Resoconto attività 2020
Polizia Postale e delle Comunicazioni

1. C.N.C.P.O.

Nel corso del 2020, il *Centro Nazionale per il Contrasto alla Pedopornografia Online* (C.N.C.P.O.) ha confermato il ruolo centrale della Polizia Postale e delle Comunicazioni nella lotta alla pedofilia e pornografia minorile online.
Dall'inizio della diffusione pandemica da COVID-19, la Polizia Postale ha intensificato il monitoraggio della rete con lo scopo di scongiurare l'aumento di reati relativi allo sfruttamento sessuale dei minori online, determinato dalle misure restrittive assunte. E' stato svolto un lavoro di valutazione settimanale dei dati relativi alla vittimizzazione dei bambini e dei ragazzi in rete, al fine di monitorare la minaccia cibernetica in un momento di fragilità emotiva nazionale.
Con la sospensione delle attività scolastiche e la conseguente attivazione della didattica a distanza per tutti gli Istituti, molteplici sono state le segnalazioni relative a episodi di intrusione nelle piattaforme dedicate alla formazione degli studenti; la Polizia Postale ha svolto un assiduo monitoraggio anche sulle *app* di messaggistica istantanea, al fine di individuare i responsabili degli accessi non autorizzati, accertando la presenza di gruppi dedicati.
Le condotte delittuose che hanno registrato un incremento di circa il **110%** rispetto allo stesso periodo dell'anno precedente, riguardano i reati relativi allo **sfruttamento sessuale dei minori online** e dell'**adescamento di minori online**, per i quali sono stati eseguiti **69** arresti e denunciate **1192** persone.

Per tale motivo, fin dall'inizio della diffusione pandemica del virus Sars-Cov-2, la Polizia Postale e delle Comunicazioni, con l'impiego di tutte le sue articolazioni territoriali (coordinate attraverso l'azione strategica assicurata da questo Servizio), ha:

a) intensificato il monitoraggio della rete, con lo scopo di scongiurare l'aumento di reati in esame;
b) rafforzato il raccordo delle investigazioni nei canali di cooperazione internazionale di polizia e giudiziaria, presupposto strategico fondamentale per disarticolare le illecite comunità virtuali caratterizzate da una struttura organizzata;

c) innalzato, laddove possibile, il livello di collaborazione con i social network più diffusi in Italia, in un'ottica di sinergia nella lotta all'utilizzo improprio del web, definendo canali preferenziali di comunicazione e gestione dei casi penalmente rilevanti;
d) aumentato l'impegno funzionale all'individuazione di un numero sempre maggiore di siti che contengono materiale pedopornografico, da inserire nella black list, gestita dal C.N.C.P.O., il cui accesso viene inibito, con modalità diverse a seconda dell'ubicazione dei server utilizzati, agli utenti internet attivi sul territorio italiano.

Tutto ciò, nel tentativo di adeguare la risposta, anche sotto il profilo della prevenzione, alle mutate esigenze connesse all'emergenza sanitaria in atto.

Tra le **14 indagini** più significative avviate dal **C**entro **N**azionale di **C**ontrasto alla **P**edopornografia **O**nline del Servizio Polizia Postale nell'ambito dei reati di sfruttamento sessuale dei minori, condotta principalmente in modalità sotto copertura online anche nelle ***Dark Net,*** si segnala:

OPERAZIONE *"LUNA PARK"*
Dopo due anni di indagini "*sotto copertura"* nel web, la Polizia Postale ha identificato **432 utenti** che condividevano su applicazioni di messaggistica istantanea foto e video pedopornografici, anche di neonati. Dei **159 gruppi individuati**, **16** erano delle vere e proprie **associazioni per delinquere**, composte da promotori, organizzatori e partecipi, con ruoli e compiti ben definiti. Sono **81** gli italiani identificati e **351 gli utenti stranieri** coinvolti nell'indagine, alcuni dei quali tratti in arresto nei loro Paesi di origine, nell'ambito della cooperazione internazionale di polizia attivata dal C.N.C.P.O.

Un'altra delicata operazione ha riguardato un filmato pubblicato in diretta su una piattaforma gratuita di ***streaming*****,** in cui un uomo abusava di una neonata. All'esito dell'indagine è stata eseguita un'ordinanza di custodia cautelare in carcere nei confronti del **nonno materno della bimba,** al quale veniva affidata quando la madre era via. Durante la perquisizione sono stati rinvenuti decine di migliaia di file pedopornografici raffiguranti minori anche in tenerissima età.

OPERAZIONE *"DARK LADIES"*
Operazione che ha portato all'arresto di due mamme e un papà i quali abusavano sistematicamente delle proprie figlie, diffondendo online le immagini delle violenze. Sono stati contestati i reati di produzione e diffusione di materiale di pornografia minorile online, nonché di violenza sessuale. Le investigazioni sono state condotte su gruppi di messaggistica istantanea a "*tema pedofilo*". Le due bambine sono state affidate ai servizi sociali e condotte in luoghi sicuri.

OPERAZIONE *"PAY TO SEE"*
L'indagine è scaturita dalla denuncia di un genitore che aveva rinvenuto sul cellulare della figlia una chat contenente un vero e proprio *listino prezzi* per prestazioni di natura sessuale online, con tariffe differenziate a seconda delle richieste (es.: *"sexchat 45 minuti in cui faccio da schiava = 30 euro"*). La Polizia Postale ha eseguito 21 perquisizioni su tutto il territorio nazionale anche nei confronti di diversi minori che avevano acquistato i "servizi" offerti dall'adolescente.

OPERAZIONE *"DANGEROUS IMAGES"*

L'attività investigativa ha portato alla denuncia di **20 minorenni** in concorso tra loro per detenzione e diffusione di materiale di pornografia minorile a delinquere. La Polizia Postale ha individuato un 15enne, organizzatore e promotore, insieme ad altri coetanei, dello scambio di innumerevoli filmati e immagini pedopornografiche, anche in forma di *stickers*, attraverso diversi social network. Il giovane era in possesso anche di numerosi files c.dd. *gore*, ovvero filmati e immagini provenienti dal Dark Web, raffiguranti suicidi, torture, mutilazioni, squartamenti e decapitazione di persone e animali.

OPERAZIONE "50 COMMUNITY"

L'attività condotta dalla Polizia Postale per diffusione e, in alcuni casi, produzione di materiale di pornografia minorile, nei confronti di 50 indagati, 3 dei quali arrestati per possesso di ingente quantità di materiale pedopornografico. L'operazione, coordinata dal C.N.C.P.O., ha coinvolto tutto il territorio nazionale ed è frutto di una cooperazione con il canadese *National Child Exploitation Coordination Center (NCECC)*. Il materiale illegale, scambiato su piattaforme di messaggistica istantanea, era diversificato e spaziava da immagini di nudo a violenze sessuali ai danni anche di neonati, scene di sadismo, etc.

OPERAZIONE AMNESIA

E' una delle indagini più significative nell'ambito dei reati di sfruttamento sessuale dei minori, che ha consentito di trarre in arresto un 30enne per detenzione di materiale di pornografia minorile, aggravato dall'ingente quantità, dall'utilizzo di mezzi di anonimizzazione e criptazione, nonché dalla particolare violenza di alcune immagini rinvenute.

In particolare, l'uomo produceva filmati di abusi sessuali ai danni di una **bambina di pochi anni, visibilmente narcotizzata**. I video sono stati poi diffusi e commercializzati nel ***dark web***.

OPERAZIONE SCACCO MATTO

L'indagine è il frutto di una lunga attività sotto copertura, scaturita da un monitoraggio sul Dark Web e dal rinvenimento di un sito contenete immagini di pornografia minorile e commenti che istigavano esplicitamente alla commissione di atti sessuali in danno di minori, che ha portato alla denuncia di 20 persone di cui 3 tratte in arresto

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 **33.681**, di cui **2.446** inseriti in *black list* e oscurati in quanto presentavano contenuti pedopornografici.

C.N.C.P.O.	**2019**	**2020**	**Incremento %**
Casi trattati	1396	3.243	+ 132,30 %
Persone indagate	617	1192	+ 93.19 %
Arrestati	37	69	+ 86.48 %

Perquisizioni	510	757	+ 48.43 %
Gb di materiale sequestrato	127.269	215.091	+ 69.00 %

2. TRUFFE ON LINE E REATI CONTRO LA PERSONA

Il fenomeno delle **truffe online,** ha riguardato anche la **contraffazione del marchio CE**. Sono state scoperte numerose partite di materiale, venduto all'ingrosso, proveniente soprattutto dall'estero, riportanti marchi CE contraffatti: la merce era destinata, in alcuni casi, alla vendita al dettaglio anche attraverso il circuito delle farmacie ignare della contraffazione.

Nei primi mesi dell'anno, sono stati riscontrati numerosi casi di truffe online nella vendita di **dispositivi di protezione individuale,** considerata la ricerca pressante di mascherine, guanti, liquidi igienizzanti, attraverso la proliferazione di numerosi siti di e-commerce truffaldini dedicati al commercio di tali prodotti.

Sono state anche raccolte numerose segnalazioni e avviate altrettante attività d'indagine, inerenti le **false raccolte fondi,** poste in essere attraverso siti web apparentemente riconducibili ad enti ospedalieri o accreditate da falsi patrocini di Istituzioni o Enti Pubblici (Regioni – Comitati vari). Il *modus operandi* dei cybercriminali, facendo leva sul generale e diffuso sentimento di vicinanza della cittadinanza al personale medico ed infermieristico, incessantemente impegnato nella lotta al **Covid-19,** dava la possibilità di effettuare dei versamenti di denaro e/o bonifici su IBAN legati a conti correnti o carte ricaricabili attivati ad hoc.

Inoltre, è stato osservato, contemporaneamente alla chiusura dei luoghi di lavoro a seguito dell'introduzione delle misure di contenimento del virus, un incremento del fenomeno dei **falsi annunci di lavoro**. Un fenomeno che racchiude in sé variegate condotte criminose, talune dirette a conseguire profitti illeciti (denaro, identità digitale e dati sensibili), altre tese ad esporre il cittadino che, inconsapevole del disegno criminoso, presta la sua opera per la realizzazione di delitti che spesso vanno ben oltre alla consueta truffa (riciclaggio di denaro), a gravi conseguenze sul piano giuridico, familiare e sociale.

Nell'ambito delle **truffe online**, nel corso del 2020 sono stati trattati complessivamente **98.000** casi.

Nel corso del periodo in esame, è stata implementata l'attività di contrasto al diffuso fenomeno del **falso trading online** (**358 casi trattati** con oltre **20 milioni** di euro di danno) che ha visto aumentare a dismisura la perdita di ingenti capitali verso Paesi esteri, con la prospettiva di facili guadagni derivanti da investimenti **"sicuri**".

Particolare attenzione è stata indirizzata all'attività di prevenzione e contrasto al **revenge porn** con **126** casi trattati e **59 denunciati;** alla **diffamazione on line** con **2.234** casi e **906** persone denunciate; **143** sono stati i casi relativi allo "**stalking" con 7 arrestati e 73 denunciati** e alla cosiddetta "**sextortion" con 636 casi trattati, una persona arrestata e 36 denunciate.**

I reati afferenti al cosiddetto **"Codice Rosso"**, le cui indagini sono profuse non soltanto per giungere all'identificazione del responsabile del reato, ma anche per rimuovere i contenuti dal web o, quantomeno, per limitarne la divulgazione massiva, hanno visto nella Polizia Postale un punto di riferimento per le tante vittime di reato.

Anche nella repressione dei reati di **minacce e molestie**, perpetrate attraverso i social network ovvero con "mezzi tradizionali", massimo è stato l'impegno della Polizia Postale con **1001 casi trattati, 2 arrestati e 270 persone denunciate.**

L'attività investigativa volta ad arginare il fenomeno dell'***hate speech***, è stata particolarmente complessa portando alla trattazione di numerose segnalazioni di utenti attraverso il Commissariato di P.S. online, e un monitoraggio attivo della rete attraverso le piattaforme social.
In questo ambito una particolare attenzione si è avuta per gli atti intimidatori posti in essere nei confronti dei **giornalisti,** con l'attiva partecipazione, in chiave operativa con idonee iniziative di prevenzione e contrasto, al Sottogruppo istituito presso la Direzione Centrale della Polizia Criminale – Servizio Analisi Criminale.
Sono stati **35** gli interventi da parte degli Uffici della Polizia Postale dislocati su tutto il territorio nazionale, coordinati dal Servizio Polizia Postale, finalizzati alla prevenzione di **intenti suicidari** da parte di utenti dei social network, anche grazie alle segnalazioni pervenute al **Commissariato di PS OnLine**.

	2019	**2020**
Diffamazione online	2.234	2.234
Stalking	168	143
Revenge porn	131	126
Sextortion	516	636

Tra le citate attività di polizia giudiziaria, si segnalano alcune di particolare rilievo:

OPERAZIONE "POSTE VITA"
A seguito di denunce presentate da PosteVita e Poste Italiane S.p.A. riguardanti riscossioni fraudolente di polizze del Ramo Vita, è stata avviata una complessa attività di indagine, dalla Polizia Postale e delle Comunicazioni, giungendo all'identificazione di una compagine criminale costituita da 16 associati che, attraverso la riscossione fraudolenta di polizze del ramo "Poste vita", era riuscita a conseguire un profitto illecito pari a 1 milione e 500.000 euro.

OPERAZIONI BREAKING NEWS
La Polizia Postale, a conclusione di un'articolata attività investigativa coordinata dalla Procura Distrettuale di Messina, ha denunciato in stato di libertà un uomo di anni 46, disoccupato, residente in provincia di Torino, ritenuto responsabile di ricettazione e violazione del diritto di autore. Nella circostanza l'individuo, tramite gruppi del servizio di messaggistica Telegram, diffondeva illecitamente quotidiani online con grave pregiudizio per le testate giornalistiche con rilevante perdita di vendite.
La Polizia Postale, nonostante le problematiche di trasparenza legate all'utilizzo della piattaforma Telegram, è riuscita a risalire all'indagato nei confronti del quale la Procura ha emesso un decreto

di perquisizione che ha condotto al sequestro delle apparecchiature informatiche utilizzate per commettere gli illeciti.

OPERAZIONE "FAKE TRAVELS"
La Polizia Postale, al termine di un'articolata attività investigativa coordinata dalla Procura della Repubblica di Ancona, hanno sgominato un sodalizio criminale dedito alla consumazione di truffe ad aziende italiane del centro/nord. Tali aziende, operanti in vari settori merceologici, venivano attirate dalla possibilità, poi risultata falsa, di concludere lucrosi affari con industrie americane. Denunciati 4 italiani, di cui due residenti all'estero, responsabili di una movimentazione fraudolenta di denaro per centinaia di migliaia di euro e di dollari che poi venivano trasferiti su conti svizzeri e statunitensi.

OPERAZIONE "SAFE SOCIAL"
La Polizia Postale, al termine di un'articolata attività investigativa coordinata dalla Procura della Repubblica di Bologna, ha svolto un'articolata attività investigativa relativa a numerose truffe online, perpetrate in danno di giovani utenti, interessati all'acquisto di capi di abbigliamento di modesto valore commerciale, posti in vendita tramite la piattaforma Instagram. Gli accertamenti effettuati hanno consentito di riscontrare profitti fraudolenti per circa 250.000,00 Euro e un numero di vittime stimato in 2400 persone, di cui oltre la metà minori. Ad esito dell'attività di indagine è stato individuato un sodalizio, operante nell'hinterland milanese e nei confronti di cinque degli indagati sono state eseguite misure cautelari e in totale 12 provvedimenti di perquisizione.

OPERAZIONE "REVENGE PORN"
La Polizia Postale e delle Comunicazioni, coordinata dalla Procura di Udine, ha svolto un'attività d'indagine relativa alle numerose denunce per cyberstalking e revenge porn, presentate da una donna triestina nei confronti dell'ex compagno, per la pubblicazione su siti pornografici di foto sessualmente esplicite, scattate durante la loro relazione. L'indagato, con precedenti penali specifici e già tratto in arresto dalla Polizia Postale, per ripetute violenze sessuali videoriprese nei confronti di una minore di 4 anni, è stato sottoposto a perquisizione che ha permesso il rinvenimento e il sequestro di materiale significativo a livello probatorio.

3. CNAIPIC

L'analisi del dato emergente dalle attività del **C**entro **N**azionale **A**nticrimine Informatico per la Protezione delle Infrastrutture Critiche (**CNAIPIC**), relativo al periodo intercorso tra **gennaio e dicembre 2020**, permette di rilevare, in primo luogo, come, sia gli attacchi diretti alle grandi infrastrutture erogatrici di servizi essenziali (approvvigionamento idrico ed energetico, pubblica amministrazione, sanità, comunicazione, trasporti, finanza sistemica), che gli attacchi apparentemente isolati (diretti a singoli enti, imprese o cittadini), siano connotati da una dimensione criminale organizzata, essendo ascrivibili all'operato di sodalizi ben strutturati, spesso operanti a livello transnazionale.

Le tipologie di eventi cyber che hanno maggiormente impegnato gli operatori del Centro sono rappresentate dagli attacchi a mezzo malware, soprattutto di tipo ransomware, attacchi DDoS con

finalità estorsiva, accessi abusivi con l'intento di carpire dati sensibili, campagne di phishing e, in ultimo, campagne APT (*Advanced Persistent Threats*), particolarmente insidiose poiché ricollegabili ad attori malevoli dotati di notevole expertise tecnico e rilevanti risorse.

L'emergenza Covid-19, in particolare, ha costituito un'ulteriore occasione per strutturare e dirigere attacchi ad ampio spettro, volti a sfruttare per scopi illeciti la situazione di particolare esposizione e maggior vulnerabilità in cui il Paese è risultato, e tuttora risulta, esposto.

Nello specifico, alcune delle più rilevanti infrastrutture sanitarie impegnate nel trattamento dei pazienti "Covid" sono state oggetto di campagne di cyber-estorsione volte alla veicolazione all'interno dei sistemi ospedalieri di sofisticati ransomware – concepiti allo scopo di rendere inservibili, mediante cifratura, i dati sanitari contenuti al loro interno - a fronte di richieste di pagamento del prezzo estorsivo, per lo più in cryptovalute (es. Bitcoin), onde ottenere il ripristino dell'operatività.

Il sistema sanitario e della ricerca è stato inoltre bersaglio di diversi attacchi APT, con lo scopo della esfiltrazione di informazioni riservate riguardanti lo stato di avanzamento della pandemia e l'elaborazione di misure di contrasto, specie con riguardo all'approntamento di vaccini e terapie anti-Covid.

Si sono moltiplicati i casi di phishing ai danni di enti ed imprese, veicolati attraverso messaggi di posta elettronica i quali, dietro apparenti comunicazioni di Ministeri, organizzazioni sanitarie ed altri enti, relative all'andamento del contagio o alla pubblicazione di misure di contrasto, nascondevano in realtà sofisticati virus informatici in grado di assumere il controllo dei sistemi attaccati (c.d. virus RAT) e procedere così all'esfiltrazione di dati personali e sensibili, alla captazione di password di accesso a domini riservati, finanche all'attivazione di intercettazioni audio-video illegali.

Sul piano degli attacchi al sistema produttivo del Paese, si è registrato un generale aumento delle minacce legato all'adozione su larga scala dei modelli di lavoro a distanza, c.d. "*smartworking*", modelli che se da un lato hanno consentito la prosecuzione di attività essenziali, hanno d'altro canto prodotto una considerevole estensione del perimetro informatico delle aziende, con una conseguente maggior esposizione ad azioni ostili esterne.

Nel delineare l'identità degli autori del reato, il *trend* legato all'andamento degli attacchi ai danni delle infrastrutture critiche fa registrare, nel complesso, l'emersione di una matrice criminale di natura puramente economica, orientata al conseguimento di profitti illeciti, che si pone in misura oggi prevalente rispetto alle condotte ispirate da ragioni di *cyber-hacktivism*, ideologicamente o politicamente orientato.

L'azione di contrasto attuata dal CNAIPIC, nell'anno in corso, è stata orientata sia all'attività di contrasto dei reati, sia, soprattutto, ad assicurare interventi di tipo preventivo e di protezione, incentrati sulla capacità di analisi e di allerta precoce finalizzata alla diffusione, in tempo reale, degli IoC (c.d. indicatori di compromissione) relativi alle minacce in corso, a beneficio dell'intero panorama delle infrastrutture critiche nazionali.

L'aggiornato quadro informativo riferibile alle specifiche fenomenologie delittuose può essere agevolmente evidenziato attraverso la tabella statistica, di seguito indicata, che offre il confronto tra il periodo **gennaio/dicembre 2019** e quello riferibile **all'anno 2020**, periodo, quest'ultimo, caratterizzato dall'emergenza epidemiologica in atto che ha favorito, come detto, l'andamento crescente del numero di attacchi complessivamente verificatisi ai danni delle Infrastrutture critiche del nostro Paese:

	2019	**2020**
Attacchi rilevati	239	507
Alert diramati	77.596	79.209
Indagini avviate	88	99
Persone arrestate	3	21
Persone denunciate	53	79
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	74	65

Dalla tabella si evince che, ad oggi, gli attacchi rilevati sono più che raddoppiati, con un conseguente quasi equivalente incremento delle persone identificate ed indagate.

Tra le attività di polizia giudiziaria più significative si segnala:

OPERAZIONE "DATA ROOM"

Il CNAIPIC nell'ambito di una lunga ed articolata attività di indagine ha effettuato quella che può essere ritenuta la prima operazione su larga scala volta alla tutela di dati personali trafugati, culminata con l'esecuzione, effettuata con l'ausilio di personale dei Compartimento Polizia Postale e delle Comunicazioni di Roma, Napoli, Perugia ed Ancona, a 13 ordinanze di custodia cautelare e 7 ordinanze che dispongono l'obbligo di dimora nel comune di residenza ed il divieto di esercitare imprese o ricoprire incarichi direttivi in imprese e persone giuridiche.

Al vertice del sistema due dipendenti infedeli di TIM S.p.A., oltre ai responsabili di alcune società che offrono servizi di call center, avevano messo i piedi una complessa ed articolata attività criminale finalizzata al commercio illecito dei dati personali di centinaia di migliaia di utenti di società operanti nella fornitura di servizi essenziali, nel settore telecomunicazioni ed energia.

I 26 indagati complessivi, tutti destinatari di provvedimenti di perquisizione locale e personale, sono stati ritenuti responsabili, a vario titolo ed in concorso tra loro, della violazione aggravata dei reati previsti all'art. 615 ter c.p. (accesso abusivo a sistema informatico), all'art.615 quater c.p. (detenzione abusiva e diffusione di codici di accesso), riguardando le condotte sistemi di pubblico interesse, e della violazione della legge sulla privacy art. 167-bis D. Lgs. 193/2003 (comunicazioni e diffusione illecita di dati personali oggetto di trattamento su larga scala).

Le estrazioni dei dati dai database dei fornitori dei servizi, per come verificato nel corso delle indagini, venivano sistematicamente portate avanti con un volume medio di centinaia di migliaia di record al mese, che gli indagati modulavano a seconda della illecita "domanda" di mercato.

Nel corso delle attività, svolte grazie alla collaborazione di TIM S.p.A. ed all'importante apporto della struttura di sicurezza aziendale dell'azienda, è venuto alla luce un complesso "sistema" che vedeva, da un lato una serie di tecnici infedeli procacciare i dati, dall'altro una vera e propria rete commerciale che ruotava attorno alla figura di un imprenditore Campano, acquirente della preziosa "merce", che poi veniva poi piazzata sul mercato dei call center, 13 sono quelli già individuati nella prima fase delle indagini, tutti in area campana, ed oggetto di altrettante attività di perquisizione.

Nell'ottica di un'efficace condivisione operativa, il Centro ha proseguito la stipula di specifici Protocolli a tutela delle infrastrutture critiche nazionali: al riguardo, nel 2020 sono **state sottoscritte 7 nuove convenzioni** con le società **Borsa Italiana, EFSA (European Food Safety Authority), IREN S.p.A., SACBO Aeroporto di Bergamo, SAIPEM S.p.A., SIA S.p.A. e SIOT TAL Oleodotto Transalpino**.

Si rappresenta, altresì, che analoghe forme di collaborazione sono state avviate dagli uffici territoriali della Specialità con strutture sensibili di rilevanza locale, sia pubbliche che private, al fine di garantire un sistema di sicurezza informatica capillare e coordinato.

4. FINANCIAL CYBERCRIME

Il diffondersi dell'epidemia da Covid-19 ha senz'altro inciso, anche sulla qualità e quantità dei fenomeni legati al *cybercrime*, con particolare riferimento al crimine di tipo economico-finanziario.

Il *phishing* finanziario fa registrare decisi incrementi, essendo aumentata la misura delle carte di credito compromesse e dei dati finanziari commercializzati sul *dark web* (così come sono in aumento i casi di *vishing*, volti a carpire dati personali e codici bancari dispositivi attraverso semplici truffe telefoniche operate da numeri telefonici apparentemente riconducibili a banche ed istituti finanziari).

In via generale, le ricerche più autorevoli hanno rilevato nei primi sei mesi un aumento del 600% nel numero di e-mail di *phishing* in tutto il mondo, che utilizzava temi correlati al Coronavirus per colpire persone e aziende. Di queste, il 45% puntava su siti-clone, inducendo gli utenti di Internet a digitare le proprie password su domini malevoli. La restante parte dei casi ha riguardato, per lo più, l'utilizzo di temi correlati al Covid-19 all'interno di messaggi email che inducevano a cliccare su allegati contenenti malware di varia natura.

Le frodi basate sul social engineering vedono stabili nei numeri i fenomeni di *Bec fraud* (frodi realizzate attraverso la compromissione di caselle di posta elettronica), che risultano tuttavia influenzati dall'epidemia del Covid-19 sia a causa dell'abbassamento delle difese aziendali, determinato dallo stato di difficoltà psicologica o "logistica" di lavoratori ed amministratori, sia dall'aumento delle comunicazioni commerciali a distanza, conseguente all'adozione su larga scala di processi di *smart-working*.

Alcuni *Bec fraud* risultano specificamente collegati al tema-Covid, perché relativi direttamente a frodi commerciali nell'acquisto di mascherine e dispositivi sanitari.

Con riguardo all'esperienza italiana, in pochi mesi, oltre ad un costante numero di casi "minori" (nell'ordine delle decine di migliaia di euro), sono **state frodate 48 grandi e medie imprese**, per un ammontare complessivo di oltre 25 milioni di euro di profitti illeciti, dei quali quasi **15 milioni** sono stati già recuperati in seguito all'intervento della Polizia Postale e delle Comunicazioni che, al 10 dicembre 2020, ha complessivamente **identificato ed indagato 674 persone di cui 24 tratte in arresto** (nell'analogo periodo del 2019 furono complessivamente indagate 531 persone di cui 8 in stato di arresto).
L'obiettivo criminale del trafugamento dei dati personali e delle credenziali di accesso a servizi finanziari, utili alla disposizione di pagamenti in frode, è raggiunto attraverso massive campagne di phishing, consumate mediante le due modalità in assoluto più ricorrenti, rappresentate dall'invio di email contenenti allegati malevoli e dall'impiego di siti-clone.
Parallelamente, il procacciamento di codici "one-time", token virtuali e password dispositive avviene mediante il ricorso all'insidiosa variante "vocale" del phishing, il cosiddetto "vishing", ed alle tecniche di sim-swap.

L'attività investigativa realizzata dalla Polizia Postale e delle Comunicazioni, funzionale al contrasto di tali fenomeni delittuosi, ha permesso di identificare ed indagare **3741 persone** a fronte dei **3473 denunciati nello stesso periodo dell'anno precedente.**
Di seguito le operazioni di Polizia Giudiziaria più significative:

OPERAZIONE "2BaGoldMule"
L'operazione che ha visto, per l'Italia la Polizia Postale agire al fianco di Europol, dell' FBI americana e delle forze di polizia informatiche di altri 14 paesi europei, ha disarticolato un'organizzazione criminale denominata QQAAZZ, attiva sin dal 2016 a livello internazionale nel cyber-riciclaggio, fungendo da piattaforma europea per ripulire i proventi di frodi informatiche messe a segno da alcuni dei più pericolosi cybercriminali del mondo.
La centrale di riciclaggio "QQAAZZ", aveva base operativa in Portogallo e Spagna e ramificazioni in tutta Europa, compresa l'Italia, dove l'organizzazione poteva contare su un altissimo numero di conti correnti bancari online, falsamente intestati ad altrettante "teste di legno" (i cosiddettti "Muli"), per spostare e rendere scarsamente rintracciabili gli ingenti profitti illeciti. Denaro che finiva anche nell'acquisto di cryptovalute o nel reimpiego in attività commerciali di copertura aperte nel Regno Unito.
In Italia, in particolare, la Polizia Postale ha identificato la branca nostrana della complessa organizzazione criminale, con l vertice due cittadini italiani residenti a Londra, in contatto con membri operativi del gruppo criminale di stanza nella capitale inglese.

OPERAZIONE "LAST CHAIN"
Nel settore del cyber-riciclaggio, nel corso dell'Operazione "Last Chain" la Polizia Postale ha identificato ed arrestato una delle più importanti organizzazioni criminali internazionali dedita alla

commissione di attacchi informatico-finanziari in tutta Europa., in collaborazione con Eurojust, Europol e con la polizia rumena, disarticolando una centrale di riciclaggio in Genova in relazione a profitti di frodi informatiche commesse in tutta Europa. Sono stati eseguiti 13 arresti in Italia e in Romania, oltre a diversi sequestri di ville, appartamenti automobili ed esercizi commerciali.
Il giro di affari dell'organizzazione criminale ammontava a 20 milioni di euro l'anno.

OPERAZIONE "ECLISSI"

Nel settore del contrasto alla **pirateria informatica**, con l'Operazione Eclissi la Polizia Postale ha messo a segno una delle più vaste operazioni di polizia mai condotte, coordinata a livello internazionale dalle agenzie Eurojust ed Europol, che ha puntato a disarticolare direttamente la complessa infrastruttura tecnologica responsabile della diffusione via Internet, attraverso numerosi siti, del segnale illegalmente captato di numerose emittenti televisive a pagamento.
Intervenendo direttamente su oltre 200 server e 80 allocati in diversi Paesi europei, che consentivano la diffusione capillare in tutta Europa del segnale, sono state bloccate "alla sorgente" 30 Iptv illegali, che raggiungevano un pubblico di circa 5 milioni di utenti solo in Italia.

OPERAZIONE "THE PERFECT STORM"

Dall'analisi tecnica dei dispositivi sequestrati in occasione della precedente operazione Eclissi, la Polizia Postale e delle Comunicazioni ha supportato la Guardia di Finanza nell'esecuzione di misure cautelari nei confronti di un'organizzazione criminale, basata in Italia e radicata in diversi stati Europei, composta da 20 cittadini italiani, 2 greci ed un maltese, ritenuti ricoprire una posizione di assoluto rilievo nel settore criminale della pirateria informatica.
Il supporto degli specialisti del Servizio Polizia Postale, richiesto dalla Procura della Repubblica di Napoli in virtù dello specifico know-how operativo maturato in occasione della precedente indagine, si è concretizzato nell'invio di dedicati team tecnici di intervento dislocati in 4 Focal point sul territorio nazionale, consentendo la geolocalizzazione, l'identificazione e l'analisi tecnologica delle nuove "Centrali", dalle quali i flussi di dati informatici illeciti venivano generati e messi a disposizione della complessiva infrastruttura criminale, che ne garantiva la diffusione agli utenti della Rete internet.

OPERAZIONE "BITGRAIL"

La complessa attività investigativa pone una pietra miliare nel settore delle indagini in materia di criptovalute. L'attività prende le mosse da una denuncia presentata dal gestore di una nota piattaforma italiana di *exchange*, relativa al furto di un'ingente somma della cryptovaluta denominata "*NANO" XRP* per un controvalore di circa 120.000.000,00 di euro, realizzato da ignoti hacker sfruttando un *bug* del protocollo *Nano* ed effettuando illecite transazioni.
L'operazione, tecnicamente senza precedenti, ha successivamente permesso di disvelare il coinvolgimento attivo nel disegno criminoso dello stesso gestore della piattaforma, sospettato autore di condotte omissive nella gestione dei protocolli di sicurezza informatica, fraudolente e distrattive nei confronti degli oltre 230 mila clienti della piattaforma. L'ideazione da parte della polizia postale di un **protocollo per il trasferimento** della criptomoneta rinvenuta nella disponibilità dell'indagato e posta sotto sequestro completa il quadro di innovatività dell'operazione in esame.

OPERAZIONE "MALA FIDES"

Quattro misure cautelari sono state eseguite sul territorio lombardo dalla Polizia Postale e delle Comunicazioni nei confronti degli autori di sedici accessi abusivi, compiuti tra aprile e luglio 2019, sul conto online di un noto Studio Commercialista milanese, da cui erano stati sottratti oltre 200.000 euro, poi riciclati attraverso operazioni speculative effettuate presso case da gioco e casinò siti in Veneto e in Liguria.

Il gruppo criminale era altresì dedito al trafugamento di assegni bancari, alle frodi mediante pubblicazione online di falsi annunci immobiliari, nonché all'organizzazione di matrimoni combinati e false adozioni, a scopo di favoreggiamento dell'immigrazione clandestina verso il nostro Paese finalizzato ad ottenere con modalità fraudolente permessi di soggiorno e concessioni della cittadinanza italiana.

OPERAZIONE "ETHEREUM"

L'operazione ha consentito di individuare il responsabile di un attacco informatico realizzato con l'utilizzo di malware di ultima generazione, il quale aveva approfittato della sua posizione lavorativa all'interno dello scalo aeroportuale di Lametia terme per sfruttare l'infrastruttura informatica della società di gestione dello scalo per "minare" - ovvero produrre - moneta virtuale, scoprendo l'esistenza di una vera e propria "MINING FARM", ovvero di una rete abusiva collegati alla rete Internet esterna attraverso i sistemi dedicati alla gestione dei servizi aeroportuali ed alimentati attraverso la fornitura di energia elettrica dell'Aeroporto. Tale architettura consentiva all'utilizzatore del sistema integrato con la rete aeroportuale, di approvvigionarsi della criptovaluta "Ethereum", prodotta senza sostenere le ingenti spese di energia elettrica necessaria per il funzionamento h24 delle apparecchiature e sfruttando la connettività fornita dagli impianti info-telematici dell'aeroporto, compromettendo la sicurezza ed esponendo i sistemi di gestione dello scalo.

OPERAZIONE NEL TRADING ONLINE

Nel settore delle truffe da falsi investimenti finanziari online, al termine di un'articolata indagine durata oltre un anno, la Polizia postale ha identificato i componenti di un sodalizio criminale dedito ai reati di abusiva attività finanziaria, truffa, riciclaggio ed estorsione, mediante una piattaforma di investimento che proponeva l'acquisto di cryptovalute, capace di sottrarre, alla sola vittima la cui denuncia ha dato corso all'attività investigativa, un danno pari ad € 380.000,00, attraverso l'esecuzione di bonifici bancari a favore di un conto corrente estero ubicato in Repubblica Ceca.

La somma è stata successivamente in buona parte recuperata, grazie al dispositivo investigativo che tuttora vede impegnate, a fianco della polizia italiana, l'Agenzia Europol e le forze di polizia cyber di altri paesi europei.

5. CYBER-TERRORISMO

Come noto, il 2020 è stato caratterizzato da eventi, sia a livello globale, sia nazionale, che hanno avuto notevoli riflessi sulle attività di prevenzione, monitoraggio ed investigative quotidianamente svolte dal personale della Polizia Postale e delle Comunicazioni e finalizzate al contrasto delle azioni eversive, del terrorismo internazionale, dei fenomeni di radicalizzazione sul web.

Ed invero, negli ultimi 12 mesi sono notevolmente incrementate rispetto all'anno precedente le segnalazioni, molte delle quali pervenute dai cittadini tramite il portale del Commissariato di P.S. Online, circa la presenza di contenuti illeciti all'interno di spazi e servizi di comunicazione online di ogni genere.
Consistenti sono stati gli sforzi dedicati al contrasto dei fenomeni di radicalizzazione jihadista, nonché volti ad arginare la propaganda del *Daesh*, che attualmente è veicolata da vari *Media Center* insistenti nelle province del Califfato che si appoggiano ai c.d. Supporter Generated Content per la diffusione dei contenuti illeciti all'interno delle varie piattaforme di comunicazione.
Nel dettaglio, tale struttura di propaganda continua a basarsi su una miriade di account, attivati quotidianamente dai supporter del Califfato (anche in forma automatizzata tramite apposite strutture dipendenti dal *Daesh* e deputate al mantenimento dell'operatività mediatica) con l'obiettivo di divulgare *magazine online* del Califfato, aggiornamenti sulle attività dei combattenti nei teatri operativi, video, documenti, manuali o pubblicazioni di esponenti di spicco della corrente radicale islamica, infografiche di minaccia etc.
L'individuazione di tale modalità operativa per la diffusione della propaganda *jhiadista* è dovuta sia a causa dell'incremento dell'azione di rimozione dei contenuti illeciti presenti sulle proprio piattaforme da parte dei maggiori fornitori di servizi Internet (tra i quali Telegram, Facebook, Google, Twitter, etc.), sia per le particolari attività di contrasto attuate dal *law enforcement*.

In questo ambito, gli investigatori della Polizia Postale e delle Comunicazioni hanno concorso con altri organi di Polizia e di intelligence alla prevenzione e al contrasto dei fenomeni di eversione e terrorismo, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica. L'attività, funzionale al contrasto del proselitismo e alla prevenzione dei fenomeni di radicalizzazione, ha permesso di sviluppare un dedicato monitoraggio di circa **36.000** spazi web e alla rimozione di diversi contenuti inneggianti alla jihad.
In particolare, nel corso del 2020 sono proseguite le attività svolte dal personale del Servizio Polizia Postale e delle Comunicazioni all'interno dei tavoli di lavoro internazionali deputati al contrasto del Cyberterrorismo, con il coordinamento di Europol e con il coinvolgimento di tutte le Forze dell'Ordine degli Stati Membri, nonché dei rappresentanti dei maggiori *Internet Service Provider*, tra i quali soprattutto *Telegram* (che è stato il fornitore di servizi online che ha ricevuto la maggior parte delle richieste di rimozione e che ha allontanato dalla propria piattaforma una parte significativa degli attori chiave all'interno della rete di diffusione della propaganda IS).
Ed ancora, in tale contesto operativo, tra le principali attività svolte nel corso del 2020 dal personale del Servizio Polizia Postale e delle Comunicazioni si evidenzia la partecipazione all'azione denominata *"RAD - Referral Action Day on instructional material online"* svoltasi il 2 luglio 2020 e promossa da Europol al fine di procedere – tramite la segnalazione ai rispettivi *Provider* interessati – alla rimozione di ogni tipo di contenuto didattico in formato digitale utilizzato per la pianificazione e realizzazione di attacchi terroristici.
L'*Action Day* ha coinvolto unità specializzate del Centro europeo antiterrorismo (ECTC) e rappresentanti di 18 Paesi, tra cui 13 Stati membri dell'U.E. e 5 Paesi extra U.E.
L'attività in argomento ha riguardato i contenuti online creati o utilizzati come materiale didattico per ispirare e commettere attacchi nel contesto del terrorismo di matrice *jihadista*, nonché dell'estremismo razziale, antagonista ed anarchico.

In particolare, appare opportuno evidenziare come i manuali fatti in casa e le guide individuate nel corso dell'operazione costituiscano il principale strumento per la realizzazione di armi devastanti, soprattutto per gli attacchi condotti da attori solitari, ovvero dai gruppi terroristici e dai loro sostenitori.
Durante l'azione, gli esperti della Sezione Cyberterrorismo hanno rilevato, valutato e segnalato i contenuti online, inclusi manuali e *tutorials* su come preparare ed attuare attacchi terroristici, come selezionare gli obiettivi, come utilizzare le armi e costruire bombe. Alcuni dei documenti individuati contenevano anche le istruzioni su come rimanere anonimi online e su come evitare di essere individuati durante la pianificazione di un attacco terroristico.
All'esito delle attività è stato segnalato per la successiva rimozione un numero complessivo di **1724** url riconducibili a **113** piattaforme web utilizzate per la propaganda jihadista e n. **182** url su **67** piattaforme web nell'ambito dei contenuti riferibili all'area dell'ultradestra ed antagonista/anarchica.
Appare evidente, dunque, come il carattere transnazionale delle operazioni di contrasto appena descritte, sia per la natura internazionale del fenomeno che per la stessa struttura della rete, comporti un'imprescindibile attivazione di strumenti di cooperazione sovranazionale che possano apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse Forze di Polizia nazionali.
Ed invero, l'analisi effettuata sulla diminuzione del corso del 2020 del numero dei siti ed account riconducibili alla propaganda jihadista ha permesso di evidenziare l'importanza delle lavoro svolto dal Servizio Polizia Postale e delle Comunicazioni, quale punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, nell'ambito degli "Action Day" promossi da Europol e che hanno determinato un massiccio "take down" di migliaia di gruppi, canali ed account che sono stati oggetto di preventiva segnalazione da parte del law enforcement, in quanto considerati responsabili della pubblicazione del settimanale di propaganda jhiadista al-Naba.
Per quanto concerne, invece, l'attività di contrasto, la Polizia Postale e delle Comunicazioni si avvale della possibilità prevista per legge di avviare attività sotto copertura, con l'impiego di profili o meglio di vere e proprie identità virtuali, costruiti ad hoc e fatti "maturare" nel tempo, gestiti da personale specializzato, con l'affiancamento dei mediatori linguistici e culturali.
Proprio l'utilizzo di tali account fittizi, nel tempo fatto "crescere" dagli investigatori nel corso delle diverse, quotidiane, attività di monitoraggio informativo e, dunque, accreditato all'interno dei canali e gruppi frequentati dagli internauti sostenitori dello Stato Islamico, ha permesso di condurre diverse, complesse, attività tecnico-investigative.
Si evidenzia, in particolare, tra gli altri, il seguente risultato investigativo:

OPERAZIONE MIRAGGIO

L'indagine è stata avviata in relazione alla segnalazione, acquisita in ambito di collaborazione internazionale, concernente la condivisione, su una piattaforma digitale di contenuti, in lingua araba, di propaganda del terrorismo di matrice jihadista. Gli approfondimenti hanno permesso di concentrare le indagini nei confronti di un soggetto italiano radicalizzato, residente a Catanzaro, titolare di numerosi account su piattaforme social (Telegram. Rocket Chat, Riot) attraverso i quali partecipava a gruppi chiusi di chiara connotazione jihadista per accedere ai quali bisognava essere accreditati e quindi ritenuti affidabili dagli amministratori dei canali.
L'analisi tecnico-informatica sui dispositivi sequestrati ha evidenziato la puntuale osservanza di regole tecniche di anonimizzazione e di archiviazione sicura del materiale informatico presenti sulle

infografiche diffuse dagli organi di propaganda del Califfato. In particolare sono stati rinvenuti manuali di istruzioni sulla realizzazione di ordigni, tutorial sulla conduzione di operazioni terroristiche, documenti esplicativi sull'auto addestramento per il compimento di attentati, nonché video ed immagini cruente di esecuzioni dell'ISIS, riviste ufficiali delle agenzie mediatiche dell'ISIS, Al Qaeda e altri gruppi terroristici, oltre a documenti in lingua araba auto-prodotti dall'indagato.
Alla luce di tali riscontri investigativi, è stato richiesto al Giudice delle Indagini Preliminari la misura cautelare personale della custodia in carcere per l'indagato, che ha trovato accoglimento con la conseguente emissione di un'ordinanza di cattura, in ordine all'ipotesi criminosa di cui agli artt. 270 *quinquies* e *sexies* c.p.

Oltre alle suindicate attività sia preventive, sia di Polizia Giudiziaria connesse al terrorismo di matrice jihadista, la Polizia Postale e delle Comunicazioni ha registrato nel corso degli ultimi anni un notevole incremento nell'ambito del settore della propaganda online legata all'estremismo razzista e xenofobo, riscontrando un trend di forum e discussioni dedicate all'argomento in costante aumento.
In particolare, anche in tale contesto il web rappresenta uno 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.
L'indottrinamento ed il reclutamento, come nel caso del radicalismo *jihadista*, avvengono sempre sulla rete, attraverso una graduale autoformazione che inizia con la visualizzazione di contenuti diffusi soprattutto nelle board "riservate", diverse dai principali social network.
La digitalizzazione delle tecnologie dell'informazione e della comunicazione ha permesso all'antisemitismo 2.0 di riprodursi in modo rapido e multimediale; contenuti contro gli ebrei si trovano sia negli spazi web antisemiti che in siti e social network generalisti, dove vengono pubblicati e condivisi commenti offensivi senza registrare l'intervento dei moderatori.
Il web 2.0, dunque, pare aver legittimato una cultura dove razzismo, intolleranza e antisemitismo sono divenuti socialmente accettabili, specie tra i giovani. La radicalizzazione verbale e l'abbassamento della soglia dei tabù si evidenzia attraverso il linguaggio, la carica di violenza, il sarcasmo razzista. In tale ambiente, la promozione delle teorie cospirative, la demonizzazione degli ebrei/sionisti e dello stato ebraico e l'uso degli ebrei/sionisti come capro espiatorio possono condurre ad una violenza reale contro gli ebrei.
Anche in tale contesto, dunque, sono stati indirizzati gli sforzi operativi del personale della Polizia Postale e delle Comunicazioni, che lo scorso 3 novembre ha preso parte all'azione operativa denominata "JAD - Joint Action Day to combat hate postings", sotto il coordinamento di Europol e la partecipazione dell'unità specializzata del Centro europeo antiterrorismo (ECTC) e rappresentanti delle polizia di diversi Paesi europei, con l'obiettivo di contrastare la pubblicazione online di messaggi d'odio connotati da aspetti xenofobi, razzisti ovvero discriminatori.
L'attività è stata condotta a livello territoriale dalle DIGOS e dai Compartimenti Polizia Postale, con il coordinamento della Direzione Centrale della Polizia di Prevenzione e del Servizio Polizia Postale e delle Comunicazioni.
Proseguendo nella descrizione delle attività svolte dalla Polizia Postale e delle Comunicazioni nell'anno in corso, appare opportuno evidenziare come la grave emergenza socio-sanitaria, tuttora

in corso, accompagnata dalle restrizioni introdotte dai decreti governativi per contrastare la diffusione del virus Covid-19, abbia determinato una rilevante attività di monitoraggio dei canali e gruppi all'interno delle varie piattaforme di comunicazione online nelle quali sono stati pubblicati numerosissimi commenti in cui emergeva la volontà di reagire alle decisioni governative attraverso vere e proprie azioni di piazza, anche violente.
Ed invero, tra le fattispecie illecite che hanno fatto registrare un considerevole incremento (come, ad esempio, accaparramento, falsificazione e sciacallaggio economico relativo ai presidi sanitari finalizzati al contenimento del contagio del COVID-19, ovvero l'intensificazione di attacchi informatici, soprattutto di tipo *ransomware*, nei confronti delle infrastrutture critiche ed, in particolare, delle strutture sanitarie pubbliche e private) è stata riscontrata da questa Specialità l'aumento dei seguenti fenomeni della rete:

- diffusione di fake news (notizie destituite di fondamento relative a fatti od argomenti di pubblico interesse, elaborate al solo fine di condizionare l'opinione pubblica, orientandone tendenziosamente il pensiero e le scelte) con le quali vengono prospettati rimedi fraudolenti per il contenimento del contagio, nonché vere e proprie "teorie del complotto" volte a destabilizzare l'ordine democratico ed indirizzare i sentimenti di rabbia nei confronti di determinate "categorie sociali";

- creazione di discussioni all'interno di piattaforme di comunicazione online nell'ambito delle quali si cercano strategie di protesta e contrasto, anche violento, alle disposizioni in materia di contenimento dell'emergenza Covid.

Appare evidente, inoltre, come i problemi economici e sanitari causati dall'emergenza coronavirus siano stati strumentalizzati da numerosi esponenti di vari movimenti non precisamente collocabili politicamente, per alimentare la disinformazione ed organizzare l'imminente "chiamata alle armi per reagire al caos globale" attraverso azioni di violenza eversiva.
In tale contesto, dunque, la Polizia Postale effettua una costante attività di monitoraggio, finalizzata alla più efficace forma di prevenzione e contrasto.

6. COMMISSARIATO DI PS ONLINE

Il portale del Commissariato di P.S. online è divenuto il punto di riferimento specializzato per chi cerca informazioni, consigli, suggerimenti di carattere generale, o vuole scaricare modulistica e fare segnalazioni.

PERIODO	NR. VISITE	ACCESSI
TOTALE 2019	1.014.446	28.580.287
TOTALE 2020	3.191.633	65.094.386
INCREMENTO %	+ 214,6 %	+ 127,7 %

Uno strumento agevole che consente al cittadino, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, di entrare nel portale ed usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente ed ininterrottamente offre agli utenti del web.
Di particolare importanza le segnalazioni giunte anche sul sito del Commissariato di P.S. on-line per i reati di cyberbullismo, perpetrati da studenti nei confronti di compagni di scuola e non, attraverso i social media, con atti denigratori e diffamatori. Alcune attività sono sfociate nell'emissione da parte dei Questori di provvedimenti di ammonimento anche al fine di responsabilizzare minori autori del reato.

ATTIVITÀ DEL COMMISSARIATO DI PS ONLINE

PERIODO	SEGNALAZIONI	INFORMAZIONI	DENUNCE
2019	23311	20923	10571
2020	55792	25743	11977
INCREMENTO %	**+ 139.3%**	**+ 23.0 %**	**+ 13,3 %**

FAKE NEWS

Nell'ambito del diversificato contesto operativo della Polizia Postale e delle Comunicazioni, particolare attenzione viene costantemente rivolta anche al fenomeno della "disinformazione", con un impegno ancor maggiore nel contesto emergenziale vissuto a causa della diffusione del virus Sars-Cov2: la crescente proliferazione delle cd. fake news, sovente caratterizzata da un potenziale impatto negativo sulla salute pubblica e sulla corretta ed efficace comunicazione istituzionale ha imposto di innalzare i livelli di attenzione nell'ottica di un efficace contenimento del particolare fenomeno.

L'azione di contrasto attuata, rispetto alle varie fenomenologie delittuose che hanno caratterizzato la fase dell'emergenza Covid-19 (talora agevolate dalla diffusione di fale notizie e/o informazioni), è stata, quindi, realizzata non soltanto sotto il profilo della repressione dei reati tentati o consumati, ma anche nell'ottica di interventi di tipo preventivo, tesi a veicolare alla cittadinanza le informazioni utili per contenere ed impedire le condotte delittuose sopra richiamate.

In tale direzione, il potenziamento dell'operatività del Commissariato di PS online ha permesso di innalzare i livelli di interazione con i cittadini, i quali, in una situazione di emergenza sanitaria, hanno mostrato un accresciuto bisogno di strumenti idonei a garantire rapidi ed efficaci riferimenti istituzionali a cui poter indirizzare le proprie segnalazioni e le proprie preoccupazioni e da cui poter apprendere informazioni corrette, utili anche a prevenire il consumarsi di condotte delittuose.

Al riguardo, dall'inizio dell'emergenza COVID-19, sono stati individuati 136 eventi, riconducibili al fenomeno della disinformazione, rispetto ai quali è stato predisposto uno specifico alert funzionale alla veicolazione delle corrette informazioni.

PERIODO	SEGNALAZIONI FAKE NEWS	ALERT DIRAMATI
TOTALE 2019	21	29
TOTALE 2020	134	136
INCREMENTO PERCENTUALE RISPETTO ALLO STESSO PERIODO DELL'ANNO PRECEDENTE	**+ 436,0%**	**+ 353,3 %**

ATTIVITA' DI PREVENZIONE

Parallelamente all'incremento dell'uso di strumenti telematici, sono cresciute le aspettative di sicurezza da parte del cittadino. La Polizia Postale e delle Comunicazioni è impegnata, ormai da diversi anni, in campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet, rivolte soprattutto alle giovani generazioni.

Nello specifico si evidenzia la campagna educativa itinerante della Polizia Postale e delle Comunicazioni "***Una Vita da Social***", grazie alla quale sino ad oggi sono stati incontrati oltre **2milioni e mezzo di studenti sia nelle piazze che nelle scuole**, **220.000 genitori, 125.000 insegnanti** per un totale di **18.500 Istituti scolastici** e **350** città raggiunte sul territorio nazionale.

Un progetto dinamico, innovativo e decisamente al passo con i tempi, che si avvicina alle nuove generazioni evidenziando sia le opportunità del web che i rischi di cadere nelle tante trappole dei predatori della rete, confezionando un vero e proprio "manuale d'uso", finalizzato ad evitare il dilagante fenomeno del cyberbullismo e tutte quelle forme di uso distorto della rete in generale e dei social network.

A disposizione degli utenti è presente la pagina **facebook e twitter** di "Una vita da social", gestita direttamente dalla Polizia Postale e delle Comunicazioni, dove vengono pubblicati gli appuntamenti, le attività, i contributi e dove i giovani internauti possono "*postare*" direttamente le loro impressioni ad ogni appuntamento.

Nel corso del **lockdown** l'attività di sensibilizzazione e prevenzione nelle scuole è proseguita attraverso piattaforme di video conferenze.

ATTIVITA DI FORMAZIONE, INNOVAZIONE E RICERCA NEL SETTORE DELLE TECNOLOGIE ICT

Anche nell'anno 2020, la Polizia Postale e delle Comunicazioni, ha avviato una serie di collaborazioni con Istituzioni Scientifiche ed Enti di Ricerca volti ad individuare nuove metodologie di lavoro in ambito info-investigativo anche attraverso la pianificazione di percorsi formativi specialistici con "focus" su varie tecnologie emergenti (5G, blockchain, IoT, AI).

In particolare, sono stati avviate collaborazioni con il mondo accademico che hanno permesso lo svolgimento di vari "lectures" sui temi della sicurezza informatica e della digital forensics. Anche per quanto riguarda la tecnologia blockchain è stato intensificato il lavoro di studio e ricerca di nuove soluzioni finalizzate al tracciamento delle transazioni in criptovalute, utilizzate per fini criminali (frodi informatiche, estorsioni, compravendita di materiale illegale nel darkweb,

riciclaggio). Sono state oggetto di approfondimento anche nuove tematiche con particolare riferimento al mondo dell'Intelligenza Artificiale e dell'Internet delle Cose.

COMPARTIMENTO POLIZIA COMUNICAZIONI PER LA CAMPANIA

Nell'ambito delle attività svolte a livello nazionale, il Compartimento Polizia delle Comunicazioni per la Campania ha conseguito ottimi risultati con riferimento alla prevenzione e alla repressione dei reati online, arrestando 10 persone, denunciandone 623 in stato di libertà ed eseguendo 213 perquisizioni. Di seguito si riportano le operazioni più rilevanti.

OPERAZIONE FUJINAMA

Il Compartimento Polizia Postale per la Campania, coordinati dalla Procura della Repubblica presso il Tribunale di Napoli, hanno eseguito due misure restrittive, della custodia cautelare in carcere e degli arresti domiciliari, emessi dal GIP del capoluogo campano rispettivamente nei confronti di un ex dipendente e di un dirigente della società Leonardo S.p.A., all'esito di complesse attività d'indagine volte a definire i contorni di un attacco informatico allo stabilimento di Pomigliano D'Arco, sede della Divisione Aerostrutture e della Divisione Velivoli e quindi alla rete informatica dell'ex Finmeccanica.

Nel 2017, la struttura di cyber security aziendale della Leonardo, società internazionale che si occupa di progettazione, sviluppo, produzione, assistenza ai clienti e marketing nei settori elettronica, elicotteri, velivoli, aerostrutture e sicurezza informatica ha rilevato e segnalato un traffico di rete anomalo, in uscita da alcune postazioni di lavoro dello stabilimento di Pomigliano D'Arco, generate da un software artefatto denominato "cftmon.exe", sconosciuto ai sistemi antivirus.

Il traffico anomalo risultava diretto verso la pagina web "www.fujinama.altervista.org".

La prime analisi, effettuate internamente dalla struttura aziendale deputata alla gestione degli incidenti informatici, avevano permesso di circoscrivere l'anomalia a 16 postazioni installate nel perimetro aziendale di Pomigliano D'Arco ed evidenziato una possibile, limitata fuoriuscita di dati, non ritenuta significativa.

La Procura di Napoli e la Polizia delle Comunicazioni, all'esito di approfonditi accertamenti tecnici, cui sono seguite a riscontro complesse attività di polizia giudiziaria, hanno ricostruito uno scenario ben più esteso e severo rispetto a quanto originariamente rilevato.

Le indagini informatiche hanno evidenziato come tra maggio 2015 e gennaio 2017 la società Leonardo S.p.A. sia stata colpita da quella che in letteratura viene definito con la sigla APT (Advanced Persistent Threat), ossia un attacco mirato e persistente con installazione nei sistemi, nelle reti e nelle macchine bersaglio, di codice malevolo, per la creazione ed il mantenimento di attivi canali di comunicazione che, all'insaputa dell'azienda attaccata, hanno consentito l'esfiltrazione silente di "informazioni ritenute di valore".

Autore dell'azione un intraneo, ovvero un dipendente esperto informatico addetto proprio alla gestione della sicurezza di Leonardo, che tra l'altro aveva in prima battuta affiancato gli investigatori della Postale nel corso delle iniziali attività d'indagine, di fatto cercando di sabotarle.

Solo all'esito di complesse attività di analisi informatica, si è riusciti a ricostruire come il software malevolo, un vero e proprio *trojan* di nuova ingegnerizzazione, fosse stato inoculato da A.D. responsabile della gestione delle postazioni di lavoro presso l'Alenia di Pomigliano, mediante l'inserimento di chiavette USB nei PC spiati.

Grazie al software malevolo, programmato in linguaggio Visual Basic, lo stabilimento di Pomigliano D'Arco era di fatto nel pieno controllo dell'attaccante, che, grazie alle proprie mansioni interne nel tempo aveva installato più versioni evolutive del malware, con capacità ed effetti sempre più invasivi e penetranti.
Attraverso una utility di Linux, il malware "cftmon.exe" è stato inserito tra i file di sistema di Windows, con la caratteristica di avviarsi automaticamente ad ogni esecuzione del Sistema Operativo.
La denominazione "cftmon.exe" non è casuale: la scelta è stata effettuata per raggirare amministratori e utenti della rete locale, mediante una tecnica di spoofing del nome attraverso la semplice inversione delle consonanti: difatti, tra i file di sistema di Windows è presente l'eseguibile "ctfmon.exe", utilizzato, tra l'altro, per l'immissione di dati e di informazioni mediante un dispositivi diverso dalla tastiera standard (ad esempio, voce, tastiera a video o penna digitale).
Dopo l'inoculazione del malware, dotato delle caratteristiche dei comuni trojan, l'hacker ha quindi potuto intercettare quanto digitato sulla tastiera (keylogging) e catturare i fotogrammi di ciò che era stato visualizzato sullo schermo (screen capturing) delle postazioni di lavoro compromesse.
I dati illecitamente carpiti venivano poi inviati (data exfiltration), a intervalli regolari di circa un minuto, verso un Centro di Comando e Controllo (C&C), ossia il sito web nella disponibilità dell'attaccante, "www.fujinama.altervista.org".
Per il trasferimento dei dati verso il C&C, l'hacker aveva aggirato i limiti imposti dalle policy di sicurezza della Leonardo, utilizzando una specifica porta di connessione (TCP 80) comunemente utilizzata per la visualizzazione delle pagine web, per mezzo dei più diffusi browser Internet (Internet Explorer, Google Chrome, Mozilla Firefox).
Le indagini hanno permesso infine di ricostruire l'attività di antiforensics dell'attaccante, che collegandosi al C&C dopo aver scaricato i dati carpiti, cancellava da remoto sul sito web "fujinama" le informazioni acquisite eliminando le tracce del malware sulle macchine compromesse.
L'attacco informatico ricostruito dalla Polizia delle Comunicazioni è stato classificato come estremamente grave, in quanto la superficie dell'attacco ha interessato ben 94 postazioni di lavoro, un numero ben più ampio rispetto alle 16 inizialmente individuate.
Dei PC infetti, 33 erano collocati presso lo stabilimento di Pomigliano D'Arco e su di essi erano configurati molteplici profili utente in uso a dipendenti impiegati, anche con mansioni dirigenziali, in un'attività d'impresa volta alla produzione di beni e servizi di carattere strategico per la sicurezza e la difesa del Paese.
La gravità dell'incidente emerge anche dalla tipologia delle informazioni sottratte, tenuto conto che dalle 33 macchine bersaglio di Leonardo risulterebbero esfiltrati 10 Giga di dati, pari a circa 100.000 files, afferenti alla gestione amministrativo/contabile, all'impiego delle risorse umane, all'approvvigionamento e alla distribuzione dei beni strumentali, nonché alla progettazione di componenti di aeromobili civili e di velivoli militari destinati al mercato interno e internazionale. Accanto ai dati aziendali, sono state oggetto di captazione anche le credenziali di accesso ed altre informazioni personali dei dipendenti della Leonardo.
Oltre ai PC presenti presso gli stabilimenti di Pomigliano della ex Finmeccanica, sono state infettate 13 postazioni di una società del gruppo Alcatel, alle quali se ne sono aggiunte altre 48, in uso a soggetti privati nonché ad aziende operanti nel settore delle produzione aerospaziale.
L'autore dell'attacco, sottoposto alla custodia cautelare in carcere, è un trentottenne di Eboli, attualmente responsabile della sicurezza informatica presso la sede di Napoli della società Accenture. L'indagato ha lavorato nel gruppo Finmeccanica/Leonardo tra il 2011 e il 2018, prima

presso la società Alenia a Pomigliano D'Arco, poi presso il C.E.R.T. di Roma e da ultimo quale addetto alla sicurezza informatica dello stabilimento di Pomigliano d'Arco.
L'hacker ebolitano è in possesso di elevate competenze informatiche, con un'approfondita conoscenza dei linguaggi di programmazione in ambienti Linux e dei software di computer forensics.
Tali capacità gli consentirono nel 2007 di realizzare un accesso abusivo al sistema informatico della base militare statunitense in Oklahoma, acquisendo la disponibilità di due account, per poi condividere in rete sia dati esfiltrati, con tanto di spiegazione delle tecniche utilizzate per carpirli.
La Procura di Napoli e la Polizia delle Comunicazioni sono risalite all'identità dell'hacker attraverso un'approfondita analisi del linguaggio di programmazione del malware "cftmon.exe", nonché mediante l'interpretazione del codice sorgente (html) delle pagine web del sito "fujinama.altervista.org".
Attraverso la lettura dei file di connessione al pannello di gestione del sito "fujinama", gli investigatori hanno infine accertato l'identità dell'hacker, amministratore dello spazio web per la raccolta dei dati esfiltrati.
Accanto agli accertamenti di natura informatica, sono state fondamentali le attività di indagine più tradizionali, che hanno permesso di ricostruire il percorso di formazione cybercriminale dell'indagato, la sua carriera professionale nel gruppo Leonardo e la cerchia di soggetti a lui più vicini, dai quali sono stati appresi elementi utili a delineare meglio le abitudini e la personalità dell'hacker.
Ulteriori approfondimenti compiuti dalla Procura di Napoli e dalla Polizia delle Comunicazioni hanno fatto emergere una condotta di depistaggio da parte del responsabile del C.E.R.T. di Leonardo, organo deputato alla gestione degli attacchi informatici subiti dall'azienda. In particolare, il dirigente della società, sottoposto agli arresti domiciliari, avrebbe inquinato il generale quadro probatorio, fornendo ai vertici aziendali, alle istituzioni pubbliche preposte alla protezione delle infrastrutture critiche, nonché all'Autorità Giudiziaria, una rappresentazione falsa e incompleta dell'incidente informatico, con particolare riferimento all'oggetto dell'attacco, alla sua estensione e quindi alla quantità ed alla tipologia del materiale esfiltrato. Il responsabile del C.E.R.T. di Leonardo, inoltre, ha omesso di svolgere accertamenti preliminari fondamentali per la gestione di incidenti informatici, il cui compimento avrebbe consentito una più celere risposta sia in termini investigativi che di remediation.

OPERAZIONE SWIMMING POOL

La Sezione di Salerno ha tratto in arresto un quarantasettenne di Salerno, con precedenti specifici, resosi responsabile di produzione e detenzione di materiale pedopornografico.
L'interessato è stato trovato in possesso di un'ingente quantità di materiale di natura pedopornografica rinvenuto a seguito di perquisizione informatica eseguita sui numerosi dispositivi a lui in uso.
L'attività di indagine, coordinata dalla Procura della Repubblica presso il Tribunale di Salerno, è frutto di un'intensa e proficua cooperazione internazionale tra il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) del Servizio Polizia Postale e delle Comunicazioni di Roma, Europol e la Polizia statunitense.
Tale sinergica collaborazione ha consentito di raccogliere e condividere il materiale probatorio relativo alle condotte dell'indagato perpetrate anche attraverso contatti altri soggetti coinvolti, anche esteri.

L’indagato, per abbassare le difese delle piccole vittime al fine di indurle a inviargli materiale pedopornografico autoprodotto, si presentava sui social con un’identità femminile e riusciva inoltre ad acquisire e scambiare con altri internauti le foto e i video pornografici prodotti utilizzando i minori.
Già nel 2016, una prima attività d’indagine internazionale della National Crime Agency britannica conduceva a individuare l’odierno indagato quale fruitore di un sito abitualmente dedito allo scambio di video e fotografie ritraenti minori in atteggiamenti sessuali.
Le indagini della Procura di Salerno, svolte, anche all'epoca, dal Compartimento Polizia Postale e delle Comunicazioni Campania e dalla dipendente Sezione di Salerno, con il coordinamento del CNCPO di Roma, consentirono di trarlo in arresto per gli stessi reati.
Il materiale probatorio acquisito ed analizzato consentì di individuare condotte criminose perpetrate da internauti esteri.
La condivisione dei dati di indagine risultò determinante per aprire nuovi scenari investigativi. In particolare, grazie a tali contributi, gli investigatori statunitensi furono in grado di risalire a un cittadino statunitense che abusava sessualmente dei propri figli, per poi condividere le relative immagini.
Le condotte criminose così ravvicinate testimoniano il compulsivo bisogno dell'indagato di acquisire materiale pedopornografico. La pericolosità del soggetto risulta evidente anche da ulteriori accertamenti che hanno dimostrato che l’indagato ha anche provato ad accreditarsi presso strutture dedite all'intrattenimento e alla cura dei minori.

OPERAZIONE BLACK
La Sezione di Salerno, coordinata dal Compartimento di Napoli e dal Servizio Polizia Postale e delle Comunicazioni, ha tratto in arresto un cinquantacinquenne della provincia di Salerno resosi responsabile di divulgazione e detenzione di materiale pedopornografico.
L’interessato è stato trovato in possesso di un’ingente quantità di materiale di natura pedopornografica rinvenuta a seguito di perquisizione informatica, eseguita sui numerosi dispositivi a lui in uso.
L’attività di indagine, diretta dalla Procura della Repubblica presso il Tribunale di Salerno, è frutto di un'intensa e proficua cooperazione internazionale tra il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) del Servizio Polizia Postale e delle Comunicazioni di Roma e le Polizie di Paesi esteri.
Tale sinergica collaborazione ha consentito di raccogliere e condividere il materiale probatorio relativo alle condotte dell'indagato perpetrate attraverso contatti con altri soggetti coinvolti, anche stranieri.
L'uomo, noto personaggio della rete internet, con migliaia di followers sui propri profili social, amato soprattutto dai giovanissimi, grazie anche a comparsate in televisione, utilizzando falsi account partecipava ad una rete internazionale dedita allo scambio di materiale pedopornografico, tra cui video di violenze raccapriccianti su neonati.