****

**Resoconto attività 2020**

**Polizia Postale e delle Comunicazioni**

L’anno 2020 è stato caratterizzato da mutamenti profondi delle nostre abitudini di vita. In modo repentino, quasi tutte le nostre attività (lavoro – scuola – tempo libero – formazione – cultura – relazioni) hanno conosciuto una rimodulazione basata in larga parte sull’utilizzo della rete, con un allargamento della platea degli utenti anche a soggetti normalmente poco adusi alle nuove tecnologie, fattore il quale, se da un lato ha accelerato un processo di modernizzazione certamente già *in nuce*, ha del pari determinato una accresciuta esposizione alle aggressioni della cyber-criminalità.

In questo scenario, l’impegno della Polizia Postale e delle Comunicazioni si è indirizzato verso la prevenzione ed il contrasto di un insieme assai vasto ed eterogeneo di attacchi informatici, diretti a colpire il patrimonio personale dei cittadini come l’integrità del tessuto economico-produttivo del Paese, la regolarità dei servizi pubblici essenziali come il mondo delle professioni, la sicurezza e la libertà personale di adulti e ragazzi con particolare riferimento alla protezione dei bambini e delle persone più vulnerabili.

L’attività operativa del Compartimento Polizia Postale e delle Comunicazioni Piemonte e Valle D’Aosta in particolare si è concentrata su oltre **1300 casi** nelle diverse materie specialistiche trattate, giungendo per l’anno 2020 ad un totale di **224 indagati**.

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** edell’**adescamento di minori online**, per i quali sono statieseguiti 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.

14 le 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, condotte principalmente in modalità sotto copertura online anche nelle ***Dark Net.***

**Tra queste si segnala l’operazione *“50 COMMUNITY”* condotta dalla Polizia Postale di Torino nei confronti di 50 indagati ed inerente la diffusione e, in alcuni casi, produzione di materiale di pornografia minorile; 4 gli arresti in flagranza effettuati per possesso di ingente quantità di materiale pedopornografico. L’operazione, coordinata dal C.N.C.P.O., ha coinvolto tutto il territorio nazionale ed ha impegnato nelle operazioni di perquisizione 15 Compartimenti e 24 Sezioni della Polizia Postale.**

**L’attività 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.; si è proceduto al sequestro di oltre 100 reperti e decine di *terabyte* di materiale pedo-pornografico conservato anche su spazi di archiviazione *cloud*.**

Di estremo rilievo inoltre l’operazione **OPERAZIONE *“LUNA PARK”*** sviluppatasi in due anni di indagini “*sotto copertura”* nel web durante le quali la Polizia Postale di Milano, coordinata dal C.N.C.P.O., 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.

**Nell’ambito di tale operazione 5 sono state le perquisizioni svolte dal Compartimento del Piemonte e Valle d’Aosta ed a carico di uno dei perquisiti, nel territorio valdostano, è scattato l’arresto per detenzione di ingente quantitativo di materiale pedopornografico.**

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 % |

Per quanto attiene l’attività operativa svolta dal Compartimento Polizia Postale e delle Comunicazioni del Piemonte e Valle D’Aosta, si evidenziano per l’anno concluso **71** indagati nel settore della pedopornografia; tra questi, **6** per lo specifico reato di adescamento realizzato online attraverso social network o piattaforme di istant messaging, **62** per detenzione e **3** per diffusione di materiale pedopornografico.

1. **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. 500 le denunce formulate presso il Compartimento di Torino, tra queste prevalgono le truffe di e-commerce, circa 418; 12 le denunce presentate invece per truffe di natura sentimentale.**

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**”.

**Il Compartimento di Torino ha ricevuto in materia 53 denunce per un danno di circa 2 mln di euro. A seguito delle stesse sono state aperte diverse indagini con proiezione internazionale che hanno fatto emergere l’esistenza di strutture complesse dedite al riciclaggio tramite piattaforme di trading fraudolente; le stesse vengono puntualmente segnalate per l’oscuramento preventivo alla Consob, autorità di vigilanza in materia.**

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; **14 i casi di sextortion sul territorio Torinese.**

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; per quanto attiene la nuova fattispecie di “revenge porn” **due sono stati i casi denunciati presso il Compartimento di Torino.**

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; **circa 100** **i casi nelle regioni Piemonte e Valle d’Aosta.**

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 |

1. **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.

**Sul territorio Piemontese sono stati denunciati 286 casi di reati riconducibili a tecniche di hacking; tra questi 181 denunce per accesso abusivo, 20 per inoculazione di malware e 85 per sostituzione di persona/furto di identità digitale.**

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.

1. **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, spesso collegati al riciclaggio, ha permesso di identificare ed indagare 3741 persone a fronte dei 3473 denunciati nello stesso periodo dell’anno precedente.

 **7 arresti e 32 gli indagati dal Compartimento di Torino .**

Di seguito le operazioni di Polizia Giudiziaria più significative:

1. **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** urlriconducibili 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.

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.

**Molte le piattaforme monitorate con continuità dal Compartimento di Torino, con oltre 200 segnalazioni preventive relative a gruppi, pagine, profili di social network meritevoli di approfondimento operativo.**

1. **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.