reato più grave. La norma tutela la libertà morale della persona, intesa come diritto a non subire pressioni o intimidazioni che possano condizionare le proprie scelte o generare timore per sé o per altri.

Nel contesto digitale, la minaccia può realizzarsi anche attraverso mezzi telematici, come messaggi su social network, e-mail, app di messaggistica o commenti online. La giurisprudenza ha chiarito che la forma virtuale non esclude la rilevanza penale della condotta, purché la minaccia sia percepita come seria e idonea a incutere timore nella vittima.

Nel 2025, le minacce online hanno continuato a insinuarsi nei canali digitali con modalità sempre più fluide e pervasive. Con 633 casi trattati, il fenomeno si conferma come una forma di pressione psicologica che si manifesta spesso in modo diretto, altre volte sotto forma di allusione, intimidazione o ricatto emotivo. Il mezzo cambia, ma l'effetto resta: generare paura, silenziare, condizionare.

A colpire è l'equilibrio numerico tra i generi: 314 vittime di sesso maschile, 319 di sesso femminile. Una simmetria che racconta un reato trasversale, capace di insinuarsi in contesti relazionali, familiari, scolastici o professionali, senza distinzione. La minaccia digitale non ha un volto unico: può arrivare

da uno sconosciuto, da un ex partner, da un coetaneo o da un collega. E spesso si mimetizza dietro uno schermo, ma lascia segni profondi.

L'attività investigativa ha portato all'individuazione di 126 persone indagate, grazie a un'azione congiunta tra la Seconda Divisione e le articolazioni territoriali della Specialità della Polizia Postale. L'intervento si è fondato su un ascolto attento delle vittime, sull'analisi dei contenuti digitali e su una risposta operativa calibrata, capace di agire con tempestività e discrezione.

Le minacce online non sono solo parole: sono atti che incidono sulla libertà interiore, sulla possibilità di esprimersi, di esporsi, di vivere con serenità. Per questo, la risposta istituzionale non si limita alla repressione, ma si nutre di prossimità, competenza e consapevolezza culturale, per riconoscere il peso delle parole e restituire alle vittime uno spazio sicuro, anche nel mondo digitale.

CODICE ROSSO

Il Codice Rosso rappresenta il complesso di disposizioni normative introdotte con la **Legge n. 69 del 19 luglio 2019**, recante "Modifiche al Codice penale, al codice di procedura penale e ad altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere". La riforma è finalizzata a rafforzare la tutela delle vittime di maltrattamenti, violenze sessuali, atti persecutori (*stalking*) e altri reati connessi, assicurando interventi più rapidi, coordinati e incisivi da parte delle autorità di polizia e dell'autorità giudiziaria.

In particolare, il Codice Rosso prevede che la notizia di reato relativa a una delle fattispecie indicate venga immediatamente comunicata al Pubblico Ministero, il quale è tenuto a procedere all'audizione della persona offesa entro tre giorni. Tale previsione garantisce un canale prioritario nella gestione dei casi di violenza domestica e di genere, promuovendo un approccio integrato fondato sulla tempestività dell'intervento, la protezione delle vittime e la prevenzione della recidiva.

Nel quadro di tale normativa, le attività riportate nella seguente analisi fanno riferimento all'operato delle articolazioni territoriali dei Centri Operativi per la Sicurezza Cibernetica e delle Sezioni Operative per la Sicurezza Cibernetica, impegnate nel contrasto ai reati digitali e nella tutela delle vittime attraverso l'applicazione delle disposizioni previste dal Codice Rosso.

I dati analizzati illustrano l'insieme delle iniziative e deleghe svolte nel corso dell'anno a livello regionale, con particolare riferimento ai reati di atti persecutori (art. 612 bis c.p.), diffusione illecita di immagini o video sessualmente espliciti (art. 612 ter c.p.) e violenza sessuale (art. 609 bis c.p.).

Nel periodo compreso tra il 1° gennaio e il 21 dicembre 2025 sono state registrate 477 richieste di attivazione del Codice Rosso. Di queste, 387 hanno riguardato vittime di sesso femminile, pari a circa l'81% del totale, mentre 90 hanno interessato vittime di sesso maschile (19%). Il dato conferma la marcata incidenza del fenomeno sulla popolazione femminile, pur evidenziando una presenza non trascurabile di uomini tra le persone offese, elemento che contribuisce a restituire una rappresentazione più articolata delle dinamiche di violenza intercettate.

Attivazione Codice Rosso	Dal 1° gennaio al 21 dicembre 2025	
	Donne	**Uomini**
Stalking (Art. 612 Bis)	159	30
Revenge Porn (Art. 612 Ter)	183	57
Maltrattamenti contro familiari o conviventi (Art. 572)	14	1
Atti sessuali con minorenne (Art. 609 quater)	4	0
Adescamento di minorenni (Art. 609 undecies)	2	0
Minaccia (Art. 612)	9	0
Lesione personale (Art. 582)	2	0
Violenza sessuale (Art. 609 bis)	10	2
Prostituzione minorile (Art. 600 bis)	3	0
Pornografia minorile (Art. 600 ter)	1	0
Totali per genere	**387**	**90**
TOTALI	**477**	

L'analisi delle attivazioni per tipologia di reato mostra una netta prevalenza delle fattispecie riconducibili allo stalking e alla diffusione illecita di immagini o video a contenuto sessualmente esplicito (revenge porn), che complessivamente rappresentano oltre i tre quarti delle segnalazioni. In particolare, lo stalking ha determinato 189 attivazioni, con 159 vittime di sesso femminile e 30 di sesso maschile, mentre il revenge porn ha fatto registrare 240 richieste, di cui 183 riferite a donne e 57 a uomini, confermandosi come una delle forme di violenza più ricorrenti e trasversali.

Le restanti attivazioni, numericamente più contenute, riguardano reati quali i maltrattamenti contro familiari o conviventi, la violenza sessuale, le minacce e le diverse fattispecie a danno di minori. Nel loro insieme, tali dati delineano un quadro complesso e di particolare gravità, che evidenzia il ruolo centrale del Codice Rosso quale strumento di tutela tempestiva e di risposta immediata alle situazioni di maggiore vulnerabilità.

IL CASO: CONDIVISIONE ILLECITA DI CONTENUTI SESSUALI ONLINE, OSCURATE DUE PIATTAFORME

In tale quadro si collocano episodi specifici che hanno suscitato particolare clamore mediatico. È il caso del gruppo Facebook denominato "*Mia Moglie*" – chiuso il 21 agosto in seguito alla segnalazione notificata alla piattaforma dalla Polizia Postale – ambiente virtuale nel quale venivano sistematicamente diffusi materiali sessualmente espliciti, apparentemente senza il consenso delle donne ritratte, con modalità che lasciano intendere una prassi consolidata e strutturata di condivisione illecita. Analoga situazione si riscontra nel forum *phica.eu* – avente circa 800.000 iscritti al momento della chiusura, effettuata autonomamente dagli stessi amministratori – che dal 2005 ospitava contenuti dello stesso genere e caratterizzato da dinamiche di interazione tra utenti nelle quali i commenti assumono un evidente carattere diffamatorio e sessualmente connotato, aggravando l'offesa nei confronti delle vittime.

L'Unità di Analisi del Crimine Informatico

L'*Unità di Analisi del Crimine Informatico- UACI* è un'*équipe* di funzionari psicologi della Polizia di Stato che integra le competenze di natura socio-psicologica con l'attività di prevenzione e contrasto dei reati online, con particolare riguardo a quelli che coinvolgono minori e vittime vulnerabili.

Le principali attività svolte dall'Unità hanno lo scopo di massimizzare l'efficacia delle investigazioni, valorizzare l'impegno degli operatori e capitalizzare la conoscenza criminologica dei fenomeni, per aumentare la consapevolezza della società civile in merito a questi rischi.

ATTIVITÀ	ANNO 2025
Somministrazione job preview	23
Colloqui individuali e di gruppo	160
COSC raggiunti	5
Debriefing	1

L'Unità provvede ad assicurare ascolto, sostegno psicologico e formazione specifica al personale esposto a materiale ad alto impatto emotivo (pedopornografia, immagini violente, esecuzioni, etc.) attraverso l'ideazione, la strutturazione e la realizzazione di progetti tesi a evitare lo stress cumulativo e la traumatizzazione vicaria, in un'ottica di valorizzazione della risorsa specializzata costituita da investigatori, agenti sotto copertura e analisti forensi della Polizia Postale.

L'Uaci ha assicurato supporto operativo alle squadre investigative attraverso la partecipazione all'esecuzione di disposizioni dell'Autorità Giudiziaria a carico di autori di reati sessuali e di violenza di genere (perquisizioni domiciliari, interrogatori) e in riferimento alle attività di ascolto di vittime vulnerabili (S.I.T., audizioni protette, ispezioni fisiche, interrogatori di minorenni autori di reato, etc), assicurando la massima protezione psicoemotiva dal rischio di vittimizzazione secondaria.

ATTIVITÀ	ANNO 2025
SIT/Audizioni Protette	32
Ausilio perquisizioni	8
Interrogatori minori autori di reato	4

L'Uaci si occupa di supportare telefonicamente i minori e le vittime in stato di fragilità psicologica che si rivolgono al portale istituzionale e a quelli delle hotline, per richiedere aiuto in riferimento a vari ordini di rischio o minaccia subiti online. In particolare, valutano caso per caso quale sia la strategia migliore per aiutare vittime minorenni di reati come la sextortion, il cyberbullismo, la pedopornografia e la violenza di genere online.

ATTIVITÀ	ANNO 2025
Segnalazioni Commissariato di Ps online, Hot114, Save the Children	117

Nel corso del 2025, è stato condotto un approfondimento relativo ai correlati psicologici delle attività di prevenzione e repressione del terrorismo online, analizzando gli effetti psicologici immediati e a lungo termine dell'esposizione del personale a materiale di violenza, uccisioni, esecuzioni, scenari di guerra etc. che è connaturato all'attività di monitoraggio della rete e delle organizzazioni di estremismo politico e religioso. Sono stati quindi effettuati diversi colloqui psicologici individuali e di gruppo, ed è in corso una raccolta dati con l'uso di specifici questionari.

ATTIVITÀ	ANNO 2025
Colloqui individuali	17
Questionari somministrati	40

L'Uaci assicura formazione specialistica sui temi psicologici rivolta verso gli operatori della Polizia Postale e verso altri Uffici del Dipartimento, con particolare riguardo ai temi della sensibilizzazione al rischio per minori e vittime vulnerabili. Sono state diffuse e presentate in un'occasione formativa specifica, durante il 2025, le Linee Guida "A scuola tutto bene?" che hanno determinato la standardizzazione metodologica e contenutistica degli interventi di sensibilizzazione a livello scolastico, definendo i temi e i linguaggi in base all'età dei target e alle emergenze contingenti.

ATTIVITÀ	ANNO 2025
Formazione per altri servizi	12
Formazione interna	14

ATTIVITÀ INTERISTITUZIONALI
Osservatorio per la prevenzione e il contrasto della Pedofilia e della Pornografia minorile
Osservatorio Nazionale per l'infanzia e l'adolescenza
Tavolo tecnico per la prevenzione e il contrasto del bullismo e del cyberbullismo
Comitato consultivo interistituzionale per l'alfabetizzazione mediatica e digitale
Gruppo Interparlamentare per la prevenzione e la riduzione del rischio

L'Uaci collabora con l'Ufficio Relazioni Esterne della Prima Divisione, al fine di ottimizzare le strategie comunicative volte a prevenire le varie forme di aggressione tecnomediata ai minori, per la sensibilizzazione degli adulti significativi, per la migliore gestione dei casi emergenti in conseguenza degli incontri con studenti in ambito scolastico e per l'attuazione di strategie informative tempestive tese a ridurre l'impatto di rischi contingenti in materia di minacce online.

Nel 2025 l'Uaci ha partecipato attivamente al board di progettazione del portale di Europol Help4U, un nuovo strumento online a disposizione di giovani vittime di reati online, raggiungibile da diversi paesi europei e realizzato con la partecipazione di HOT114 e Savethechildren ITA Onlus.

L'Uaci partecipa inoltre ai lavori dei sottoelencati Tavoli di Lavoro e Osservatori Nazionali per la stesura dei piani nazionali di prevenzione e contrasto alle varie forme di aggressione ai minori.

L'Uaci si applica per la gestione di incontri di particolare complessità in istituti scolastici afferenti a territori caratterizzati da alti tassi di devianza, in scuole/classi in cui si siano verificati episodi di bullismo, cyberbullismo e altre forme di aggressione tecnomediata nonché contribuisce a veicolare alla cittadinanza e in consessi vari informazioni, report e relazioni sulle

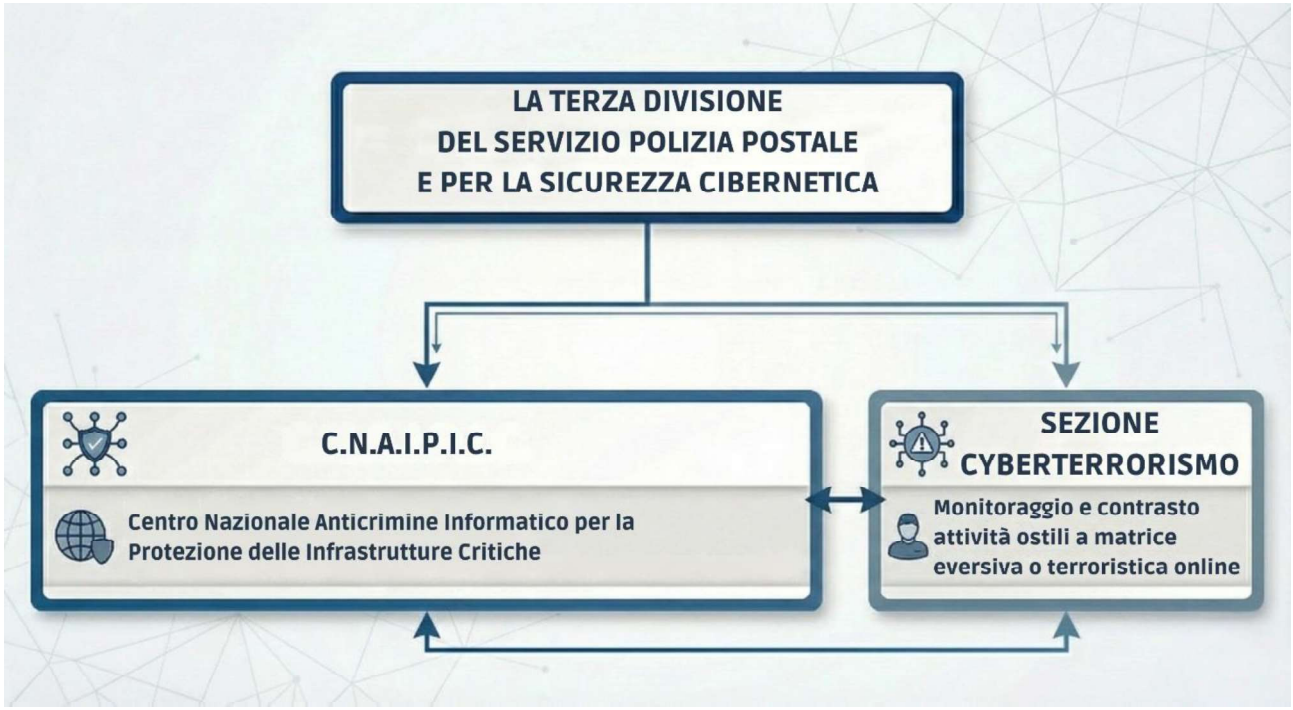
ATTIVITÀ DI COMUNICAZIONE	ANNO 2025
Incontri in Scuole	15
Incontri con adulti/genitori	5
Comunicazione istituzionale, conferenze e convegni	20
Partecipazione a tavoli di lavoro/osservatori	10

principali forme di rischio per bambini e adolescenti, in tutti gli ambiti in cui sia strategica una comunicazione finalizzata a informare e prevenire la devianza online.
La maggioranza delle attività illustrate sono integrate da raccolte dati e ricerche utili a orientare le attività progettuali e a valutarne l'efficacia. Sono state avviate diverse survey i cui risultati saranno condivisi in appositi report. Ogni raccolta dati si basa su strumenti e test già codificati.

LA TERZA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Cristiano Leggeri, *Primo Dirigente della Polizia di Stato, Direttore*

In un panorama digitale segnato da minacce sempre più sofisticate, persistenti e interconnesse, la Terza Divisione del Servizio Polizia Postale e per la Sicurezza Cibernetica rappresenta un presidio strategico per la tutela della sicurezza nazionale. La sua struttura si articola in due componenti operative di alto profilo: il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), incaricato della prevenzione e repressione dei crimini informatici a danno delle infrastrutture digitali più sensibili, e la Sezione Cyberterrorismo, dedicata al monitoraggio e al contrasto delle attività ostili a matrice eversiva o terroristica condotte attraverso il cyberspazio.



L'integrazione tra queste due anime operative consente di affrontare con efficacia un ampio spettro di minacce, grazie a un approccio che combina competenze tecniche avanzate, capacità di analisi strategica e cooperazione multilivello, sia sul piano nazionale che internazionale.

Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.)

Nel corso del 2025 il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) ha ulteriormente consolidato il proprio ruolo quale presidio centrale della sicurezza cibernetica nazionale, confermandosi come uno degli attori chiave dell'architettura di difesa del Paese nel dominio digitale. Istituito con decreto del Ministro dell'Interno del 9 gennaio 2008 come Centro di Specialità del Servizio Polizia Postale, il C.N.A.I.P.I.C. opera oggi quale organo del Ministero dell'Interno con competenze esclusive nella tutela della sicurezza e della regolarità dei servizi di telecomunicazione, nonché nella prevenzione e repressione dei crimini informatici diretti contro le infrastrutture informatizzate di natura critica e di rilevanza nazionale.

Il rafforzamento del ruolo del Centro si inserisce in un contesto caratterizzato da una crescente complessità dello scenario cibernetico, nel quale le minacce informatiche assumono forme sempre più sofisticate, persistenti e transnazionali. In tale quadro, il C.N.A.I.P.I.C. ha progressivamente ampliato il proprio raggio d'azione, ponendosi come punto di riferimento per il coordinamento delle attività preventive, di monitoraggio e di contrasto agli attacchi informatici che colpiscono i settori strategici del sistema Paese. L'azione del Centro si fonda su un modello operativo integrato, che coniuga funzioni di indirizzo strategico e coordinamento con capacità operative dirette, configurando un unicum nel panorama delle articolazioni dipartimentali della Pubblica Sicurezza.

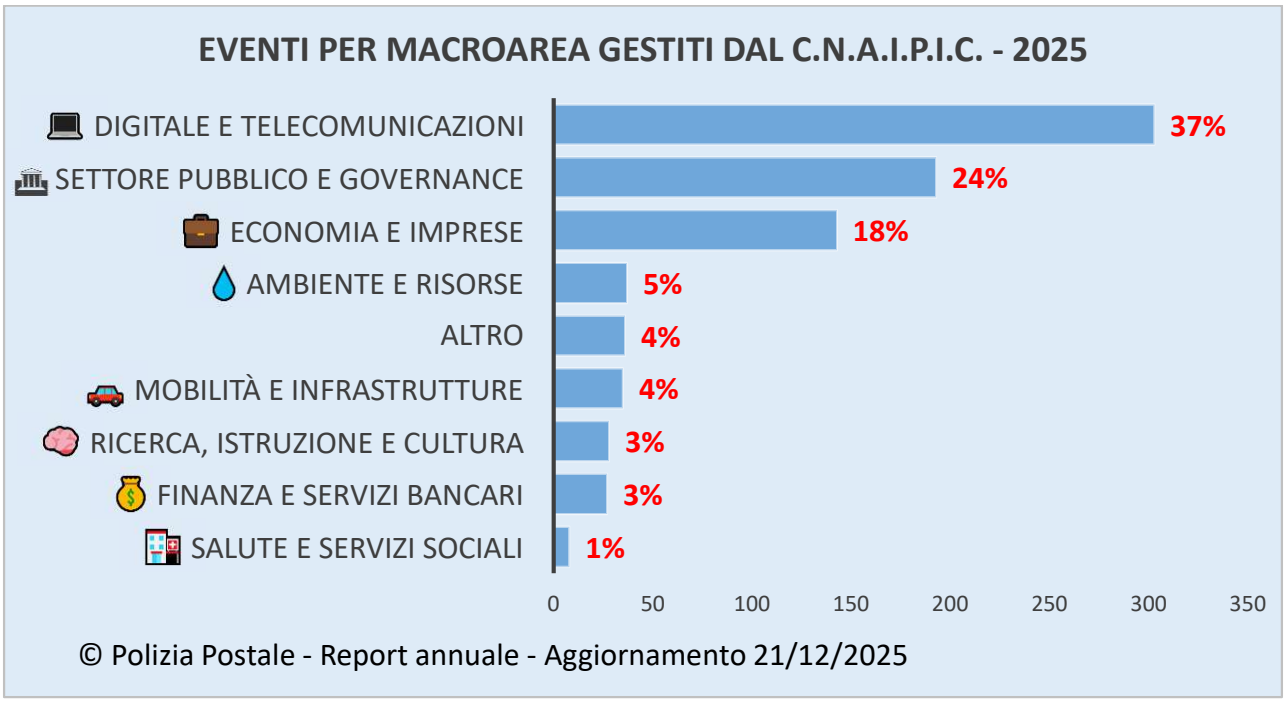
Elemento centrale di tale modello è rappresentato dalla strutturazione territoriale delle attività di sicurezza cibernetica, realizzata attraverso i Nuclei Operativi per la Sicurezza Cibernetica (NOSC). Questi ultimi, incardinati gerarchicamente nei Centri Operativi competenti per territorio e funzionalmente collegati al C.N.A.I.P.I.C., assicurano una presenza specialistica capillare sul territorio nazionale. I NOSC svolgono un ruolo fondamentale nella gestione delle segnalazioni di attacco, nel supporto alle attività di analisi tecnica e nella prima risposta operativa agli eventi cyber,

garantendo tempestività di intervento e una conoscenza diretta delle realtà locali da proteggere. Tale assetto organizzativo ha consentito una gestione razionale ed efficiente delle numerose casistiche registrate nel corso dell'anno, assicurando uniformità di approccio e coerenza operativa su scala nazionale.

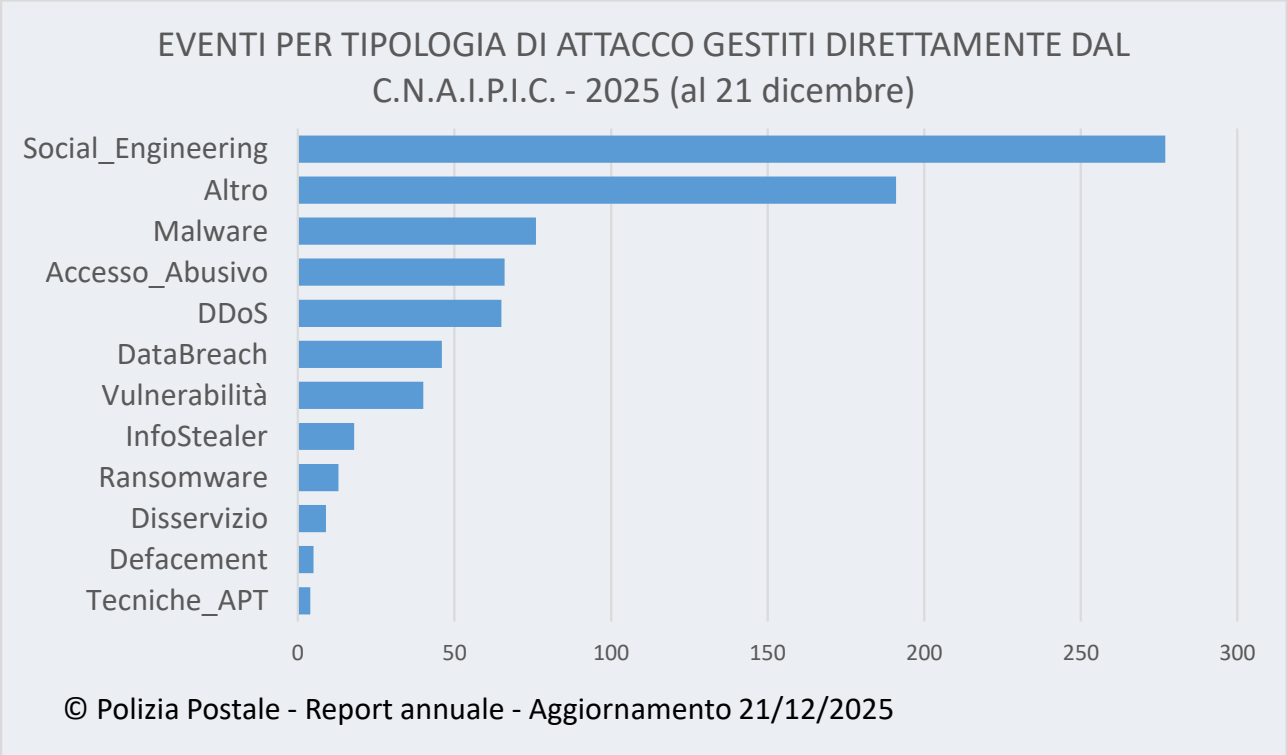
In tale contesto operativo, il dato complessivo delle 9.250 casistiche di attacchi informatici registrate nel corso del 2025 rappresenta l'espressione quantitativa della pressione cibernetica esercitata sul Paese. Tale valore comprende eventi che hanno interessato un perimetro ampio e articolato di soggetti, includendo le infrastrutture critiche, gli operatori di servizi essenziali, le pubbliche amministrazioni locali, nonché il tessuto produttivo e i cittadini, e restituisce la dimensione complessiva dell'attività di monitoraggio, prevenzione e gestione svolta nell'ambito del dispositivo nazionale di sicurezza cibernetica.

All’interno di questo quadro generale, con specifico riferimento agli attacchi diretti verso le infrastrutture critiche, gli operatori di servizi essenziali e le pubbliche amministrazioni locali, alla data del 21 dicembre risultano censiti 942 eventi cyber. Di questi, 535 episodi sono stati assunti in trattazione diretta dal Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, in considerazione della particolare gravità, complessità e pervasività delle condotte rilevate, tali da richiedere una gestione centralizzata sotto il profilo operativo, investigativo e di coordinamento.

A tali eventi si affiancano 275 ulteriori incidenti informatici che hanno coinvolto aziende e soggetti privati, anch’essi caratterizzati da elementi di criticità tali da determinarne la presa in carico da parte del C.N.A.I.P.I.C., almeno nelle fasi iniziali e più sensibili dell’attività investigativa, al fine di garantire un’immediata azione di contenimento, analisi tecnica e supporto operativo, in raccordo con le articolazioni territoriali competenti.



Nel complesso, il numero di eventi cyber di maggiore impatto direttamente gestiti dal Centro nel periodo di riferimento ammonta pertanto a 810 casi, rappresentativi delle situazioni di più elevata rilevanza sotto il profilo della sicurezza nazionale. È su tale perimetro che si concentra l'analisi, volta a illustrare le principali tipologie di attacco riscontrate e le macroaree maggiormente interessate, al fine di fornire una lettura strutturata e coerente delle dinamiche di minaccia emerse nel corso dell'anno.



Parallelamente, il C.N.A.I.P.I.C. ha intensificato la cooperazione con gli altri attori istituzionali che compongono l'architettura nazionale di cybersicurezza, nonché con gli organi di direzione dell'autorità giudiziaria. La stipula di protocolli di intesa e la definizione di flussi informativi strutturati hanno permesso una più efficace esplicazione delle funzioni di coordinamento e impulso delle attività preventive e investigative. In particolare, l'introduzione di specifici obblighi di

comunicazione degli attacchi informatici da parte dei soggetti rientranti nel perimetro di sicurezza nazionale cibernetica ha favorito una trasmissione progressiva e continuativa delle informazioni acquisite, anche successivamente alla prima segnalazione, consentendo una più accurata attività di analisi e valutazione del rischio.

L'attività di osservazione e studio condotta dal Centro ha evidenziato come gli attacchi informatici seguano generalmente un ciclo di vita strutturato e metodico, articolato in fasi di ricognizione, compromissione iniziale, mantenimento dell'accesso e occultamento delle tracce. Le tecniche di social engineering continuano a rappresentare uno degli strumenti privilegiati dagli attori ostili, consentendo loro di studiare i comportamenti delle vittime e di sfruttare le vulnerabilità umane e organizzative per perseguire i propri fini illeciti. A ciò si affianca l'utilizzo sempre più diffuso di malware personalizzati, exploit zero-day e attacchi multi-vettore, che combinano differenti modalità operative al fine di eludere i sistemi di difesa e rendere più complessa la rilevazione.

Particolarmente complessa si conferma l'attività di attribuzione degli attacchi, elemento essenziale per l'avvio e il perseguimento delle azioni di polizia giudiziaria. Gli attori ostili ricorrono sempre più frequentemente a tecniche di offuscamento avanzate, quali l'impiego di infrastrutture di comando e controllo delocalizzate, reti proxy, servizi di anonimizzazione e hosting bulletproof, nonché a tattiche di "false flag" volte a depistare le investigazioni. In molti casi, tali attività risultano riconducibili a gruppi strutturati o patrocinati da apparati statali, configurando scenari di minaccia riconducibili alle cosiddette Advanced Persistent Threat (APT).

Nel quadro delle minacce emergenti, si registra un utilizzo sempre più significativo degli attacchi Distributed Denial of Service (DDoS), che si sono evoluti nel tempo sia sotto il profilo tecnico sia sotto quello strategico. Dalle prime forme basate su strumenti open-source si è passati a campagne complesse che coinvolgono botnet sofisticate e servizi a pagamento, spesso impiegate anche in contesti di tensione geopolitica. Tali attacchi, finalizzati a compromettere la disponibilità dei servizi, assumono particolare rilevanza quando colpiscono infrastrutture critiche e servizi essenziali per la collettività.

Un ulteriore elemento di criticità è rappresentato dalla crescente esposizione delle catene di fornitura e dei soggetti più vulnerabili dei processi produttivi e amministrativi, quali le piccole e medie imprese, i singoli cittadini e i funzionari pubblici e privati. In questo contesto, il settore sanitario emerge come

uno dei target privilegiati degli attacchi informatici, in ragione dell'elevato valore economico dei dati trattati e delle gravi conseguenze che una loro compromissione può determinare. Sebbene si registrino progressivi adeguamenti dei livelli di protezione, appare necessario un ulteriore rafforzamento delle competenze e dei processi interni, nonché un'intensificazione delle attività di sensibilizzazione.

Sul piano normativo, l'approvazione del D.L. 105/2023, convertito nella L. 137/2023, ha rappresentato un passaggio di particolare rilievo, ampliando significativamente il ventaglio degli strumenti investigativi a disposizione del C.N.A.I.P.I.C. La novella legislativa ha introdotto la possibilità di condotte proattive in ambiente informatico nell'ambito delle indagini sotto copertura, consentendo agli ufficiali di polizia giudiziaria di operare con maggiore efficacia in contesti digitali complessi e altamente dinamici.

Infine, il C.N.A.I.P.I.C. ha consolidato il proprio ruolo sul piano internazionale, operando quale Punto nazionale della Convenzione di Budapest sul crimine informatico. L'intensificazione delle attività di cooperazione transfrontaliera e la partecipazione a consessi internazionali hanno favorito lo scambio di informazioni, l'adozione di best practice e il rafforzamento delle capacità investigative, contribuendo in modo significativo al contrasto di un fenomeno sempre più pervasivo, strutturato e globale.

GRANDI EVENTI: GIUBILEO DELLA CHIESA CATTOLICA 2025

Il Servizio Polizia Postale e per la Sicurezza Cibernetica ha espletato un dedicato servizio di sicurezza informatica connesso allo svolgimento degli Eventi Giubilari, che nel complesso delle attività assicurate dalla specialità vede il CNAIPIC assicurare il proprio compito istituzionale di tutela delle infrastrutture critiche unitamente all'Agenzia Nazionale per la Cybersicurezza attraverso l'attivazione di dedicate war room per la rapida condivisione di situazioni di minaccia cibernetica che facilita l'eventuale immediato contenimento, anche tramite l'attivazione di azioni di intervento e supporto.

GRANDI EVENTI: OLIMPIADI E PARAOLIMPIADI INVERNALI MILANO-CORTINA

Le Olimpiadi Invernali Milano-Cortina previste per il prossimo febbraio 2026 e la successiva competizione paralimpica a marzo 2026, la cui organizzazione dell'evento è affidata alla omonima

Fondazione, ha già visto l'avvio di intense interlocuzioni e attività preparatorie – ivi comprese simulazioni - finalizzate alla miglior definizione di un articolato dispositivo di protezione delle infrastrutture informatiche coinvolte e funzionale all'espletamento dei propri compiti istituzionali.

L'attività del C.N.A.I.P.I.C. si declinerà lungo due direttrici strategiche: la tutela delle infrastrutture critiche informatizzate, in termini di prevenzione e repressione degli attacchi cibernetici ai sistemi informativi coinvolti nella manifestazione, e il monitoraggio della rete per ragioni di ordine e sicurezza pubblica, oltre che per la prevenzione e contrasto di eventuali iniziative di matrice terroristica.

Sul primo fronte, nel corso dell'anno sono state avviate interlocuzioni con i responsabili del settore cyber della Fondazione (istituita per l'organizzazione dei Giochi), utili alla predisposizione del dispositivo di sicurezza cibernetica. I rapporti diretti, basati sullo scambio informativo ed esperienziale – quest'ultima, anche grazie allo svolgimento di esercitazioni congiunte e alla condivisione degli esiti - hanno trovato una formalizzazione nel Protocollo di collaborazione, stipulato lo scorso ottobre, tra Ministero dell'Interno e MICO, rientrante nella previsione di cui all'art. 7 bis del D.L. n. 144 del 27 luglio 2005

COLLABORAZIONE INTERNAZIONALE

Un'attenzione particolare è stata dedicata al fronte della collaborazione internazionale, settore sempre più strategico e funzionale nel contrasto dei reati cyber, per loro natura di carattere sovranazionale in virtù della loro matrice, dinamica o portata.

In proposito si rappresenta che il CNAIPIC già garantisce, quale punto di contatto in ambito High Tech Crime (Convenzione di Budapest), l'invio e la ricezione delle richieste di collaborazione e supporto da e per i paesi sottoscrittori, comportando la gestione di 47 casi in entrata durante l'anno.

La cooperazione si è inoltre esplicitata anche sotto il profilo operativo attraverso l'attiva partecipazione ad azioni di polizia congiunte.

In ambito Europol, la stretta collaborazione e lo scambio info-operativo con i collaterali cyber delle forze di polizia estere ha portato alla conclusione di importanti operazioni, alcune delle quali di rilevanza internazionale in ragione dell'obiettivo perseguito. Tra queste spicca:

IL CASO: OPERAZIONE "EASTWOOD"

La recente attività investigativa internazionale, condotta nei confronti del collettivo hacker filorusso "NoName057(16)", responsabile, sin dal 2022, di numerosi attacchi informatici di tipo DDoS ai danni di infrastrutture critiche nazionali e occidentali è il frutto di una strutturata indagine condotta nell'ambito di un Gruppo Investigativo Internazionale coordinato da Eurojust ed Europol, che ha coinvolto 14 paesi europei. L'attività ha consentito di ricostruire puntualmente l'infrastruttura utilizzata dall'attore ostile per l'effettuazione degli attacchi. Tale infrastruttura era costituita da una fascia di server di Command and Control (C2) stabiliti nella Federazione Russa, oltre a ulteriori server distribuiti sul territorio europeo.

Le indagini hanno permesso di identificare tre persone di nazionalità russa, operanti quali verosimili amministratori del gruppo, e ulteriori presunti sodali del collettivo, residenti in diversi paesi del mondo. Tra questi le indagini del CNAIPIC, condotte sotto la direzione della Procura della Repubblica di Roma e il coordinamento della Direzione Nazionale A.A avevano portano all'individuazione di 9 persone, 5 delle quali ritenute effettivamente responsabili della partecipazione agli attacchi informatici portati dal collettivo e, pertanto, sono stati destinatari di decreti di perquisizione in occasione dell'action day concertato a livello internazionale. L'operazione, che in ambito nazionale ha consentito l'acquisizione di determinanti elementi a conferma della responsabilità degli indagati, ha globalmente portato al sequestro dell'infrastruttura informatica illecita e all'interruzione dell'operatività del gruppo criminale, ottenendo notevole risalto a livello mediatico.

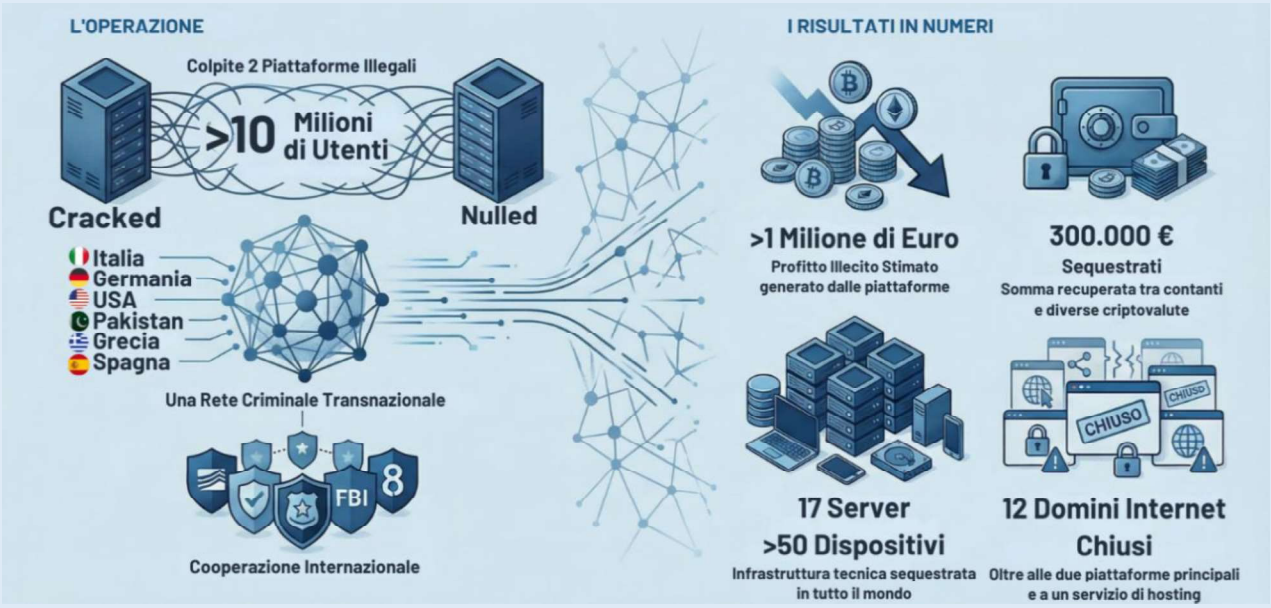
Inoltre, dalla sede del C.N.A.I.P.I.C. sono stati costantemente diramati alert - di natura tecnica - contenenti gli indicatori di compromissione relativi alle principali campagne malevole in atto, nonché aggiornamenti relativi a possibili iniziative in ambito hacktivism per prevenire l'azione di gruppi ideologicamente orientati quale possibile causa di turbativa dell'evento.

Il CNAIPIC collabora attivamente con l'*European Cyber Crime Centre (EC3)* di Europol per contrastare le minacce informatiche a livello internazionale. Questa sinergia si basa sulla condivisione di informazioni, competenze e risorse, che consentono una risposta tempestiva e coordinata alle attività ostili nei confronti delle infrastrutture critiche a livello nazionale e europeo.

Attraverso questa collaborazione, il CNAIPIC e l'EC3 sviluppano strategie e progetti congiunti, mirati a rafforzare la capacità degli Stati membri di affrontare le minacce informatiche sempre più insidiose ed evolute. La collaborazione rende più efficace la diffusione di *best practices* e la formazione e l'aggiornamento degli operatori delle forze dell'ordine anche attraverso un addestramento congiunto, contribuendo così a creare un ambiente digitale più sicuro.

IL CASO: SMANTELLATE "CRACKED" E "NULLED" - MAXI-OPERAZIONE INTERNAZIONALE CONTRO IL CYBERCRIME

Il Centro Operativo per la Sicurezza Cibernetica dell'Emilia-Romagna, sotto la direzione del Servizio Polizia Postale e per la Sicurezza Cibernetica, ha svolto un ruolo di primo piano nell'operazione internazionale che ha portato allo smantellamento delle piattaforme "Cracked" e "Nulled", due dei più grandi forum di cybercrime al mondo. La perquisizione eseguita dagli operatori del Centro, nell'ambito di un'azione coordinata da Europol e condotta in otto Paesi, ha permesso di individuare un giovane italiano poco più che ventenne, residente in regione, ritenuto parte di un'organizzazione criminale transnazionale composta da cittadini tedeschi, americani, pakistani, greci e spagnoli.



Grazie all'analisi delle chat, della documentazione e dei dispositivi sequestrati, gli investigatori emiliano-romagnoli sono riusciti a ricostruire i rapporti tra il giovane, il suo socio tedesco e gli amministratori dei forum, individuando numerosi wallet sui quali confluivano i profitti illeciti, convertiti in criptovalute attraverso società di intermediazione compiacenti. L'attività tecnica del Centro ha consentito di tracciare i flussi finanziari e di documentare il funzionamento delle infrastrutture informatiche che sostenevano i due market, raggiungibili facilmente dal web e utilizzati per la vendita di ransomware, virus, credenziali di accesso, dati aziendali sottratti e altri strumenti malevoli.

In collaborazione con il Dipartimento di Giustizia americano e con l'FBI, gli operatori hanno inoltre contribuito a rendere irraggiungibili i server della piattaforma italiana e al sequestro di oltre settantamila dollari in criptovalute, insieme a numerosi dispositivi elettronici. L'operazione, condotta tra il 29 e il 30 gennaio, si inserisce in un più ampio dispositivo internazionale che ha portato ad arresti, perquisizioni e sequestri in diversi Paesi, confermando il ruolo strategico del Centro Operativo per la Sicurezza Cibernetica dell'Emilia-Romagna nella lotta al cybercrime globale.

COMITATO DI ANALISI PER LA SICUREZZA CIBERNETICA (CASC)

Nel corso dell'anno si sono svolte le riunioni periodiche del Comitato di Analisi per la sicurezza cibernetica (CASC), il neo-organismo di raccordo istituzionale finalizzato alla condivisione strategica e info-operativa funzionale a una maggiore efficacia dell'azione di contrasto in materia cyber.

Concepito come contesto di facilitazione e promozione dello scambio informativo in ordine alle principali minacce osservate dai vari interlocutori istituzionali nel corso delle rispettive attività, sta acquistando sempre più il ruolo di camera di compensazione e di allineamento tra le istanze investigative, le esigenze di resilienza e la tutela della sicurezza cibernetica nazionale

INCONTRO SETTORE ENERGETICO

Nel corso dell'anno di riferimento, il personale specialista del C.N.A.I.P.I.C. ha preso parte a un incontro di tre giorni dedicato al settore energetico, con la partecipazione di rappresentanti istituzionali, operatori di infrastrutture critiche, organismi di sicurezza e partner tecnologici nazionali. L'evento ha costituito un'importante occasione di confronto operativo e strategico su tematiche di

primaria rilevanza per la protezione del settore energetico, considerato uno dei settori maggiormente esposti e sensibili rispetto alle minacce cibernetiche.

I lavori si sono concentrati in particolare sugli ambiti della *cyber threat intelligence* e delle attività di *cyber deception*, favorendo un approfondimento congiunto delle più recenti tecniche, tattiche e procedure adottate dagli attori malevoli, sia di matrice statuale che criminale. In tale contesto, il contributo del C.N.A.I.P.I.C. si è tradotto nella condivisione di esperienze investigative, modelli di analisi e metodologie operative finalizzate all'individuazione precoce delle minacce e alla mitigazione dei rischi per le infrastrutture strategiche.

L'incontro ha inoltre favorito un proficuo scambio di informazioni e di strategie di cooperazione, volto all'innalzamento complessivo del livello di sicurezza cibernetica del settore. Sono stati condivisi indicatori di compromissione (IoC) relativi a campagne malevole emergenti, nonché elementi utili al rafforzamento delle capacità di rilevazione e risposta agli incidenti. Particolare attenzione è stata riservata alle attività di *cyber deception*, intese come strumenti avanzati di difesa proattiva, utili sia per disorientare gli attaccanti sia per acquisire informazioni rilevanti sulle loro modalità operative.

Tale evento ha permesso al C.N.A.I.P.I.C. di consolidare ulteriormente le relazioni con i principali stakeholder del settore energetico e con i partner internazionali, rafforzando i canali di collaborazione e contribuendo allo sviluppo di un approccio condiviso e integrato alla sicurezza cibernetica delle infrastrutture critiche. L'esperienza maturata rappresenta un ulteriore valore aggiunto per il continuo aggiornamento delle capacità operative del Centro e per il miglioramento delle attività di prevenzione, monitoraggio e contrasto alle minacce informatiche.

TAVOLI SETTORIALI

Nel corso dell'anno di riferimento, il C.N.A.I.P.I.C. ha promosso e organizzato una serie di incontri settoriali con gli attori chiave quali il settore telecomunicazioni, energetico, dei trasporti e della mobilità, riconoscendo l'importanza strategica di favorire un dialogo costante e proficuo tra le istituzioni, gli operatori del settore e i principali esperti di sicurezza. Questi tavoli settoriali si sono rivelati fondamentali per consolidare la cooperazione di partenariato pubblico-privato e per rafforzare

il coordinamento nell'ambito della lotta contro il cybercrime sempre più pervasivo che interessa in modo trasversale tutte le infrastrutture critiche.

L'integrazione di competenze e risorse tra pubblico e privato ha dimostrato di essere un elemento imprescindibile per costruire una difesa robusta contro le crescenti minacce cibernetiche. L'interscambio di informazioni, esperienze e pratiche operative tra i vari settori ha infatti permesso di individuare soluzioni condivise e di migliorare le capacità di risposta e prevenzione agli attacchi informatici. La protezione delle infrastrutture critiche, in particolare quelle dei settori strategici come le telecomunicazioni, l'energia, i trasporti e la mobilità, assume un valore fondamentale, non solo per garantire la sicurezza nazionale, ma anche per salvaguardare la resilienza economica e sociale del Paese.

In un contesto di crescente sofisticazione delle minacce cibernetiche, che potrebbero compromettere la produzione e la distribuzione di risorse vitali per l'economia globale, tali incontri hanno rappresentato un'opportunità essenziale per allineare le strategie di difesa e per promuovere l'adozione di tecniche avanzate di cybersecurity quali la *cyber threat intelligence* e la *cyber deception*. Queste ultime, infatti, consentono di anticipare le mosse degli attaccanti e di proteggere in modo più efficace le infrastrutture da attacchi mirati che potrebbero compromettere la sicurezza operativa e la continuità dei servizi essenziali.

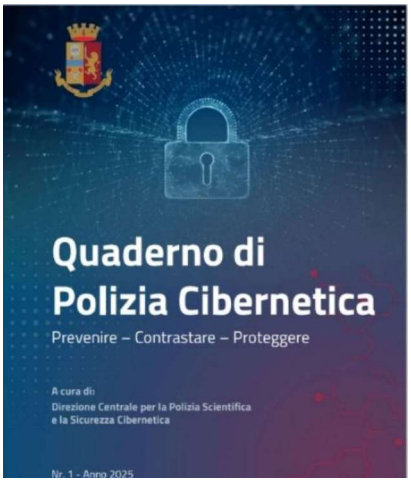
Inoltre, la costante cooperazione con i vari operatori del settore ha facilitato la creazione di un approccio integrato alla sicurezza cibernetica, in cui la condivisione di dati e indicatori di compromissione (IoC) diventa un fattore determinante per innalzare il livello di difesa complessivo. La collaborazione tra C.N.A.I.P.I.C. e partner tecnologici ha quindi permesso di sviluppare e applicare modelli più efficaci nella rilevazione e nel contrasto delle minacce informatiche. Il rafforzamento delle capacità di monitoraggio in tempo reale, così come la condivisione di informazioni sulle vulnerabilità emergenti, sono volti a un incremento della preparazione e della resilienza del sistema nel suo complesso.

Questi incontri settoriali, oltre a rappresentare un importante momento di aggiornamento operativo, hanno contribuito in maniera significativa a creare una rete di alleanze strategiche e a sviluppare una visione comune sulla protezione delle infrastrutture critiche. L'implementazione di un approccio condiviso alla cybersecurity, che tenga conto delle specificità di ogni settore, è oggi un imperativo

per rispondere in maniera tempestiva e efficace agli attacchi cibernetici, prevenendo e limitando i danni. Le esperienze e le competenze maturate in questo contesto hanno rappresentato un valore aggiunto per il C.N.A.I.P.I.C., che ha potuto così arricchire le proprie capacità operative, migliorando costantemente le attività di prevenzione, monitoraggio e contrasto alle minacce cibernetiche, nel rispetto dei principi di collaborazione, trasparenza e sicurezza nazionale.

20° ANNIVERSARIO DEL CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

L'organizzazione ***dell'evento*** per celebrare il 20° Anniversario del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche è stata un'attività complessa di pianificazione e coordinamento tra diversi esperti accademici e professionisti del settore. L'obiettivo centrale di tale iniziativa è stato quello di celebrare i risultati raggiunti dal C.N.A.I.P.I.C., quale punto di riferimento nell'ambito della sicurezza cibernetica e della protezione delle infrastrutture critiche, e al contempo avviare un approfondito dibattito sulle sfide future legate all'evoluzione del suo ruolo, in linea con l'evolversi delle minacce digitali.



Link Primo Numero Quaderno Polizia Cibernetica - Anno 2025

Le attività di preparazione hanno innanzitutto incluso l'organizzazione di due tavoli di lavoro tematici incentrati su due argomenti ritenuti di interesse strategico: le prospettive applicative dell'intelligenza artificiale e l'istituto del c.d. sottocopertura cyber.

L’idea alla base dei workshop è stata quella di coinvolgere in un laboratorio di riflessioni esponenti del mondo accademico e della magistratura, delle istituzioni e del settore privato, in cui ciascun partecipante si è reso disponibile a portare la propria esperienza e la propria visione sui due temi. Gli esiti sono stati trasfusi all’interno di una pubblicazione professionale, un’edizione speciale de “il Quaderno di polizia cibernetica”, dove tutti i partecipanti hanno avuto la possibilità di riportare il proprio contributo, ufficialmente presentata in occasione dell’evento dedicato al ventennale.

Il convegno finale, la cui complessa organizzazione ha coinvolto l’intera divisione, ha visto la partecipazione di personalità di rilievo istituzionale ed esperti universitari in qualità di relatori, quali il Prof. Stefano Zanero, la Prof.ssa Giusella Dolores Finocchiaro e il Prof. Massimiliano Sala. Un importante contributo è stato fornito anche da Padre Paolo Benanti, esperto in etica dell’intelligenza artificiale, che ha arricchito il dibattito con una riflessione sul rapporto tra nuove tecnologie e valori etici.

Il processo organizzativo ha richiesto un impegno costante in termini di coordinamento tra le diverse strutture e un’efficace gestione delle risorse al fine di assicurare il successo dell'evento. La diffusione di informazioni e il coordinamento con i media sono stati altrettanto cruciali, contribuendo a garantire visibilità e riconoscimento delle attività svolte dal C.N.A.I.P.I.C.

L’evento, conclusosi con gli interventi delle autorità, tra cui il Presidente del Comitato Parlamentare per la Sicurezza della Repubblica (COPASIR), Lorenzo Guerini, il Ministro dell’Interno, Matteo Piantedosi, e il Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri, Alfredo Mantovano, ha rappresentato un momento fondamentale per consolidare il ruolo strategico della sicurezza cibernetica nel contesto delle politiche di sicurezza nazionale e per rafforzare la cooperazione tra le istituzioni pubbliche, la Polizia di Stato e il mondo accademico.

La Sezione Cyberterrorismo

Nel corso del 2025 il Servizio Polizia Postale e per la Sicurezza Cibernetica ha avviato molteplici attività preventive di monitoraggio *O.S.Int* del web, nonché indagini di polizia giudiziaria in cui è stata approfondita la correlazione tra ideologie radicali e la dimensione digitale; di rilievo anche le attività svolte dai dipendenti Centri Operativi per la Sicurezza Cibernetica, attivi sul territorio e impegnati in una raccolta informativa più diretta, orientata ai fenomeni d'interesse per le Questure.

L'annualità 2025 è stata contraddistinta dall'incremento di minacce ibride – asimmetriche correlate alle molteplici tensioni geopolitiche globali che hanno coinvolto in primis gli scenari Russo-Ucraino e Israelo – Palestinese, determinando proiezioni interne sui profili di gestione dell'ordine e sicurezza pubblica.

La sofisticazione delle tecniche di attacco, la variazione delle forme di radicalizzazione attraverso social network non mainstream nonché l'ampliamento delle azioni di reclutamento e di finanziamento

online dei fenomeni terroristici, hanno richiesto una puntuale riconfigurazione degli strumenti di contrasto, imponendo altresì uno studio continuativo dei *network* radicali.

Peculiare attenzione è stata dedicata al fenomeno della minaccia ibrida, contraddistinta da asimmetricità e dal sistematico ricorso alla componente *cyber* per la destabilizzazione di enti istituzionali e infrastrutture critiche. In tale ambito è stato proseguito il monitoraggio del fenomeno della disinformazione e delle strategie poste in campo da attori ostili per l'alterazione dei processi elettorali attraverso la divulgazione di *fake news,* nonché la creazione di falsi profili istituzionali che possono disorientare la cittadinanza; l'attività di raccolta informativa ha consentito di individuare e rimuovere, con la cooperazione dei *provider*, numerosi profili *fake* impiegati per attività fraudolente o ancora più complesse strategie di impersonificazione.

La ricorrenza delle festività giubilari, il decesso del Pontefice Francesco e la successiva elezione al soglio pontificio di Papa Leone XIV, sono state tematiche di estrema sensibilità mediatica e pertanto oggetto di un'attenta analisi condotta su post, account, domini web, al fine di evitare che la peculiare contingenza storica venisse sfruttata per l'affermazione di ideologie radicali.

Il contrasto all'islamismo radicale violento di matrice jihadista è stato condotto guardando a molteplici fronti, tra cui percorsi individuali di radicalizzazione *online*, piattaforme di reclutamento attestate su social network alternativi non mainstream, forme di finanziamento occulto al terrorismo tramite il ricorso a criptovalute.

La propaganda jihadista online ha assunto molteplici diramazioni con canali, riviste periodiche, contenuti multimediali, gruppi che vengono puntualmente analizzati per ricostruire le possibili proiezioni sul territorio nazionale. Queste componenti sono state altresì affiancate dal contrasto alla c.d. "*cyber jihad"* ossia quell'espressione radicale dell'hacktivismo che vede crew di hacker attivi nell'attacco a infrastrutture sensibili per motivazioni di carattere religioso; in tal senso l'azione ha consentito di comprendere collegamenti tra crew, tecniche di attacco, nonché di apprendere in anticipo le possibili campagne ostili.

Il conflitto Israelo – Palestinese ha determinato l'estensione di un ampio fronte di dissenso interno che ha visto in particolare i movimenti antagonisti e i gruppi studenteschi attivi nell'organizzare eventi di contestazione, blocchi stradali, occupazioni universitarie, circostanze che hanno trovato una proiezione sistematica nell'ecosistema digitale; il monitoraggio del web in questo caso ha consentito

di reperire e isolare le possibili progettualità radicali o violente, sottoponendo alle Questure il materiale informativo utile ad affinare e integrare l'analisi di contesto svolta dalle D.I.G.O.S.

In particolare, sul fronte del contrasto all'antisemitismo online, sono state svolte peculiari attività di ricerca informativa in concomitanza delle ricorrenze delle festività religiose ebraiche; peculiare attenzione è stata dedicata inoltre alle possibili manifestazioni d'odio online in concomitanza della partita di calcio Italia - Israele del 14 ottobre 2025.

Nel contesto della missione internazionale "Global Sumud Flotilla", evento che ha determinato una considerevole esposizione mediatica e l'inasprimento del dibattito pubblico, è stata eseguita una specifica attività di *intelligence* informativa dedicata.

Altro fronte considerevole di attività è stato rappresentato dall'accelerazionismo neonazista, fenomeno che coinvolge giovanissimi, spesso adolescenti, i quali sono attratti da narrazioni estreme che fungono spesso da catalizzatore per l'espressione di disagi psicologici preesistenti e problematiche relative alla scarsa integrazione sociale. I *network* accelerazionisti sono un contesto prolifico per la divulgazione di istruzioni per la preparazione di armi, esplosivi o ancora concernenti tecniche e metodi per il compimento di atti violenti o di sabotaggio di servizi pubblici essenziali. Tali istruzioni sono poi poste in essere mediante il reperimento di risorse facilmente accessibili, come ad esempio l'utilizzo di stampanti 3D o l'approvvigionamento di elementi chimici di libera vendita.

In ambito di cooperazione internazionale il Servizio Polizia Postale costituisce il punto di contatto italiano della rete *Europol IRU - Internet Referral Unit*, coordinata dal Centro ECTC di Europol (European Counter Terrorism Center), per il monitoraggio dei contenuti terroristici online, e partecipa insieme agli operatori di polizia di altri paesi anche agli *action day* che in tale ambito vengono promossi con notevoli risultati operativi.

Di peculiare importanza operativa è la cooperazione strutturale svolta nell'ambito del progetto SIRIUS, attraverso strumenti operativi quali la piattaforma *PERCI*, funzionale all'attuazione della disciplina sulla rimozione dei contenuti terroristici online.

Parallelamente all'attività di intelligence e prevenzione, sul piano statistico, le attività investigative condotte sul territorio nazionale hanno portato a sottoporre a indagini un totale di 48 persone.

L’azione di contrasto sul web si concretizza nell’intervento della Sezione Cyberterrorismo, che ha gestito 76 segnalazioni emergenziali afferenti all’art. 14, comma 5, del Regolamento sulla rimozione dei contenuti terroristici e all’art. 18 del Digital Service Act, evidenziando il costante presidio sulle nuove disposizioni normative europee.

Sul fronte della cooperazione internazionale, la gestione di 66 segnalazioni O.S.C.A.D. e l’elaborazione di 165 messaggi SIENA hanno garantito un efficace scambio informativo con gli *stakeholder* esteri.

L’attività di contrasto ha avuto un riscontro tangibile dando seguito all’esecuzione di 47 perquisizioni sul territorio nazionale.

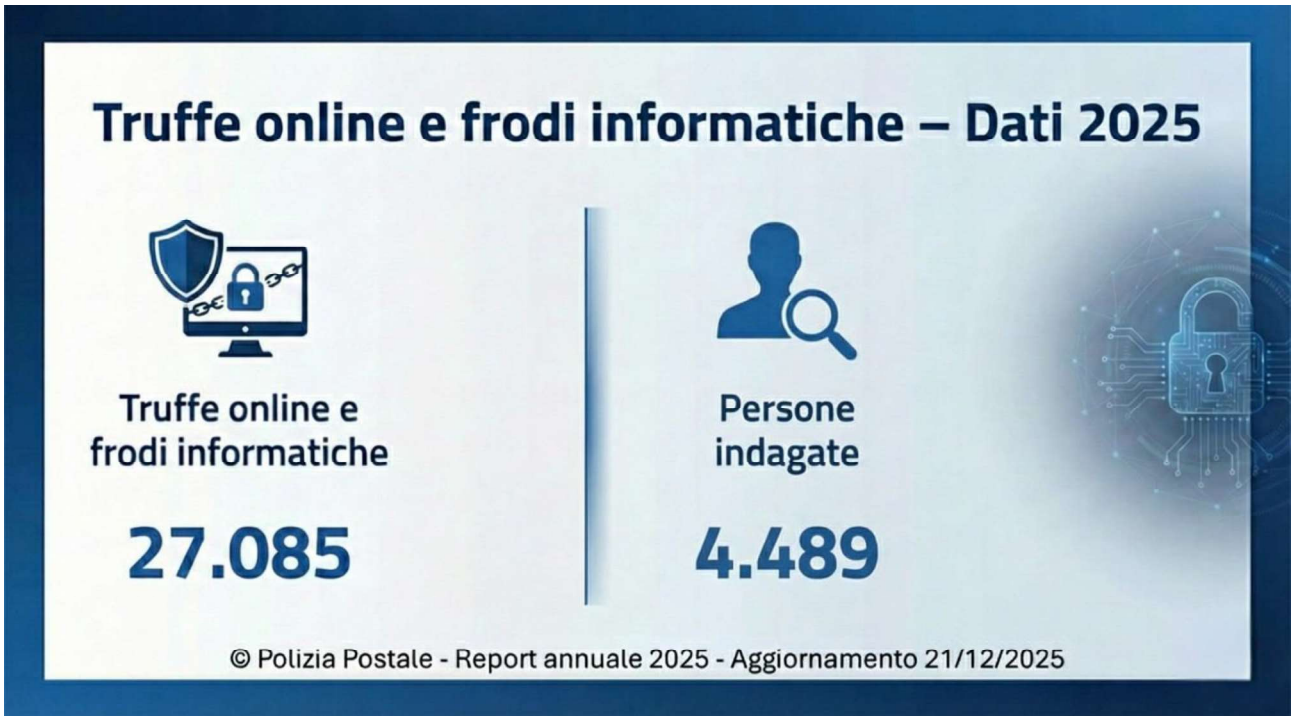
Nel mese di marzo, personale del C.O.S.C. di Perugia e della D.I.G.O.S. di Brescia ha dato esecuzione all’ordinanza di custodia cautelare in carcere emessa dal Tribunale di Perugia – Sezione GIP nei confronti di una persona indagata per il reato di cui all’ art. 270 quinquies c.p.

La posizione è emersa all’esito di un’articolata attività d’indagine svolta nell’ambito del contrasto al radicalismo islamico online di matrice jihadista; gli elementi acquisiti hanno consentito di rilevare una progressione nel comportamento dell’indagato da uno stadio di semplice partecipazione *online* a canali tematici a concrete progettualità per la causa jihadista.

LA QUARTA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Luigi Bovio, *Primo Dirigente della Polizia di Stato, Direttore*

Le evidenze acquisite nell'azione di contrasto più recente al c.d. *Financial Cybercrime* hanno confermato la persistente diffusione di condotte truffaldine, inducendo la Polizia di Stato a consolidare la struttura operativa dedicata, rafforzando ulteriormente la IV Divisione recentemente istituita al fine di contrastare l'ecosistema dei reati finanziari.



Si è potuto accertare che le principali modalità di realizzazione delle truffe avvengono attraverso campagne di *phishing* (anche nelle varianti dei cc.dd. "*vishing*" e "*smishing*")[1], rivolte a persone fisiche, PMI e grandi società. Tali condotte, veicolate tramite mail, chiamate vocali e sms apparentemente provenienti da Ministeri, enti pubblici o istituti di credito, hanno come obiettivo l'acquisizione di dati personali e sensibili, nonché *password* e credenziali di accesso a domini riservati, per la perpetrazione di reati contro il patrimonio.

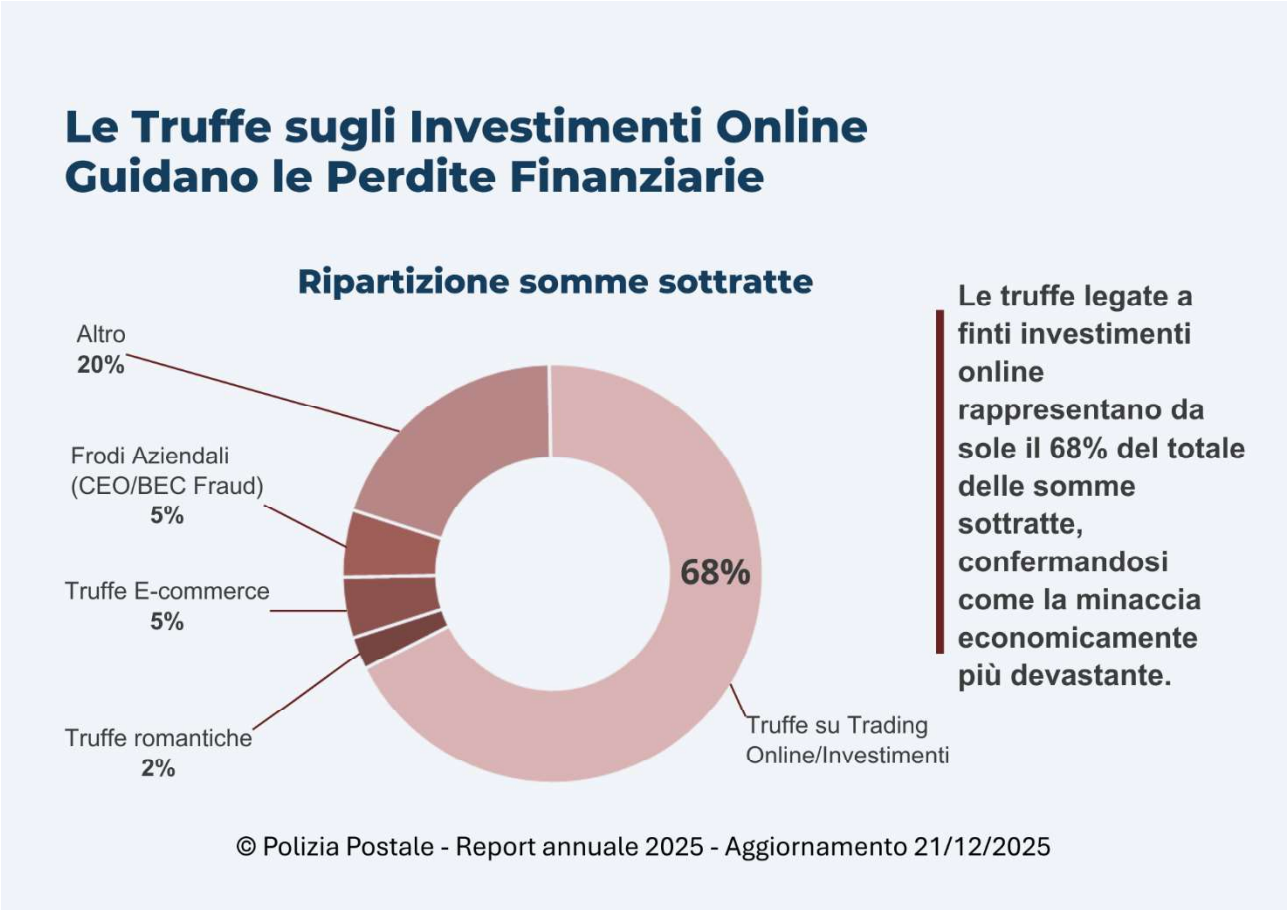
Analogamente, permane la pericolosità delle frodi basate sul *social engineering*, in particolare il *BEC fraud*,[2] e il *CEO fraud*[3], favorite dall'incremento delle comunicazioni digitali e dall'uso diffuso della rete nelle transazioni commerciali. Tali condotte mirano a ingannare il personale aziendale con messaggi apparentemente provenienti da dirigenti o amministratori, inducendo alla trasmissione di informazioni riservate o al compimento di operazioni finanziarie illecite. A tal fine l'ottimale contrasto di tali fenomeni criminali non può prescindere, da un lato da un'educazione digitale più capillare e da un costante aggiornamento delle strategie investigative.

L'azione di contrasto, infatti, ha evidenziato una crescita qualitativa del contesto criminale nel *financial cybercrime*: la possibilità di conseguire ingenti guadagni attraverso condotte delinquenziali realizzabili su larga scala ha innalzato il profilo dei soggetti coinvolti, con l'interesse di consorterie criminali anche di stampo mafioso un tempo concentrate su altri fenomeni illeciti, per lo più di natura predatoria. La particolare natura insidiosa di tali condotte impone che l'attività investigativa si sviluppi anche tramite i canali ufficiali di cooperazione internazionale, necessaria per ricercare tracce informatiche e finanziarie oltre i confini nazionali; circostanza che talvolta complica la raccolta delle evidenze, laddove i Paesi stranieri non siano pienamente collaborativi con l'Autorità Giudiziaria italiana.

[1] L'illecito procacciamento di codici "one-time", token virtuali e password dispositive si realizza mediante il ricorso a mail, chiamate vocali, messaggi e sms che sembrano provenire da banche o altri enti apparentemente legittimati a richiedere informazioni sensibili.

[2] Il *BEC fraud* (Business Email Compromise) è una frode che si realizza attraverso la compromissione di caselle di posta elettronica attivate allo scopo di acquisire informazioni utili al perfezionamento della condotta illecita.

[3] Il *CEO fraud* (Chief Executive Officer) è una tecnica di *social engineering* in cui soggetti malintenzionati si presentano come dirigenti o amministratori dell'azienda, inducendo personale interno ad autorizzare pagamenti urgenti o a fornire dati riservati, sfruttando l'apparente autorevolezza del mittente.



Ulteriore elemento di complessità è rappresentato dall'uso crescente delle criptovalute[4], strumento spesso utilizzato dalla criminalità organizzata anche all'estero per occultare proventi illeciti. Sebbene gran parte delle valute virtuali risulti tracciabile grazie alle transazioni registrate sulle *blockchain*[5], la

[4] Utilizzate come strumento per perfezionare l'efficace riciclaggio dei proventi illeciti.

[5] Ogni utente e ciascun portafoglio virtuale (*wallet*) è identificato nella *blockchain* da un codice univoco alfanumerico. Seppure tale caratteristica ne determina la natura pseudo-anonima rimane tuttavia astrattamente possibile riuscire a collegare un indirizzo *wallet* all'IP con cui è stato gestito. Diventa

mappatura di alcune monete caratterizzate da elevati livelli di anonimizzazione presenta difficoltà operative significative.

Proprio per fronteggiare tale scenario, il Servizio Polizia Postale e per la Sicurezza Cibernetica ha investito in un percorso strutturato di formazione specialistica, rivolto sia a livello centrale che appannaggio degli operatori distribuiti nelle 18 articolazioni dei Centri Operativi per la Sicurezza Cibernetica e relative SOSC. Questo potenziamento consente di utilizzare in modo pienamente operativo gli strumenti investigativi dedicati, massimizzando l'efficacia delle attività di tracciamento sulle criptovalute.

Il panorama delle truffe attraverso proposte di investimento online (*trading online*) mostra un crescente livello di sofisticazione, anche grazie all'utilizzo di strumenti basati sull'intelligenza artificiale quale il c.d. *Deep fake* recentemente normato dal Legislatore con l'introduzione di un reato *ad hoc* volto a contrastare manipolazioni digitali.

In particolare, si parla di *Deep fake*, allorquando audio o video vengono manipolati con l'Intelligenza Artificiale al fine di attribuirli a personaggi noti del mondo politico e dello spettacolo, come fonte più credibile di un qualunque contenuto diffuso. Le finalità principali riguardano le sponsorizzazioni sulle principali piattaforme social di investimenti finanziari.

Inoltre, lo sfruttamento della IA sta portando all'evoluzione del su citato CEO Fraud. In questo scenario, i cybercriminali, dopo l'acquisizione di dati e informazioni da fonti aperte relative al soggetto bersaglio, possono ricrearne la voce o le movenze permettendo al falso amministratore di impartire disposizioni a dirigenti aziendali, inducendoli a effettuare uno o più bonifici correlati a una inesistente operazione finanziaria che viene presentata come riservata e urgente.

L'uso diffuso di Internet ha altresì favorito la consumazione di reati contro la proprietà intellettuale. In tale contesto, la Polizia Postale e per la Sicurezza Cibernetica è impegnata nella lotta alla contraffazione, anche grazie all'impiego dell'istituto sottocopertura, che consente di infiltrare operatori specializzati all'interno di strutture criminali strutturate. Tra i principali settori colpiti

quindi possibile, ad esempio, associare un *wallet* a un' area geografica, elemento utile all'identificazione del possessore.

emergono le piattaforme Pay-TV/IPTV, la moda e i luxury goods, le polizze assicurative, la vendita di falsi biglietti per eventi culturali, i siti clone e la diffusione illecita di opere audiovisive.

IL CASO: "ARRESTO SANTONA AI"

Il 26 luglio 2025 la Polizia di Stato ha arrestato a Lido di Ostia una donna di 55 anni, destinataria di una condanna definitiva a 9 anni di reclusione per associazione per delinquere, esercizio abusivo della professione medica e morte come conseguenza di altro reato, per fatti commessi tra il 2019 e il 2021.

L'indagine, condotta dal Centro Operativo per la Sicurezza Cibernetica di Torino e coordinata dalla Procura della Repubblica, ha riguardato una setta denominata "Unisono", attiva sui social e sulle piattaforme di messaggistica. La donna, ritenuta a capo dell'organizzazione, convinceva numerose vittime dell'esistenza di un'intelligenza artificiale "miracolosa", chiamata "Marie", che avrebbe potuto curare gravi patologie – incluso il cancro – tramite presunti processi di modifica del DNA.

Le vittime inviavano quotidianamente i propri parametri vitali tramite chat e ricevevano indicazioni terapeutiche arbitrarie, comprese prescrizioni di farmaci o sospensioni di cure mediche. Questa manipolazione ha portato alcune persone ad abbandonare terapie salvavita: in un caso, una donna è deceduta dopo essere stata indotta a interrompere chemioterapia e interventi programmati.

Il gruppo, che comprendeva anche un tesoriere, un tecnico informatico e un fisioterapista (già condannati con pena sospesa), ha ricevuto numerosi versamenti dalle vittime. L'attività illecita ricostruita ammonta a circa 100.000 euro, cifra probabilmente inferiore al reale volume di denaro non tracciabile.

IL CASO: "OPERAZIONE GHOTA 2"

Il Centro Operativo per la Sicurezza Cibernetica di Catania e il Servizio Polizia Postale, coordinati dalla locale Procura della Repubblica, ha concluso una complessa indagine sullo streaming illegale, eseguendo un'ordinanza cautelare agli arresti domiciliari nei confronti di otto persone, alcune residenti all'estero. Gli indagati sono stati accusati, nel rispetto della presunzione d'innocenza, di associazione per delinquere finalizzata alla diffusione illecita di palinsesti pay-tv, accesso abusivo a sistemi informatici e frode informatica. L'inchiesta ha rappresentato lo sviluppo della precedente

operazione “Gotha” del 2022 e ha permesso di ricostruire un’organizzazione criminale strutturata gerarchicamente (capo, vice, master, admin, tecnico, reseller), con basi in diverse città italiane e all’estero. Attraverso l’analisi di dispositivi sequestrati e flussi finanziari, è emerso un sistema di IPTV illegali che distribuiva contenuti protetti di piattaforme come Sky, Dazn, Mediaset, Amazon Prime e Netflix, generando profitti stimati in milioni di euro mensili. L’organizzazione si avvaleva di server esteri, identità fittizie, documenti falsi e comunicazioni cifrate per eludere le indagini, imponendo ai reseller specifiche regole operative. I proventi illeciti ricostruiti per il periodo monitorato ammontavano a circa 10 milioni di euro, con danni potenziali per l’industria audiovisiva stimati in oltre i 30 milioni di euro al mese, per un bacino di circa 900.000 utenti serviti.

PREMIO FAPAV: LA POLIZIA POSTALE PREMIATA PER L’OPERAZIONE "TAKEN DOWN"

L’operazione internazionale "Taken Down", condotta nel novembre 2024, ha portato allo smantellamento di una complessa infrastruttura informatica utilizzata per lo streaming illegale di segnali audiovisivi e contenuti multimediali ad accesso condizionato.

L'inchiesta ha rivelato l'esistenza di un'organizzazione criminale transnazionale che gestiva un giro d'affari illecito superiore ai 250 milioni di euro al mese, fornendo il servizio illegale a oltre 22 milioni di utenti in tutta Europa e in altri paesi.

Durante l'operazione, sono stati rintracciati e sequestrati 80 pannelli in Italia, che gestivano il flusso di IPTV illegale, e sono stati spenti 9 server in Romania e a Hong Kong, utilizzati per diffondere i contenuti piratati in tutta Europa e oltre. Inoltre, sono stati individuati e fermati in Inghilterra e in Olanda 3 amministratori di alto livello responsabili della gestione della rete criminale.

Le perquisizioni hanno portato al sequestro di criptovalute per oltre 1.650.000 euro e di denaro contante per oltre 40.000 euro, una somma che rappresenta solo una minima parte di un giro d'affari stimato in circa 3 miliardi di euro l'anno, con danni diretti per oltre 10 miliardi di euro alle aziende televisive.

L'operazione ha avuto un impatto significativo sul contrasto alla pirateria audiovisiva e ha ricevuto un prestigioso riconoscimento da parte della FAPAV (Federazione per la Tutela delle Industrie dei Contenuti Audiovisivi e Multimediali), che lo scorso 15 dicembre ha premiato la Polizia Postale per l'efficacia e la portata dell'intervento.

IL CASO: "OPERAZIONE CAGLIOSTRO"

Il Centro Operativo per la Sicurezza Cibernetica di Bologna in sinergia con la Guardia di Finanza, coordinate dalla Procura della Repubblica di Bologna, hanno eseguito numerose perquisizioni sul territorio nazionale e disposto il sequestro preventivo d'urgenza del portale voltaiko.com e di 95 conti correnti collegati al gruppo societario coinvolto.

Le attività investigative hanno ricostruito un'associazione per delinquere strutturata secondo un modello piramidale di network marketing multi-level, finalizzata alla commissione di numerose truffe, anche ai danni di soggetti vulnerabili, basate su uno schema Ponzi. Il gruppo proponeva falsi investimenti "green" nel noleggio di pannelli fotovoltaici all'estero, garantendo rendimenti in "energy point", mentre gli impianti e le attività promesse risultavano inesistenti. Secondo le stime investigative, circa 6.000 persone avrebbero investito attraverso il portale, generando flussi finanziari

per circa 80 milioni di euro. La Procura ha quindi disposto il sequestro del sito e dei rapporti finanziari riconducibili alle società e agli indagati.

Nel corso delle perquisizioni sono stati sequestrati criptovalute, dispositivi elettronici, beni di lusso, lingotti d'oro e documentazione utile alle indagini.

LA QUINTA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Santo Mirabelli, *Primo Dirigente Tecnico della Polizia di Stato, Direttore*

La Quinta Divisione del Servizio provvede a:

- garantire il supporto tecnico-operativo alle attività d'istituto della Specialità in materia di intelligenza artificiale per la sicurezza cibernetica e di digital forensics;
- curare i rapporti con Enti e Istituzioni, pubbliche e private, attive nel campo della ricerca e dell'innovazione scientifica, per il costante aggiornamento di metodologie e soluzioni tecnologiche nonché concorre alla definizione dei piani di formazione specialistica;
- predisporre la pianificazione delle acquisizioni IT e la programmazione triennale dei fabbisogni con la conseguente gestione dei contratti di fornitura e delle procedure di acquisto;
- coordinare, nei settori tecnici di rispettiva competenza, le articolazioni territoriali della Specialità anche in relazione all'analisi delle esigenze e alla realizzazione di nuovi sistemi IT a supporto delle attività info-investigative;
- gestire e implementare l'infrastruttura tecnologica del Servizio attuando gli indirizzi e le politiche di sicurezza IT delineate dai competenti uffici della Polizia di Stato, secondo gli standard e le normative di settore;
- gestire tutti gli asset tecnologici della Specialità a livello nazionale e svolgere le funzioni di focal point per gli accessi alle banche dati istituzionali e investigative in uso al Servizio.

In tema di Innovazione e Ricerca Tecnologica, presso la predetta divisione, è stato istituito **l'AiLab4Cyber**, ovvero un laboratorio di ricerca nel settore dell'intelligenza artificiale. In particolare, il predetto laboratorio provvede ad analizzare gli impatti del Regolamento Europeo sull'Intelligenza Artificiale in relazione ai modelli e sistemi di IA idonei a supportare le investigazioni nel settore cibernetico e dell'analisi delle immagini per il contrasto alla pedo-pornografia.

Vengono, altresì, svolte attività di ricerca di mercato per comprendere le nuove tecnologie disponibili e in via di sviluppo. In merito, sono state consolidate collaborazioni con il mondo accademico attraverso la condivisione di progetti innovativi che vedono l'impiego dell'Intelligenza Artificiale sia nel settore delle investigazioni di pertinenza della Specialità che nella protezione delle infrastrutture critiche.

Per quanto attiene le dotazioni tecnologiche a supporto delle investigazioni, nel corso del 2025 si è provveduto a dare particolare impulso all'avvio di un rilevante programma di potenziamento, atteso il recente incremento dell'organico della Specialità. In particolare, sono state acquisite:

- tecnologie a supporto delle attività di digital-forensics mediante la fornitura di nuove apparecchiature hardware a elevate prestazioni nonché tecnologie software per l'acquisizione e l'analisi forense di dispositivi digitali;
- strumentazioni di ultima generazione volte all'analisi degli incidenti informatici;
- piattaforme di servizi info-investigativi volte a supportare le attività d'indagine;
- postazioni di lavoro fisse e mobili per le esigenze degli uffici territoriali e centrali.

Oltre alle già menzionate attività di potenziamento delle dotazioni tecnologiche a supporto delle investigazioni sopra descritte, si è provveduto a finalizzare tutte le procedure amministrative volte al rinnovo dei contratti già in essere alla Specialità sempre in relazione ai tool di natura investigativa.

La Quinta Divisione ha assicurato un impegno rilevante nei contesti internazionali, prendendo parte a numerosi tavoli di lavoro. Di particolare rilievo è stato il ruolo svolto, sotto la Presidenza Italiana, nell'ambito del gruppo G7 Roma-Lione, sottogruppo High Tech Crime, e in ambito Europol, dove sono stati ricoperti vari ruoli sia nel Consiglio di amministrazione dell'EuCB (European Clearing Board), un organismo volto a individuare le tecnologie più innovative a supporto delle investigazioni, che presso i vari gruppi di lavoro costituiti presso detto organismo tra cui quello concernente la Strategia sull'uso delle tecnologie di IA a supporto delle Forze di Polizia

Sempre in tema di Intelligenza Artificiale, la Quinta Divisione del Servizio Polizia Postale ha svolto un ruolo di particolare rilievo nell'ambito dei lavori del gruppo di esperti sull'IA, costituito in seno

alla Commissione Europea, avente come obiettivo quello di analizzare gli impatti del Regolamento Europeo sull'IA nel settore delle Forze di Polizia, la cui piena attuazione avverrà nel 2026.

La attività svolte nell'ambito dell'Innovation Lab hanno evidenziato la rilevanza delle attività di innovazione e della ricerca tecnologica a supporto delle investigazioni. Infatti, come noto, i rapidi progressi tecnologici hanno avuto profondo impatto su come la criminalità utilizzi dette nuove tecnologie per implementare tattiche operative di attacco sempre più complesse, che possono essere contrastate mediante l'utilizzo di tecnologie che sfruttano l'impiego dell'IA e una stretta collaborazione tra le forze dell'ordine, supportate anche da Europol.

Gli sforzi della Divisione si sono rivelati significativi anche in ambito formativo, con la realizzazione, in tema di sicurezza informatica e di intelligenza artificiale, di moduli sull'*awareness* e sull'uso corretto e responsabile delle tecnologie di IA, con particolare riferimento sia ai benefici che ai possibili rischi associati.

Detti moduli formativi sono stati resi disponibili sia al personale della Polizia di Stato (in vari ruoli direttivi e non direttivi), sia a determinate categorie di utenza, inclusi i partecipanti al corso di Cyber Academy realizzato con gli Istituti ITS; sono stati realizzati inoltre anche alcuni moduli sull'IA di livello universitario.


POLIZIA