Resoconto attività 2022
della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica

Nel 2022 la Polizia Postale è stata chiamata a far fronte a continue e sempre più evolute sfide investigative sulle macro-aree di competenza, in particolare negli ambiti della prevenzione e contrasto alla pedopornografia online, della protezione delle infrastrutture critiche di rilevanza nazionale, del financial cybercrime e di quelle relative alle minacce eversivo-terroristiche, riconducibili sia a forme di fondamentalismo religioso che a forme di estremismo politico ideologico, anche in contesti internazionali.

CENTRO NAZIONALE PER IL CONTRASTO ALLA PEDOPORNOGRAFIA ONLINE (C.N.C.P.O.)

In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, lo sforzo della Polizia Postale e delle Comunicazioni nell'anno 2022 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati in danno di minori.

Il **Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)** nel 2022 ha confermato il suo ruolo di punto di riferimento e di coordinamento nazionale dei **Centri Operativi Sicurezza Cibernetica – COSC** della Polizia Postale nella lotta alla pedofilia e pornografia minorile online.

L'analisi dei dati relativi all'anno di riferimento ha confermato la lieve diminuzione dei casi trattati già evidenziata nella rilevazione di medio termine. La flessione negativa dei dati è stata riscontrata anche in riferimento al numero delle segnalazioni provenienti da organismi internazionali attivi nella protezione dei minori in rete. L'impegno profuso dalla Specialità si è concentrato nel reprimere episodi di particolare gravità, con l'effetto rilevabile di evidenziare un maggior numero di individui sottoposti a pene detentive.

Nell'ambito poi delle segnalazioni relative alla pubblicazione di contenuti pedopornografici su social network, si è evidenziato un fenomeno per il quale veniva intaccata

la reputazione dei vari titolari di profili social attraverso la pubblicazione di materiale scabroso di natura pedopornografica con accessi abusivi massivi a profili privati di ignari cittadini e di persone dotate di rilevanza mediatica, politica o di altra natura.

La fine dell'emergenza sanitaria, con la progressiva ripresa delle attività nella direzione di un recupero della normalità, potrebbe aver contribuito a ridurre l'isolamento sociale, facendo rilevare nel 2022 una riduzione della circolazione globale di materiale pedopornografico su circuiti internazionali, che non ha però inciso sull'attività di contrasto. Infatti, **è stato registrato un aumento dei soggetti individuati e deferiti per violazioni connesse ad abusi in danno di minori**.

In particolare, nell'ambito dell'attività di contrasto coordinata dal Centro sono stati trattati complessivamente **4.542 casi**, che hanno consentito di indagare **1.463 soggetti**, di cui **149 tratti in arresto** per reati connessi alla materia degli abusi tecnomediati in danno di minori, con un aumento di persone tratte in arresto di circa il **+8%** rispetto allo stesso periodo dell'anno precedente.

Per quanto concerne l'attività di prevenzione svolta dal C.N.C.P.O. attraverso una continua e costante attività di monitoraggio della rete, sono stati visionati **25.696** siti, di cui **2.622** inseriti in black list e oscurati, in quanto presentavano contenuti pedopornografici.

PEDOPORNOGRAFIA E ADESCAMENTO ONLINE	**2021**	**2022***	**Variazione percentuale**
Persone indagate	1.419	1.463	**+3%**
Siti in Black List	2.543	2.622	**+3%**
* - dati rilevati il 27/12/2022			

Adescamento online

Nel periodo di riferimento sono stati trattati **424** casi per adescamento online: anche quest'anno la fascia dei preadolescenti (età 10-13 anni) è quella più coinvolta in interazioni sessuali tecnomediate, **229** rispetto al totale.

Continua a preoccupare il lento incremento dei casi relativi a bambini adescati di età inferiore ai 9 anni, trend che è diventato più consistente a partire dalla pandemia. Social network e videogiochi online sono i luoghi di contatto tra minori e adulti più frequentemente teatro delle interazioni nocive, a riprova ulteriore del fatto che il rischio si concretizza con maggiore probabilità quando i bambini e i ragazzi si esprimono con spensieratezza e fiducia, nei linguaggi e nei comportamenti tipici della loro età.

Cyberbullismo

Si registra una leggera flessione anche dei casi di cyberbullismo che può essere interpretata come effetto della normalizzazione delle abitudini dei ragazzi: non si può escludere che il ritorno ad una vita sociale priva di restrizioni abbia avuto un'influenza positiva sulla qualità delle interazioni sociali, delle relazioni tra coetanei e che la costanza dell'opera di

sensibilizzazione svolta dalla Polizia Postale, presso le strutture scolastiche, abbia mantenuto alta l'attenzione degli adulti e dei ragazzi stessi sulla necessità di agire responsabilmente e correttamente in rete.

Nel periodo di riferimento sono stati trattati **323** casi di cyberbullismo.

CYBERBULLISMO	**2021**	**2022***
Casi trattati vittime 0-9 anni	27	17
Casi trattati vittime 10-13 anni	112	87
Casi trattati vittime 14-17 anni	319	219
TOTALE	**458**	**323**
* - dati rilevati il 27/12/2022		

	2021	**2022***
Minori denunciati per Cyberbullismo	117	128
* - dati rilevati il 27/12/2022		

Sextortion

È un fenomeno che di solito colpisce gli adulti in modo violento e subdolo, fa leva su piccole fragilità ed esigenze personali, minacciando, nel giro di qualche click, la tranquillità delle persone.

Recentemente le **sextortion** stanno interessando sempre più spesso vittime minorenni, con effetti lesivi potenziati: la vergogna che i ragazzi provano impedisce loro di chiedere aiuto ai genitori o ai coetanei di fronte ai quali si sentono colpevoli di aver ceduto e di essersi fidati di perfetti e "avvenenti" sconosciuti.

La sensazione di sentirsi in trappola che sperimentano le vittime è amplificata spesso dalla difficoltà che hanno nel pagare le somme di denaro richieste. Nel corso dell'anno sono stati trattati **130 casi,** la maggior parte dei quali nella fascia **14-17 anni,** più spesso in danno di vittime maschili.

C.N.C.P.O. – ATTIVITÀ DI POLIZIA GIUDIZIARIA

Si riportano di seguito, le attività investigative di maggior rilievo coordinate dal Centro Nazionale per il Contrasto alla Pedopornografia online:

OPERAZIONE "*MEET UP*", condotta in modalità sotto copertura dal personale del Centro Operativo Sicurezza Cibernetica della Polizia Postale Piemonte e Valle D'Aosta, all'interno di canali *Telegram* dedicati alla diffusione, anche mediante sottoscrizione di abbonamenti a pagamento, di contenuti realizzati mediante sfruttamento sessuale di minori. Gli investigatori, interagendo direttamente in *chat* con gli utenti responsabili della diffusione, anche grazie alla capitalizzazione delle tracce informatiche e finanziarie enucleate, hanno potuto identificare gli

utilizzatori dei *nicknames* destinatari dei 26 decreti di perquisizione emessi dall'A.G. procedente, che hanno consentito di indagare 26 persone, 3 delle quali tratte in arresto.

OPERAZIONE "*GREEN OCEAN*", svolta in modalità sotto copertura dal Centro Operativo Sicurezza Cibernetica della Polizia Postale di Palermo su piattaforme di *file sharing* e di messaggistica utilizzate per la diffusione di contenuti di pornografia minorile. All'esito dell'indagine sono state eseguite, su tutto il territorio nazionale, coordinate dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, 32 perquisizioni nei confronti di altrettanti indagati, che hanno consentito di trarre in arresto 13 persone per detenzione di ingente quantità di materiale pedopornografico. In un caso, la perquisizione informatica effettuata sui dispositivi ha messo in luce l'esistenza di abusi fisici in danno di due minori, all'epoca dei fatti dell'età di 2 e 3 anni.
L'attività in argomento ha consentito, inoltre, di individuare centinaia di account riconducibili a utenti esteri, per i quali sono stati interessati i relativi collaterali.

OPERAZIONE *"FAMIGLIE DA ABUSI"*, svolta in modalità sotto copertura nell'ambito del contrasto alla pedopornografia online sul gruppo *Telegram* "Famiglie da Abusi" e condotta dai Centri Operativi Sicurezza Cibernetica di Roma, Bologna, Milano, Napoli e Catania, coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, ha consentito di arrestare 5 persone ritenute responsabili di diffusione e detenzione di materiale di sfruttamento sessuale di minori online.
In particolare, gli indagati appartenevano a una comunità ristretta dedita allo scambio di materiale pedopornografico, anche autoprodotto dagli stessi partecipanti.

OPERAZIONE *"REVELATUM"*, condotta dal Centro Operativo Sicurezza Cibernetica della Polizia Postale della Puglia nell'ambito del contrasto alla pedopornografia online, ha visto coinvolti 72 indagati, destinatari di altrettanti decreti di perquisizione su tutto il territorio nazionale, emessi dall'A.G. procedente.
L'indagine, avviata alla fine del 2020, ha preso le mosse dall'analisi delle tracce informatiche collegate a un *link* afferente a un *cloud* attestato sulla piattaforma di *file hosting* "Mega.nz".
Gli Uffici territoriali della Polizia Postale, coinvolti nella fase esecutiva dell'operazione e coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, hanno denunciato 59 persone per detenzione e diffusione di materiale pedopornografico e altre 7 sono state tratte in arresto in flagranza di reato per detenzione di ingente quantitativo di materiale realizzato mediante sfruttamento dei minori degli anni 18.

OPERAZIONE *"BROKEN DREAMS"*, avviata dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni a seguito di una segnalazione di operazioni sospette pervenuta, tramite Banca d'Italia, dalla società statunitense *Paypal*, dedita alla fornitura di servizi di pagamento e trasferimento digitale di denaro.
Dall'analisi di un portafoglio elettronico riconducibile a una minore di nazionalità dominicana residente in Italia, gli investigatori hanno ricostruito le tracce relative alle transazioni in ingresso, caratterizzate da causali riconducibili alla sottoscrizione di abbonamenti periodici afferenti a sessioni di *"Live Distant Child Abuse"*, realizzate in *streaming* su piattaforme di

videochat. L'indagine ha consentito di individuare 18 soggetti per i quali l'Autorità giudiziaria ha emesso altrettanti decreti di perquisizione, attività che si sono concluse con 17 indagati, due dei quali in stato di arresto.

OPERAZIONE *"LUNA"*, avviata dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale del Friuli Venezia Giulia sulla scorta delle risultanze emerse a seguito dell'analisi forense eseguita sui supporti informatici sequestrati a un indagato nell'ambito di altra operazione di polizia giudiziaria, si è conclusa con la denuncia di 25 persone, 7 delle quali minorenni e una tratta in arresto. L'attività, che ha coinvolto tutti gli Uffici territoriali della Specialità, coordinati dal C.N.C.P.O. del Servizio Polizia Postale e delle Comunicazioni, ha consentito di indagare 25 soggetti, di cui uno in stato di arresto.

OPERAZIONE *"ESTOTE PARATI":* L'attività di indagine del Centro Operativo Sicurezza Cibernetica della Polizia Postale di Palermo trae origine dalla più ampia Operazione "DICTUM", avviata a seguito di una segnalazione pervenuta nell'ambito della cooperazione internazionale di polizia, che ha condotto all'individuazione di numerosi soggetti responsabili di aver condiviso in rete materiale pedopornografico tramite la piattaforma *Mega.nz*.
L'analisi del materiale detenuto in *cloud,* ha consentito la denuncia di 27 persone, 3 delle quali sono state tratte in arresto in flagranza di reato per detenzione di ingente quantitativo di materiale realizzato mediante lo sfruttamento sessuale di minori.

OPERAZIONE *"AREA PEDONALE"*, avviata in modalità sotto copertura dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale Piemonte e Valle D'Aosta, con il coordinamento di questo Servizio, sulla piattaforma di messaggistica istantanea *Telegram*, sotto la direzione della Procura della Repubblica di Torino. Sono state eseguite contestualmente 12 perquisizioni su tutto il territorio nazionale, ad esito delle quali sono stati denunciati in stato di libertà 9 utenti per diffusione e detenzione di materiale pedopornografico, mentre altri 3 sono stati tratti in arresto in flagranza di reato.

OPERAZIONE *"BLACK ROOM"*: condotta in modalità sotto copertura dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Napoli all'interno di canali *Telegram*, ha consentito la denuncia di 21 persone e l'arresto di altrettante 5, tra cui figura l'amministratore della pagina, creatore di un bot *ad hoc* per la condivisione automatica di materiale a fronte del pagamento di corrispettivi in denaro.

OPERAZIONE *"COCITO":* il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Milano ha arrestato un trentatreenne romano per violenza sessuale aggravata ai danni della propria figlia, per detenzione, produzione e cessione di materiale pedopornografico e per adescamento di minorenne. L'attività è stata condotta in modalità sotto copertura all'interno di un canale *Telegram*, ove era avvenuta la condivisione del materiale multimediale inerente ali abusi, a cura degli operatori sul territorio con il costante coordinamento e supporto del C.N.C.P.O.

OPERAZIONE *"DICTUM III":* L'attività di indagine del Centro Operativo Sicurezza Cibernetica della Polizia Postale per la Toscana trae origine dalla più ampia Operazione "DICTUM", avviata a seguito di una segnalazione pervenuta nell'ambito della cooperazione internazionale di polizia, che ha condotto all'individuazione di numerosi soggetti responsabili di aver condiviso in rete materiale pedopornografico tramite la piattaforma *Mega.nz*.
All'esito delle attività, sono state denunciate 30 persone accusate di aver condiviso materiale pedopornografico tramite la citata piattaforma di cloud, di cui 5 sono state tratte in arresto in flagranza di reato per detenzione di ingente quantitativo di materiale realizzato mediante lo sfruttamento sessuale di minori.

OPERAZIONE "POISON": Condotta dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Pescara, è scaturita su impulso del CNCPO a seguito di una segnalazione del Servizio Emergenza Infanzia 114, relativa alla condivisione, su gruppi social, oltre che di contenuti pedopornografici, anche di carattere zoofilo, necrofilo, *scat*, *splatter*, nonché di violenza estrema, apologia del nazismo/fascismo, atti sessuali estremi e mutilazioni, atti di crudeltà verso essere umani e animali, che ha interessato, nella fase esecutiva, diverse articolazioni territoriali della Specialità.
All'esito delle attività sono stati denunciati in stato di libertà 7 minori per diffusione e detenzione di materiale pedopornografico.

ARRESTO FIRENZE: Personale del Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Firenze ha tratto in arresto un cittadino statunitense trovato in possesso di ingente quantitativo di materiale pedopornografico realizzato utilizzando minori di anni diciotto. La vicenda trae origine da una segnalazione che il CNCPO ha ricevuto dal collaterale statunitense.

CENTRO NAZIONALE ANTICRIMINE PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.)

Nell'esercizio della propria missione istituzionale, il Servizio Polizia Postale e delle Comunicazioni - Organo del Ministero dell'interno per la sicurezza delle telecomunicazioni garantisce, fra l'altro, ai sensi dell'art. 7 bis DL 144 del 2005 e del DM 15 agosto 2017 - Direttiva sul riordino dei comparti di Specialità delle Forze di Polizia – la protezione delle infrastrutture critiche informatizzate del Paese.

Nell'attuale e particolare contesto internazionale, l'*escalation* delle tensioni geopolitiche connesse al conflitto in Ucraina continua ad avere significativi riverberi anche in materia di sicurezza cibernetica. Risultano, infatti, in corso campagne massive a livello internazionale dirette verso infrastrutture critiche, sistemi finanziari e aziende operanti in settori strategici quali comunicazione e difesa, tra le quali figurano campagne di *phishing*, diffusione di *malware* distruttivi (specialmente *Ransomware*), attacchi Ddos, campagne di disinformazione e *leak* di database. Inoltre, alcuni tra i più pericolosi gruppi di hacker criminali

hanno deciso di schierarsi a favore della Russia, altri con l'Ucraina, prendendo di fatto parte al conflitto nel c.d. "dominio cibernetico".

In tal senso, come noto, il conflitto russo-ucraino ha comportato una recrudescenza nell'attività di attori ostili, connotati per l'esecuzione di attacchi ransomware – volti a paralizzare servizi e sistemi critici mediante la cifratura dei dati contenuti – campagne DDoS, volti a sabotare la funzionalità di risorse online e, soprattutto, attacchi di tipo ATP (Advanced Persistent Threat), condotti da attori ostili di elevato expertise tecnico, in grado di penetrare i sistemi più strategici mediante tecniche di social engineering o sfruttamento di vulnerabilità, al fine di garantirsi una persistenza silente all'interno dei sistemi a scopo di spionaggio o successivo danneggiamento.

La proliferazione di gruppi ostili, si è attuata poi mediante il ricorso a crew hacker di c.d. *crime as a service*, ordinariamente attive nel fornire supporto tecnologico ad attori criminali ed oggi sempre più contigue a gruppi di ascendenza statuale.

In particolare, il Servizio polizia postale ha implementato l'attività informativa e di monitoraggio ad ampio spettro, esteso anche al *dark web*, attivando canali di diretta interlocuzione dedicati allo scenario in atto con Europol, oltre che con Interpol e FBI, con l'obiettivo di elevare il livello di attenzione con particolare riguardo al settore economico/finanziario, tradizionalmente oggetto di interesse da parte di compagini criminali con connotazione *state sponsored*.

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), attraverso dedicati *alert* ha diffuso indicatori di compromissione e avvisi di informazione di sicurezza alle infrastrutture informatiche dicasteriali, alle infrastrutture critiche nazionali e ai potenziali *target* di azioni ostili, individuati attraverso la permanente attività informativa assicurata dal Centro.

I Centri Operativi per la Sicurezza Cibernetica della Polizia Postale hanno svolto adeguati servizi di monitoraggio e analisi, condividendo ogni evidenza utile in relazione al quadro internazionale in parola.

L'attività del CNAIPIC del Servizio Polizia Postale e delle Comunicazioni, oltre agli approfondimenti investigativi, si è tradotta nell'analisi tecnica della minaccia, volta all'elaborazione di informazioni di sicurezza preventiva, nonché nel supporto operativo alle infrastrutture attaccate, che hanno contribuito al ritorno alla piena operatività dei sistemi informatici colpiti.

Attacchi infrastrutture critiche ad istituzioni, aziende e privati	**2021**	**2022***	**Variazione percentuale**
Attacchi rilevati	**5.434**	**12.947**	**+138%**
Persone indagate	**187**	**332**	**+78%**
Alert diramati	**110.524**	**113.226**	**+2%**
Richieste di cooperazione HTC	**60**	**77**	**+28%**
* - dati rilevati il 27/12/2022			

SEZIONE OPERATIVA

Nell'ambito delle competenze della Polizia Postale si segnala il rafforzamento dell'attività di prevenzione attraverso il monitoraggio attivo della rete e un'articolata attività di contrasto alle **truffe online** con **3541 persone deferite all'Autorità Giudiziaria**, in particolare nel settore dell'e-commerce e *market place.*

Truffe OnLine	**2021**	**2022***	**Variazione percentuale**
Casi trattati	15.083	15.508	**+3%**
Persone indagate	3.403	3.541	**+4%**
Somme sottratte	€ 73.245.740	€ 115.457.921	**+58%**
* - dati rilevati il 27/12/2022			

Nell'ambito delle truffe sul web anche nel corso del 2022, importante l'incremento degli illeciti legati al fenomeno del **trading online** (**3.020** ***i casi trattati, 130 le persone)***, con l'aumento del numero di portali che propongono programmi speculativi, apparentemente redditizi, e l'utilizzo di tecniche molto sofisticate per contattare le vittime. L'attività investigativa, qualora la denuncia sia tempestiva, prevede l'immediata attivazione dei canali di Cooperazione Internazionale di Polizia, con la richiesta del blocco urgente delle somme versate e l'espletamento di accertamenti sui flussi finanziari normalmente destinati all'estero.

Proprio per dare maggior impulso alle indagini che vedono coinvolti cittadini stranieri, la Sezione Operativa della Polizia Postale, nel corso dell'anno 2022, ha attivato **260 richieste di cooperazione internazionale** attraverso il canale Europol che, in più di un'occasione, si sono rivelate determinanti per l'individuazione degli autori dei reati investigati.

Particolare attenzione è rivolta inoltre ai fenomeni del **revenge porn, con *244 casi trattati (di cui 34 in danno di minori) e 71 persone denunciate*** e delle **truffe romantiche,** con ***442 casi trattati (di cui 4 in danno di minori) e 103 persone denunciate***, spesso sommersi in quanto caratterizzati da un forte coinvolgimento emotivo che induce la vittima a non denunciare.

Sono stati **15** i casi di ***Codice Rosso*** che hanno visto la Polizia Postale impegnata attivamente nel contrasto dei reati contro la persona commessi attraverso la rete.

Reati contro la persona perpetrati OnLine[1]	**2021**	**2022***
Casi trattati	10.297	9.278
Persone indagate	1.693	1.167
[1] – *Stalking* / diffamazione online / minacce / *revenge porn* / molestie / sextortion / illecito trattamento dei dati / sostituzione di persona / hate speech / propositi suicidari * - dati rilevati il 27/12/2022		

Specifiche iniziative sono state rivolte all'attività di prevenzione e contrasto al fenomeno degli atti intimidatori nei confronti della categoria dei giornalisti e servizi di monitoraggio dei canali

di diffusione, costituiti da siti web, piattaforme di digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube), finalizzati ad arginare la diffusione del linguaggio d'odio (hate speech).

La Sezione Operativa è stata impegnata anche nell'individuazione di proposte di vendita online di prodotti contraffatti o all'utilizzo illecito di segni distintivi dei marchi registrati, per la tutela del c.d. *italian sounding.*

Il monitoraggio di siti e spazi *web* (blog, gruppi social e siti dedicati) dediti a giochi e scommesse clandestine è un'altra attività operativa particolarmente seguita dalla Polizia Postale e delle Comunicazioni, sia per contrastare la diffusione irregolare o illegale, che per tutelare gli interessi dei consumatori, specie se minori d'età: numerosi sono i siti con sedi legali presso paesi esteri, che operano in Italia anche se privi della prevista autorizzazione per poter esercitare legalmente la raccolta di scommesse.

Nel corso del 2022 sono state implementate anche le attività di monitoraggio relative alla vendita online di tabacchi, sigarette elettroniche e liquidi da inalazione in rete, su siti sprovvisti delle relative autorizzazioni da parte dell'Agenzia delle Dogane e Monopoli.

In ultimo, ma comunque di primaria importanza, è stata l'attività rivolta all'individuazione di quelle persone che, sfruttando principalmente la cassa di risonanza che i social media offrono, hanno manifestato intenti suicidari in conseguenza dei quali sono state attivate tutte le procedure necessarie per la salvaguardia delle persone coinvolte con l'ausilio degli uffici di polizia competenti territorialmente (***64 le segnalazioni veicolate attraverso il Commissariato di P.S. OnLine e 51 gli interventi eseguiti sul territorio dalla Polizia Postale e delle Comunicazioni*** *).*

SEZIONE OPERATIVA – ATTIVITÀ DI POLIZIA GIUDIZIARIA

TRUFFA PAYPAL (MARZO 2022) **-** Il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Pescara ha effettuato 25 perquisizioni nei confronti di altrettanti indagati componenti un sodalizio criminale dedito alle truffe in danno di una società che opera attraverso una piattaforma di mediazione per i pagamenti on-line. L'attività investigativa, coordinata dal Servizio Polizia Postale e delle Comunicazioni di Roma, ha consentito di accertare che gli indagati hanno acquistato, con conti incapienti, merce on-line da numerosi venditori italiani ed esteri. I venditori ricevevano il pagamento dei beni, dato che gli acquisti avvenivano tramite la piattaforma PayPal, ma quest'ultima subiva un danno economico di circa due milioni di euro poiché i conti correnti di riferimento erano privi di giacenza. Tale modus operandi ha consentito al sodalizio criminale di acquistare fraudolentemente i più svariati beni: orologi di lusso, preziosi, smartphone di ultima generazione, apparecchi per la casa e finanche generi alimentari.

OPERAZIONE "GENOVA" (MAGGIO 2022) **-** Il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Genova, con il coordinamento del Servizio Polizia Postale e delle Comunicazioni, sotto la direzione della Procura della Repubblica presso il Tribunale di

La Spezia ha indagato 11 individui resisi responsabili di una serie di truffe.
La compagine criminale si avvaleva di "telefonisti" che avevano il compito di agganciare le vittime direttamente dalle proprie abitazioni, situate in Veneto e Friuli Venezia Giulia, contattavano i venditori, fingendosi fortemente interessati all'acquisto della merce e desiderosi di effettuare il pagamento nel più breve tempo possibile.
Facendo leva sulla fretta, convincevano l'ignara vittima a recarsi presso uno sportello automatico, per ricevere l'accredito della somma pattuita direttamente sulla propria carta.
Quindi, sfruttando la non perfetta conoscenza degli strumenti bancari delle vittime, il truffatore forniva loro tutta una serie di istruzioni e codici, grazie ai quali, invece di ricevere il pagamento sul proprio conto, i malcapitati erano indotti a ricaricare una carta di pagamento nella disponibilità del sodalizio criminale. In numerosi casi il malcapitato addirittura è stato indotto a compiere numerose ricariche, prima di accorgersi di essere caduto in un tranello.
Proprio tale solido rapporto fiduciario aveva generato una sorta di network che si occupava dell'intera gestione delle operazioni fraudolente, dalla commissione delle truffe alla successiva monetizzazione, il cosiddetto cash-out presso l'ATM di riferimento.
Per garantirsi l'anonimato ed eludere così l'attività investigativa, i membri dell'organizzazione erano soliti ricorrere a sistemi di "anonimizzazione" delle conversazioni o ad applicazioni crittografate come Telegram ed ICQ.

OPERAZIONE "ESEGUI E CONFERMA" - La complessa ed articolata attività di indagine svolta dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Perugia ha trovato il suo culmine con l'esecuzione, in collaborazione dei C.O.S.C. dell'Emilia Romagna, Toscana, Veneto, coordinati del Servizio Polizia Postale di Roma, di 5 misure cautelari tra cui 2 in carcere e 3 agli arresti domiciliari, nonché 6 decreti di perquisizione in alcune Regioni del Centro Nord.
Le misure coercitive sono state disposte nei confronti di un sodalizio criminoso che, dopo essere entrato nella disponibilità di fittizie utenze telefoniche, carte Postepay e copia di documenti intestati a terze persone, è riuscito a mettere a segno, in soli sei mesi, truffe *e-commerce* per un ammontare di circa € 100.000.
In particolare i malviventi dichiarandosi interessati all'acquisto del bene e fornendo generalità fittizie, anche attestate da fotografie di documenti di identità di comodo, raggiravano i venditori mediante false indicazioni, in ordine alle modalità di pagamento, in modo tale che le vittime, recatesi presso ATM, procedessero loro stesse all'accredito dei relativi corrispettivi, anziché ricevere il prezzo di vendita dall'interlocutore.
Appena conclusa tale operazione, i sedicenti acquirenti, direttamente o tramite la collaborazione degli associati, provvedevano a monetizzare i proventi tramite prelievi presso gli ATM dislocati sul territorio.
L'esito dell'attività investigativa è stata agevolata anche dalla proficua e attenta collaborazione di Poste Italiane che ha permesso di ostacolare il conseguimento di ulteriori proventi illeciti grazie ai tempestivi accertamenti eseguiti dalla Società stessa.

OPERAZIONE "PANGEA XV" - L'attività della Specialità è stata caratterizzata, inoltre,

da un sempre maggiore impegno nella cooperazione internazionale, con l'adesione a specifici programmi di contrasto al commercio illegale di farmaci ed al fenomeno della contraffazione. La Polizia Postale e delle Comunicazioni ha aderito all'Operazione denominata "Pangea XV" che il Segretariato Generale Interpol di Lione ha organizzato nell'ambito dell'"Illicit Goods and Global health Programme", il cui obiettivo strategico è il contrasto al commercio online di farmaci contraffatti ed illegali, con particolare riferimento a quelli utilizzati per la cura del virus Sars Co2 – Covid 19. Il Servizio Polizia Postale e delle Comunicazioni ha coordinato le attività condotte dal Centro Operativo per la Sicurezza Cibernetica di Ancona che, unitamente a quello di Pescara, ha predisposto una significativa azione di monitoraggio della rete grazie alla quale sono stati individuati numerosi siti dediti all'attività illecita oggetto di indagine. Le risultanze investigative hanno consentito di ottenere dalla Procura della Repubblica presso il Tribunale di Ancona un decreto di sequestro preventivo in relazione al reato di cui all'art 445 c.p. (Somministrazione di medicinali in modo pericoloso per la salute pubblica), notificato a 171 Internet Service Provider, che ha permesso di oscurare 43 siti, rendendoli irraggiungibili dall'Italia, così da interrompere la vendita, sul territorio nazionale, di farmaci non autorizzati.

Operazione "Rear Window" (GIUGNO 2022) - Gli investigatori della Polizia Postale di Milano e del Servizio Polizia Postale e delle Comunicazioni di Roma, coordinati dalla Procura della Repubblica di Milano, sono riusciti a disarticolare un vero e proprio "sistema" criminale finalizzato alla violazione, mediante intrusioni informatiche, di impianti di videosorveglianza installati per lo più presso private abitazioni effettuando 10 perquisizioni su tutto il territorio nazionale.

L'inquietante fenomeno è stato scoperto grazie alla segnalazione di un cittadino e agli sviluppi dell'analisi forense compiuta sullo smartphone sequestrato a uno degli indagati nell'ambito di un altro procedimento penale, relativo a reati di altra natura.

Nell'ambito dei due gruppi criminali scoperti dagli investigatori (per uno dei quali - il più corposo - si configura una vera e propria associazione per delinquere), gli indagati avevano ruoli e compiti ben definiti: i più esperti in materia informatica scandagliavano la rete alla ricerca di impianti di videosorveglianza connessi ad internet; una volta individuati, li facevano oggetto di veri e propri attacchi informatici che consentivano, ricorrendo determinate condizioni, di scoprire le password degli NVR (ossia dei videoregistratori digitali a cui normalmente vengono collegate le telecamere di videosorveglianza) e di accedere ai relativi impianti. Raccolte le credenziali di accesso, era compito di altri appartenenti ai gruppi criminali verificare la tipologia degli impianti, gli ambienti inquadrati e la qualità delle riprese, allo scopo di individuare telecamere che riprendessero luoghi particolarmente "intimi", come bagni e camere da letto. L'obiettivo finale era infatti quello di carpire immagini che ritraessero le ignare vittime durante la consumazione di rapporti sessuali o atti di autoerotismo. In alcuni casi, le immagini facevano riferimento a telecamere installate presso alberghi, studi medici e spogliatoi di palestre e piscine. Al termine di tale selezione, le credenziali di accesso venivano affidate ad altri sodali che, attraverso "vetrine" online create ad hoc, le mettevano in vendita sulla rete. I proventi illeciti venivano reinvestiti nell'acquisto di sempre più aggiornati software per proseguire la loro attività delittuosa nel perpetrare ulteriori attacchi informatici.

OPERAZIONE "KILLER SUL DARKWEB" (LUGLIO 2022) - Il Servizio Polizia Postale e delle Comunicazioni, unitamente al C.O.S.C. di Venezia e alla S.O.S.C. di Treviso, coordinati dalla Procura della Repubblica del Tribunale di Treviso, attraverso complesse indagini connotate dall'elevato contenuto tecnico, sono riusciti ad identificare un utente che, approfittando dell'anonimato garantito dalla cosiddetta "parte oscura" della Rete, il DARKWEB, aveva effettuato un pagamento in criptovalute per commissionare ad un altro utente, amministratore di un sito specializzato in omicidi su commissione, l'uccisione di un rivale in amore.
L'intera vicenda trae origine da un'attività di cooperazione internazionale di polizia con l'FBI americano che informava il Servizio Polizia Postale che un quarantacinquenne del trevigiano era stato indicato come potenziale vittima di un "servizio" a pagamento di omicidio su commissione. I primi accertamenti sulla rete effettuati dalla S.O.S.C. di Treviso hanno permesso di dare un nome e cognome alla vittima, che, grazie all'attività di controllo del territorio approntata dal Commissariato di Conegliano, veniva discretamente "vigilato" per garantirne l'incolumità.
Ulteriori approfondimenti sulle informazioni comunicate dagli americani, hanno permesso di individuare importanti tracce telematiche connesse alle transazioni in criptovaluta effettuate, riuscendo così a risalire al "mandante" e richiedente il particolare servizio criminale, un trentaquattrenne della provincia trevigiana.

OPERAZIONE "PELLET" (OTTOBRE 2022) - La Sezione Operativa per la Sicurezza Cibernetica di Ferrara, coordinata dal Servizio Polizia Postale e dal Centro Operativo per la Sicurezza Cibernetica dell'Emilia Romagna, ha avviato un'attività di indagine partendo da una denuncia dello scorso settembre per truffa patita da un cittadino che, a fronte di un ordine di due bancali di pellet, dell'importo di circa 500 euro, non si è visto recapitare la merce.
Gli uomini della Polizia Postale hanno avuto modo di ricostruire un fenomeno che andava ben oltre l'ambito provinciale: ne è emerso un quadro composto da numerosissime vittime sparse sul territorio nazionale, con un giro d'affari criminale stimabile – almeno parzialmente – in decine di migliaia di euro.
Nei giorni scorsi il sito web che proponeva la vendita del pellet è stato messo offline, dando esecuzione al provvedimento di oscuramento emesso dal G.I.P. di Ferrara su richiesta della locale Procura; sono tuttora in atto le indagini volte all'individuazione degli autori del reato.

OPERAZIONE "CAGLIARI" (NOVEMBRE 2022) - Il Centro per la Sicurezza Cibernetica di Cagliari, coordinato dal Servizio Polizia Postale, ha eseguito la misura cautelare degli arresti domiciliari nei confronti di un uomo quarantenne residente nel Sud della Sardegna, resosi responsabile dei reati di interferenza illecita nella vita privata, di accesso abusivo ad un sistema informatico nei confronti di undici vittime (finora accertate), nonché del reato di detenzione di materiale pedopornografico.
L'attività investigativa ha preso spunto da due querele relative ad una presunta inoculazione di virus informatici nei personal computer delle querelanti, insospettite dalla comparsa del medesimo *alert* di sistema nei propri monitor con cui si segnalava il pericolo di

surriscaldamento ogniqualvolta coprivano la *webcam*.
Le attività di polizia giudiziaria e tecniche compiute dal Centro Operativo hanno permesso di riscontrare l'effettiva presenza, nei dispositivi informatici delle vittime, di un virus spia che permette il controllo da remoto e l'accesso in tempo reale alla webcam e di identificare, quale responsabile dell'inoculazione nei dispositivi del predetto virus, il soggetto titolare di una ditta individuale, sita in un comune del Sud della Sardegna, che svolge attività di servizio di assistenza e manutenzione di dispositivi informatici (Personal Computer, tablet, etc.).
Le complesse attività tecniche, data l'elevata quantità dei file memorizzati nei diversi supporti informatici sequestrati all'indagato, hanno consentito di accertare come il predetto abbia violato, tra il 2019 e il 12 ottobre 2020, almeno 740 computer appartenenti o in uso ad ignari utenti, in larga parte clienti della sua attività commerciale. Inoltre, sono stati rinvenuti diversi video di carattere pedopornografico raffiguranti minori di anni diciotto nel compimento di atti sessuali e/o nudi.

OPERAZIONE TORINO "TRADING ON LINE" (DICEMBRE 2022) - Il Centro Operativo Sicurezza Cibernetica di Torino, con il coordinamento del Servizio Polizia Postale, ha eseguito tre arresti nel torinese e perquisizioni e sequestri sul territorio nazionale. L'indagine, articolata su tre diversi procedimenti penali, ha portato ad individuare un'organizzazione criminale gerarchizzata che agiva tra l'Italia e l'Albania con l'intento di ripulire il denaro proveniente dalle truffe dei falsi investimenti ai danni di ignari utenti del web; gli approfondimenti investigativi hanno interessato in modo trasversale evidenze informatiche, bancarie e societarie, ricostruite e messe a sistema anche mediante il ricorso a prolungate attività tecniche di pedinamento informatico che hanno fatto emergere il coordinamento unitario nella gestione del fenomeno criminale.
Particolarmente complesso è stato il lavoro svolto dal Servizio Polizia Postale e delle Comunicazioni nell'ambito della cooperazione internazionale, finalizzato all'acquisizione di notizie e dati per la ricostruzione dei flussi finanziari.
Ai vertici della struttura un cittadino albanese residente nel torinese che, secondo i riscontri investigativi, forniva ai suoi complici precise disposizioni sugli importi ed i conti correnti dove far convergere ingenti somme di denaro per occultarne la provenienza delittuosa; alle sue dirette dipendenze, sempre secondo l'accusa, due torinesi che mettevano a disposizione i conti correnti bancari intestati a società riferibili a loro direttamente o tramite prestanome.
Lo svolgimento delle attività tecniche ha consentito l'individuazione di un gruppo di 16 soggetti residenti nel torinese, le cui abitazioni e società, nello specifico 4, operanti nel settore del *digital marketing e lead generation*, sono state oggetto di perquisizione delegate dalla Procura.
Accanto alle attività di riciclaggio, è stata ricostruita la diretta partecipazione alla realizzazione dei falsi siti di pubblicità di trading, utilizzati per recuperare illecitamente le generalità lasciate dagli ignari internauti interessati ad investire. Tali siti sono stati oscurati ed ora non sono più visibili agli utenti italiani.
Nel contesto sono stati aggrediti i patrimoni illeciti mediante l'esecuzione di 9 decreti di sequestro di beni per equivalente nei confronti di altrettanti soggetti titolari di quote societarie ovvero figure aventi un ruolo di compartecipazione nella attività di ripulitura del denaro di provenienza illecita.

SEZIONE CYBERTERRORISMO

Nel corso degli ultimi anni, il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e di applicazioni di messaggistica istantanea, ha determinato un'allarmante diffusione di contenuti propagandistici riconducibili al terrorismo, ad una platea pressoché illimitata, sia di matrice islamista (*jihadista, ISIS, Al Qaeda, Al Shabaab* ed altre articolazioni locali), sia di formazioni suprematiste di estrema destra (neonazismo, neofascismo, tifoserie strutturate), nonché di estrema sinistra (movimenti di lotta armata, anarco/insurrezionalisti, antagonisti).

Cyberterrorismo[1]	2021	2022*
Casi trattati	1.321	1.193
Persone indagate	80	66
Spazi virtuali monitorati	126.998	173.306

[1]- Estremismo internazionale religioso / estremismo razziale, antagonista ed anarchico
* - dati rilevati il 27/12/2022

In tale ambito, la Polizia Postale garantisce sia l'esecuzione di una costante attività di monitoraggio investigativo della rete e dei canali di messaggistica istantanea, per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione dei contenuti illeciti, sia un costante scambio informativo con la Direzione Centrale della Polizia di Prevenzione competente in materia di contrasto al terrorismo.

Trattandosi, in particolare, di un fenomeno di carattere transnazionale, sia per la natura internazionale del fenomeno che per la stessa connaturata struttura della rete, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali.

In ambito europeo, proprio al fine di garantire la cooperazione internazionale, il Servizio Polizia Postale e delle Comunicazioni rappresenta il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti terroristici diffusi in rete e di orientarne l'attività.

In tale ambito, l'attività di monitoraggio del web effettuata dalla Specialità ha permesso di riscontrare, in primis, come la diffusione di contenuti propagandistici jihadisti, nel corso del tempo, abbia subito un sensibile peggioramento "qualitativo", determinato sia dal ridimensionamento del Califfato sul territorio, sia dalle perdite di tecnici e social media manager cui era devoluto l'incarico di gestire la propaganda, nonché per l'utilizzo sempre più frequente dell'Intelligenza Artificiale sulle principali piattaforme web, per la scansione (e rimozione) dei contenuti pubblicati dagli utenti.

Sul punto, tra le attività effettuate dalla Specialità si segnala quella effettuata dal Centro Operativo per la Sicurezza Cibernetica e dalla DIGOS di Perugia, all'esito della quale un cittadino marocchino di 54 anni è stato espulso dal territorio nazionale, in quanto autore di una prolifica attività propagandistica sul social network Facebook realizzata attraverso numerosi post e commenti a sostegno dei "fratelli musulmani" e del Jihad, specificamente della Palestina contro Israele, nel corso della quale si è definito un "mujahidin" pronto ad aiutare la causa.

In analogia a quanto sin qui evidenziato con riferimento alla propaganda jihadista, anche nell'ambito dei fenomeni di radicalizzazione online legati all'ideologia neofascista e xenofo/razziale, il web si conferma lo strumento strategico per la diffusione della propaganda delle ideologie estremiste e violente, nonché per il reclutamento di nuovi combattenti, il finanziamento, lo scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.

Appare opportuno evidenziare come il movimento "suprematista" si basi su una importante attività di propaganda di dottrine ideologiche come il neonazismo, il razzismo, l'identitarismo e l'etnocentrismo, che avviene soprattutto all'interno di piattaforme di comunicazione online "riservate", diverse dai principali social network.

La costante attività di monitoraggio informativo ed investigativo ha permesso di accertare come nel corso degli ultimi mesi si sia stato registrato un notevole incremento dei trend e delle discussioni all'interno di chat in diverse piattaforme; si passa dai tradizionali gruppi Facebook (molti dei quali risultano essere già stati bloccati) a social meno noti, come Reddit, fino a piattaforme come 8chan, vk.com (Vkontakte), nonché Telegram, privilegiando tutte quelle piattaforme che per la propria policy garantiscono l'anonimato e rendono più complicata l'identificazione degli autori dei messaggi.

Alla luce di quanto premesso, appare opportuno evidenziare come gli operatori della Specialità abbiano intensificato le attività di monitoraggio proprio in tali contesti e, in raccordo con la Direzione Centrale della Polizia di Prevenzione, abbiano avviato numerose attività investigative, con il deferimento alle competenti Autorità Giudiziarie dei soggetti identificati – anche attraverso attività sotto copertura e perquisizioni – quali autori dei messaggi connotati dalla discriminazione razziale, etnica e religiosa.

Tra le numerose attività investigative espletate dalla Specialità nel corso del 2022, si segnala quelle che ha condotto al deferimento alla competente A.G. da parte del Centro Operativo di Milano di un uomo di 60 anni, residente nella provincia di Como, quale utilizzatore di un account Twitter, autore di due messaggi contenenti gravi minacce nei confronti del Capo dello Stato.

Ed ancora, appare opportuno evidenziare quella che ha permesso di identificare l'amministratore di un canale Telegram – caratterizzato dalla presenza di numerosi messaggi connotati da ideologie antisemite, da teorie complottiste contrarie ai vaccini, dall'incitamento alla violenza nel corso di manifestazioni pubbliche, nonché per la presenza di gravi minacce nei confronti di varie cariche istituzionali, tra le quali il Presidente del Consiglio Mario Draghi, il Presidente U.S.A. Joe Biden - in un cinquantenne originario della provincia di Napoli, ma da tempo domiciliato in Germania per motivi professionali.

Sulla base degli accertamenti compiuti, l'amministratore del canale Telegram monitorato, è stato fermato al momento del suo ingresso nel territorio nazionale, proveniente dalla Germania, proprio per partecipare ad una manifestazione no-vax in programma nella città di Roma, per la quale aveva esortato i componenti della chat, oltre 21.418 iscritti, ad armarsi e a sopraggiungere in gran numero, fornendo precise indicazioni volte a eludere le attività di prevenzione e controllo delle Forze dell'Ordine.

L'uomo è stato deferito alla competente Autorità Giudiziaria dal personale del Centro Operativo per la Sicurezza Cibernetica di Napoli che, unitamente alla locale DIGOS, ha dato esecuzione al decreto di perquisizione informatica, emesso nei suoi confronti dalla Procura della Repubblica presso il Tribunale del capoluogo partenopeo, riscontrando utili tracce informatiche in merito alla pubblicazione dei messaggi di propaganda e istigazione a delinquere per motivi di discriminazione razziale ed etnica.

Un'ulteriore attività d'indagine che merita di essere menzionata per importanza, è quella avviata dal Servizio Polizia Postale e coordinata dalla Procura della Repubblica di Roma, all'esito della quale, operatori dei Centri Operativi di Milano, Trieste e Venezia, unitamente a personale delle DIGOS di Milano, Vicenza ed Udine hanno eseguito perquisizioni delegate a carico di tre internauti nei cui confronti sono stati riscontrati elementi indiziari tali da farli ritenere autori della pubblicazioni di messaggi minatori rivolti all'ex Ministro degli Esteri Luigi Di Maio.

Ed ancora, a seguito di articolate indagini condotte dal C.O.S.C. e dalla D.I.G.O.S. di Torino è stato individuato un gruppo di matrice nazi-fascista, attestato sulla piattaforma Telegram, sul canale "*Brudershaft thule*" ("Fratellanza di Thule") e sul connesso gruppo di discussione "*Meine Ehre Heißt Treue*" ("Il mio onore si chiama lealtà"), partecipato da militanti stanziati su tutto il territorio nazionale e anche all'estero, in Germania, tutti denunciati per riorganizzazione del disciolto partito fascista e propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa.

In particolare la Sezione Cyberterrorismo della Polizia Postale, nell'ambito del monitoraggio preventivo dei contesti virtuali d'area, ha individuato sui due spazi Telegram contenuti violenti ed istigatori, contraddistinti inoltre da una rievocazione idolatrica del nazi-fascismo con un'ampia diffusione di materiale a carattere apologetico; il linguaggio che gli utenti impiegavano nei post denotava un forte odio per le diversità etniche, politiche e religiose, nonché l'esaltazione dell'atto violento, da perpetrare con raid punitivi.

Il canale "*Brudershaft Thule*" era a sua volta collegato a un gruppo di discussione in lingua italiana, denominato "*Meine Ehre heißt Treue*" (frase attribuita ad Adolf Hitler, divenuta motto nazional-socialista, che letteralmente significa "Il mio onore si chiama lealtà").

All'esito dell'attività di indagine, lo scorso 17 marzo, i sopra menzionati uffici hanno eseguito n. 8 perquisizioni delegate nelle città di Torino, Brescia, Brindisi, Rieti, Alessandria, Lodi e, previo Ordine di Indagine Europeo, anche nella città di Aalen in Germania nei confronti dell'amministratore del canale.

Nel corso delle perquisizioni, oltre a diversi supporti elettronici, è stata sequestrata numerosa documentazione d'area, inerente l'esaltazione del fascismo, del nazismo e della superiorità

della razza bianca, nonché diversa documentazione manoscritta attinente il complottismo antigiudaico; sono stati altresì sequestrate armi (baionette, pugnali, munizioni, fucile ad aria compressa) e ritirate cautelarmente diverse armi comuni da sparo e munizionamento.

Tra le numerose attività investigative effettuate nella tematica in argomento, si segnala anche quella avviata dal Centro Operativo per la Sicurezza Cibernetica di Bari e dalla DIGOS di Lecce, che ha permesso di identificare e deferire alla competente A.G. l'autore dell'intrusione informatica nella seduta del Consiglio Comunale di Trieste, tenutasi online nel mese di febbraio 2022 mediante la piattaforma "GoToMeeting", diffondendo immagini di soggetti (non visibili in volto) che esibivano delle magliette con il noto logo del movimento di protesta "*V_V*", nonché frasi provocatorie e diffamatorie di chiaro orientamento "No-vax" e "no green-pass", rendendo di fatto impossibile la prosecuzione della seduta del Consiglio Comunale.

Ed ancora, su disposizione della Procura della Repubblica di Siracusa, personale della Polizia Postale di Catania e della DIGOS di Siracusa, ha eseguito una perquisizione nei confronti di uomo di 27 anni, disoccupato, residente nella provincia aretusea, indagato per violenza privata aggravata nei confronti del Presidente del Consiglio Giorgia Meloni.

In particolare, gli operatori del Servizio Polizia Postale di Roma avevano rilevato sull'account ufficiale Twitter del Presidente del Consiglio la pubblicazione di messaggi di minacce di morte finalizzati ad evitare l'eliminazione del reddito di cittadinanza. Nonostante l'utente utilizzasse uno pseudonimo, le attività tecnico investigative hanno permesso l'identificazione dell'odierno indagato.

Sulla base delle evidenze investigative, l'Autorità Giudiziaria ha disposto la perquisizione domiciliare ed informatica nei confronti dell'uomo. Gli operatori specializzati del Centro di Sicurezza Cibernetica Sicilia Orientale della Polizia Postale hanno proceduto al sequestro di apparecchiature informatiche e dell'account social utilizzato per la condotta criminosa.

Degna di essere menzionata risulta essere l'attività investigativa che ha portato in data 30/11 u.s., all'esecuzione di perquisizione a carico di sei soggetti, tre maggiorenni e tre minorenni, anche per il reato di propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604 bis c.p.).

L'indagine è stata avviata nell'ambito del monitoraggio del gruppo Telegram "Blocco Est Europa" nel quale venivano condivisi contenuti violenti riconducibili a materiale diffuso da gruppi terroristici islamisti di matrice jihadista, messaggi e post inerenti alla pornografia minorile, uccisioni brutali, stragi terroristiche, razzismo, misoginia, "school shooting" e violenza in genere con esplicite dichiarazioni di propaganda dell'odio razziale accompagnate dall'istigazione al compimento di atti di violenza di matrice discriminatoria e attentati contro le istituzioni a livello nazionale.

Il canale - creato il 23 gennaio 2022 e sospeso dal provider il successivo 2 aprile - è stato utilizzato per divulgare messaggi basati sull'odio antisemita e nei confronti delle persone di colore, attestazioni di stima per Hitler e le teorie naziste accompagnate dal disprezzo per le Istituzioni e le Forze dell'Ordine oltre ad un'accentuata misoginia da cui deriva divertimento

per la visione di video di donne, per lo più minorenni, che si suicidano o che vengono violentate o uccise.

Sul gruppo "Blocco Est Europa" sono state inoltre postate immagini relative ad addestramenti con armi ad aria compressa effettuati dagli indagati verso bersagli raffiguranti persone esistenti, tra cui importanti Personalità dello Stato.

Correlato alle predette finalità è anche il progetto di realizzare uno "*school shooting"* come dimostrato da commenti e fotografie riferite a stragi compiute da giovanissimi nelle scuole.

Sempre mediante il predetto canale, gli indagati hanno inoltre condotto un'intensa attività di propaganda ispirata all'odio razziale e al nazionalsocialismo, alla misoginia e all'intolleranza e alla violenza in generale e condiviso numerosi file dai contenuti pedopornografici.

Proprio quest'ultima circostanza ha determinato per i tre maggiorenni, tutti di 21 anni, l'emissione da parte della competente A.G. di due ordinanze di misura cautelare in carcere ed una ai domiciliari. Mentre i restanti tre minorenni, con età compresa tra i 13 e i 14 anni, sono stati denunciati a piede libero.

Infine, considerando il carattere transnazionale che spesso connota le attività investigative in argomento, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali. In ambito europeo, il Servizio Polizia Postale e delle Comunicazioni è il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti di propaganda terroristica diffusi in rete e di orientarne l'attività.

Lo scambio delle informazioni tra Paesi Membri viene effettuato attraverso l'utilizzo di specifiche piattaforme tecnologiche appositamente create in ambito IRU a supporto del monitoraggio e delle indagini in materia di terrorismo in Internet.

Proprio nell'ambito della lotta ai crimini ispirati dall'odio, nello scorso mese di aprile, la Polizia Postale ha partecipato alla giornata di azione congiunta a livello dell'U.E., sostenuta da *Europol,* che, oltre l'Italia, ha coinvolto 10 Paesi (Austria, Bulgaria, Francia, Germania, Lituania, Lussemburgo, Norvegia, Portogallo, Romania e Spagna).

Le attività investigative hanno permesso di identificare in tutta Europa 176 persone in relazione alla diffusione online di messaggi di incitamento all'odio xenofobo-razziale, nonché istigazione alla violenza.

Nella circostanza, le Forze dell'ordine degli Stati membri hanno anche lavorato insieme per far aumentare la consapevolezza di individui e gruppi che Internet non rappresenta un "vuoto giuridico", dando così un chiaro segnale alle persone che diffondono odio violento online che le azioni investigative congiunte saranno sempre più frequenti e consistenti.

Da ultimo, lo scorso 15 dicembre, la Polizia Postale e la D.C.P.P. hanno partecipato ad una seconda giornata congiunta, coordinata dall'European Union Internet Referral Unit (EU IRU) di Europol, nell'ambito del *Referral Action Day* (RAD) contro i contenuti violenti

dell’estremismo di destra e del terrorismo online. L'attività ha coinvolto anche le Unità specializzate di 14 Paesi, tra cui 13 Stati membri dell'Unione Europea e un Paese non appartenente all’ UE.

Le autorità partecipanti sono state coinvolte nell'individuazione e nella segnalazione di contenuti terroristici ai fornitori di servizi online e nel valutare le loro risposte. Le attività hanno portato alla segnalazione di **831 elementi a 34 piattaforme** interessate. Il materiale in questione include contenuti vietati prodotti da organizzazioni estremiste di destra o in favore di queste, nonché contenuti diffusi relativi ad attacchi terroristici motivati dall'estremismo violento.

Tali materiali includono *livestream*, manifesti, rivendicazioni e celebrazioni di attentati. L'estremismo violento è ancora una preoccupazione crescente dopo i fatti di Bratislava (Slovacchia) e Buffalo (USA).

Gli autori di questi attentati facevano parte di comunità *online* transnazionali e si sono ispirati ad altri estremisti di destra violenti e terroristi. Nei loro manifesti, i terroristi hanno evidenziato il ruolo centrale della propaganda *online* nei processi di radicalizzazione. Questo dimostra come l'abuso di internet continui ad essere centrale per l’avvio di percorsi di radicalizzazione e reclutamento della destra violenta.

Dal primo *Referral Action Day* dedicato a questo tipo di contenuti online nel 2021, la minaccia rappresentata dall'estremismo violento e dal terrorismo è ancora in aumento.

I RAD consolidano gli sforzi delle forze dell'ordine per contrastare la creazione e la diffusione di propaganda estremista e terroristica online. Durante le attività coordinate, i partecipanti segnalano i contenuti legati al materiale di propaganda ai fornitori di servizi online invitandoli a valutare e rimuovere i contenuti che violano i loro termini di servizio. Le piattaforme sono invitate a rafforzare i loro protocolli di moderazione per evitare questo tipo di abuso in futuro.

FINANCIAL CYBERCRIME

L’anno 2022 ha vissuto, subendoli, gli strascichi dell’emergenza sanitaria da Covid19, che ha comportato il cambiamento radicale di alcune abitudini di vita consolidate. La sostituzione della socializzazione diretta con quella telematica e lo svolgimento dell’attività lavorativa non in presenza, imposti dall’avvio della pandemia fin dal 2020, si sono, in parte, stabilizzati, aprendo la strada a nuove consuetudini: molte aziende hanno proseguito con forme di telelavoro e *smartworking*, contribuendo a incrementare la frequenza di navigazione in rete da parte dei soggetti adulti anche attraverso *devices* quali *tablet*, *smartphone*, pc molto spesso utilizzati anche per scopi personali a scapito della sicurezza.

Nel solco di questi cambiamenti si è registrato un aumento dei reati informatici che ha raggiunto livelli altissimi, mettendo in luce come il crimine post pandemia nel nostro Paese stia cambiando radicalmente.

Il settore del *financial cybercrime* rappresenta un bacino molto remunerativo ed appetibile sfruttato da molte organizzazioni criminali, anche estere, come veicolo per finanziare le proprie attività illecite, il più delle volte attraverso l'utilizzo di sofisticate tecniche di *social engineering* per manipolare le vittime e indurle a fornire informazioni riservate.

Le conseguenze di un attacco riuscito possono essere drammatiche e avere effetti devastanti non solo su singoli utenti o investitori, ma anche con riverberi negativi per ciò che concerne piccole e medie imprese, con ingenti perdite economiche e danni d'immagine difficilmente quantificabili.

Nel settore del contrasto al *financial cybercrime*, il fenomeno dei "*money mules*" rappresenta senz'altro una delle modalità più frequenti e consolidate per realizzare frodi online: con la funzione di "teste di legno" cibernetiche, personalità di dubbia moralità si prestano ad essere l'ultimo anello della catena attraverso il quale i criminali monetizzano i proventi del reato. La diffusione di questa modalità e il numero dei soggetti che si prestano a svolgere tale funzione criminale sono in costante crescita e rappresentano ormai una realtà criminale quasi endemica in tutto il mondo.

Anche il 2022, inoltre, è stato caratterizzato dalla crescita dell'interesse per le ***Cryptovalute***: i cittadini italiani, anche con bassa scolarizzazione informatica, sono sempre più frequentemente attratti dagli investimenti in ***Cryptovalute***, con la speranza di realizzare i facili e veloci guadagni pubblicizzati.

Quello delle *Cryptovalute* costituisce un mondo eterogeneo e virtuale, peraltro, non dissimile da quello reale. In tale contesto sono realizzate attività investigative finalizzate a fermare i tentativi di *phishing* verso i ***Wallet*** che le contengono: i truffatori informatici agganciano le vittime attraverso richieste di natura tecnica, su chat ufficiali o semi ufficiali, con la promessa di risolvere i loro problemi gestionali previa cessione delle chiavi private, che permettono la movimentazione delle Crypto (cd. SEED), in realtà queste consentono ai malfattori di prendere il pieno possesso del *Wallet* e di impadronirsi del contenuto.

Forte anche l'impegno per contrastare il fenomeno del riciclaggio perpetrato attraverso la conversione delle somme frodate in *Cryptovalute*, sono state infatti coordinate dal Servizio Polizia Postale diverse attività investigative che hanno visto truffe informatiche ad alto contenuto tecnico conosciute come le BEC, le CEO fraud, *Vishing*, *phishing* tentare di realizzare i proventi criminali inviando le somme sottratte tramite bonifico bancario ad *exchange* di *cryptovalute* non collaborativi con la Polizia, convertendo la valuta ufficiale in *Bitcoin* o *Ethereum*. Tale procedimento consente facilmente lo spostamento e spacchettamento delle somme, in attesa di fare *cashout*.

Per tale ragione è stata intensificata la collaborazione con le grandi società di Exchange di Crypto per i report operativi e per il congelamento delle somme sottratte, così come è stata intensificata anche l'analisi delle transazioni *Crypto* con la collaborazione degli specialisti di Europol.

La mancanza di confini geografici in Internet consente sempre più frequentemente la formazione di gruppi criminali con nazionalità eterogenee ed è questo che caratterizza ormai quasi l'intero panorama dei reati commessi attraverso le nuove tecnologie.

In Italia sono state **frodate 156 grandi, medie e piccole imprese**, per un ammontare complessivo di **oltre 20 milioni di euro** di profitti illeciti, dei quali oltre **4 milioni** sono stati recuperati in seguito all'intervento della Polizia Postale e delle Comunicazioni.

In merito ai fenomeni di *phishing, smishing e vishing,* tecniche utilizzate per carpire illecitamente dati personali e bancari, per operare sui sistemi di *home banking*, sono state **identificate ed indagate 853 persone (+9% rispetto all'anno precedente).**

Frodi Informatiche	2021	2022*	Variazione percentuale
Persone indagate	779	853	**+9%**
Somme sottratte	€ 33.258.422	€ 38.678.134	**+16%**
* - dati rilevati il 22/12/2022			

FINANCIAL CYBERCRIME – ATTIVITÀ DI POLIZIA GIUDIZIARIA

OPERAZIONE "FIDEL SCAM" - Nella giornata del 17 novembre, personale della Polizia di Stato ha eseguito 7 decreti di perquisizione personale, locale e informatica contestuali alla misura cautelare dell'obbligo di dimora e presentazione alla P.G. emessi dalla Procura della Repubblica di Brescia, nei confronti di soggetti appartenenti ad un'associazione per delinquere finalizzata alla commissione di una serie di truffe, tentate o consumate, ai danni di piccole medie imprese nazionali.
In particolare, nell'ambito delle indagini, è emerso che le società bersaglio venivano contattate mediante PEC contenenti proposte di falsi finanziamenti, apparentemente erogati da importanti istituti bancari, garantiti da Cassa Depositi e Prestiti e concessi alla sola condizione della sottoscrizione di una polizza assicurativa fittizia che veniva incassata dal sodalizio criminale.
La Sezione Operativa per la Sicurezza Cibernetica di Crotone, coadiuvata per il coordinamento dal Servizio della Polizia Postale e delle Comunicazioni, è riuscita a porre sotto sequestro 15 dispositivi elettronici, 2 hard disk, 15 utenze telefoniche, 6 account email, 4 tera byte di dati, 10 carte di pagamento elettroniche e circa 20.000 euro in contanti, interrompendo così l'attività del sodalizio criminoso**.**

OPERAZIONE "EMMA" - Si è conclusa a fine novembre 2022, l'Operazione di polizia ad alto impatto denominata EMMA (European Money Mules Action), giunta alla sua settima edizione, messa in campo anche quest'anno dalla Polizia Postale e delle Comunicazioni e dalle Forze di polizia cyber di altre 24 Nazioni e coordinata da Europol ed Interpol.
I numeri complessivi dell'Operazione nei diversi Paesi europei, frutto del lavoro di tutte le Forze di polizia estere impegnate insieme alla Polizia italiana, sono ragguardevoli: anche grazie al supporto di oltre **1.800 istituti bancari** e altre istituzioni finanziarie, sono state individuate **4.089 transazioni** bancarie fraudolente, sono state avviate **oltre 1.600 autonome indagini**, riuscendo a prevenire frodi per un danno stimato in **17,5 milioni di euro**. Più di **8.755 i muli** individuati, **222 organizzatori e coordinatori** di muli identificati.
L'iniziativa è stata resa possibile anche grazie alla fattiva collaborazione delle banche e degli istituti di credito italiani, che, attraverso CERTFin e ABI, hanno assicurato un supporto in tempo reale agli investigatori, grazie alla piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente dall'Italia al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica.

OPERAZIONE "GHOTA" - Il Centro Operativo Sicurezza Cibernetica per la Sicilia Orientale, con il coordinamento del Servizio della Polizia Postale e delle Comunicazioni, è riuscito ad individuare una serie di centrali di distribuzione del segnale pirata dislocate in particolare in Sicilia, Puglia e nelle Marche.

Nella mattinata del 10 novembre personale della Polizia di Stato ha eseguito 52 decreti di perquisizione personale, domiciliare e informatica emessi dalla Procura della Repubblica di Catania, a carico di altrettanti soggetti residenti in Italia e all'estero, facenti parte di un'associazione a delinquere a carattere transnazionale, strutturata secondo un modello organizzativo di tipo verticistico con l'aggravante del metodo mafioso, finalizzata al compimento di diversi reati tra i quali la diffusione di palinsesti televisivi ad accesso condizionato, attraverso le cosiddette IPTV (*Internet Protocol Television*),
Il complesso apparato organizzativo, impiantato dagli indagati, prevedeva di acquisire il segnale digitale proveniente da una serie di abbonamenti legittimamente acquisiti - successivamente inviato ad una struttura – e veniva convertivo in dato informatico (IP), attraverso specifiche apparecchiature dette "encoder". Una volta convertito veniva trasmesso in via informatica dalla sorgente ad uno o più server, allo scopo di renderne possibile la fruizione dei relativi contenuti audio e video presso migliaia di utenti finali dietro un corrispettivo di pagamento.
Dal 2016 l'attività illegale degli indagati, ha generato un volume di affari accertato di circa 10 milioni di euro, creando un mancato profitto alle società che forniscono il servizio di "Pay Tv".

OPERAZIONE "PERUGIA 1" - Il Centro Operativo per la sicurezza Cibernetica della Polizia Postale per l'Umbria, sotto la direzione del Servizio Polizia Postale in collaborazione con i C.O.S.C. di Milano, Napoli, Bologna e Ancona, ha dato esecuzione a 5 ordinanze di applicazione della misura cautelare degli arresti domiciliari, emesse dalla Procura della Repubblica di Perugia, nei confronti di alcuni cittadini italiani e stranieri originari del Marocco e della Costa d'Avorio per il reato di truffa attraverso dei raggiri effettuati mediante l'impiego di messaggi telefonici o di chiamate.
La tecnica utilizzata era sostanzialmente quella di carpire informazioni riservate dal punto di vista economico attraverso messaggi via cellulare: gli indagati, dopo aver individuato le ignare vittime ed aver accertato in capo a questi ultimi la titolarità di conti correnti, inviavano un SMS che, apparentemente proveniente dall'Istituto di Credito, anticipava una chiamata telefonica motivata da un accesso abusivo all'home banking da parte di ignari malfattori.
Dopo pochi minuti l'utente riceveva realmente una chiamata - da un finto operatore - nel corso della quale veniva comunicata la presenza di un virus installato sul dispositivo mobile; a quel a quel punto il finto l'operatore, seguendo una procedura ormai ampiamente consolidata, chiedeva alla vittima di spegnere e riaccendere il dispositivo al fine di formattare il sistema e ripristinare le nomali funzioni dell'apparato.
Tale operazione consentiva però l'installazione sull'applicazione bancaria del dispositivo - telefono o computer - di un dispositivo elettronico per mezzo del quale si rendeva possibile l'accesso al conto corrente della vittima.
I soldi prelevati venivano poi fatti confluire dagli indagati su carte di debito in modo da averne una immediata disponibilità. Attraverso questa tecnica è stato stimato un danno causato di circa 50mila euro.
Nel corso dell'esecuzione delle misure sono stati recuperati e sottoposti a sequestro circa 16mila euro di cui 8mila in contanti di vario taglio, unitamente a carte di credito e dispositivi informatici che saranno sottoposti a successiva analisi tecnica.

OPERAZIONE "PERUGIA 2" - In data 27 luglio 2022 questa Specialità, unitamente all'Arma dei Carabinieri, ha dato esecuzione a 11 Ordinanze di Custodia Cautelare di cui 4 in carcere, 3 domiciliari e 4 con obbligo di presentazione alla P.G e altrettanti decreti di

perquisizione locale e personale con contestuale sequestro, eseguite nelle città di Napoli, Padova e Perugia.
La complessa e articolata attività di indagine svolta ha permesso di evidenziare la sussistenza di un nutrito gruppo criminale composto da soggetti residenti nell'area campana ed umbra, con ramificazioni nel Nord Italia, dedito alla realizzazione di una pluralità di reati perpetrati con il seguente *modus operandi*:

- Truffe alle finanziarie ed agli Istituti di Credito finalizzate ad ottenere prestiti personali di denaro attraverso l'esibizione di documentazione fiscale e d'identità falsa e/o artatamente alterata, da destinare prevalentemente all'acquisto di veicoli di alta gamma per la successiva rivendita grazie a una fitta rete di soggetti compiacenti. Nello specifico, il sodalizio dopo aver reclutato una persona solitamente priva di reddito o con reddito molto basso, mette a disposizione, oltre alla documentazione in questione, un copione con le istruzioni da seguire prima di recarsi presso l'ente finanziario. Dopo di che, ottenuto il prestito, l'organizzazione distribuisce la somma tra i sodali ed effettua solamente il pagamento delle prime tre rate del debito.

- Frodi informatiche perpetrate attraverso "*Smishing*" e "*Vishing*", nonché indebito utilizzo di sistemi di pagamento elettronico. Il gruppo campano realizza le frodi informatiche avvalendosi della rete di *money mules* presenti anche nel territorio umbro.

Operazione "DREAM EARNINGS" - Gli investigatori del Centro Operativo per la sicurezza Cibernetica della Polizia Postale del Friuli Venezia Giulia e della Squadra Mobile di Pordenone, con il coordinamento del Servizio Centrale Operativo, del Servizio Polizia Postale e delle Comunicazioni di Roma e la collaborazione del Servizio per la Cooperazione Internazionale di Polizia, unitamente all'Unità Crimini Informatici della Polizia albanese hanno disarticolato un'organizzazione dedita alle truffe perpetrate per mezzo del falso trading online.
Complesse tecniche d'indagine tradizionali e cibernetiche hanno portato alla luce uno schema criminale particolarmente complesso, dedito al riciclaggio di somme di denaro sottratte in diversi Paesi membri U.E., fra i quali Cipro, Lituania, Estonia, Olanda e Germania, e la loro conversione in criptovalute. Le misure cautelari e i decreti di perquisizione sono state eseguite nei confronti di cittadini albanesi, tutti residenti a Tirana e facenti parte di un'organizzazione che si stima abbia truffato diverse centinaia di cittadini italiani.
L'ammontare della frode è di svariati milioni di euro ma questa potrebbe essere solo la punta dell'iceberg; solo all'esito dell'analisi dei sistemi informatici sequestrati sarà possibile determinare gli importi reali.
Nel corso di più di 42.000 intercettazioni telefoniche effettuate dagli investigatori italiani, è infatti emerso quanto i truffatori fossero abili nell'utilizzo di vere e proprie tecniche di persuasione e plagio, al punto da convincere le vittime a indebitarsi e versare, nel tempo, svariate centinaia di migliaia di euro.

Operazione "KAFKA" - La Polizia di Stato, a conclusione di una delicata attività d'indagine condotta dal Servizio Polizia Postale e delle Comunicazioni, ha eseguito 16 decreti di perquisizione personale e domiciliare, emessi dalle Procure della Repubblica di Brescia e Vicenza, con l'ausilio dei Compartimenti di Polizia Postale di Milano, Torino, Pescara, Trieste, Venezia e Roma.
Proprio come nel libro "Il processo" dello scrittore boemo, ignari utenti della rete hanno scoperto di essere stati accusati, processati e condannati per delitti mai commessi; l'indagine trae spunto dall'invio massivo di mail estorsive, apparentemente provenienti da Autorità

istituzionali, contenenti una falsa citazione in Tribunale per fatti afferenti alla pedopornografia. Solo nel periodo di circa 2 mesi i proventi illeciti sono stati di oltre mezzo milione di euro.
La corrispondenza telematica oggetto di indagine riproduce un falso documento governativo e presenta nell'intestazione falsi loghi di Forze di polizia e di Ministeri italiani, tra i quali il Ministero dell'Interno e il Ministero della Difesa - affiancati a quelli di Agenzie internazionali quali Europol ed Interpol.
Il falso documento a firma di vertici di Istituzioni statuali quali il Capo della Polizia Lamberto Giannini, piuttosto che del Comandante Generale dell'Arma dei Carabinieri, Teo Luzi, dal Direttore del Servizio Polizia Postale, pro tempore, Nunzia Ciardi e dall'attuale Direttore Supplente del Servizio Polizia Postale, Ivano Gabrielli.
L'atto fraudolento contesta all'utente violazioni gravissime, commesse attraverso la rete Internet, legate a condotte penalmente rilevanti riferite a delitti di molestie sessuali su minori.
Il documento minaccia di inoltrare le prove ad un non meglio specificato "Procuratore" ed ai media, invitando a fornire giustificazioni entro 72 ore.
Il passo successivo è una richiesta di denaro per far "decadere" le accuse e l'indicazione delle coordinate bancarie verso le quali corrispondere le somme estorte.
Il fenomeno che ha una rilevanza europea, colpisce in particolare Francia, Austria, Spagna, Belgio e Italia. Sono in corso i rituali accertamenti tecnici sul materiale informatico oggetto di perquisizione, al fine di delineare le responsabilità dei soggetti indagati nell'attività delittuosa e la rete dei contatti coinvolti nell'invio delle mail estorsive con particolare attenzione ai collegamenti con l'estero.

Operazione "MOSCOW MULE 2" - Gli investigatori del Centro Operativo per la Sicurezza Cibernetica per la Liguria, coordinati dalla locale Procura della Repubblica, hanno ottenuto l'aggravamento degli arresti domiciliari e hanno arrestato nuovamente M.N., quarantenne cittadina russa.
La donna era già stata arrestata nel capoluogo ligure nel mese di ottobre 2021. Nella vita di tutti i giorni si nascondeva dietro alla parvenza di una tranquilla madre di famiglia, in realtà si tratta di un'avvenente esperta hacker: un ingegnere informatico con la passione per il crimine e le cryptovalute.
Il Tribunale di Genova, nel mese di marzo 2022, aveva concesso alla donna gli arresti domiciliari presso un'associazione di volontariato del centro genovese impegnata nel recupero dei detenuti.
Le particolari attitudini, l'alto profilo criminale, hanno indotto gli investigatori della Polizia Postale a pianificare stretti contatti con la struttura presso la quale "l'ingegnere" era stata posta agli arresti domiciliari. Le continue richieste della donna di poter utilizzare un telefono o un computer hanno ulteriormente insospettito gli investigatori, che hanno predisposto delle attività tecniche di intercettazione ambientali e telematiche.
Da queste si è potuto avere la certezza che la donna, nonostante fosse agli arresti domiciliari aveva da subito cercato di riorganizzarsi, iniziando nuovamente a commettere frodi informatiche a danno di ignari cittadini.
L'hacker ha oltremodo dimostrato la propria capacità criminale avvedendosi dell'intercettazione telematica procedendo ripetutamente in continui tentativi di eludere le investigazioni e di cancellare le prove a proprio carico.
Nel corso della perquisizione domiciliare, gli esperti della Sezione Financial Cybercrime della Polizia Postale hanno sequestrato numeroso materiale, tra l'altro reperito dalla donna durante la detenzione domiciliare, che è tuttora sottoposto ad esame per ulteriori risvolti investigativi.

Operazione "SIM SWAP" - Nella giornata del 22 marzo 2022 personale della Specialità ha eseguito 2 provvedimenti di custodia cautelare degli arresti domiciliari, emessi dal Tribunale di Bologna, nei confronti di 2 soggetti italiani, operanti sul territorio nazionale, dediti alla frode informatica effettuata attraverso la tecnica c.d. "SIM SWAP".
L'attività nasce dalla denuncia di una vittima del ravennate, alla quale i due soggetti hanno sottratto la somma di circa 75.000 euro.
Tale somma è stata distolta con diversi bonifici a favore di conti correnti aperti presso banche italiane ma soprattutto estere.
Le attività di perquisizione eseguite contestualmente ai sopra citati provvedimenti hanno permesso di confermare, oltre al *modus operandi*, come l'attività criminale posta in essere fosse attuale e ancora in corso in quanto gli indagati sono stati trovati in possesso oltre all'attrezzatura informatica, di migliaia di dati relativi alle credenziali di accesso a conti correnti con la relativa indicazione dell'Istituto di Credito.

Operazione "BOLTON" - Al termine di un'accurata attività investigativa in materia di abusivismo finanziario effettuato promuovendo la compravendita di strumenti finanziari dietro la promessa di profitti elevati, il Centro operativo per la sicurezza cibernetica di Cagliari unitamente a personale della Guardia di Finanza, in data 16 aprile 2022 ha dato seguito a misure cautelari personali e patrimoniali disposte dal Giudice per le indagini preliminari del Tribunale di Cagliari nei confronti di 6 persone gravemente indiziate, unitamente ad altri 4 indagati denunciati a piede libero.
L'indagine, che trae origine da numerose denunce per frode, ha consentito di ricostruire lo schema illecito utilizzato (c.d. schema Ponzi) e la rete posta in essere dai sodali.
Gli indagati, per i delitti di associazione per delinquere finalizzata alla truffa, al riciclaggio ed autoriciclaggio, avevano costituito un reticolo di società finanziarie, anche di diritto estero, strumentali al procacciamento di clienti.
Nel corso dell'operazione sono stati eseguiti sequestri preventivi, finalizzati alla confisca anche per equivalente, di beni e disponibilità finanziarie per un importo complessivo di oltre 4.500.000 euro. Tra i beni sequestrati vi sono disponibilità finanziarie, quote societarie ed una struttura alberghiera ubicata dell'hinterland cagliaritano, del valore stimato di circa 1.500.000 euro, la cui acquisizione da parte del *dominus* dell'associazione criminale è avvenuta mediante il coinvolgimento di un prestanome.

COMMISSARIATO DI P.S. ONLINE

L'uso crescente delle nuove tecnologie ha reso necessario lo sviluppo e il potenziamento di nuovi strumenti di comunicazione che consentissero alla Polizia di Stato di mettersi in contatto diretto con gli utenti del *web*.

In tale ottica, il portale del Commissariato di PS online ha permesso al cittadino, abituato ormai a utilizzare la rete internet per svolgere le principali attività quotidiane, di rivolgersi agli agenti della Polizia Postale in qualsiasi momento e ovunque si trovi. Attraverso il computer, l'utente può segnalare comportamenti che giudica illeciti e chiedere aiuto per superare difficoltà e problematiche, anche nei casi in cui potrebbe essere fonte di disagio rappresentarle di persona.

La facilità con cui il cittadino ha interagito con la piattaforma dedicata, ha reso possibile raccogliere le segnalazioni di quegli utenti che, mossi da spirito altruistico e di collaborazione, si sono rivolti alla Polizia Postale in un'ottica di sicurezza partecipata - nella sua declinazione online - fornendo utili evidenze su fenomeni emergenti potenzialmente lesivi, così

contribuendo, in termini di efficace prevenzione, ad evitare che altri internauti potessero cadere nelle trappole della Rete.

L'esigenza di innalzare al massimo i livelli dell'azione preventiva ha imposto di introdurre una nuova sezione, dedicata agli *alert*, dove vengono raccolti e pubblicati gli "avvisi agli utenti" che, proprio perché costantemente aggiornati e facilmente raggiungibili, costituiscono un efficace strumento di autotutela messo a disposizione del cittadino.

Tra i fenomeni riscontrati con maggior frequenza nell'anno 2022 annoveriamo, a titolo esemplificativo, i furti di *account social*, le estorsioni a sfondo sessuale, il *phishing* ai danni di correntisti di istituti bancari, le proposte di falsi investimenti online, nonché falsi siti di vendita di quei prodotti che, in un determinato contesto temporale, risultano essere maggiormente richiesti sul mercato.

Le segnalazioni che richiedono l'intervento tempestivo del Commissariato di PS online sono molteplici. Emblematico è quanto avvenuto lo scorso 18 marzo, quando è giunta la richiesta di aiuto di una figlia preoccupata per la madre, vittima di una truffa sentimentale.

In particolare, la donna è stata contattata attraverso un noto social network da un uomo dalle maniere gentili che ha iniziato a corteggiarla con insistenza fino a farla innamorare. Dopo aver conquistato la fiducia della donna, il truffatore, confidandole di avere una figlia gravemente malata, che necessitava di cure molto costose alle quali non riusciva a far fronte, le ha richiesto un sostanzioso aiuto economico. La vittima, particolarmente colpita dalla triste vicenda, ha iniziato a inviare a più riprese ingenti somme di denaro sino a dilapidare il suo intero patrimonio.

Tutti i tentativi esperiti dai familiari della donna per farle capire di essere caduta vittima di un raggiro, sono risultati vani.

A quel punto, a seguito della segnalazione, il poliziotto del Commissariato di PS online, contattando la donna, è riuscito a farle comprendere che la persona che credeva essere il suo amato era in realtà un abile truffatore.

Grazie a questo intervento, la donna, oramai consapevole di quanto le era accaduto, ha interrotto la relazione e trovato il coraggio di sporgere denuncia.

Sul sito, inoltre, giungono segnalazioni da parte di utenti che si trovano in situazioni di pericolo o che minacciano gesti estremi; in tali circostanze, ai poliziotti della sala operativa del Commissariato di PS online è richiesto un tempestivo e coordinato intervento che coinvolge gli uffici territoriali delle Questure interessate dall'evento.

Lo scorso 19 gennaio, ad esempio, il personale del Commissariato ha gestito una segnalazione proveniente da un ragazzo che aveva manifestato l'intenzione di togliersi la vita dopo essere stato vittima di un'estorsione sessuale.

Il poliziotto che ha preso in carico la segnalazione ha immediatamente contattato telefonicamente il giovane che si è mostrato inizialmente reticente, timoroso e particolarmente spaventato, rifiutando di fornire indicazioni utili alla sua localizzazione.

Intuendo il suo grave disagio, e nonostante la ritrosia dimostrata dal ragazzo, l'operatore è riuscito ad instaurare un rapporto di empatia e fiducia col suo giovane interlocutore convincendolo a non commettere gesti estremi.

Il poliziotto ha intrattenuto il ragazzo al telefono per consentire agli operatori della Sala di esperire tutti gli accertamenti necessari per identificarlo e, una volta geolocalizzato, con l'ausilio di una pattuglia è stato possibile prestargli l'assistenza necessaria.

Gli interventi finalizzati alla prevenzione di **intenti suicidari** da parte di utenti dei vari social network, segnalati attraverso il Commissariato di P.S. online **sono stati 64.**

L'analisi delle oltre **100.000** segnalazioni ricevute dal sito del Commissariato di PS online nell'anno 2022, ha evidenziato che in molti casi gli internauti sconoscono e/o non adottano

quelle piccole e necessarie accortezze di *cyber hygiene* che consentirebbero loro di prevenire e limitare la maggior parte degli attacchi informatici e il perpetrarsi di attività delittuose.

Per questo motivo, è stata introdotta sul sito una specifica sezione con cui vengono veicolate al cittadino pillole di sicurezza informatica, funzionali a ridurre al minimo i rischi legati all'uso di dispositivi informatici.

La popolarità del sito è avvalorata dal numero degli accessi che sono stati, nel periodo di riferimento, oltre **42.200.000**.

Nella costante ricerca di nuove e incisive strategie di comunicazione per fornire ad un'utenza sempre più ampia, si è passati da una comunicazione verso il cittadino a una interazione con il cittadino.

ATTIVITA' DI PREVENZIONE

La Polizia Postale se da un lato svolge un'incisiva attività di repressione dei reati informatici, dall'altro lato svolge un'importante azione preventiva a tutela dei minori, soprattutto per quanto concerne il fenomeno del cyberbullismo e di tutte le forme di prevaricazione online, fenomeni che destano grande allarme sociale.

Tra le iniziative educative si riporta il coinvolgente format teatrale itinerante e in streaming **#cuoriconnessi** che ha coinvolto oltre 270mila studenti sul territorio nazionale.

Di rilievo è anche la campagna educativa itinerante di sensibilizzazione e prevenzione sui rischi e pericoli legati ad un uso non corretto della rete internet da parte dei minori denominata *Una vita da social*.

L'iniziativa, arrivata quest'anno alla sua X edizione, ha coinvolto oltre **2milioni e 8oomila studenti,** attraverso il truck didattico multimediale della Polizia Postale, e ha proseguito la sua attività itinerante in Italia e all'estero.

Il progetto si cala nella filosofia dei giovani interlocutori, interagendo con un linguaggio comunicativo semplice ma esplicito, adatto a tutte le fasce di età, coinvolgendo così dai più piccoli ai docenti ai genitori, con la finalità di combattere la violenza e la prevaricazione dei giovani bulli.

L'impegno profuso dagli specialisti della Polizia Postale nell'azione di sensibilizzazione e informazione ha consentito, nell'anno appena trascorso, di realizzare incontri con docenti e genitori in oltre 2.800 istituti scolastici e di coinvolgere oltre **820mila** studenti.

ATTIVITA' DI FORMAZIONE INNOVAZIONE E RICERCA NEL SETTORE DELLE TECNOLOGIE ICT E DI REALIZZAZIONE DEL CERT MINISTERO DELL'INTERNO

Nel corso dell'anno 2022, la Polizia Postale e delle Comunicazioni ha proseguito nell'attività di collaborazione con diverse Istituzioni Scientifiche ed Enti di Ricerca volta ad individuare e valorizzare nuove tecniche e metodologie di lavoro nel contesto info-investigativo. In tal senso, di significativa rilevanza è la pianificazione di percorsi formativi di settore, con particolare

riferimento alle tecnologie emergenti (5G, blockchain, IoT, AI) ed al complesso mondo dei sistemi criptati ed al loro dilagante utilizzo criminale.
Di assoluta importanza è stata l'attività di progettazione ed alta formazione specialistica finalizzata all'avvio del CERT (Computer Emergency Response Team) – Ministero Interno. Tale costituendo organismo, che opererà sotto l'egida della nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, sarà chiamato a svolgere un'efficace attività di presidio e risposta interdipartimentale contro incidenti informatici, coordinando le attività di contenimento e ripristino, per la prevenzione e la gestione degli attacchi cibernetici, delle reti e dei sistemi informativi del Ministero dell'Interno.
Si è dato avvio ad una formazione specialista di altissimo profilo a beneficio degli operatori già impegnati nello specifico contesto.