COMMISSIONE PARLAMENTARE DI INCHIESTA SUI FENOMENI DELLA CONTRAFFAZIONE, DELLA PIRATERIA IN CAMPO COMMERCIALE E DEL COMMERCIO ABUSIVO

RESOCONTO STENOGRAFICO

72.

SEDUTA DI GIOVEDÌ 9 MARZO 2017

PRESIDENZA DEL PRESIDENTE **MARIO CATANIA**

INDICE

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE MARIO CATANIA

La seduta comincia alle 14.15.

(La Commissione approva il processo verbale della seduta precedente).

Audizione di Ufficiali del Comando Unità Speciali della Guardia di Finanza.

PRESIDENTE. L'ordine del giorno reca l'audizione di Ufficiali del Comando Unità Speciali della Guardia di Finanza in materia di contrasto della contraffazione nel settore del *dark web*. Come è noto il cosiddetto *dark web* (o « rete oscura ») costituisce una parte del *Deep Web* (o rete sommersa o invisibile), ossia quella parte del *World Wide Web* non indicizzata dai comuni motori di ricerca ma raggiungibile attraverso *software* particolari che collegano *Internet* e la « *Darknet* ». *Il dark web* è spesso utilizzato per attività illegali, sia nel settore della contraffazione, sia ad esempio in settori quali il contrabbando o lo smercio di stupefacenti.

Abbiamo pertanto chiesto alla Guardia di Finanza – che desidero espressamente ringraziare per la costante e preziosa assistenza che assicura ai lavori della Commissione – la disponibilità ad illustrare, con una presentazione pratica, i contorni di tale fenomeno, trattandosi di un tema che richiede un approfondimento tecnico, anche in rapporto all'esame di una proposta di relazione sul tema « Contraffazione sul web », attualmente in discussione.

Sono presenti il Generale Gennaro Vecchione, Comandante delle Unità Speciali della Guardia di Finanza, accompagnato dal Colonnello Giovanni Parascandolo, Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza.

Do la parola quindi al Generale Vecchione per lo svolgimento della sua relazione con la correlata dimostrazione pratica.

GENNARO VECCHIONE, *Comandante Unità Speciali della Guardia di Finanza*. Signor presidente, desidero innanzitutto porgere il mio ringraziamento, oltre a quello del Comandante generale e del comandante dei Reparti speciali, per questa ulteriore occasione offerta alla Guardia di Finanza di esporre la propria testimonianza e il proprio punto di vista in merito a talune tematiche di grande attualità e particolare interesse operativo, quali quelle riconducibili al mondo cibernetico e più specificamente al cosiddetto *deep web*.

Sono il generale Gennaro Vecchione, Comandante delle Unità Speciali, vale a dire il reparto deputato prioritariamente alla collaborazione con autorità ed organismi indipendenti tra cui le Commissioni parlamentari d'inchiesta, dal quale dipendono i Nuclei Speciali, che sono anche interessati a vario titolo nell'azione di contrasto ai fenomeni illeciti che interessano il *cyber space*.

È con me il Colonnello Giovanni Parascandolo, Comandante del Nucleo Speciale Frodi Tecnologiche, a cui è affidato il compito del monitoraggio e contrasto degli illeciti economico-finanziari commessi sulla rete, ivi compresi contraffazione e pirateria, oltre a fornire il supporto tecnico-specialistico a tutte le componenti operative del Corpo nello sviluppo di investigazioni caratterizzate dall'uso di tecnologie.

In linea di continuità con i contenuti della mia precedente audizione, tenuta innanzi a codesta Commissione a febbraio 2016, e di quella del Comandante generale

a settembre 2016, fornirò ulteriori elementi informativi circa l'impegno istituzionale profuso dalle Unità Speciali a presidio di questo particolare settore operativo, partendo da una necessaria analisi di contesto, che ci permetterà di entrare più nel vivo nella materia.

A tal riguardo l'analisi di contesto che in parte è già nota a questa Commissione è nel documento che lascio agli atti, quindi ometto di indicarla.

Entrando direttamente sulla tematica di interesse, il *deep web* è un insieme di siti internet, pagine e contenuti *web*, che, non essendo indicizzati, non possono essere raggiunti dagli utenti attraverso i comuni motori di ricerca (Google, Bing). Solo conoscendo il *link* esatto o disponendo eventualmente di *username* e *password* in un certo modo di accesso potremmo avere campo libero alla navigazione di certi contenuti. Questo è un aspetto fondamentale per il tema che ci riguarda e per il settore della contraffazione.

Ci riferiamo anche a *paper* accademici e scientifici, però teniamo a sottolineare che il cosiddetto *deep web* non significa che abbia necessariamente contenuti illeciti, anzi.

Nello specifico, il traffico del *deep web* è formato essenzialmente da bit che veicolano tra l'altro interrogazioni *database*, operazioni di iscrizione e *login* e in generale transazioni protette da *password*, pagine accessibili solo mediante l'attivazione di servizi a pagamento, pagine non linkate da nessun'altra pagina del *web*, tecnologie come quelle CAPTCHA, che vengono utilizzate per impedire l'accesso a risorse *web* da parte di sistemi automatizzati.

Si tratta di una quantità tale di dati e informazioni da rappresentare la quasi totalità dell'intero mondo internet, anzi dai dati offerti da riviste specializzate si parla di circa 400 miliardi di documenti complessivi presenti nel *deep web*, a fronte di poco più di 3,9-4 miliardi di pagine *web* indicizzate dal motore di ricerca Google, quindi, la maggior parte dei contenuti del *web*, sebbene sembri strano, è contenuta nel *deep web*.

L'immagine offerta nella relazione che consegno dà l'idea di quello che è il *web* di superficie, che è il 10 per cento di internet, il *deep web* che rappresenta il 90 per cento, e nell'ambito di questa escrescenza di ghiaccio che viene rappresentata in questa figura c'è il *dark web*, che ha appunto servizi nascosti e il *web* cosiddetto *darknet*. Nel substrato più profondo del *deep web* troviamo quindi il *dark web* o più correttamente il *darknet*, perché come vedremo è un collegamento di nodi.

Darknet, definizione. Volendo entrare più nel dettaglio, si tratta di un insieme di reti e tecnologie che utilizzano applicazioni e protocolli di comunicazione già esistenti (http, FTP), usati per la condivisione di contenuti digitali, che non sono separati fisicamente da internet, ma resi intenzionalmente invisibili e non accessibili dai comuni *browser*, per essere poi raggiungibili solo da *software* progettati per instaurare comunicazioni assolutamente anonime.

È quindi di tutta evidenza che i termini *deep web* e *dark web*, sebbene spesso usati come sinonimi, non possono essere considerati tali, essendo il secondo, *dark web*, un sottoinsieme del primo, *deep web*, con proprie specifiche caratteristiche che ne fanno un mondo a sé stante.

Volendo sintetizzare quanto fin qui illustrato potremmo dire di ricondurre le risorse *web* a tre macro insiemi: accessibili e indicizzate, quindi *clear* o *surface web*, accessibili e non indicizzate, *deep web*, nascoste non indicizzate, *dark web* o *darknet*.

È proprio in questa porzione di mondo virtuale nascosto o *dark* che possono annidarsi pericolose organizzazioni criminali, gruppi di *hacker*, cellule antagoniste o addirittura soggetti legati a frange terroristiche. Qui come nel *clear web* è possibile trovare una rete di *marketplace*, dove apparentemente si può comprare di tutto (droga, armi, materiale pedopornografico, documenti di identità, numeri di carte di credito che vengono venduti ovviamente previa clonazione, *mail list*, prodotti contraffatti o piratati e tanto altro ancora).

È possibile inoltre acquistare o affittare veri e propri servizi su misura per compiere attività di hackeraggio, quindi anche l'acquisto di *malware*, di *software* malevoli,

oppure di *phishing* o per compiere azioni dimostrative contro istituzioni pubbliche o aziende private.

Alcuni esempi delle inserzioni che è possibile trovare (li vedremo nell'ambito della dimostrazione con il video del colonnello Parascandolo): una pistola Beretta a 900 euro, una mitraglietta di fabbricazione russa a 2.000, pacchetto contenente informazioni personali di un utente a un dollaro, *account paypal* a partire da 300 dollari, *account* per *on line banking* a prezzi compresi tra 200 e 500 dollari.

Nel *marketplace* maggiormente in ordine al *dark web* le compravendite sono garantite (questa è la parte più preoccupante) da un sistema di *feedback*, cioè di effettività, quindi quando vediamo 5 armi vendute sono 5 armi effettivamente vendute perché c'è il *feedback* degli utenti molto efficace, basato sulla credibilità del venditore e sui quantitativi di prodotti ceduti.

Inoltre le modalità di pagamento, che sono assistite da un servizio di *Escrow*, ovvero un accordo secondo il quale la somma relativa al pagamento di un bene/servizio acquistato prima di essere accreditata sul conto del venditore viene trattenuta da una terza parte, che quindi fa da garante, fino al momento in cui l'acquirente conferma l'avvenuta consegna della merce, quindi ci sono sistemi di garanzia che dimostrano che le transazioni non sono soltanto truffaldine, ma anche effettive. Desideriamo però richiamare l'attenzione della Commissione sul fatto che molte di queste inserzioni sono riconducibili a tentativi di truffa o di sottrarre dati e informazioni sensibili dell'utente.

Un aspetto fondamentale è quello della Rete TOR, perché uno dei principali sistemi per accedere ai contenuti rinvenibili all'interno della *darknet* è sicuramente questo TOR, che è un acronimo, The Onion Router, cioè un conduttore, un instradatore cipolla, perché è a strati, come l'efficace ortaggio individuato come emblema.

Tale sistema di comunicazione anonima è basato sulla seconda generazione del protocollo di rete *Onion routing*, è nato nel 1995 come internet per esigenze della difesa americana, per garantire le comunicazioni durante attacchi nucleari o elettromagnetici che avrebbero collassato le comunicazioni operative. Poi è stato sviluppato e sostenuto da soggetti anche privati. Ovviamente entro nel dettaglio su alcuni aspetti, però lascio il testo completo.

La peculiarità principale della tecnologia fornita dal TOR è la sicurezza dell'anonimato. Questo è l'aspetto più inquietante per le forze di polizia, perché rende difficile l'individuazione rispetto all'attività normalmente svolta nel tempo di oscuramento dei siti. L'IP di connessione che viene assunto è infatti quello che è stato associato temporaneamente al *software* in parola e non quello che l'*internet service provider* ossia il gestore telefonico che fornisce la connessione ha assegnato alla macchina collegata alla rete internet.

Di contro, tutta l'architettura non poteva non presentare un tallone d'Achille derivante dalla velocità di connessione, perché diventa molto lenta in quanto per garantire la sicurezza la navigazione dell'utente deve avvenire per salti, passando da tutti i nodi del sistema.

Il funzionamento del *software* in parola non è lo stesso della rete tradizionale. La comunicazione tra *client* e *server* non è diretta, ma, come indicato, viene rimbalzata attraverso altri *server* denominati *relay* messi a disposizione dai volontari che, fungendo da *router*, da instradatori, rendono molto difficile poter intercettare l'origine, la destinazione e il contenuto dei messaggi e dei dati trasferiti.

Una volta avviato il *software* TOR ed avuto accesso al circuito, è possibile navigare sia nel *web* di superficie sia nel *deep web*. In quest'ultimo caso, vista l'inefficacia dei motori di ricerca, si deve necessariamente fare affidamento a liste compilate di indirizzi (*link*) proprio perché – ribadisco – non c'è un'indicizzazione dei motori di ricerca, ma è un'individuazione, un collegamento, un *link* a soggetti, a *link* già individuati, a indirizzi già noti.

A complicare ancora di più la situazione sono le continue mutazioni degli indirizzi delle pagine presenti dell'*Uniform Resource Locator* (URL), che per ragioni di riserva-

tezza vengono molto spesso resi inaccessibili definitivamente o temporaneamente dagli stessi proprietari, quindi ulteriori livelli di difficoltà.

I *marketplace* aprono e talvolta spariscono anche nel giro di pochi giorni, gli stessi indirizzi cambiano in continuazione così come i forum, che finiscono spesso *offline* a seguito di attacchi informatici, o messi momentaneamente in *stand-by*.

Non solo, ma le URL di questi siti *web* invisibili rinvenibili nell'*underground* della rete internet, pur rispettando la costruzione sintattica di un normale sito *web* tradizionale (nome dominio più TLD) non prevedono la *top level domain* convenzionale, ovvero riconosciuta dagli standard internazionali come « .com », « .it », « .net », ma utilizzano l'estensione « .onion » (cipolla), che li rende inaccessibili dal *clear web* ed esclusi dall'autorità dell'ICANN, l'*Authority* internazionale per la gestione dei nomi a dominio a indirizzamento IP, quindi è sottratta a qualunque tipo di controllo internazionale delle autorità preposte.

L'evoluzione tecnologica rende possibile oggi navigare nel *dark web* (ulteriore aspetto preoccupante perché avvicina molto i giovani al *dark web* e soprattutto i criminali) anche tramite *smartphone* e *tablet*, utilizzando apposite *app* specifiche per IOS e Android, come ad esempio Orbot, che, opportunamente configurate, consentono dagli apparati *mobile* l'accesso a questo spazio virtuale nascosto. Questa circostanza renderà nell'imminente futuro la navigazione nella *darknet* un'operazione semplice e alla portata di tutti, con un incremento esponenziale dell'utenza di fruitori. Su questo ci sono degli aspetti statistici che lascio alla lettura.

Criptovalute. In questo contesto particolare interesse riveste per la Guardia di Finanza l'aspetto finanziario, che, come è noto alla Commissione, soprattutto sulla pirateria digitale attraverso il sistema *follow the money* e poi adesso *follow the hosting* ci ha consentito di anemizzare centinaia di siti rispetto al passato e quindi di far venir meno la convenienza economica. È il tema delle valute virtuali o criptovalute, che offrono anche garanzia di anonimato.

La modalità di pagamento ancora abbastanza macchinosa, in quanto subordinata al possesso a priori di un portafoglio virtuale, limita tuttavia la diffusione dello strumento tra l'utenza media dei naviganti.

Inizialmente la moneta di cambio utilizzata quasi in modo esclusivo nel *dark web* era il bitcoin, grazie all'elevato standard di anonimato garantito. Poiché è una formula matematica, possono essere emessi per una capitalizzazione di 21 milioni di bitcoin. Oggi abbiamo una capitalizzazione di 16 milioni, quindi a breve, nel giro di uno o due anni, il bitcoin avrà esaurito perché, come spiegheremo, è una stringa matematica di una elaborazione di altissimo livello con computer molto potenti, ma arrivato ai 21 milioni di bitcoin non si potrà più utilizzare.

Questo però non è un problema, perché nel frattempo, come si descrive nel testo, sono emerse ulteriori criptovalute tra cui Monero. Mi permetto di lasciare agli atti della Commissione l'elenco delle 100 criptovalute che stanno girando oggi nel *web* e che quindi vengono utilizzate per queste transazioni lecite, ma la maggioranza illecite.

Questo è il quadro generale. Nella Guardia di Finanza su questo aspetto specifico svolge un ruolo fondamentale (ringrazio per aver autorizzato la partecipazione del comandante) il Nucleo Speciale Frodi Tecnologiche, che è demandato per conto della Guardia di Finanza al monitoraggio della rete anche nascosta. L'organizzazione e le funzioni dei Reparti Speciali sono puntualmente documentate con un particolare approfondimento, però a completamento anche delle precedenti audizioni, e comunque sono a disposizione per eventuali approfondimenti e domande.

Solo per presentare il comandante del Nucleo che farà a breve la presentazione del video, il Nucleo ha alle proprie dipendenze quattro gruppi operativi: uno che fa il monitoraggio della rete quindi è dedicato esplicitamente a questa attività, il secondo e terzo gruppo svolgono un'attività operativa repressiva soprattutto di polizia giudi-

ziaria, il quarto gruppo si occupa di ricerca e sviluppo (*research*) e quindi di acquisire nuovi strumenti, di tenersi aggiornato, di partecipare a convegni.

Tenuto conto degli obiettivi che il legislatore ha assegnato alla Guardia di Finanza, il nostro tema principale è quello della repressione degli illeciti di natura economico-finanziaria, che sono sul *web*. Molta attenzione e molte risorse del reparto sono quindi assegnate all'area dell'evasione fiscale, all'area della spesa pubblica, alla tutela del mercato, con particolare riferimento all'abusivismo bancario e finanziario, al contrasto alla criminalità organizzata, riciclaggio di denaro, finanziamento al terrorismo, traffico d'armi e di stupefacenti, contraffazione e pirateria.

Il reparto si è specializzato sulle scommesse *on line*, dove, come ben noto, c'è una grossa interferenza della criminalità organizzata. Quindi monitoraggio del web e, poiché è un argomento che riprenderà il comandante del Nucleo, chiudo il mio intervento.

L'unica cosa che voglio sintetizzare in queste pagine è l'estrema difficoltà di svolgere attività repressiva. Poiché non c'è un'individuazione né tramite indicizzazione, né tramite altra strada (soprattutto complicata dal pagamento tramite queste criptovalute) per individuare questi siti che vendono anche prodotti contraffatti, per svolgere un'attività investigativa su questo è necessaria l'attivazione di onerosissime procedure di acquisto simulato e operazioni sotto copertura.

Una recente operazione nel settore del bitcoin della Polizia postale (noi facciamo da rimbalzo a loro e loro lo fanno a noi) ha consentito di smantellare un traffico molto insidioso, ma hanno impiegato due anni per individuare tutti i siti, perché per entrare in queste comunità e ottenere queste informazioni bisogna presentarsi, accreditarsi, acquistare, proporsi, non ci si può improvvisare, quindi è un'operazione di costruzione di figure di agenti provocatori che è molto impegnativa e costosa.

Si parla addirittura di due anni di investigazioni sotto copertura, per cui un'indagine del *dark web* e nel *deep web* è assolutamente complessa e attualmente costosa e, quand'anche avessimo tutte le risorse finanziarie e anche le professionalità, dovremmo impiegare risorse per la conduzione di un solo servizio per mesi, se non addirittura anni, quindi ne deve valere la pena, presidente. Questo è l'aspetto importante da sottolineare.

Sul tema della contraffazione noi abbiamo fatto delle considerazioni che anticipo, semplicemente dicendo che noi monitoriamo il settore della contraffazione del *deep web*, e lo vedremo perché ci sono le offerte di merce, non riguarda gli acquirenti ordinari che vanno sul *web* normale, quindi quelli che comprano Prada pensando che sia l'*outlet* di Prada, perché è difficile e gli acquisti spesso vengono fatti con bitcoin, procedura che non è conosciuta, non ci si fida, magari cela una truffa.

Dalla parte dell'utenza riteniamo (potremmo essere smentiti, ma non credo) che non ci siano livelli di preoccupazione significativi, tuttavia per quanto riguarda i siti esistenti abbiamo la sensazione che il *deep web* venga utilizzato per le vendite tra grossisti, cioè io vendo per essere coperto, perché nelle offerte dicono che devi acquistare un tot minimo di prodotti, quindi non può essere il singolo acquirente che si fa mandare il pacco della borsa Prada, Bulgari.

Questo al momento lo stiamo monitorando, si tratta di poche decine di borse, però potrebbe avere uno sviluppo parallelamente a quel discorso del *mobile*, quindi delle *app* che possono essere scaricate, considerando la dimestichezza che si sta acquisendo da parte degli internauti di utilizzare queste criptovalute in maniera più semplice, più facile.

Questa è la sintesi, però per l'illustrazione di quello che rappresenta il *dark web* lascerei – col consenso del presidente – la parola al colonnello Parascandolo.

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Signor presidente, avevamo pensato che fosse utile illustrare quello che quotidianamente fac-

ciamo nella navigazione *on line* sia in chiaro che in questo caso sul *dark web*.

Tre passi fondamentali, necessari prima di avviare una navigazione *on line* sono questi: l'installazione del *software* di navigazione, che non è ovviamente il semplice Google, la messa in sicurezza dell'ambiente di esplorazione, perché è vero che noi andiamo a cercare i criminali, però i criminali potrebbero scoprirci, quindi dobbiamo approntare tutte le difese necessarie ad evitare che qualcuno scopra che questa navigazione parta da una caserma della Guardia di Finanza, e l'esplorazione dei *marketplace*, di questi posti dove non dico che si millanta, ma sicuramente si illustra tutta una serie di vendite di beni e servizi anche di natura illegale.

Si parte sempre dal *clear web*, dal *surface web*: basta digitare su Google TOR Project e compare questa icona di TOR a forma di cipolla per installare il *software* come se volessimo installare sul nostro computer iTunes, un qualsiasi programma, Windows o quant'altro, quindi *download* e compare questa scritta. Si sceglie una lingua, si sceglie dove installare il programma, velocemente avviene in automatico senza necessità di *password* o di altro, ed ecco che sul nostro *desktop* come appare l'icona di Google, di iTunes o di Safari appare l'icona di Tor Browser. Cliccando sopra a questo punto è possibile cominciare a navigare sia in chiaro, ma soprattutto in modalità nascosta, anonima.

A questo punto accennavamo alla necessità di mettere in sicurezza il computer da dove navighiamo noi, cosa che si fa attraverso due strumenti, la VPN (*virtual private network*) e la *virtual machine*. Perché ? Perché se qualcuno dovesse scoprire che è una forza di polizia che sta navigando e tentasse di infettare il nostro computer, infetterebbe in realtà questa macchina virtuale, che è un servizio esterno che sarebbe allocato su un *server* diverso e quindi non comprometterebbe i nostri strumenti di navigazione.

Nell'esempio che abbiamo illustrato durante questa fase abbiamo addirittura scelto la possibilità di instaurare una doppia VPN, in maniera tale da avere un doppio filtro di sicurezza, e, una volta installata questa doppia VPN, questa rete virtuale, abbiamo scelto da quale Paese collegarci. Ovviamente noi eravamo a Roma, ma abbiamo fatto in modo che il nostro segnale passasse per Taiwan e a chi volesse scoprirlo sembrerebbe arrivare da Hong Kong. La nostra connessione risulterebbe quindi partire da Hong Kong, se qualcuno la volesse analizzare, con questo indirizzo IP, quindi non desterebbe preoccupazione immediata da parte del destinatario.

Da dove comincio ? Come giustamente diceva il signor generale Vecchione, non sono pagine indicizzate, cioè non esiste una lista, non si può semplicemente andare su Google e cercare armi, droga, prostituzione, pedopornografia o quant'altro, ma è necessario già conoscere una serie di pagine con l'indirizzo esatto, perché (purtroppo qui si legge male, ma si vedrà meglio nel dettaglio) l'indirizzo non è un « gan.com » o « rifle.com », ma è tutta una serie di lettere e di numeri che si susseguono apparentemente senza significato.

PRESIDENTE. Mi scusi, colonnello, quindi questa lista è stata costruita da voi ?

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Questa lista si trova nella navigazione in chiaro. Devo andare in The Hidden Wiki, che è una sorta di Wikipedia del *dark web* però ancora in chiaro, quindi vado su Google, digito « The Hidden Wiki », trovo questa lista e vado sul *dark web*, infatti adesso abbiamo provato a cercare *counterfeit*, cioè contraffazione. La maggior parte dei casi è relativa ad armi, pornografia, documenti falsi, carte di credito clonate. Con il termine contraffazione, invece, vedremo che digitando *counterfeit* compare qualcosa, questo httpqkj4, che immediatamente si vede che si tratta di valuta contraffatta, di US dollar.

Nel *dark web* il termine contraffazione è tendenzialmente riferito alle monete o ai documenti di identità, quindi, copiato quel link molto strano su TOR, comincio a navigare sul *dark web* e mi compare un sito che vende dollari falsi. Nella descrizione

viene anche riportata la qualità di queste banconote, che sono fatte su carta di cotone, quindi assolutamente di alta qualità, e c'è il cambio. Per un prezzo equivalente di circa 600 dollari si paga un bitcoin di valore. Ed ecco che la questione delle criptovalute di cui ha parlato prima il generale Vecchione evidenzia immediatamente la problematica. Sul *dark web* ovviamente tutti i pagamenti avvengono con valute virtuali, è impensabile fare un bonifico o pagare con una carta di credito, perché sarebbe uno strumento immediatamente rintracciabile.

Qui vado velocemente, perché si illustra semplicemente tutta la possibilità di avere informazioni e altre liste di *marketplace*, che ormai sono abbastanza diffuse sul *clear web*, una volta copiate le utilizzo per andare sul *dark web*.

Questi sono i primi 5-6 *marketplace* più famosi al mondo, in passato probabilmente si sarà sentito parlare di *Silk road*, la strada della seta, che era il principale *marketplace*, chiuso nel 2014 dall'FBI, e il suo posto è stato preso da questi nuovi *marketplace*. Qui vi è il riferimento a cui faceva cenno il generale Vecchione circa la percentuale che questi *marketplace* prendono nelle transazioni, nonché la possibilità di essere tutelati da truffe da parte degli acquirenti, perché è previsto un deposito cauzionale prima di poter concludere la vendita.

Una volta avuto accesso al *darknet* tramite questi indirizzi di *marketplace*, posso scegliere l'argomento che più mi interessa dal punto di vista tendenzialmente criminale, e vediamo che c'è anche un piccolo settore che riguarda l'audio o la musica, i video, i libri, la tutela della proprietà intellettuale. Ovviamente la parte del leone all'interno del *dark web* viene fatta dallo spaccio di stupefacenti, che ad oggi risulta essere il principale interesse dei cybernaviganti.

Si tratta però, anche in base alle esperienze operative in corso, di acquisti di stupefacenti per il consumo personale, quantitativi che non possono essere riferiti a grossi traffici internazionali di stupefacenti.

PRESIDENTE. In questo caso non è un problema di relazione tra operatori commerciali, ma qui c'è l'utente finale che compra, che deve essere in grado di pagare con bitcoin...

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Esatto, nel documento è riportata anche una recente operazione.

GENNARO VECCHIONE, *Comandante Unità Speciali della Guardia di Finanza*. Mi inserisco, nel documento le operazioni sono una del Nucleo speciale di polizia valutaria sulla falsificazione monetaria nell'area campana e una sugli stupefacenti all'aeroporto di Malpensa, a Milano, sul *dark web*.

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Per quanto attiene la contraffazione nello specifico e in genere la tutela dei *brand* e della proprietà intellettuale, abbiamo riscontrato qualcosa, però uno dei siti è una semplice radio, senza finalità commerciali. Utilizza il *dark web* perché fa una sorta di propaganda per finalità politiche o religiose diverse, ma non di estremismo. C'è chi da un punto di vista intellettuale tende a sottrarsi all'utilizzo di uno strumento ampiamente diffuso e preferisce una forma più riservata, per poter liberamente illustrare le proprie idee.

Abbiamo riscontrato anche la presenza di pirateria audiovisiva con film, musica, eventi sportivi.

MATTIA FANTINATI. Una domanda tecnica, essendo arrivato un poco in ritardo. Come faccio io a entrare nel *dark web*, mi serve una connessione protetta ?

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Si parte da Google, l'installazione del *browser* TOR, quindi il primo *step* è andare su Google e digitare TOR Project.

MATTIA FANTINATI. E questo è un browser normalissimo.

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Sì, normalissimo, che viene anche utilizzato per la navigazione in chiaro, non necessariamente *dark*. Digitando TOR Project, compare questo *browser*, l'*homepage*, e relativo *download*.

MATTIA FANTINATI. Chiaro. Quindi quando ho installato questo *browser* e ho una porta per il *dark*...

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Assolutamente.

MATTIA FANTINATI. Però è tracciato quando entro nel *dark web*.

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. No, dal momento in cui comincio a utilizzare il *browser* TOR divento immediatamente anonimizzato, in automatico.

MATTIA FANTINATI. Anche con un IP normale ?

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Anche con un IP statico, privato.

MATTIA FANTINATI. È tipo Telecom ?

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Assolutamente, anche Fastweb, Vodafone da casa. Questa è l'icona che appare. Nel momento in cui comincio a navigare con TOR, lo posso utilizzare sia per finalità di *deep web*, quindi cercare un *marketplace* con quell'indirizzo dell'URL particolarmente strano, sia utilizzare TOR come Google.

GENNARO VECCHIONE, *Comandante Unità Speciali della Guardia di Finanza*. Però un aspetto fondamentale è la differenza tra i due, in quanto mentre quando va su Google la ricerca è indicizzata, quindi scrive Gennaro Vecchione e vengono fuori tutti i risultati, se va su TOR per quanto riguarda la navigazione su *deep web* non verrà mai indicizzato perché è tutto anonimo, non c'è il rilascio di un elenco di siti, ma lei deve conoscere il sito, l'URL, il *link* preciso. Questa è la differenza fondamentale.

MATTIA FANTINATI. Cioè non è un motore di ricerca, è un *browser*.

GENNARO VECCHIONE, *Comandante Unità Speciali della Guardia di Finanza*. Se lei non conosce il *link*, non entrerà mai in *deep web*, perché non ha il riferimento. A navigare così naviga per niente, mentre su Google, sul *surface*, sul *clear web* digitando qualunque cosa le rilascia un elenco di siti. Questo nel *deep* non c'è.

MATTIA FANTINATI. Anche se apro il mio *browser* nudo e crudo senza Google, devo sapere l'URL.

GENNARO VECCHIONE, *Comandante Unità Speciali della Guardia di Finanza*. Assolutamente, altrimenti non entra. Ad esempio, scrivendo borse Prada nel *deep web*, non uscirà mai, devi conoscere l'indirizzo.

Abbiamo detto che sono 400 miliardi, il 90 per cento dei contenuti su internet è nel *deep web*, non nel *clear web*, quindi la cosa è veramente impressionante. Ci sono due questioni: c'è una serie di *link* nel *deep web* che sono noti, e il collega ha detto quelli che stava vedendo in rosso, sui quali non c'è alcuna segretezza. Ma gli altri, quelli importanti, dove più avanti andremo e dove loro hanno fatto una minima attività sotto copertura senza commettere reati per fare questa dimostrazione, bisogna avere il *link* preciso per commissionare omicidi, armi, droga, qualunque illecito.

Per avere quel *link* sui traffici veri, quelli di armi, quelli importanti, per avere

quella informazione bisogna agire sotto copertura per quasi due anni. Dei colleghi della Polizia postale ci hanno messo due anni per arrivare a individuare questo. Questa è la difficoltà, per questo segnalavamo i limiti nel discorso della contraffazione. Siamo convinti che non vengano acquistati singoli beni contraffatti dal cliente, come succede nei siti normali (Prada, finto *outlet* di Bulgari), ma che, seppur a livelli molto modesti di dieci o quindici borse, possano avvenire transazioni tra grossisti, perché sono coperte e di difficile penetrazione.

Questa è la differenza, quindi contraffazione sul *deep web*, ma non per i clienti finali, ma per quanto riguarda vendite di grossisti.

L'altra cosa importante è l'utilizzo di criptovalute, che rende ancora più anonimi e impossibili da individuare l'acquirente e il destinatario.

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza* Tornando all'illustrazione questo è un altro *marketplace* che si occupa di video, cartoni animati, film, prodotti tutelati dalla proprietà intellettuale. Questi sono i principali *marketplace* cui accennavo in precedenza, sono cinque, monopolizzano quasi tutto il settore *e-commerce* del *deep web*, da AlphaBay a Valhalla, Acropolis.

Prendiamo ad esempio AlphaBay, avuto l'accesso a questo è come trovarsi su eBay: troviamo i vari settori merceologici, la suddivisione dei vari articoli, è necessario effettuare una registrazione che non richiede un'e-mail perché sarebbe troppo semplice per noi rintracciare un'e-mail. Da un'e-mail chiederemmo all'*internet service provider* chi sia l'autore di quella mail che, seppure con nome falso, comunque ci conduce a un indirizzo IP, come lei giustamente diceva in precedenza. Quindi soltanto una *password* e non una *username*. Noi ci siamo per esempio registrati con questo acronimo, Calinix.

Ci sono degli elementi di dettaglio (la data di registrazione, il nostro balance, il nostro portafoglio), non abbiamo effettuato transazioni né in bitcoin né in Monero, che è la moneta a cui accennava il generale Vecchione, perché non abbiamo potuto svolgere attività illegale. Ha anche la rappresentazione del cambio della valuta in tempo reale.

Qui si può fare una ricerca per argomento: stupefacenti, pedopornografia, armi. All'interno del *market*, quindi, una volta raggiunto, è possibile effettuare una ricerca per argomenti. Sulla *homepage* ci sono gli ultimi aggiornamenti per post più recenti, ci sono anche le ultime notizie, si può fare una ricerca per filtri in base al prezzo, all'origine del prodotto o al Paese dove è possibile spedirlo.

Proprio perché non vi è un indirizzo *e-mail* da poter utilizzare, pena l'immediata tracciabilità da parte di una forza di polizia, vi è un servizio di messaggistica all'interno, quindi ci si scambia messaggi come un *messenger* di Windows, ma all'interno della piattaforma stessa, quindi non necessita di un elemento di conduzione di messaggi esterno, quale può essere una *e-mail*.

C'è il saldo di tutti gli ordini che abbiamo effettuato, gli archivi, gli ordini correnti, quelli in giacenza, e vi è il nostro profilo. Abbiamo un *trust level* D1, quindi estremamente basso perché non abbiamo né comprato, né venduto nulla (i livelli sono 9 e un livello di 5-6 è già molto alto) e vi sono soprattutto anche i *feedback*, come si diceva in precedenza.

Posso arricchire il mio profilo con una serie di elementi che voglio far conoscere ai miei potenziali acquirenti, e vi è un forum sul quale mi posso registrare anche con un nome diverso rispetto alla prima registrazione che ho fatto su AlphaBay, perché non voglio correlare quello che dico sul forum in base al venditore, sarebbe un elemento di identificazione pericoloso per il venditore, quindi posso avere un doppio tipo di registrazione.

Vediamo diviso per settori: le frodi ovviamente la fanno da padrona insieme alla vendita di stupefacenti. Vi sono anche dei *tutorial*, delle guide su come creare una qualsiasi cosa. La vendita di armi, *weapon seller*, è un aspetto estremamente delicato e concreto, ma c'è anche la possibilità di

acquistare dei *malware* per attaccare qualcuno, o la vendita di servizi spam. Se voglio attaccare qualcuno con un'attività di spam, ho la possibilità di acquistare questo tipo di servizio.

Qui per esempio c'è tutta una serie di vendita di *gan, handle weapon* e tutto quello che attiene soprattutto al traffico di armi. Questo effettivamente sembra avere una sua concretezza, una sua fondatezza importante all'interno soprattutto di questi *market*.

Questa invece è la vendita di identità a tutti gli effetti, quindi carte, carte di credito, patenti, credenziali, *social security number*, ovviamente è molto spostato sull'utenza statunitense perché è il mercato più vasto, più importante. La possibilità di acquistare i dati di una persona....

MATTIA FANTINATI. Quanto costa più o meno la carta di credito ?

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Adesso le illustro. Questo è un elenco di soggetti ai quali è stata rubata l'identità, ma ancora non ne sono a conoscenza ovviamente, altrimenti avrebbero bloccato. Si va da 9 a 12 dollari, da 7,43 a 29 dollari. Come si vede, gli Stati sono i più differenti.

Abbiamo provato a inserire l'Italia nella stringa Stato, abbiamo ottenuto questi 12 risultati di persone a cui è stata sottratta l'identità, due di Napoli, due di Milano, uno di Roma, e il prezzo si attesta sui 30 dollari, quindi è possibile acquistare per 30 dollari la carta di credito di questo soggetto, Adam B di Milano, spendere immediatamente 2-3.000 euro con la sua carta di credito prima che lui se ne accorga, che riceva sms dalla sua banca, e intanto il danno è stato fatto. La cosa inquietante è che questo signor Adam B ignora che gli siano stati sottratti i dati della sua carta di credito.

Per quanto riguarda nello specifico il *counterfeit*, la contraffazione di prodotti, nella data di navigazione della nostra attività risultavano 2.167 annunci, per quanto riguarda l'abbigliamento 947, *jewellery* tendenzialmente sono gli orologi, i Rolex la fanno da padrona in un rapporto di 1: 134 con il totale degli annunci, quindi per adesso una porzione sicuramente inferiore dell'intera offerta di AlphaBay, però sicuramente in espansione.

Questo è un esempio dei più significativi, perché un venditore di livello 5 ha un *trust*, una credibilità di livello 5, quindi assolutamente significativi, però dal 2015 risulta aver effettuato 118 vendite, quindi sicuramente un dato importante, ma per adesso non preoccupante. Come si vede, non è specificato da dove proviene questa merce, l'origine è *worldwide*, dappertutto, spedisce però anche dappertutto, quindi non si pone limiti di spedizione dei suoi prodotti.

Questa lista di *feedback* in un primo momento sembra negativa, sembra non esserci nulla. In questo caso vediamo anche con attenzione l'immagine, qui viene indicato come Paese di origine la Cambogia e la possibilità di spedire ovunque. Effettivamente sembra abbastanza credibile l'origine Cambogia, perché anche ad un occhio non esperto la qualità del prodotto sembra abbastanza scarsa, non particolarmente elevata. Siamo abituati a vedere prodotti contraffatti sicuramente meglio fatti, meglio prodotti, però anche qui registriamo un livello di *trust* e di venditore abbastanza elevato, o meglio elevato in relazione al settore merceologico, perché per avere un livello del genere nella vendita di armi o stupefacenti invece c'è necessità di una serie di *feedback* e di riscontri positivi estremamente più elevata, quindi può essere elevata nel settore della contraffazione, ma non in maniera assoluta.

È significativo il commento, questi tre *feedback:* paghi per quello che ricevi, cioè il suo valore è quello e si è anche rotto subito. Per adesso non è una cosa molto allarmante.

Questo indica sei vendite da agosto 2015, livello alto, però con sei vendite nel settore degli stupefacenti per esempio non avrebbe sicuramente un livello così alto. L'origine del Paese viene indicata in Afghanistan, ma pensiamo che non sia vero anche perché l'Afghanistan è il primo Paese che compare

nel menu a tendina quando si sceglie di indicare un Paese di provenienza. La spedizione invece è *worldwide* e i *feedback* sono positivi, si riscontra un livello di apprezzamento soddisfacente da parte degli acquirenti, che dicono di aver trovato un prodotto che sembra uguale al reale, però anche in questo caso appena due *feedback*.

Come accennavo, il settore della gioielleria è molto più ricco perché sono tendenzialmente gli orologi, quindi dal Breitling al Vacheron Constantin al Rolex c'è veramente tanta possibilità. Qui viene indicato come Paese di origine la Cina, potrebbe essere veritiero, e la possibilità di spedire anche qui in tutto il mondo è assolutamente prevista. Vi sono molti più *feedback*, tutti molto positivi, tutti di persone soddisfatte.

Come accennavamo in precedenza, per quanto riguarda la contraffazione sono tendenzialmente contraffazioni di banconote, di euro e di dollari, e sembra effettivamente esserci un mercato molto florido.

Un esempio: abbiamo provato a digitare Gucci per cercare prodotti contraffatti e la risposta è stata negativa, non c'è nessun risultato, a dimostrazione di una piattaforma non ancora ben sviluppata nel settore della contraffazione, perché almeno Gucci o Prada avrebbero dovuto dare qualche riscontro, quindi a dimostrazione che per quanto riguarda la contraffazione dei capi di abbigliamento più famosi dà un riscontro negativo perché non sembra esserci ancora un'offerta estremamente significativa. Lo stesso risultato con Prada.

Ci siamo posti un'ulteriore domanda. Abbiamo visto AlphaBay che è un *black market* generico come eBay, però esistono *black market* dedicati, specifici, solo per la contraffazione ? Abbiamo provato a navigare, a risalire, e siamo riusciti a individuare questo soggetto, China world seller Richard Sport.

Ci siamo meravigliati perché una piattaforma che venda solo merce contraffatta era la prima volta che ci capitava, ma poi abbiamo scoperto che è un soggetto che avevamo già trovato su AlphaBay e che vende solo questi cinque cap, cioè delle magliette NFL, dei Ray-Ban e delle scarpe Jordan, quindi ha soltanto cinque inserzioni e probabilmente è ancora l'embrione di quello che potrebbe essere in futuro un *black market* specifico, dedicato alla contraffazione. Esistono solo questi cinque prodotti, in quantità neanche specificate, che non sembrano da un punto di vista qualitativo di alto livello. Questi sono gli annunci che indica su questo *black market*: le magliette della National Football League americana o gli occhiali Ray-Ban da aviatore, quindi nulla di particolarmente specifico.

In conclusione, possiamo dire che sì una presenza c'è sicuramente, non è per il momento a livelli allarmanti, sicuramente è qualcosa da monitorare e da tenere d'occhio, che va di pari passo con la tematica delle criptovalute, di cui parlava il generale Vecchione, perché il pagamento può avvenire esclusivamente tramite criptovalute per non essere rintracciati, quindi è uno strumento ancora non nella disponibilità immediata, quotidiana di tutti, ma che comunque si sta diffondendo sempre di più. Grazie per l'attenzione.

PRESIDENTE. Vi ringrazio moltissimo, è stata un'audizione molto utile e istruttiva. Il messaggio che ne traggo, che è in sintonia con le sue conclusioni, colonnello, ma anche con le considerazioni del generale, è che nel *deep web* per ora la contraffazione ha un ruolo minore rispetto ad altri illeciti ben più importanti, e questo forse ha anche un senso, perché oggi andare nel *web* sulla contraffazione si può fare facilmente sulla parte in chiaro, non c'è bisogno di andare sul *deep web*, e in più non c'è il vincolo dei bitcoin, invece per vendere armi è chiaro non si può andare in rete nella parte in chiaro. Prego, onorevole Cenni.

SUSANNA CENNI. Solo una brevissima domanda, scusandomi per il ritardo, ma oggi i lavori di Aula hanno scombinato tutti i nostri programmi.

Vedendo quello che voi siete riusciti a ricostruire anche all'interno di queste piat-

taforme raggiungibili attraverso la strada che ci avete illustrato, avete parlato di una sorta di spazio per la messaggeria interna, come del resto funziona anche in altri *social*. Volevo fare una domanda in relazione a una delle indagini che stiamo facendo in merito alla connessione fra la criminalità organizzata e il fenomeno della contraffazione.

Anche alla luce di alcuni ragionamenti illustrati da indagini di carattere internazionale, ci viene detto che questa relazione c'è e ha riguardato anche un pezzo della vicenda che riguarda il terrorismo internazionale come forma di finanziamento.

Volevo capire se indagando questa parte del vostro lavoro abbiate avuto sentore o anche riscontro di relazioni con il mondo della criminalità organizzata.

GENNARO VECCHIONE, *Comandante Unità Speciali della Guardia di Finanza*. Per il momento – poi completerà il collega per la parte operativa – tra criminalità organizzata e i settori contraffazione, armi, scommesse *on line* e tutto quello che passa sul *web* è già dimostrato anche dagli accordi con organizzazioni asiatiche per spartirsi il mercato, per sviluppare questo *business* che non si fanno mancare.

Per quanto riguarda il *dark web*, come abbiamo spiegato all'inizio, la difficoltà è quella di investigare in modo completamente diverso da come avviene nel *web* in chiaro, perché è complesso entrare in rapporti diretti con soggetti non identificati, né identificabili proprio per la struttura a nodi, perché un nodo conosce quello a fianco, ma l'intera filiera non la conosce nessuno.

La stessa FBI per Silk Road, questo *marketplace* molto grande, ha sequestrato dei bitcoin e li ha messi sul mercato per trasformarli in dollari e tradurre in concreto il sequestro penale, ma la difficoltà è che ci vogliono operazioni lunghissime sotto copertura, di infiltrazione, di accreditamento.

Queste sono di gran lunga più impegnative di un'attività sotto copertura ordinaria, in cui uno si inserisce in un'organizzazione fisicamente e costruisce la società fittizia, c'è una disponibilità bancaria, frequenta, compra, vende droga con facilità, mentre l'estrema diffidenza che c'è nel *web* non consente di entrare. La difficoltà investigativa è che sono sostanzialmente pochissime le operazioni fatte.

Da qui è difficile pensare che si possano collegare anche fatti legati a stupefacenti (ma si tratta di trafficanti minori, certamente non collegati alla criminalità organizzata) verosimilmente al traffico d'armi internazionale, ancorché non si tratti di quantitativi rilevanti, perché si tratta della mitraglietta o della pistola, anche usata, quindi anche tracciata dalle forze di polizia. Si tratta secondo me di malviventi ordinari, di criminali certamente di spessore perché vendere un'arma o piccoli quantitativi di droga comunque li individua come tali, però non mi sento di affermare che ci sia una connessione con la criminalità organizzata.

GIOVANNI PARASCANDOLO, *Comandante del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza*. Condivido totalmente quanto detto dal generale Vecchione anche in base a un altro elemento: il bitcoin, la valuta. È impensabile effettuare un cambio di un milione di euro con 50 bitcoin, perché non ci sarebbe la possibilità di avere un cambiavalute che ti cambia 50 milioni di euro in contante con un bitcoin, quindi poco si presta a un traffico di stupefacenti a livello internazionale o a un traffico di beni contraffatti ad alto livello, a livello di grossista, proprio perché mancherebbe lo strumento della corresponsione, cioè la moneta virtuale, il cambio ovviamente non è ancora un'attività non dico lecita, perché ci sono i cambiavalute, ma regolamentata, quindi sarebbe veramente difficile per un'organizzazione criminale trovare qualcuno che dia 1.000 bitcoin a fronte di una quantità di moneta contante molto elevata.

PRESIDENTE. Grazie. Devo dire che raramente un'audizione è stata così utile a mio parere, perché è stata veramente illuminante la dimostrazione, e anche il testo della relazione che ci avete lasciato è particolarmente esaustivo rispetto a tutti gli

aspetti di questa tematica, quindi grazie ancora al generale Vecchione, al colonnello Parascandolo e a tutta la squadra che ci ha lavorato.

Dispongo che la documentazione trasmessa sia allegata al resoconto stenografico della seduta odierna e dichiaro conclusa l'audizione.

La seduta termina alle 15.25.

Licenziato per la stampa
il 20 gennaio 2018

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO

Guardia di Finanza
COMANDO UNITÀ SPECIALI

**COMMISSIONE PARLAMENTARE DI INCHIESTA
SUI FENOMENI DELLA CONTRAFFAZIONE,
DELLA PIRATERIA IN CAMPO COMMERCIALE
E DEL COMMERCIO ABUSIVO**

**AUDIZIONE
DEL COMANDANTE DELLE UNITÀ SPECIALI
DELLA GUARDIA DI FINANZA
GEN.D. GENNARO VECCHIONE
"IL CONTRASTO ALLA CONTRAFFAZIONE
E ALLA PIRATERIA NEL DEEP WEB"**

Roma, 9 marzo 2017

INDICE

SIGNOR PRESIDENTE, SIGNORI MEMBRI DEL COMITATO,

DESIDERO ANZITUTTO PORGERE IL MIO RINGRAZIAMENTO, OLTRE A QUELLO DEL COMANDANTE GENERALE E DEL COMANDANTE DEI REPARTI SPECIALI, PER QUESTA ULTERIORE OCCASIONE OFFERTA ALLA GUARDIA DI FINANZA DI ESPORRE LA PROPRIA TESTIMONIANZA E IL PROPRIO PUNTO DI VISTA IN MERITO A TALUNE TEMATICHE DI GRANDE ATTUALITA' E PARTICOLARE INTERESSE OPERATIVO, QUALI QUELLE RICONDUCIBILI AL MONDO CIBERNETICO E, PIU' SPECIFICATAMENTE, AL C.D. "DEEP WEB".

SONO IL GEN.D. GENNARO VECCHIONE, COMANDANTE DELLE UNITA' SPECIALI, VALE A DIRE IL REPARTO DEPUTATO, PRIORITARIAMENTE, ALLA COLLABORAZIONE CON AUTORITA' ED ORGANISMI INDIPENDENTI, TRA CUI LE COMMISSIONI PARLAMENTARI D'INCHIESTA, DAL QUALE DIPENDONO I NUCLEI SPECIALI CHE SONO ANCHE INTERESSATI, A VARIO TITOLO, NELL'AZIONE DI CONTRASTO AI FENOMENI ILLECITI CHE INTERESSANO IL CYBERSPACE.

E' CON ME IL COL. T.ST GIOVANNI PARASCANDOLO, COMANDANTE DEL NUCLEO SPECIALE FRODI TECNOLOGICHE, A CUI E' AFFIDATO IL COMPITO DEL MONITORAGGIO E CONTRASTO DEGLI ILLECITI ECONOMICO-FINANZIARI COMMESSI SULLA RETE, IVI COMPRESE LA CONTRAFFAZIONE E PIRATERIA, OLTRE A FORNIRE IL SUPPORTO TECNICO-SPECIALISTICO A TUTTE LE COMPONENTI OPERATIVE DEL CORPO NELLO SVILUPPO DI INVESTIGAZIONI CARATTERIZZATE DALL'USO DI TECNOLOGIE.

IN LINEA DI CONTINUITA' CON I CONTENUTI DELLA MIA PRECEDENTE AUDIZIONE TENUTA INNANZI A CODESTA COMMISSIONE A FEBBRAIO 2016 E DI QUELLA DEL COMANDANTE GENERALE A SETTEMBRE 2016, FORNIRO' ULTERIORI ELEMENTI INFORMATIVI CIRCA L'IMPEGNO ISTITUZIONALE PROFUSO DALLE UNITA' SPECIALI A PRESIDIO DI QUESTO PARTICOLARE SETTORE OPERATIVO, PARTENDO DA UNA NECESSARIA ANALISI DI CONTESTO CHE CI PERMETTERA' DI ENTRARE PIU' NEL VIVO DELLA MATERIA.

MI SOFFERMERO' POI SU ALCUNI ASPETTI DI SPECIFICO INTERESSE PER QUESTA COMMISSIONE, PER CONCLUDERE CON LA PROIEZIONE DI UN FILMATO CHE MOSTRERA' UNA VERA E PROPRIA NAVIGAZIONE DELLA

"DARKNET".

1. ANALISI DI CONTESTO

LE TECNOLOGIE CARATTERIZZANO E CONDIZIONANO ORAMAI IN MODO DETERMINANTE LA VITA DELLE SOCIETA' MODERNE, FINENDO PER AMPLIARE IL PERIMETRO DI QUELLO CHE FINO AD OGGI ABBIAMO CHIAMATO IL MONDO REALE.

SI TRATTA DI UNA NUOVA DIMENSIONE SPAZIALE, COMUNEMENTE DENOMINATA "MONDO CIBERNETICO", CHE POTREMMO DEFINIRE COME QUELL'INSIEME DI INFRASTRUTTURE TECNOLOGICHE INTERCONNESSE, RETE INTERNET COMPRESA, CHE SI ESTENDE A TUTTI GLI APPARATI TECNOLOGICI (SISTEMI DI TELECOMUNICAZIONE, COMPUTER E LORO COMPONENTI, PRODOTTI HI-TECH, ECC.) IN GRADO DI COLLEGARSI TRA LORO.

UN MONDO FATTO DI STRUTTURE FISICHE, PROCESSI MATEMATICI, SOFTWARE ED INFORMAZIONI, CHE FINISCONO PER RAPPRESENTARE UN SISTEMA ARTICOLATO E COMPLESSO, NON SEMPRE CONOSCIUTO IN TUTTE LE SUE PARTI (SI PENSI APPUNTO AL "DEEP WEB"), CAPACE DI GENERARE INGENTI PROFITTI MA ANCHE SIGNIFICATIVE PERDITE PER LE ECONOMIE ED I SISTEMI PAESE.

VALE LA PENA DI CITARE ALCUNI NUMERI PER COMPRENDERE LA DIMENSIONE DEL QUADRO DI RIFERIMENTO:

- PIU' DI 3,42 MILIARDI SONO, NEL MONDO, GLI UTENTI CHE ACCEDONO AL WEB, CHE SIGNIFICA IL 46% DELLA POPOLAZIONE MONDIALE. DI QUESTI 2,31 MILIARDI UTILIZZANO NORMALMENTE I SOCIAL MEDIA. QUASI 4 MILIARDI SONO INVECE GLI UTENTI "MOBILE", SEMPRE PIU' INTERCONNESSI CON TALI DISPOSITIVI ALLA RETE;
- GUARDANDO ALL'ITALIA, SONO 37,6 MILIONI GLI UTENTI CHE ACCEDONO AL WEB DI CUI 28 MILIONI UTILIZZANO PIATTAFORME SOCIAL (PRINCIPALMENTE FACEBOOK, WHATSAPP, MESSENGER, GOOGLE+, SKYPE, TWITTER, INSTAGRAM, ECC.). OLTRE 80 MILIONI SONO I DISPOSITIVI "MOBILE" IN USO, PIU' O MENO DUE PER CITTADINO ATTIVO.

UN'INSIEME QUASI INDEFINITO DI INFRASTRUTTURE, DISPOSITIVI E PERSONE CHE SONO TRA LORO PERMANENTEMENTE COLLEGATE (E LO SARANNO SEMPRE DI PIU'!), INDIPENDENTEMENTE DAI CONFINI STATUALI E DALLE GIURISDIZIONI, E RISPETTO ALLE QUALI SI DEVONO CONFRONTARE OGNI GIORNO LE ISTITUZIONI DEI SINGOLI PAESI IN TERMINI DI RISPETTO DELLE REGOLE E BUON ANDAMENTO DELLE RELAZIONI SOCIO-ECONOMICHE.

MA LO SPAZIO TELEMATICO GLOBALE, DI DIMENSIONI VIRTUALMENTE INFINITE, E' OGGI UN QUALCOSA DI PIU' COMPLESSO, SOPRATTUTTO SE LO SI GUARDA DAL LATO DEL RISCHIO SISTEMICO.

NON SOLO LUOGO DI INTERESSE DI RETI CRIMINALI ORGANIZZATE, IL CUI OBIETTIVO È DI SOTTRARRE DENARO, TRUFFARE O RAGGIRARE A SCOPO DI LUCRO CITTADINI ED ORGANIZZAZIONI O, ANCORA, DI AGENZIE DI SPIONAGGIO NON GOVERNATIVE, IN GRADO DI SOTTRARRE INFORMAZIONI RILEVANTI ALLA BUSINESS COMMUNITY, FALSANDO IN QUESTO MODO LA LEALE CONCORRENZA, QUANTO NUOVO INEDITO CAMPO DI BATTAGLIA E DI COMPETIZIONE GEOPOLITICA.

SENZA CONSIDERARE POI LE NUOVE CRITICITA' DOVUTE ALLA CRESCITA ESPONENZIALE DI TUTTE QUELLE ATTIVITA' ILLECITE CHE TROVANO PARTICOLARE AGIO NELLA PARTE PIU' PROFONDA DELLA RETE, IN QUELLA AREA NASCOSTA DEL DEEPWEB (NOTA COME "DARKNET"), NON INDICIZZATA DAI MOTORI DI RICERCA, CHE OFFRE AMPIA GARANZIA DI ANONIMATO GRAZIE ANCHE AI NUMEROSI SERVIZI NASCOSTI IVI PRESENTI (HIDDEN SERVICE) E ALL'USO MASSIVO DI TRANSAZIONI FINANZIARIE OPERATE ATTRAVERSO CRYPTOVALUTE.

2. IL "DEEP WEB"

A. GENERALITA'

CON IL TERMINE "**DEEP WEB**" SI INTENDE **L'INSIEME DEI SITI INTERNET, DELLE PAGINE E DEI CONTENUTI WEB CHE, NON ESSENDO INDICIZZATI, NON POSSONO ESSERE RAGGIUNTI DAGLI UTENTI ATTRAVERSO I COMUNI**

MOTORI DI RICERCA (ES., GOOGLE, BING, ECC.). SOLO CONOSCENDO IL LINK ESATTO O DISPONENDO, EVENTUALMENTE, DI USERNAME E PASSWORD DI UN CERTO MODULO DI ACCESSO, POTREMMO AVERE CAMPO LIBERO ALLA NAVIGAZIONE DI CERTI CONTENUTI (SI PENSI, AD ES., A FORUM, PORTALI AZIENDALI, SERVIZI ISTITUZIONALI, ECC...).

CI RIFERIAMO, PER FARE QUALE ESEMPLIFICAZIONE, A "PAPER" ACCADEMICI E SCIENTIFICI, DOCUMENTI LEGALI, CARTELLE MEDICHE, RISORSE CONTENUTE IN DATABASE GOVERNATIVI O DI AZIENDE PRIVATE; DUNQUE, **NON NECESSARIAMENTE CONTENUTI ILLECITI**.

NELLO SPECIFICO, IL TRAFFICO DEL "DEEP WEB" È FORMATO, ESSENZIALMENTE, DA BIT CHE VEICOLANO, TRA L'ALTRO:

- INTERROGAZIONI DI DATABASE;
- OPERAZIONI DI ISCRIZIONE/LOGIN E, IN GENERALE, TRANSAZIONI PROTETTE DA PASSWORD;
- PAGINE ACCESSIBILI SOLO MEDIANTE L'ATTIVAZIONE DI SERVIZI A PAGAMENTO;
- PAGINE NON "LINKATE" (COLLEGATE) DA NESSUN'ALTRA PAGINA DEL WEB;
- TECNOLOGIE, COME QUELLE CC.DD. "CAPTCHA", CHE VENGONO UTILIZZATE PER IMPEDIRE L'ACCESSO A RISORSE WEB DA PARTE DI SISTEMI AUTOMATIZZATI.

SI TRATTA, A BEN GUARDARE, DI UNA QUANTITA' TALE DI DATI E INFORMAZIONI DA RAPPRESENTARE LA QUASI TOTALITA' DELL'INTERO MONDO INTERNET.

VOLENDO FORNIRE, CON TUTTE LE APPROSSIMAZIONI DEL CASO, UN ORDINE DI GRANDEZZA IN TERMINI NUMERICI, ALCUNE RECENTI ANALISI PARLANO DI **CIRCA 400 MILIARDI DI DOCUMENTI COMPLESSIVI PRESENTI NEL "DEEP WEB"** A FRONTE DI **POCO PIU' DI 3.9 MILIARDI DI** PAGINE WEB INDICIZZATE DAL MOTORE DI RICERCA "GOOGLE".

L'IMMAGINE CHE SEGUE DA UNA SINTETICA RAPPRESENTAZIONE DELLA

SITUAZIONE APPENA DESCRITTA.

NEL SUBSTRATO DEL "DEEP WEB" TROVIAMO, POI, IL "**DARK WEB**" (O PIÙ CORRETTAMENTE LA "**DARKNET**"), IL CUI FUNZIONAMENTO RICHIEDE SPECIFICI SOFTWARE E CONFIGURAZIONI DI SISTEMA PARTICOLARI.

B. "DARKNET"

VOLENDO ENTRARE PIU' NEL DETTAGLIO, SI TRATTA DI UN INSIEME DI RETI E TECNOLOGIE, CHE UTILIZZANO APPLICAZIONI E PROTOCOLLI DI COMUNICAZIONE GIA' ESISTENTI (AD ES., HTTP, FTP, ECC.), USATI PER LA CONDIVISIONE DI CONTENUTI DIGITALI, CHE NON SONO SEPARATI FISICAMENTE DA INTERNET, MA **RESI INTENZIONALMENTE INVISIBILI E NON ACCESSIBILI DAI COMUNI BROWSER, PER ESSERE POI RAGGIUNGIBILI SOLO DA SOFTWARE PROGETTATI PER INSTAURARE COMUNICAZIONI ASSOLUTAMENTE ANONIME**.

E' QUINDI DI TUTTA EVIDENZA CHE I TERMINI "**DEEP WEB**" E "**DARK WEB**", MALGRADO MOLTO SPESSO VENGANO USATI COME SINONIMI, NON POSSONO ESSERE CONSIDERATI TALI, ESSENDO **IL SECONDO UN**

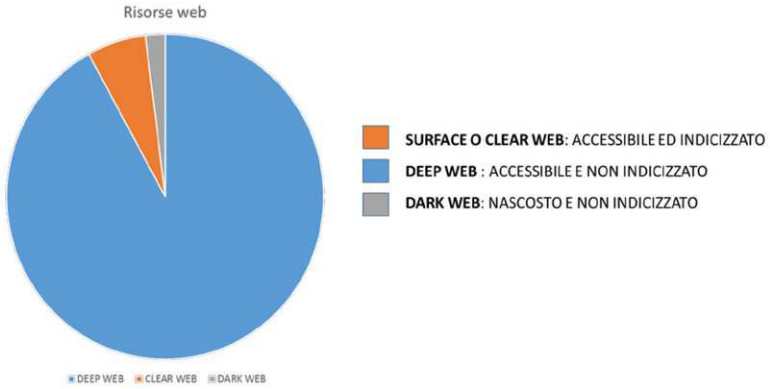
8

SOTTOINSIEME DEL PRIMO, CON PROPRIE E SPECIFICHE CARATTERISTICHE CHE NE FANNO UN MONDO A SE' STANTE.

VOLENDO SINTETIZZARE QUANTO FIN QUI ILLUSTRATO, POTREMMO DIRE DI RICONDURRE LE RISORSE WEB A TRE MACRO INSIEMI:

QUELLE:

- ACCESSIBILI E INDICIZZATE (SURFACE O CLEAR WEB);
- ACCESSIBILI E NON INDICIZZATE (DEEP WEB)
- NASCOSTE E NON INDICIZZATE (DARK WEB)



È PROPRIO IN QUESTA PORZIONE DEL MONDO VIRTUALE "NASCOSTO" (O "DARK") CHE POSSONO ANNIDARSI PERICOLOSE ORGANIZZAZIONI CRIMINALI, GRUPPI DI HACKER, CELLULE ANTAGONISTE O, ADDIRITTURA, SOGGETTI LEGATI A FRANGE TERRORISTICHE.

QUI, COME NEL "**CLEAR WEB**", E' POSSIBILE TROVARE UNA RETE DI "**MARKETPLACE**" DOVE, APPARENTEMENTE, SI PUO' COMPRARE DI TUTTO: DROGA, ARMI, MATERIALE PEDOPORNOGRAFICO, DOCUMENTI DI IDENTITA', NUMERI DI CARTE DI CREDITO, MAIL LIST, PRODOTTI

CONTRAFFATTI O PIRATATI E TANTO ALTRO ANCORA.

E POSSIBILE, INOLTRE, ACQUISTARE O AFFITTARE DEI VERI E PROPRI SERVIZI SU MISURA PER COMPIERE ATTIVITA' DI HACKERAGGIO OPPURE DI PHISHING O, ANCORA, PER COMPIERE AZIONI DIMOSTRATIVE CONTRO ISTITUZIONI PUBBLICHE O AZIENDE PRIVATE.

ECCO ALCUNI ESEMPI DELLE INSERZIONI CHE E' POSSIBILE TROVARE:

- PISTOLA BERETTA A € 900 O MITRAGLIETTA DI FABBRICAZIONE RUSSA A € 2000;
- "PACCHETTO" CONTENENTE INFORMAZIONI PERSONALI DI UN UTENTE (PII RECORD) A UN DOLLARO;
- ACCOUNT PAYPAL ACQUISTABILI A PARTIRE DA $300;
- ACCOUNT PER ONLINE BANKING A PREZZI COMPRESI TRA $200 E $500 IN FUNZIONE DEL SALDO CONTABILE E DELLE INFORMAZIONI CARPITE;
- SCANSIONI DI DOCUMENTI DI IDENTITÀ E PATENTI AD UNA CIFRA COMPRESA TRA I $10 ED I $35;
- DOCUMENTI CONTRAFFATTI A PREZZI COMPRESI DAI $100 AI $1000 (AD ES. UNA PATENTE AMERICANA FALSA COSTA INTORNO A $100-$150);
- SISTEMA DI HACKING DI UN ACCOUNT FACEBOOK, TWITTER O DI ALTRE PIATTAFORME DI SOCIAL NETWORKING DAI $50 AI $200 DOLLARI;
- SOFTWARE DI VIRUS INFORMATICI (REMOTE ACCESS TROJAN) DAI $150 AI $400;
- CODICE SORGENTE DI UN "MALWARE" BANCARIO CON ANNESSA PERSONALIZZAZIONE DAI $900 AI $1500;
- CAPI DI ABBIGLIAMENTO, BORSE E OROLOGI CONTRAFFATTI;
- FILE MP3, LIBRI, FILM, SERVIZI STREAMING, ECC.

NEI "MARKETPLACE" MAGGIORMENTE NOTI NEL "*DARK WEB*", LE COMPRAVENDITE SONO GARANTITE DA UN **SISTEMA DI "FEEDBACK"** DEGLI UTENTI MOLTO EFFICACE, BASATO SULLA CREDIBILITÀ DEL VENDITORE E SUI QUANTITATIVI DI PRODOTTI CEDUTI. INOLTRE, LE MODALITÀ DI PAGAMENTO CHE SONO ASSISTITE DA UN **SERVIZIO DI "ESCROW",** OVVERO UN ACCORDO SECONDO IL QUALE LA SOMMA

RELATIVA AL PAGAMENTO DI UN BENE/SERVIZIO ACQUISTATO, PRIMA DI ESSERE ACCREDITATA SUL CONTO DEL VENDITORE, VIENE TRATTENUTA DA UNA TERZA PARTE (SOLITAMENTE GLI AMMINISTRATORI DEL *MARKETPLACE* O SOGGETTI AD ESSI COLLEGATI) FINO AL MOMENTO IN CUI L'ACQUIRENTE CONFERMA L'AVVENUTA CONSEGNA DELLA MERCE.

TUTTAVIA, È BENE PRECISARE, CHE ALCUNE DI QUESTE INSERZIONI POTREBBERO VEROSIMILMENTE RIFERIRSI A TENTATIVI DI TRUFFA O A CONDOTTE FINALIZZATE ALLA SOTTRAZIONE DI DATI O INFORMAZIONI SENSIBILI. INFATTI SONO NUMEROSI I CASI DI VERA E PROPRIA CLONAZIONE DEI "MARKETPLACE" CHE VENGONO POI MESSI ONLINE DA TERZI SOGGETTI, COSI' DA SFRUTTARE LA CONFUSIONE CHE PUO' ESSERE GENERATA DALLA MOLTEPLICITÀ DI INDIRIZZI DISPONIBILI PER ACCEDERE ALLE PREDETTE PIATTAFORME.

C. RETE TOR

UNO DEI PRINCIPALI SISTEMI UTILIZZATI PER ACCEDERE AI CONTENUTI RINVENIBILI ALL'INTERNO DELLE "DARKNET", È SICURAMENTE "**TOR** (THE ONION ROUTER)[1]".

TALE SISTEMA DI COMUNICAZIONE ANONIMA BASATO SULLA SECONDA GENERAZIONE DEL PROTOCOLLO DI RETE DI "ONION ROUTING", È NATO NEL 1995 QUANDO LA MARINA STATUNITENSE NE INIZIA LO SVILUPPO PER PROTEGGERE LE COMUNICAZIONI GOVERNATIVE GRAZIE A "CRITTOGRAFIA" A STRATI ("ONION": CIPOLLA APPUNTO).

SUCCESSIVAMENTE, NEL 1997, L'IMPLEMENTAZIONE DEL PROGETTO VIENE AFFIDATA ALLA "DARPA", AGENZIA GOVERNATIVA STATUNITENSE INCARICATA DI STUDIARE E SVILUPPARE NUOVE TECNOLOGIE PER L'IMPIEGO IN AMBITI MILITARI.

DAL 2004 LA "ELETTRONIC FRONTIER FOUNDATION", UN ORGANIZZAZIONE

[1] Ne esistono, tuttavia, tantissime altre che, fondamentalmente, condividono lo stesso principio: creare una rete sulla rete che garantisca anonimato e comunicazioni sicure e cifrate. Una di esse è la rete c.d. I2P.

NO PROFIT CHE DAL 1990 SI OCCUPA DI DIRITTI E LIBERTÀ DIGITALI, INIZIA A FINANZIARE LO SVILUPPO DI "TOR", I CUI CODICI NEL FRATTEMPO ERANO STATI RILASCIATI CON LICENZA LIBERA, PER ESPANDERE IL SUO FUNZIONAMENTO OLTRE L'AMBITO MILITARE-GOVERNATIVO.

DAL 2004 AD OGGI MOLTE ALTRE SOCIETÀ (COME GOOGLE NEL 2011) ED ORGANIZZAZIONI NON GOVERNATIVE HANNO FINANZIATO LO SVILUPPO DI "TOR".

LA PECULIARITÀ PRINCIPALE DELLA TECNOLOGIA FORNITA DA TOR È SICURAMENTE LA **SICUREZZA DELL'ANONIMATO**.

L'IP[2] DI CONNESSIONE CHE VIENE ASSUNTO, INFATTI, È QUELLO CHE È STATO ASSOCIATO TEMPORANEAMENTE DAL SOFTWARE IN PAROLA E NON QUELLO CHE REALMENTE L'"INTERNET SERVICE PROVIDER" (OSSIA IL GESTORE TELEFONICO CHE FORNISCE LA CONNESSIONE) HA ASSEGNATO ALLA MACCHINA COLLEGATA ALLA RETE INTERNET.

DI CONTRO TUTTA L'ARCHITETTURA NON POTEVA NON PRESENTARE UN TALLONE D'ACHILLE. LA VELOCITÀ DI CONNESSIONE, INFATTI, IN RAGIONE DEL SUO FUNZIONAMENTO, RISULTA MOLTO LENTA IN QUANTO, PROPRIO PER GARANTIRE LA SICUREZZA, LA NAVIGAZIONE DELL'UTENTE DEVE AVVENIRE EFFETTUANDO MOLTEPLICI "SALTI" TRA I DIVERSI NODI PRESENTI E ATTIVI ALL'INTERNO DEL CIRCUITO TOR.

IL FUNZIONAMENTO DEL SOFTWARE IN PAROLA NON È LO STESSO DELLA RETE "TRADIZIONALE": LA COMUNICAZIONE TRA IL CLIENT ED IL SERVER NON È DIRETTA MA, COME INDICATO, VIENE "RIMBALZATA" ATTRAVERSO ALTRI SERVER DENOMINATI "RELAY" MESSI A DISPOSIZIONE DAI VOLONTARI CHE, FUNGENDO DA ROUTER, **RENDONO MOLTO DIFFICILE POTER INTERCETTARE L'ORIGINE, LA DESTINAZIONE E IL CONTENUTO DEI MESSAGGI E DEI DATI TRASFERITI**.

UNA VOLTA AVVIATO IL SOFTWARE "TOR" ED AVUTO ACCESSO AL CIRCUITO È POSSIBILE NAVIGARE SIA NEL WEB DI SUPERFICIE, SIA NEL

[2] etichetta numerica che identifica univocamente un dispositivo (computer, tablet ecc.) detto "host" collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete.

"DEEP WEB".

IN QUEST'ULTIMO CASO, VISTA L'INEFFICACIA DEI MOTORI DI RICERCA, SI DEVE NECESSARIAMENTE FARE AFFIDAMENTO A LISTE COMPILATE DI INDIRIZZI (LINK) COME LE "HIDDEN WIKI", "TORCH", "GRAMS", "CANDLE", ECC. O QUELLE PUBBLICIZZATE NEI FORUM DI UTENTI.

A COMPLICARE, ANCOR DI PIU', LA SITUAZIONE SONO LE CONTINUE MUTAZIONI DEGLI INDIRIZZI DELLE PAGINE PRESENTI (C.D. "UNIFORM RESOURCE LOCATOR", O URL), CHE, PER RAGIONI DI RISERVATEZZA, VENGONO MOLTO SPESSO RESI INACCESSIBILI, DEFINITIVAMENTE O TEMPORANEAMENTE, DAGLI STESSI PROPRIETARI.

I "MARKETPLACE", DUNQUE, APRONO E TALVOLTA SPARISCONO ANCHE NEL GIRO DI POCHI GIORNI; GLI STESSI INDIRIZZI CAMBIANO IN CONTINUAZIONE, COSI' COME I FORUM CHE FINISCONO SPESSO OFFLINE A SEGUITO DI ATTACCHI INFORMATICI O MESSI MOMENTANEAMENTE IN "STAND-BY" PER UN'EMERGENZA O UNA VULNERABILITÀ.

LE URL DI QUESTI SITI WEB "INVISIBILI", RINVENIBILI NELL'UNDERGROUND DELLA RETE INTERNET, PUR RISPETTANDO LA COSTRUZIONE SINTATTICA DI UN NORMALE SITO WEB TRADIZIONALE (NOMEDOMINIO.TLD), NON PREVEDONO UN "TOP LEVEL DOMAIN" CONVENZIONALE OVVERO RICONOSCIUTO DAGLI STANDARD INTERNAZIONALI (.COM, .IT, .NET, ETC), **MA UTILIZZANO L'ESTENZIONE ".ONION",** CHE LI RENDE INACCESSIBILI DAL "CLEAR WEB" ED ESCLUSI DALL'AUTORITÀ DELL'"ICANN", L'AUTHORITY DI INTERNET PER LA GESTIONE DI NOMI A DOMINIO E INDIRIZZAMENTI IP.

L'EVOLUZIONE TECNOLOGICA RENDE POSSIBILE OGGI NAVIGARE NEL "DARKWEB" ANCHE TRAMITE "SMARTPHONE" E "TABLET" UTILIZZANDO APPOSITE "APP" SPECIFICHE PER "IOS" E "ANDROID", COME AD ES. "ORBOT", CHE, OPPORTUNAMENTE CONFIGURATE, CONSENTONO DAGLI APPARATI "MOBILE" L'ACCESSO A QUESTO SPAZIO VIRTUALE NASCOSTO.

QUESTA CIRCOSTANZA RENDERA' NELL'IMMINENTE FUTURO LA NAVIGAZIONE DELLA "DARKNET" UN'OPERAZIONE SEMPLICE E ALLA PORTATA DI TUTTI, CON UN INCREMENTO ESPONENZIALE DELL'UTENZA DI

13

FRUITORI, SOPRATTUTTO GIOVANI, CHE ANDRANNO AD ALIMENTARE UN MERCATO NEBULOSO, OGGI ANCORA IRRILEVANTE IN TERMINI NUMERICI, MA POTENZIALMENTE MOLTO PERICOLOSO, SOPRATTUTTO SE SI GUARDA ANCHE ALLA SEMPRE MAGGIORE FAMILIARITA' DEGLI INTERNAUTI CON LE VALUTE VIRTUALI.

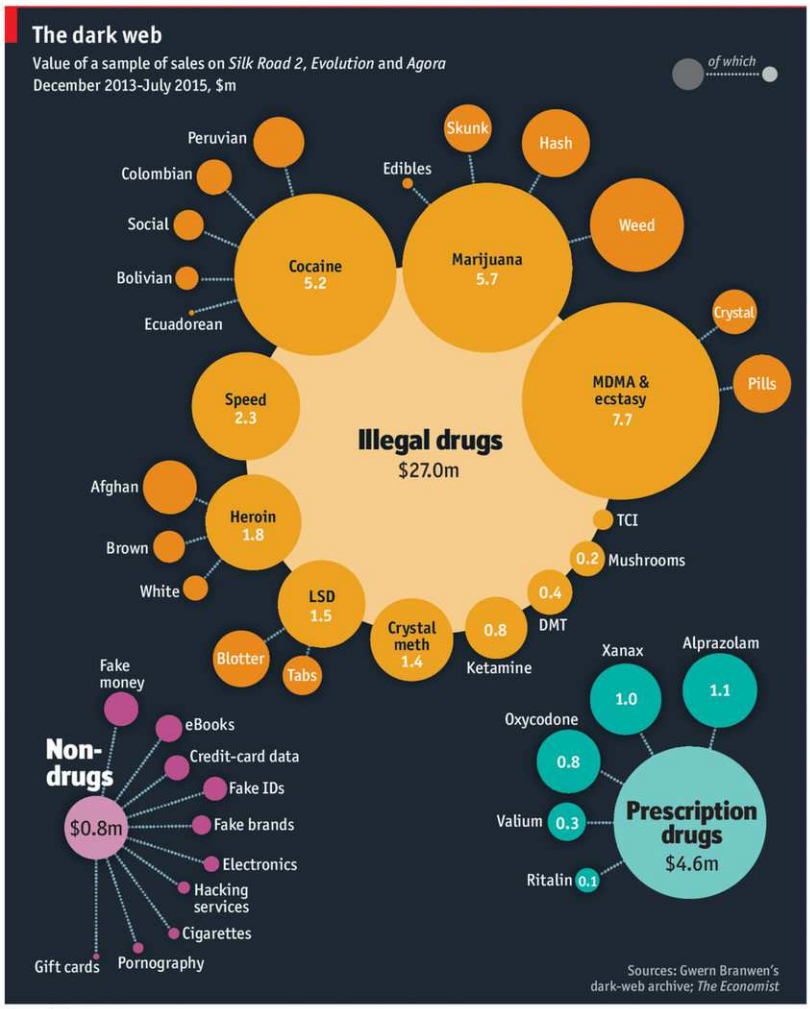
PER FAR MEGLIO COMPRENDERE ALCUNI ASPETTI DI QUESTA PARTICOLARE PORZIONE DELLE RETE, VALE LA PENA CITARE UNO STUDIO, POI RIPRESO DA "IL SOLE 24 ORE", DI COLAS CHRISTIN, RICERCATORE DELLA "CARNEGIE MELLON UNIVERSITY", CHE HA PROVATO A MISURARE IL FATTURATO DI "SILK ROAD", UNO DEI PIU' FAMOSI BAZAR DI VENDITA DELLE DROGHE NELLA "DARKNET", CHIUSO NEL 2014 DALL'FBI.

DOPO OTTO MESI DI RICERCHE, CON PIU' DI 24.000 ARTICOLI PASSATI AL SETACCIO, IL RICERCATORE HA CALCOLATO CHE IL BUSINESS TOTALE REALIZZATO DA TUTTI I VENDITORI SI AGGIRAVA A POCO PIÙ DI 1,2 MILIONI DI DOLLARI AL MESE, CON RITORNO IN COMMISSIONI PER I GESTORI DI "SILK ROAD" PER 92 MILA DOLLARI.

UN'ANALISI DI "ECONOMIST" SU PIU' DI UN 1,6 TB DI DATI RECUPERATI SU "SILK ROAD" ATTRAVERSO ATTIVITÀ DI "SCRAPING" (RACCOLTA MASSIVA DI DATI), HA PERMESSO DI MAPPARE BEN 360 MILA VENDITE PER UN VALORE CHE GIRA INTORNO AI 50 MILIONI DI DOLLARI, TANTO DA STIMARE, SE SI RESTA NELL'AMBITO DELLE DROGHE, UN TURNOVER CHE VA DAI 150 E I 180 MILIONI DI DOLLARI.

DI SEGUITO UNA IMMAGINE CHE SINTETIZZA I RISULTATI DI TALE ATTIVITA' DI RICERCA.

14



DUNQUE, DATI CHE CONFERMANO COME QUESTO MERCATO STIA ASSUMENDO UN CERTO PESO NELL'AMBITO DELLE FONTI DI FINANZIAMENTO DELLE ORGANIZZAZIONI CRIMINALI A LIVELLO MONDIALE, SEPPUR ANCORA CARATTERIZZATO DA TALUNE SPECIFICHE FORME DI ILLECITO E FORTEMENTE COLLEGATO ALLA DIFFUSIONE DELLE MONETE VIRTUALI ANONIME.

D. CRYPTOVALUTE

DA QUANTO FIN QUI EMERSO, APPARE CHIARO CHE LA QUASI TOTALITÀ DELLE TRANSAZIONI "COMMERCIALI" CHE AVVENGONO NEL DARK WEB SONO REMUNERATE CON VALUTE VIRTUALI CHE OFFRONO AMPIE GARANZIE DI ANONIMATO.

TUTTAVIA, LA MODALITA' DI PAGAMENTO, ANCORA ABBASTANZA MACCHINOSA, IN QUANTO SUBORDINATA AL POSSESSO A PRIORI DI UN PORTAFOGLIO VIRTUALE (C.D. "E-WALLET"), LIMITA ANCORA LA DIFFUSIONE DELLO STRUMENTO TRA L'UTENZA MEDIA DEI NAVIGANTI.

INIZIALMENTE, LA MONETA DI SCAMBIO UTILIZZATA QUASI IN MODO ESCLUSIVO NEL DARKWEB ERA IL **BITCOIN**, GRAZIE ANCHE ALL'ELEVATO STANDARD DI ANONIMATO GARANTITO.

MA LA PRIVACY E SICUREZZA FIN QUI RICONOSCIUTA AGLI UTILIZZATORI, VENGONO OGGI CONSIDERATE MINACCIATE DALLE NUOVE TECNICHE DI TRACCIAMENTO, SEPPUR NON SEMPRE EFFICACI, SVILUPPATE DA INTELLIGENCE GOVERNATIVA E OPERATORI DI POLIZIA.

IL SISTEMA CHE STA ALLA BASE DELLE TRANSAZIONI BITCOIN FA SÌ CHE ESSE SIANO CONCATENATE IN UN ARCHIVIO PUBBLICO PERMANENTE, LA C.D. "BLOCKCHAIN"[3], CHE CONSENTE DI RICOSTRUIRE LO STORICO DELLE OPERAZIONI RIFERITE A UN SINGOLO "E-WALLET".

TUTTAVIA, ESISTONO SERVIZI DI RIPULITURA DEI BITCOIN, DENOMINATI "MIXER", I QUALI SONO IN GRADO DI MISCELARE E PARCELLIZZARE I FLUSSI DI SCAMBIO AL FINE DI RENDERLI DEL TUTTO NON RINTRACCIABILI O, COMUNQUE, NON ASSOCIABILI A UN DETERMINATO "E-WALLET".

RECENTEMENTE, PROPRIO IN RAGIONE DELL'AFFINAMENTO DELLE TECNICHE INVESTIGATIVE, STA PRENDENDO PIEDE NEL MERCATO DEL "DARKWEB" UN'ALTRA CRIPTOMONETA, PRESENTE IN RETE GIÀ DAL 2014,

[3] La blockchain è un registro delle transazioni, pubblico e condiviso, cui si affida l'intera rete Bitcoin. Tutte le transazioni confermate vengono incluse nella blockchain senza nessuna eccezione. In questo modo si può verificare che chi esegue una nuova transazione impieghi dei Bitcoin effettivamente posseduti. La crittografia è impiegata per mantenenre integrità ed ordine cronologico della blockchain.

DENOMINATA "**MONERO"**, CHE PER IL SUO SISTEMA DI FUNZIONAMENTO, ASSICURA, ALLO STATO ATTUALE, L'ASSOLUTO ANONIMATO.

IL MONERO, INFATTI, A DIFFERENZA DEL BITCOIN, UTILIZZA UN DIVERSO PROTOCOLLO, CHIAMATO CRYPTONOTE, IL QUALE PRESENTA UNA BLOCKCHAIN CHE CONTIENE TUTTE LE TRANSAZIONI EFFETTUATE SINO AD UN DETERMINATO MOMENTO, MA IN QUESTO CASO I MITTENTI E I DESTINATARI DELLE TRANSAZIONI RIMANGONO ANONIMI. LE UNICHE PERSONE CHE HANNO ACCESSO A TUTTE LE INFORMAZIONI SONO SOLO CHI INVIA E CHI RICEVE IL DENARO PER QUELLA TRANSAZIONE.

IN RETE SONO GIÀ PRESENTI OLTRE 700 CRYPTOMONETE E PERIODICAMENTE NE NASCONO DI NUOVE, CIASCUNA CON LE PROPRIE CARATTERISTICHE. L'ULTIMA NATA, NEL 2016, È LO "**ZCASH"**, UNA CRIPTOMONETA CHE, IN TERMINI DI CAPITALIZZAZIONE, AVREBBE GIÀ RAGGIUNTO UN VOLUME PARI AD OLTRE 20 MILIONI DI DOLLARI, ATTESTANDOSI AL 18 POSTO NELLA GRADUATORIA CHE VEDE IN TESTA IL "**BITCOIN"** CON OLTRE 16 MILIARDI DI DOLLARI ED AL QUINTO POSTO "**MONERO**" CON OLTRE 170 MILIONI DI DOLLARI.

VA, TRA L'ALTRO, CONSIDERATO CHE ESISTE LA POSSIBILITÀ IN RETE DI CONVERTIRE UNA CRYPTOVALUTA IN UN'ALTRA. TALE SERVIZIO È, CHIARAMENTE E FORTEMENTE, UTILIZZATO DA CHI INTENDE MASCHERARE E/O NASCONDERE FLUSSI FINANZIARI DI PROVENIENZA SOSPETTA.

NON È POI DA ESCLUDERE LA POSSIBILITÀ CHE QUESTE MONETE VIRTUALI UTILIZZATE NEL "DARK WEB" VERRANNO NEL TEMPO SUPERATE DA ALTRI STRUMENTI DI PAGAMENTO, IN UNA RINCORSA SENZA FINE, IN RAGIONE DELL'EVOLUZIONE DELLE TECNOLOGIE CHE PORTERA' AD INDEBOLIRE GLI ATTUALI STANDARD DI RISERVATEZZA DI TALUNE A VANTAGGIO DI ALTRE.

E. BREVI CONSIDERAZIONI

IN CONCLUSIONE, LE CARATTERISTICHE PROPRIE DELLA RETE NASCOSTA, ASSOCIATE A FORME DI PAGAMENTO ANONIMIZZATE, COME NEL CASO DELLE CRYPTOVALUTE, RENDONO I MERCATI DEL DARK WEB DIFFICILMENTE CONTROLLABILI, COSI' DA RICHIEDERE, ANCHE DA PARTE DELLE AUTORITÀ DI LAW ENFORCEMENT, UNA PROFESSIONALITA' SPECIFICA CHE SI RAPPORTI NEL TEMPO CON L'EVOLUZIONE TECNOLOGICA. E' QUESTO UN PERCORSO OBBLIGATO, CHE STA PORTANDO, COME VEDREMO, AD UNA SEMPRE MAGGIORE COOPERAZIONE E SCAMBIO DI ESPERIENZE TRA TUTTI GLI ATTORI IN CAMPO.

3. RUOLO DELLA GUARDIA DI FINANZA A PRESIDIO DEL CONTESTO DIGITALE

A. GENERALITA'

LA PRESA DI COSCIENZA DELLE GRAVI MINACCE CHE DERIVANO DALL'UTILIZZO ILLECITO DELLE NUOVE TECNOLOGIE HA PORTATO LA GUARDIA DI FINANZA A RAFFORZARE IL DISPOSITIVO DI CONTRASTO ALLE CONSEGUENTI CONDOTTE CRIMINALI CHE IMPATTANO SUL TESSUTO ECONOMICO E FINANZIARIO, PERALTRO IN CONTINUA EVOLUZIONE.

IN TALE QUADRO, L'ATTIVITA' SVOLTA DAL CORPO SI DECLINA, IN RAGIONE DEI POTERI AD ESSA ATTRIBUITI, IN ATTI DI POLIZIA TRIBUTARIA, AMMINISTRATIVA E GIUDIZIARIA, ESTESI AD AMBITI SEMPRE PIU' DIVERSIFICATI SUL PIANO TECNOLOGICO E TERRITORIALE, COPRENDO, NELLO SPECIFICO, LA RETE INTERNET E PIU' IN GENERALE LE TECNOLOGIE E SUPERANDO, SEMPRE PIU' SPESSO, LA SOGLIA DEI CONFINI NAZIONALI IN COOPERAZIONE CON I PAESI ADERENTI ALLE DIVERSE ORGANIZZAZIONI INTERNAZIONALI PREVISTE DA SINGOLI TRATTATI O CONVENZIONI.

LA GUARDIA DI FINANZA, IN OGNI SUA ESPRESSIONE OPERATIVA, SI MUOVE SEMPRE TRASVERSALMENTE NELL'AMBITO DELLA MISSIONE ISTITUZIONALE DI POLIZIA ECONOMICO-FINANZIARIA CHE GLI È AFFIDATA ATTRAVERSO UN APPROCCIO PER SUA NATURA MULTIDISCIPLINARE.

18

I MODULI D'AZIONE, ANCHE NELLE INVESTIGAZIONI CHE IMPATTANO CON IL MONDO DIGITALE, SONO, QUINDI, CONTESTUALMENTE ORIENTATI:

- AL CONTROLLO ECONOMICO DEL TERRITORIO VIRTUALE, ATTRAVERSO IL **MONITORAGGIO DELLA RETE TELEMATICA, ANCHE NASCOSTA**, PER VERIFICARE L'ESISTENZA DI SACCHE D'ILLEGALITÀ E AD INTERCETTARE I FLUSSI FINANZIARI "SOSPETTI", ANCHE MEDIANTE LA TECNICA CD."**FOLLOW THE MONEY**" O, DA ULTIMO, CD."**FOLLOW THE HOSTING**";
- A VERIFICARE LA POSIZIONE FISCALE DEI SOGGETTI INVESTIGATI PER L'EVENTUALE TASSAZIONE DEI PROVENTI LECITI ED ILLECITI SOTTRATTI ALL'IMPOSIZIONE;
- AD INTERVENIRE, TRASVERSALMENTE, SU ALTRI PROFILI DI RILIEVO, QUALI, AD ESEMPIO, QUELLI IN MATERIA DI REATI CONTRO LA PUBBLICA AMMINISTRAZIONE, VALUTA E MEZZI DI PAGAMENTO, PRIVATIVA INTELLETTUALE E SICUREZZA PRODOTTI, CONCORRENZA E MERCATO, PRIVACY E SICUREZZA DELLE COMUNICAZIONI.

LE INIZIATIVE AVVIATE DALLE UNITÀ OPERATIVE DELLA GUARDIA DI FINANZA SI BASANO, OGGI, SEMPRE PIÙ SU UNA STRETTA E CONTINUA INTERAZIONE TRA LE DIVERSE COMPONENTI DEL CORPO, NELL'OTTICA DI SVILUPPARE SINERGIE CHE DIANO CONCRETA ATTUAZIONE A QUELL'APPROCCIO TRASVERSALE E MULTIDISCIPLINARE TIPICO DELLA POLIZIA ECONOMICO-FINANZIARIA, IN GRADO DI INCIDERE PIU' PROFONDAMENTE SULLE CONDOTTE CRIMINALI E CIO' COSTITUISCE UN "UNICUM" NEL PANORAMA MONDIALE.

IN LINEA CON TALE INDIRIZZO, ANCHE NEL CONTRASTO AGLI ILLECITI DI CARATTERE ECONOMICO E FINANZIARIO REALIZZATI SU INTERNET, OVVERO PER MEZZO DI DISPOSITIVI TECNOLOGICI, IL CORPO INTERVIENE ATTRAVERSO DUE DIRETTRICI CHE SONO IN CONTINUO CONTATTO FUNZIONALE TRA LORO:

- LA RETE DEI **REPARTI TERRITORIALI**, CAPILLARMENTE DISTRIBUITI SUL

TERRITORIO NAZIONALE, CON IL COMPITO DI ASSICURARE, NEI RISPETTIVI AMBITI, L'EFFICIENTE TUTELA DI TALI FUNZIONI. TRA QUESTI I NUCLEI DI POLIZIA TRIBUTARIA, ULTERIORMENTE RAFFORZATI DA SPECIFICHE PROFESSIONALITA', SI PONGONO COME UNITÀ INVESTIGATIVE DI PUNTA;

- I **REPARTI SPECIALI** CHE SI AFFIANCANO AI PRIMI E CHE, ISTITUITI PER L'INVESTIGAZIONE IN SPECIFICHE MATERIE, SONO INCARICATI DI REALIZZARE DIRETTAMENTE, OVVERO CON AZIONI DI SUPPORTO ALLE UNITÀ OPERATIVE, MODULI INVESTIGATIVI CONNOTATI DA ELEVATI STANDARD QUALITATIVI.

QUESTI ULTIMI, PROPRIO IN RAGIONE DELLA SEMPRE MAGGIORE COMPLESSITA' DEI FENOMENI CRIMINALI, ASSUMONO UN RUOLO FONDAMENTALE, E DIREI QUASI INDISPENSABILE, NELLA STRATEGIA DI CONTRASTO A TALE TIPOLOGIA DI ILLECITI ATTRAVERSO:

(1) L'ANALISI OPERATIVA, NELLA DUPLICE PROIEZIONE DI:

(A) ANALISI DI CONTESTO E/O DI RISCHIO, CON RIFERIMENTO A SETTORI CONSIDERATI NEL LORO COMPLESSO, PER DELINEARNE L'EVOLUZIONE E RILEVARNE I FATTORI E/O I SOGGETTI DI INTERESSE AI FINI OPERATIVI. IN TAL SENSO, INDIVIDUANO LE TENDENZE E LE DINAMICHE DEI FENOMENI ILLECITI, LE RELATIVE TIPOLOGIE, I SOGGETTI;

(B) ANALISI FINALIZZATA ALL'ELABORAZIONE DI DATI D'INTELLIGENCE, CONFRONTANDO LE RISULTANZE DI PIÙ INDAGINI, ONDE FAR EMERGERE ELEMENTI COMUNI, IDONEI A RILANCIARE, OVVERO AD AVVIARE SUL TERRITORIO ATTIVITÀ DI SERVIZIO;

(2) LA PREDISPOSIZIONE DI "PROGETTI OPERATIVI", VALE A DIRE SPECIFICI E DETTAGLIATI PIANI DI ATTIVITÀ, IN LINEA CON LE DIRETTIVE STRATEGICHE, DA REALIZZARE ATTRAVERSO L'IMPIEGO CONGIUNTO DI RISORSE DELLE COMPONENTI SPECIALE E TERRITORIALE;

(3) IL RACCORDO OPERATIVO CON AUTORITÀ, ENTI ED ISTITUZIONI DI RIFERIMENTO NEL PROPRIO SETTORE, PER ORIENTARE/INNESCARE ATTIVITÀ DI SERVIZIO;

(4) LO SVILUPPO DELL'ANALISI TATTICA - INTESA COME ANALISI D'INTELLIGENCE RELATIVA A SINGOLE OPERAZIONI - NELL'AMBITO DI PROGETTI, DI ATTIVITÀ ESECUTIVE DI COMPETENZA O A SUPPORTO DELLA COMPONENTE TERRITORIALE;

(5) IL SUPPORTO DI CONOSCENZE, ACQUISENDO ED AGGIORNANDO COSTANTEMENTE UN PATRIMONIO CONOSCITIVO E TECNICO SPECIALISTICO UTILE ALL'AZIONE DI TUTTI I REPARTI. IN TAL SENSO, ELABORANO PIATTAFORME DI SERVIZI FRUIBILI NELL'ESECUZIONE DI ATTIVITÀ COMPLESSE, FORNENDO ALTRESÌ IL NECESSARIO SUPPORTO NELLO SVILUPPO DI RELAZIONI INTERISTITUZIONALI;

(6) L'ATTIVITÀ DI ESECUZIONE, QUANDO ESPRESSAMENTE PREVISTO, CON RIFERIMENTO AD AMBITI OPERATIVI CHE, PER VINCOLO NORMATIVO O PER LA STRUTTURAZIONE DEI PROCESSI DI LAVORO, NON DETERMINANO SOVRAPPOSIZIONI CON I REPARTI TERRITORIALI;

(7) L'ESERCIZIO DELLA DIREZIONE OPERATIVA, CHE SI SOSTANZIA NELLA DELEGA DI FUNZIONI PROPRIE O DI ATTIVITÀ CONNESSE AD INCARICHI RICEVUTI DA ORGANI ESTERNI, CANALIZZANDO IL CORRISPONDENTE FLUSSO DI RITORNO;

(8) IL SUPPORTO TECNICO-LOGISTICO, PONENDO A DISPOSIZIONE DEI REPARTI TERRITORIALI CHE LO RICHIEDANO MEZZI DI TECNOLOGIA AVANZATA E PERSONALE IN POSSESSO DI SPECIFICHE CONOSCENZE PROFESSIONALI E/O TECNICHE.

VISTI GLI ARGOMENTI TRATTATI, CI SOFFERMEREMO PIU' NEL DETTAGLIO SULLE ATTIVITA' DEL **NUCLEO SPECIALE TUTELA PROPRIETÀ INTELLETTUALE** E DEL **NUCLEO SPECIALE FRODI TECNOLOGICHE**, LE CUI ATTRIBUZIONI E STRUTTURE ORDINATIVE SARANNO MEGLIO DESCRITTE PIU' AVANTI.

ALTRI NUCLEI CHE INTERVENGONO, "RATIONE MATERIAE", IN TALE AMBITO SONO:

- **NUCLEO SPECIALE PER LA RADIODIFFUSIONE E L'EDITORIA**, REFERENTE PER IL CORPO CON L'AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI, CURA, TRA L'ALTRO, LE ATTIVITÀ DI SERVIZIO IN MATERIA DI VIOLAZIONI AL DIRITTO D'AUTORE "ON-LINE";
- **NUCLEO SPECIALE ANTITRUST**, REFERENTE PER IL CORPO CON L'AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO PER L'ESERCIZIO DELLE COMPETENZE AD ESSA AFFIDATE, TRA LE QUALI EVIDENZIO LA TUTELA DEL CONSUMATORE, CHE HA COMPORTATO INIZIATIVE OPERATIVE ANCHE NELLE NUOVE FORME DI COMMERCIO ABUSIVO ON-LINE E, SIA PUR INDIRETTAMENTE, AL CONTRASTO DELLA CONTRAFFAZIONE "ON LINE";
- **NUCLEO SPECIALE PRIVACY,** REFERENTE PER IL CORPO CON L'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, SVILUPPA LA SUA AZIONE OPERATIVA A PROTEZIONE DEI DATI PERSONALI.

AD OGNI BUON CONTO, VALE LA PENA DI SOTTOLINEARE, GIA' IN QUESTA FASE, COME L'ESPERIENZA MATURATA IN QUESTI ANNI DALLE UNITA' SPECIALI IN SCENARI OPERATIVI COMPLESSI ABBIA DIMOSTRATO L'ASSOLUTO VALORE AGGIUNTO CHE DERIVA DALLE SINERGIE INVESTIGATIVE E PROFESSIONALI OTTENUTE DALL'IMPIEGO DI PATTUGLIE MISTE DI PERSONALE IN FORZA AI DIVERSI NUCLEI SPECIALI.

IN QUESTO SENSO, DIVENTA FONDAMENTALE IL RUOLO DI INDIRIZZO, DIREZIONE E CONTROLLO DEL COMANDO UNITA' SPECIALI CHE, VERIFICATA LA POSSIBILITA' DI FORMARE UNITA' MISTE TRA LE COMPONENTI SPECIALI, SI ATTIVA SUBITO PER AVVIARE QUELLA FASE DI COORDINAMENTO E RACCORDO NECESSARIA PER L'ECONOMIA DEL SERVIZIO E IL PIU' PROFICUO IMPIEGO DELLE PROFESSIONALITA' DISPONIBILI.

CIO' HA PERMESSO DI OTTENERE, IN NUMEROSE OPERAZIONI DI SERVIZIO, MAGGIORE PENETRAZIONE INFORMATIVA ED UNA PIU' QUALIFICATA AZIONE INVESTIGATIVA IN RAGIONE DELLE SPECIFICHE COMPETENZE MESSE IN CAMPO DA CIASCUN MILITARE, SOPRATTUTTO SE SI TIENE CONTO DEGLI INNUMEREVOLI PROFILI CHE SONO RICONDUCIBILI A CONTESTI OPERATIVI FORTEMENTE CARATTERIZZATI DA APPARECCHIATURE ELETTRONICHE O STRUMENTAZIONI INTERCONNESSE.

A TAL RIGUARDO, IL PRESIDIO DEL CORPO TROVA ULTERIORI RAGIONI DI INTERESSE ANCHE PER UN AREA DI INTERVENTO NUOVA E DIFFICILE COME QUELLA DEL "DEEP WEB" E DELLA "DARKNET", AGEVOLE TERRENO DI PROFITTO PER LE CONSORTERIE CRIMINALI.

B. AZIONE OPERATIVA DELLE UNITA' SPECIALI

UN QUADRANTE OPERATIVO COSI' COMPLESSO IMPONE, COME ABBIAMO GIA' AVUTO MODO DI DIRE, UNA COSTANTE AZIONE DI INNOVAZIONE TECNOLOGICA E PROFESSIONALE, CAPACE DI CORRISPONDERE CON RAPIDITA' ED EFFICACIA ALLE REPENTINE MUTAZIONI DELLE AREE DI SERVIZIO DA PRESIDIARE.

LA GUARDIA DI FINANZA È NATURALMENTE PREDISPOSTA, IN VIRTÙ DEI PROPRI COMPITI ISTITUZIONALI, ALL'ESECUZIONE DI COMPLESSE ANALISI ECONOMICO-FINANZIARIE NELL'AMBITO DI SCENARI INVESTIGATIVI COSI' ARTICOLATI, CARATTERIZZATI DALLA COSTANTE INTERAZIONE TRA SOGGETTI, OPERAZIONI ECONOMICHE E TRANSAZIONI FINANZIARIE. NE SONO TESTIMONIANZA CONCRETA LE OPERAZIONI "TORRE D'AVORIO" (TRANSAZIONI FINANZIARIE CON SAN MARINO DI MIGLIAIA DI SOGGETTI) E "PANAMA PAPERS" (SOGGETTI CON DISPONIBILITA' FINANZIARIE A PANAMA), CHE VEDONO ANCOR OGGI OPERARE UNITA' INTEGRATE, COMPOSTE DA PERSONALE DI PIU' NUCLEI SPECIALI, CHE SVOLGONO ANALISI MASSIVE A MEZZO DI SPECIFICI SOFTWARE SU BASE DATI

COMPLESSE CAPACI DI AFFINARE ALCUNE POSIZIONI DA SVILUPPARE OPERATIVAMENTE.

LE STESSE METODOLOGIE VENGONO PROFICUAMENTE APPLICATE ANCHE A QUESTO PARTICOLARE SETTORE CRIMINALE, IN RAGIONE DELLA SPECIFICA PROFESSIONALITA' CHE POSSONO METTERE IN CAMPO LE UNITA' SPECIALI, SOPRATTUTTO LADDOVE EMERGANO ASPETTI ECONOMICO-FINANZIARI CHE PERMETTONO DI ESALTARE SPECIFICHE ESPERIENZE MATURATE IN QUESTO SEGMENTO, SECONDO MODELLI DI INTERVENTO AMPIAMENTE COLLAUDATI.

SI TRATTA DI RIPRODURRE SUL WEB, FATTI SALVI I DOVUTI DISTINGUO, QUEL "KNOW HOW" INVESTIGATIVO MULTIDISCIPLINARE MATURATO DAL CORPO IN TUTTI I SETTORI DELLA PROPRIA "MISSION" ISTITUZIONALE.

IN TAL SENSO, SI E' PROVVEDUTO ALL'ADOZIONE O SVILUPPO DI SISTEMI TECNOLOGICI APPROPRIATI E ALLA PARAMETRAZIONE DELLE CLASSICHE METODOLOGIE OPERATIVE IN RAGIONE DEL CONTRASTO DEI FENOMENI ILLECITI PERPETRATI SUL WEB O ATTRAVERSO L'USO DI APPARATI INFORMATICI.

FONDAMENTALI PER QUESTO OBIETTIVO SONO ALCUNI STRUMENTI E PIATTAFORME A SUPPORTO DELL'ATTIVITÀ DI INTELLIGENCE, TRA CUI:

- MOTORI DI RICERCA SEMANTICA OPERANTI SU FONTI APERTE FINALIZZATI ALL'INDIVIDUAZIONE DI TARGET OPERATIVI;
- SISTEMI DI ANALISI VISUALE DELLE INFORMAZIONI E DELLE RELAZIONI TRA ENTITÀ;
- LINEE-DATI APPOSITAMENTE CONFIGURATE PER L'ACCESSO AD INTERNET SENZA RESTRIZIONI E IN FORMA ANONIMA, PER IL MONITORAGGIO DEI SOCIAL NETWORK E DI ALTRE PIATTAFORME, INCLUSE QUELLE PRESENTI NEL "DEEP WEB" E NELLA "DARKNET".

TUTTO QUESTO RICHIEDE, OVVIAMENTE, UN COSTANTE AGGIORNAMENTO PROFESSIONALE, ANCHE ATTRAVERSO IL CONTINUO CONFRONTO CON OMOLOGHE STRUTTURE DI "LAW ENFORCEMENT" NAZIONALI ED ESTERE,

CENTRI RICERCHE, MONDO ACCADEMICO, ASSOCIAZIONI DI CATEGORIA, PRINCIPALI OPERATORI ECONOMICI IN MATERIA DI TECNOLOGIE E SICUREZZA DELLE COMUNICAZIONI.

VALE LA PENA DI ACCENNARE AL CONTRIBUTO FORNITO DAL NUCLEO SPECIALE FRODI TECNOLOGICHE PER LA REALIZZAZIONE DEL RAPPORTO SULLA SICUREZZA ICT IN ITALIA PER IL 2016 FORNITO ALL'ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA DELL'UNIVERSITÀ DEGLI STUDI DI MILANO – CLUSIT, ALLA PARTECIPAZIONE ATTIVA A NUMEROSI PROGETTI FINANZIATI DALL'UNIONE EUROPEA UNITAMENTE AD ISTITUZIONI INTERNAZIONALI, UNIVERSITA', FORZE DI POLIZIA ESTERE, ASSOCIAZIONI DELLE IMPRESE E DEI CONSUMATORI PRINCIPALI PLAYER TECNOLOGICI MONDIALI.

NUMEROSE POI SONO LE PARTECIPAZIONI DELLE UNITA' SPECIALI A:

- TAVOLI DI LAVORO INTERFORZE A LIVELLO NAZIONALE E INTERNAZIONALE (PRINCIPALMENTE PRESSO INTERPOL, EUROPOL, ORGANIZZAZIONE MONDIALE DELLE DOGANE, COMMISSIONE UE, OLAF);
- OPERAZIONI CONGIUNTE TRASNAZIONALI DI PARTICOLARE RESPIRO CHE TOCCANO I PRINCIPALI SETTORI OPERATIVI, QUALI IL CRIMINE ORGANIZZATO, IL RICICLAGGIO, IL FINANZIAMENTO AL TERRORISMO, L'USO INDEBITO DEI MEZZI DI PAGAMENTO, LA CONTRAFFAZIONE, LA PIRATERIA DIGITALE, LA SICUREZZA PRODOTTI E LA TUTELA DEL CONSUMATORE, IL CONTRABBANDO E LA VENDITA DI FARMACI;
- PRESENZE QUALIFICATE, IN ITALIA E ALL'ESTERO, AD EVENTI FORMATIVI, WORKSHOP, VISITE ISTITUZIONALI, CONVEGNI, MANIFESTAZIONI FIERISTICHE, QUALI UTILI MOMENTI DI CONFRONTO, AGGIORNAMENTO E SCAMBIO DI ESPERIENZE TRA ADDETTI AI LAVORI, OLTRE CHE OCCASIONE PER MIGLIORARE I RAPPORTI INTER-ISTITUZIONALI.

25

C. NUCLEO SPECIALE TUTELA PROPRIETA' INTELLETTUALE

È STATO GIA' SOTTOLINEATO PIU' VOLTE, IN OCCASIONE DELL'AUDIZIONI DEL FEBBRAIO E SETTEMBRE 2016, COME INTERNET, PER LE SUE CARATTERISTICHE DI RETE GLOBALE, BEN SI PRESTA ALLA DIFFUSIONE DELLA CONTRAFFAZIONE, DEL COMMERCIO ABUSIVO E DELLA PIRATERIA DIGITALE, CON TUTTE LE FACILITAZIONI DERIVANTI DALLA POSSIBILITÀ DI ANONIMIZZARE LE OPERAZIONI, RENDENDO LE INVESTIGAZIONI PIÙ ARTICOLATE E GRAVOSE; TALCHÉ, SUL PIANO REPRESSIVO, IL CONTRASTO ALL'USO ILLECITO DEL WEB RICHIEDE UN'ALTISSIMA COMPETENZA INFORMATICA ED ANCHE UNA FATTIVA ED INDISPENSABILE COLLABORAZIONE INTERNAZIONALE.

CON L'ESPANSIONE DEI SOCIAL NETWORK, MA SOPRATTUTTO CON LA DIFFUSIONE DEI DISPOSITIVI "MOBILE", HANNO AVUTO UNA RAPIDA CRESCITA ALTRE MODALITA' DI PROCACCIAMENO O FIDELIZZAZIONE DEI CLIENTI, FINALIZZATE AD INVOGLIARE GLI UTENTI DELLA RETE A CONSULTARE TALUNI SITI CONTRAFFATTIVI.

IN QUESTE PIATTAFORME (TRA LE PIÙ NOTE FACEBOOK, INSTAGRAM, TWITTER, WHATSAPP ETC.) SONO SPESSO PUBBLICIZZATI INDIRIZZI DI RISORSE WEB DEDICATE A TALE VENDITA ILLECITA O, ADDIRITTURA, PROMOSSE DELLE VERE E PROPRIE "SUCCURSALI" DEL MERCATO DEL "FALSO" ATTRAVERSO LA CREAZIONE DI GRUPPI CHIUSI O RETI INTERCONNESSE DI PERSONE.

UN'AMPIA PARTE, POI, E' STATA DEDICATA ALLA DESCRIZIONE DELLE MODALITA' DI INTERVENTO OPERATIVO A CONTRASTO DELLA CONTRAFFAZIONE E PIRATERIA SUL WEB, CHE VEDE INTERAGIRE, CIASCUNO IN VIRTU' DELLE PROPRIE COMPETENZE E PROFESSIONALITA', LE DIVERSE UNITA' SPECIALI.

IN TALE AMBITO SI INSERISCE IL **NUCLEO SPECIALE TUTELA PROPRIETÀ INTELLETTUALE** DELLA GUARDIA DI FINANZA, REPARTO CHE ESPLICA LA PROPRIA ATTIVITÀ DI SERVIZIO A TUTELA DI MARCHI, BREVETTI E ALTRI

DIRITTI DI PRIVATIVA INDUSTRIALE, SICUREZZA E CONFORMITÀ DEI PRODOTTI, PIRATERIA AUDIOVISIVA E INFORMATICA, REATI CONTRO L'ECONOMIA PUBBLICA, L'INDUSTRIA E IL COMMERCIO.

AL SUO INTERNO, DAL 1 GENNAIO 2014, È ATTIVO IL "**S.I.A.C." (SISTEMA INFORMATIVO ANTI-CONTRAFFAZIONE)**, NOTO A QUESTA COMMISSIONE PARLAMENTARE D'INCHIESTA PER AVERLO VISITATO IN DATA 13 LUGLIO 2016.

INOLTRE, PER POTENZIARE E RENDERE PIÙ EFFICACE IL REPERIMENTO DI INFORMAZIONI DALLA RETE E LA SUCCESSIVA ANALISI, IL CORPO SI STA DOTANDO DI NUOVI SOFTWARE CHE AGEVOLERANNO LA RICERCA E L'ESTRAZIONE DI DATI E NOTIZIE DAL WEB E LA LORO INTERPRETAZIONE IN CHIAVE INVESTIGATIVA, MEDIANTE IL RICORSO ANCHE AD EFFICIENTI STRUMENTI DI VISUALIZZAZIONE GRAFICA DELLE RELAZIONI CHE SARÀ POSSIBILE RICOSTRUIRE TRA LE VARIE ENTITÀ EMERSE.

CERTAMENTE LA PIÙ IMPORTANTE È LA PIATTAFORMA DENOMINATA "**COLIBRÌ**", STRUTTURATA PER FORNIRE PREZIOSI SUGGERIMENTI ED INDICAZIONI OPERATIVE.

D. NUCLEO SPECIALE FRODI TECNOLOGICHE

IL SEMPRE MAGGIORE UTILIZZO DI RISORSE E DISPOSITIVI TECNOLOGICI PER COMPIERE ILLECITI DI VARIA NATURA OD OCCULTARE LE PROVE E/O I PROVENTI DELLE ATTIVITÀ CRIMINOSE E LA PROGRESSIVA DIGITALIZZAZIONE DI AMBIENTI E STRUMENTI DI LAVORO HANNO RESO NECESSARIO, COME DETTO, IL POTENZIAMENTO DELLE STRUTTURE DEL CORPO DEPUTATE ALLA PREVENZIONE ED AL CONTRASTO DI TALI FENOMENOLOGIE ILLECITE.

INOLTRE, NELL'ESECUZIONE DELLE ATTIVITÀ INVESTIGATIVE, DIVENTA SEMPRE PIU' NECESSARIO L'ESAME DEGLI APPARATI E DEI SISTEMI INFORMATICI O DI COMUNICAZIONE IN DOTAZIONE ALLE PERSONE, OVVERO AI SOGGETTI INVESTIGATI, LA CUI ANALISI PUÒ CONSENTIRE

L'ACQUISIZIONE DI INFORMAZIONI O PROVE INDISPENSABILI PER L'ACCERTAMENTO DI EVENTUALI VIOLAZIONI.

A TAL FINE, NEL 2001, È STATO ISTITUITO IL **NUCLEO SPECIALE FRODI TECNOLOGICHE**, CHIAMATO AD OPERARE A SUPPORTO DELLE COMPONENTI SPECIALI E TERRITORIALI NEL CONTRASTO AGLI ILLECITI ECONOMICO-FINANZIARI PERPETRATI ATTRAVERSO LA RETE, FORNENDO, INOLTRE, AI REPARTI COMPETENTI, OGNI POSSIBILE SPUNTO INFORMATIVO SUSCETTIBILE DI SVILUPPO OPERATIVO A SEGUITO DELLA COSTANTE AZIONE DI MONITORAGGIO OPERATA SISTEMATICAMENTE IN TALE SEGMENTO OPERATIVO.

L'ATTUALE ASSETTO ORDINATIVO, CHE E' STATO RECENTEMENTE RAFFORZATO IN RAGIONE DELLA CRESCENTE MINACCIA, PREVEDE OGGI QUATTRO GRUPPI DI SEZIONE. NELLO SPECIFICO:

- IL I GRUPPO È DEPUTATO AD EFFETTUARE IL MONITORAGGIO DELLA RETE AI FINI DELLO SVILUPPO O PER L'AVVIO DI ATTIVITÀ OPERATIVE ANCHE DA PARTE DI ALTRI REPARTI DEL CORPO IN CASO DI REPERIMENTO DI INDIZI SINTOMATICI DI ILLECITI ECONOMICO-FINANZIARI REALIZZATI VIA WEB. L'ARTICOLAZIONE SVOLGE, ALTRESÌ, ATTIVITÀ DI ANALISI OPERATIVA, PIANIFICANDO SPECIFICI PROGETTI NEI SETTORI DI COMPETENZA;
- IL II ED IL III GRUPPO SONO INCARICATI DELL'IDEAZIONE, ORGANIZZAZIONE ED ESECUZIONE DIRETTA DI INVESTIGAZIONI NEI SETTORI DI COMPETENZA ISTITUZIONALE, NONCHÉ DI FORNIRE SUPPORTO TECNICO-LOGISTICO AI REPARTI DEL CORPO IMPEGNATI SUL TERRITORIO IN INVESTIGAZIONI CHE RICHIEDANO, PER LA PARTICOLARE DELICATEZZA E RILEVANZA, IL POSSESSO DI SPECIFICHE COMPETENZE NEL CAMPO INFORMATICO;
- IL IV GRUPPO È RIVOLTO ALLO SVILUPPO DI SISTEMI TECNOLOGICI E APPLICATIVI INFORMATICI DI AUSILIO ALLE INDAGINI, NONCHÉ ALLO STUDIO E ALL'INDIVIDUAZIONE DI METODOLOGIE OPERATIVE MAGGIORMENTE EFFICACI E, IN QUANTO TALI, UNIFORMEMENTE

APPLICABILI IN AMBITO NAZIONALE. A TAL FINE, INTRATTIENE LE NECESSARIE RELAZIONI ISTITUZIONALI.

IN TALE AMBITO, IL NUCLEO SPECIALE FRODI TECNOLOGICHE, SULLA BASE DELLE DIRETTIVE RICEVUTE, INDIRIZZA LA PROPRIA ATTIVITÀ INVESTIGATIVA SUL WEB PRIORITARIAMENTE NEI SEGUENTI SETTORI:

- AREA TUTELA DELLE ENTRATE:
  - STRUTTURE DI AGGRESSIVE TAX PLANNING;
  - RACCOLTA DI SCOMMESSE E GIOCHI ON-LINE.
- AREA TUTELA SPESA PUBBLICA:
  - FINANZIAMENTI PUBBLICI;
  - SPESA SANITARIA;
  - CONTRABBANDO TLE.
- AREA TUTELA DEL MERCATO:
  - ABUSIVA ATTIVITA' FINANZIARIA, BANCARIA, E DI SERVIZI/GESTIONE DI INVESTIMENTI.
- AREA CONTRASTO ALLA CRIMINALITÀ ORGANIZZATA
  - RICICLAGGIO DI DENARO;
  - FINANZIAMENTO AL TERRORISMO;
  - TRAFFICO D'ARMI E DI STUPEFACENTI;
  - CONTRAFFAZIONE E PIRATERIA.

LA NECESSITA' DI DISPORRE DI UNITA' D'INTERVENTO ALTAMENTE SPECIALIZZATE HA RICHIESTO UN FORTE IMPEGNO SUL PIANO DELLA FORMAZIONE DEL PERSONALE DA DESTINARE A TALE SEGMENTO OPERATIVO. PER TALE MOTIVO E' STATA ISTITUITA UNA SPECIFICA FIGURA PROFESSIONALE DENOMINATA "COMPUTER FORENSICS E DATA ANALYSIS", LA CUI QUALIFICA VIENE ATTRIBUITA ALL'ESITO DI APPOSITO CORSO PRESSO LA SCUOLA DI POLIZIA TRIBUTARIA E DOPO LA

FREQUENZA DI UN "TIROCINIO PRATICO" PRESSO IL MEDESIMO NUCLEO SPECIALE FRODI TECNOLOGICHE.

AL TERMINE DEL PERCORSO FORMATIVO SOPRA INDICATO, TALE PERSONALE È ASSEGNATO A TUTTI I NUCLEI SPECIALI (COMPRESO LO S.C.I.C.O. - SERVIZIO CENTRALE INVESTIGAZIONE CRIMINALITA' ORGANIZZATA) ED AI NUCLEI DI POLIZIA TRIBUTARIA, CON IL COMPITO DI FORNIRE AUSILIO IN TEMA DI INFORMATICA OPERATIVA, COSI' DA DARE SUPPORTO TECNICO ALLE INVESTIGAZIONI PER LA RACCOLTA DI ELEMENTI DI PROVA SULLA RETE, SU SISTEMI INFORMATICI O APPARECCHIATURE "MOBILE" (NETWORK, COMPUTER E MOBILE FORENSICS) ED OPERANDO L'ELABORAZIONE, L'INTEGRAZIONE E L'ANALISI DEI DATI (DATA ANALYSIS) ACQUISITI NEL CORSO DELL'ATTIVITÀ INVESTIGATIVA.

IL PERSONALE COSI' QUALIFICATO E' ORA IN GRADO DI GESTIRE LE PRINCIPALI CASISTICHE D'INTERVENTO, QUALI:

- MONITORARE LA RETE INTERNET (CLEAR E DEEP WEB) E SVILUPPARE INDAGINI TECNOLOGICHE;
- ACQUISIRE LA PROVA DIGITALE SENZA MODIFICHE O ALTERAZIONI;
- GARANTIRE CHE LE PROVE ACQUISITE SU ALTRO IDONEO SUPPORTO SIANO IDENTICHE A QUELLE ORIGINALI;
- ANALIZZARE I DATI RACCOLTI SENZA MODIFICARLI.

NEL CASO POI VI SIA LA NECESSITÀ DI EFFETTUARE OPERAZIONI TECNICHE PARTICOLARMENTE COMPLESSE, NON RISOLVIBILI CON L'IMPIEGO DEI MILITARI IN POSSESSO DELLA QUALIFICA IN OGGETTO, I REPARTI DEL CORPO POSSONO COMUNQUE RICHIEDERE L'AUSILIO DEL NUCLEO SPECIALE FRODI TECNOLOGICHE, CHE VALUTA ANCHE LA POSSIBILITÀ DI UN AUTONOMO INTERVENTO, CON PROPRIO PERSONALE, QUALORA LA PROBLEMATICA NON SIA RISOLVIBILE TRAMITE SCAMBIO INFORMATIVO.

30

E. MONITORAGGIO DEL "CLEAR" E "DARK" WEB

COME GIA' RICORDATO NEL CORSO DELL'AUDIZIONE, LA RETE TROVA OGGI, NELLA PARTE PIU' PROFONDA E NASCOSTA IL PROLIFERARE DI NUMEROSE ATTIVITA' ILLECITE, PARTICOLARMENTE INSIDIOSE SE SI PENSA A FENOMENI GRAVI COME QUELLI DEL TRAFFICO D'ARMI, DI DROGA, DI DOCUMENTI FALSI, ECC.

LA CARATTERISTICA PECULIARE CHE RENDE IL "**DARK WEB"** APPETIBILE PER LA PERPETRAZIONE DI PRATICHE ILLEGALI, VERE O PRESUNTE, È - LO RIPETIAMO - L'ALTO GRADO DI ANONIMATO CHE ESSO OFFRE, CAPACE DI CELARE, SENZA POSSIBILITA' ALCUNA DI IDENTIFICARNE MITTENTI E DESTINATARI, FLUSSI DI COMUNICAZIONE O SCAMBI DI MATERIALE ELETTRONICO DI OGNI GENERE.

AD ES., LA RICHIESTA DI UNA PAGINA WEB COMUNE, PRIMA DI ARRIVARE AL SERVER DI DESTINAZIONE, PASSA PER UNA MOLTITUDINE DI NODI INTERMEDI, SEMPRE DIVERSI, SFRUTTANDO UNA COMUNICAZIONE CHE AGGIUNGE UN LIVELLO ULTERIORE DI CIFRATURA DEI DATI PER OGNI NODO ATTRAVERSATO. COSI' COME LA MAIL INVIATA CON UN SERVIZIO NASCOSTO NELLA "DARKNET" ARRIVA AL DESTINATARIO ATTIVO NELLA STESSA RETE IN ASSOLUTA SICUREZZA E GARANZIA DI ANONIMATO.

VOLENDO ANDARE PIU' NEL DETTAGLIO, L'UTILIZZO DI TALE SISTEMA NON RENDE POSSIBILE DAL LATO MITTENTE CONOSCERE L'INDIRIZZO IP DEI NODI INTERMEDI, COSÌ COME IL SERVER FINALE NON È IN GRADO DI CONOSCERE TUTTI GLI INDIRIZZI IP, NÉ DEI NODI INTERMEDI, NÉ DEL CLIENT CHE HA RICHIESTO LA RISORSA.

IN PRATICA, OGNI NODO FACENTE PARTE DI UNA COMUNICAZIONE (CLIENT E SERVER COMPRESI) È IN GRADO DI CONOSCERE ESCLUSIVAMENTE I SUOI ADIACENTI NEL PERCORSO MITTENTE-DESTINATARIO, MA NESSUN DETTAGLIO SULLA COMUNICAZIONE COMPLESSIVA.

AVVALENDOSI DI QUESTE CARATTERISTICHE, È POSSIBILE GARANTIRE SERVIZI DI ANONIMATO SIA, COME DETTO, AL SINGOLO CLIENT, MA

ANCHE AD UN SERVER, NEL CASO IN CUI ESSO NON SIA ESPOSTO SULLA RETE INTERNET MA RISIEDA ALL'INTERNO DEL "DARK WEB".

IN QUESTO MODO NESSUN PROVIDER SARA' IN GRADO DI CONOSCERE QUESTE INFORMAZIONI, NE' DI DIRCI DOVE FISICAMENTE SI TROVA APPOSTATA LA STRUTTURA TECNOLOGICA CHE CONTIENE LA RISORSA WEB, **IMPEDENDO DI FATTO QUALSIASI REAZIONE DELLE AUTORITA' COMPETENTI, IVI COMPRESA LA POSSIBILITA' DI SOTTOPORRE A SEQUESTRO O INIBIRE IL RELATIVO DOMINIO O SERVER**.

IN TERMINI DI ECONOMIA D'INDAGINE SIGNIFICA DOVER ABBANDONARE MODELLI OPERATIVI CHE SI BASANO SULLE TRADIZIONALI INFORMAZIONI NELLA DISPONIBILITA' DI OPERATORI DI RETE, GESTORI DI CARTE DI PAGAMENTO, PUBBLICI REGISTRI ELETTRONICI CONSULTABILI GRATUITAMENTE O DIETRO UN CANONE DI ABBONAMENTO SUL WEB.

NON SARA' POSSIBILE, AD ES., ASSOCIARE IL "DOMINIO ONION" INDIVIDUATO AD UN NUMERO IP REALE E, QUINDI, RICHIEDERNE LA RISOLUZIONE; AVERE INFORMAZIONI SUL REGISTRANTE DELLA RISORSA WEB; OTTENERE, A SUA VOLTA, IL NUMERO TELEFONICO AD ESSA ASSOCIATO E, CONSEGUENTEMENTE, I DATI DELL'INTESTATARIO E L'INDIRIZZO DI UBICAZIONE DELL'APPARECCHIO TELEFONICO, ECC.

IN RAGIONE DI CIO' SONO NUMEROSE LE INIZIATIVE IN CAMPO INTERNAZIONALE VOLTE A DEFINIRE STRATEGIE INVESTIGATIVE COMUNI IN TALE AMBITO, ANCHE IN RAGIONE DELLE POCHE ESPERIENZE MATURATE SUL CAMPO DALLE SINGOLE FORZE DI POLIZIA E PER LE QUALI E' SEMPRE MAGGIORE L'INTERESSE AD UN'AMPIA CONDIVISIONE.

TRA QUESTE SI SEGNALA IL **PROGRAMMA "MEMEX"**, ATTIVO DAL 2014 E FINANZIATO DAL DIPARTIMENTO DELLA DIFESA STATUNITENSE, IL CUI OBIETTIVO È QUELLO DI REALIZZARE UN MOTORE DI RICERCA CHE AIUTI LE FORZE DELL'ORDINE A CONTRASTARE I TRAFFICI ILLECITI GRAVI, SCANDAGLIANDO LE PARTI MENO VISIBILI DELLA RETE ("DEEP" E "DARK" WEB).

32

IN AMBITO EUROPEO, LA RICONOSCIUTA PERICOLOSITA' A LIVELLO UNIVERSALE DEL "DARK WEB", QUALE AREA DI INTERESSE DEL CRIMINE ORGANIZZATO, HA PORTATO LE PIU' IMPORTANTI ISTITUZIONI DI "LAW ENFORCEMENT" DEI PAESI MEMBRI AD AVVIARE SPECIFICI PIANI D'AZIONE, CON LA FINALITA DI PRESIDIARE, CON TUTTI I LIMITI DEL CASO, ANCHE LA PARTE NASCOSTA DEL WEB, COSI' DA PERMETTERE UN AFFINAMENTO DELLE TECNICHE DI MONITORAGGIO E DI INTERVENTO OPERATIVO. IN QUESTO QUADRO SI INSERISCE L'**OPERAZIONE CONGIUNTA "ARES"** CHE COINVOLGE LE FORZE DI POLIZIA E DOGANE DELL'UNIONE EUROPEA IMPEGNATE NELLA LOTTA CONTRO LA CRIMINALITA' ORGANIZZATA TRASFRONTALIERA. TRATTASI DI UNA OPERAZIONE MULTIDISCIPLINARE, CHE ABBRACCIA VARI SETTORI OPERATIVI, BASATA SULL'INTELLIGENCE DI POLIZIA, DOGANALE E DI ALTRE AUTORITÀ QUALE AZIONE PROPEDEUTICA ALL'EFFETTUAZIONE DI MIRATI CONTROLLI INVESTIGATIVI.

VOLENDO FARE CENNO AD ALCUNE ESPERIENZE OPERATIVE DEL CORPO, IL **NUCLEO SPECIALE POLIZIA VALUTARIA** HA ESEGUITO RECENTEMENTE UNA COMPLESSA INDAGINE DI POLIZIA GIUDIZIARIA TESA AL CONTRASTO DEI REATI IN MATERIA DI FALSO MONETARIO, IL CUI SVILUPPO È STATO REALIZZATO ANCHE TRAMITE L'INTERESSAMENTO DI EUROPOL E DI MOLTEPLICI FORZE DI POLIZIA ESTERE. IL SERVIZIO HA PERMESSO DI INDIVIDUARE UN'ASSOCIAZIONE PER DELINQUERE FINALIZZATA ALLA FALSIFICAZIONE DI BANCONOTE, NONCHÉ DI ATTI E DOCUMENTI (PATENTI DI GUIDA E PERMESSI DI SOGGIORNO). E' STATA RICOSTRUITA L'ATTIVITÀ DI DISTRIBUZIONE, SUL MERCATO NAZIONALE ED EUROPEO, DI BANCONOTE IN VALUTA EURO FALSE, SFRUTTANDO LE ABILITÀ INFORMATICHE DI UN SODALE IL QUALE INDIVIDUAVA I CLIENTI FINALI MEDIANTE LA PUBBLICAZIONE DI APPOSITI ANNUNCI SUL "DEEP WEB". L'AUTORITÀ GIUDIZIARIA HA EMESSO UN'ORDINANZA DI CUSTODIA CAUTELARE PERSONALE NEI CONFRONTI DEGLI APPARTENENTI ALLA CONSORTERIA CRIMINALE.

ANALOGAMENTE, CON L' **OPERAZIONE "BIG SURPRICE"** LE **FIAMME GIALLE DI MALPENSA**, SUPPORTATE DAL **NUCLEO SPECIALE FRODI TECNOLOGICHE,** HANNO PROCEDUTO A DISARTICOLARE UNA ORGANIZZAZIONE INTERNAZIONALE DEDITA AL TRAFFICO DI STUPEFACENTI ATTRAVERSO IL "DARK WEB", CHE PREVEDEVA IL PAGAMENTO IN BITCOIN, POI CONVERTITI IN VALUTA LEGALE, TRASFERITA AGLI ARRESTATI SEMPRE ONLINE. TALE ATTIVITA' HA PORTATO AL SEQUESTRO DI SOSTANZE STUPEFACENTI E ALL'ARRESTO DI 4 PERSONE.

DIVERSE SONO, INVECE, LE ATTIVITA' D'INDAGINE IN CORSO, PER LE QUALI SONO ALL'OPERA DIVERSI REPARTI TERRITORIALI E SPECIALI.

CONTEMPORANEAMENTE, PROSEGUE IL COSTANTE IMPEGNO DELLE UNITA' OPERATIVE DEL CORPO A PRESIDIO DEL WEB E DELLA "DARKNET", FINALIZZATO IN LARGA PARTE AD UN APPROFONDITO E CONTINUO MONITORAGGIO DEL FENOMENO, NELLE SUE DECLINAZIONI ECONOMICHE E FINANZIARIE, CAPACE DI FORNIRE IN MODO CONTINUATIVO UN QUADRO AGGIORNATO SU MODALITA', TIPOLOGIA E DIMENSIONI DELLE CONDOTTE POTENZIALMENTE ILLECITE PRESENTI, DA CUI FAR SCATURIRE, NEI CASI POSITIVI, VERE E PROPRIE INDAGINI DI POLIZIA GIUDIZIARIA. CIO', ANCHE IN FUNZIONE DI DISPORRE DI PIU' PENETRANTI POTERI, QUALI AD ES. LA POSSIBILITA' DI AVVIARE UN'ATTIVITA' SOTTO COPERTURA.

F. BREVI CONSIDERAZIONI

QUANTO PRECEDE TESTIMONIA IL QUOTIDIANO IMPEGNO INVESTIGATIVO DELLA GUARDIA DI FINANZA NEL CONTRASTO AGLI ILLECITI ECONOMICO-FINANZIARI ONLINE, IVI COMPRESI QUELLI COMMESSI NELLA PARTE NASCOSTA DI INTERNET.

SI TRATTA DI UN'ATTIVITA' COMPLESSA E TALVOLTA DISPENDIOSA IN TERMINI DI IMPEGNO OPERATIVO SE SI CONSIDERANO LE ARTICOLATE FASI CHE SOTTENDONO ALL'ESECUZIONE DI UN'INVESTIGAZIONE

34

TECNOLOGICA, DOVENDO LA POLIZIA GIUDIZIARIA, UNA VOLTA TERMINATA L'ATTIVITA' DI MONITORAGGIO ED INDIVIDUATA LA CONDOTTA ILLECITA, ACQUISIRE LA PROVA DIGITALE ATTRAVERSO UN PROCESSO DI "NETWORK INVESTIGATION", OVVERO UN "DUMP" DELLA RISORSA WEB E RIPORTARE IL TUTTO IN UN'ANNOTAZIONE DI POLIZIA GIUDIZIARIA DA TRASMETTERE ALL'AUTORITA' GIUDIZIARIA.

QUINDI, ATTENDERE CHE VENGA ASSEGNATO IL FASCICOLO AD UN PUBBLICO MINISTERO, IL QUALE, ASSUMENDO LA DIREZIONE DELLE INDAGINI, SE RITERRA' FONDATA LA NOTIZIA DI REATO DELLA POLIZIA GIUDIZIARIA, FORMALIZZERA' APPOSITA RICHIESTA MOTIVATA DI SEQUESTRO O INIBIZIONE DEL SITO AL GIUDICE PER LE INDAGINI PRELIMINARI.

NEL CASO CHE IL GIP ACCOLGA LA RICHIESTA, VERRA' EMESSO IL PROVVEDIMENTO, SUCCESSIVAMENTE NOTIFICATO AGLI INTERNET SERVICE PROVIDER, SENZA TENER CONTO DEL FATTO CHE, NELLA MAGGIOR PARTE DI CASI, I PIRATI SONO PORTATI AD UTILIZZARE SERVER UBICATI IN TERRITORIO ESTERO.

IN QUESTI CASI, FATTA SALVA LA POSSIBILITA' DI AVANZARE AL PAESE ESTERO UNA RICHIESTA DI ASSISTENZA GIUDIZIARIA INTERNAZIONALE, ONEROSA, CON TEMPI NON BREVI E NON PREVENTIVABILI, ALLE AUTORITA' NAZIONALI NON RESTA ALTRO CHE NOTIFICARE AI CITATI INTERNET SERVICE PROVIDER UN MERO PROVVEDIMENTO DI INIBIZIONE CHE PREVEDA IL REINDIRIZZAMENTO DELLE "CHIAMATE" A QUEL SITO SU UN NUMERO IP INDICATO DALL'AUTORITA' PUBBLICA, DOVE SOLITAMENTE APPOSTARE UN AVVISO DELL'ESISTENZA DI UN PROVVEDIMENTO RESTRITTIVO DELL' AUTORITA' GIUDIZIARIA.

35

IL "DISALLINEAMENTO TEMPORALE" E', PERTANTO, DI PALESE EVIDENZA, SOLO CONSIDERANDO LA RAPIDITA' EVOLUTIVA ED ADATTATIVA DEL WEB E DEI CYBER CRIMINALI, AGGRAVATO, NEL CASO DELLA "DARKNET", DA OGGETTIVI LIMITI TECNOLOGICI E PROCEDURALI.

G. IL DOCUMENTO "IOCTA 2016"

IN TAL SENSO, APPARE OPPORTUNO RICHIAMARE I CONTENUTI DEL DOCUMENTO "IOCTA 2016 - INTERNET ORGANISED CRIME THREAT ASSESSMENT", CON CUI **EUROPOL** HA EVIDENZIATO UNA RILEVANTE PROBLEMATICA CHE OSTACOLA LE ATTIVITÀ INVESTIGATIVE DELLE FORZE DI POLIZIA DELL'UNIONE EUROPEA E NON SOLO.

NELLO SPECIFICO, I REGISTRAR AL MOMENTO DELLA REGISTRAZIONE DI UN SITO WEB, OFFRONO AI TITOLARI (REGISTRANT) L'OPPORTUNITÀ DI FRUIRE DEL SERVIZIO DI "PRIVACY E PROXY" (P/P) AL FINE DI TUTELARE LA PROPRIA PRIVACY.

CON QUESTA OFFERTA, INFATTI, È CONSENTITA L'OMISSIONE DELLE PROPRIE INFORMAZIONI SUGLI ARCHIVI WHOIS, DATABASE DI LIBERO

ACCESSO NEL QUALE SONO CONSERVATI GLI ESTREMI DEI TITOLARI DI QUALSIASI DOMINIO WEB.

IN TAL SENSO, L'**ICANN (INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS),** ENTE DI GESTIONE INTERNAZIONALE CUI È DEMANDATO, TRA L'ALTRO, L'INCARICO DI ASSEGNARE GLI INDIRIZZI IP E DI GESTIONE DEL SISTEMA DEI NOMI A DOMINIO DI PRIMO LIVELLO (TOP-LEVEL DOMAIN) GENERICO (GTLD), DEL CODICE INTERNAZIONALE (CCTLD) E DEI SISTEMI DI ROOT SERVER, E CON IL QUALE IL CORPO INTRATTIENE RAPPORTI DI COLLABORAZIONE[4], SI È IMPEGNATO AD INDIVIDUARE UN PROGRAMMA DI ACCREDITAMENTO PER I DIVERSI FORNITORI DEI CITATI SERVIZI P/P, I QUALI DOVRANNO GARANTIRE LA MASSIMA COLLABORAZIONE CON LE AUTORITÀ, AL FINE DI PREVENIRE I FREQUENTI ABUSI DA PARTE DI ORGANIZZAZIONI CRIMINALI CHE SI AVVALGONO DI QUESTA "SCHERMATURA" DEI PROPRI DATI PER RENDERE MAGGIORMENTE DIFFICOLTOSA LA LORO IDENTIFICAZIONE.

TUTTAVIA, LA RACCOMANDAZIONE EMANATA DAL BOARD DELL'ICANN NON HA RECEPITO IN TOTO LE PERPLESSITÀ ESPRESSE DALLA ORGANI DI "LAW ENFORCEMENT" COMUNITARI, IN QUANTO È STATO STABILITO CHE:

- I FORNITORI DI SERVIZI P/P, SOLTANTO A FRONTE DI UN UN'ESPLICITA RICHIESTA DEL TRIBUNALE, SONO OBBLIGATI A NON COMUNICARE AL PROPRIO CLIENTE L'ESISTENZA DI UNA RICHIESTA A SUO CARICO DA PARTE DI UN ORGANO DI POLIZIA;
- I MEDESIMI FORNITORI POTREBBERO RISPONDERE SOLTANTO A RICHIESTE PROVENIENTI DA ORGANI DI POLIZIA RIENTRANTI NELLA MEDESIMA GIURISDIZIONE, CON EVIDENTE LIMITAZIONI IN DANNO DELLE INDAGINI, CHE DATA LA NOTA NON TERRITORIALITÀ DELLA RETE, ASSUMONO SISTEMATICAMENTE CARATTERE

[4] Proprio recentemente, in data 6 febbraio u.s., presso il Nucleo Speciale Frodi Tecnologiche, si è tenuto un incontro tra il Vice Direttore di ICANN, Dave Piscitello, e Ufficiali dell'Ufficio Relazioni Internazionali e Cooperazione con Enti collaterali del Comando Generale, assistiti da specialisti del citato Nucleo Speciale, per discutere ed approfondire le tecniche di investigazione sul tema "Investigating Domain Names & Internet Numbers"

TRANSFRONTALIERO;

- I TITOLARI DI DOMINI CHE SI OCCUPANO ATTIVAMENTE DI TRANSAZIONI COMMERCIALI POTRANNO AVVALERSI LIBERAMENTE DEI SERVIZI P/P.

PROPRIO IN RELAZIONE AL FUNZIONAMENTO ED ALL'UTILIZZO DATABASE WHOIS, L'ICANN HA AVVIATO UNO STUDIO FINALIZZATO ALL'INDIVIDUAZIONE DI UN SISTEMA ALTERNATIVO CHE POSSA GARANTIRE LA CORRETTEZZA E VERIDICITÀ DEI DATI INSERITI RELATIVI AI TITOLARI DEI DOMINI ED IL CONCOMITANTE RISPETTO DEGLI STANDARD EUROPEI IN MATERIA DI PROTEZIONE DEI DATI.

QUEST'ULTIMO ASPETTO POTREBBE ESSERE RISOLTO CONSENTENDO LA CONSULTAZIONE DEL DATABASE SOLTANTO A DETERMINATI UTENTI APPOSITAMENTE ACCREDITATI.

IN RELAZIONE, INVECE, ALLA TECNOLOGIA "CGN" (CARRIER-GRADE NETWORK ADDRESS TRANSLATION), NEL SUCCITATO DOCUMENTO VENGONO EVIDENZIATI I RISULTATI DI UNO STUDIO CONDOTTO DA EC3 TRA GLI STATI MEMBRI UE, DAL QUALE È EMERSO CHE NEI CASI IN CUI QUESTI SISTEMI SONO IMPIEGATI DAGLI INTERNET SERVICE PROVIDER, IL 90% DEI CYBER-INVESTIGATORI INTERVISTATI HA RISCONTRATO DIFFICOLTÀ NELL'IDENTIFICAZIONE DEI RESPONSABILI DI REATI INFORMATICI.

CON QUESTA TECNICA GLI INTERNET SERVICE PROVIDER HANNO LA POSSIBILITÀ DI FAR FRONTE AGLI ATTUALI LIMITI QUANTITATIVI IN TERMINI DI NUMERI IP ASSEGNABILI IMPOSTI DAL PROTOCOLLO IPV4. IN SOSTANZA L'ARCHITETTURA DEGLI ISP È STRUTTURATA SU UNA RETE INTERNA (O PIÙ), ALLA QUALE SONO COLLEGATI ATTRAVERSO INDIRIZZI DI RETE PRIVATI I PROPRI UTENTI FINALI. QUESTI ULTIMI, ATTRAVERSO DISPOSITIVI PRESENTI NEL NETWORK DELL'OPERATORE, IN MANIERA DEL TUTTO AUTOMATICA, UTILIZZANO, ANCHE CONTEMPORANEAMENTE, UN MEDESIMO INDIRIZZO IP PUBBLICO PER FRUIRE DEI CONTENUTI DELLA RETE INTERNET, MOLTIPLICANDO, IN TAL MODO, LE POSSIBILITÀ

DI ACCESSO AL WEB.

PER QUESTA RAGIONE, PER CERCARE DI ASSOCIARE UN DETERMINATO NUMERO IP AD UN'UTENZA SPECIFICA, LE FORZE DI POLIZIA SONO OBBLIGATE A RICHIEDERE AGLI OPERATORI TELEFONICI/TELEMATICI ELEMENTI DI MAGGIOR DETTAGLIO, QUALI IL NUMERO IP SORGENTE E DI DESTINAZIONE, PORTA SORGENTE E DATA E ORA ESATTA DI CONNESSIONE (CON APPROSSIMAZIONE AL SECONDO).

TUTTAVIA, LA MANCANZA DI UNA NORMATIVA ARMONIZZATA IN EUROPA CIRCA LA CONSERVAZIONE DEI DATI COMPORTA CHE NON IN TUTTI I PAESI VI SIA L'OBBLIGO DI MEMORIZZARE E METTERE DISPOSIZIONE DELLE AUTORITÀ QUESTE ULTERIORI INFORMAZIONI.

4. CONCLUSIONI

PER QUANTO FIN QUI ESPOSTO, APPARE EVIDENTE COME L'HABITAT TELEMATICO IN PAROLA SIA IL LUOGO MENO FAVOREVOLE ALLA RIVENDITA DI PRODOTTI CONTRAFFATTI E PIRATATI, I QUALI, SEPPURE ILLEGALI, NECESSITANO DELLE BASILARI REGOLE DEL COMMERCIO, OVVERO PROMUOVERE E PUBBLICIZZARE I PROPRI PRODOTTI ALLA PLATEA PIÙ VASTA POSSIBILE DI POTENZIALI ACQUIRENTI. ESATTAMENTE L'OPPOSTO DI CIÒ CHE AVVIENE NEI MERCATI DEL DEEP/DARKWEB, NOTORIAMENTE FREQUENTATO DA UN NUMERO DI UTENTI NOTEVOLMENTE INFERIORE A QUELLO DEL WEB DI SUPERFICIE.

TRA L'ALTRO, LA COMPLESSITÀ DELLA STRUTTURA DI QUESTA PORZIONE DI INTERNET, NONCHÉ LA DIFFICOLTÀ PER L'UTENTE MEDIO DI MUOVERSI AL SUO INTERNO, CIRCOSCRIVONO ANCORA DI PIÙ LA FREQUENTAZIONE DI UTENTI ALLA RICERCA DI TALI PRODOTTI.

ANCHE SE ULTIMAMENTE STANNO NASCENDO SEMPRE PIÙ SERVIZI E STRUMENTI DI RICERCA O MONITORAGGIO DI QUELLO CHE ACCADE NELL'INTERNET PIÙ PROFONDO (L'ULTIMO IN ORDINE TEMPORALE È IL SITO DNSTATS.NET – ACCESSIBILE ANCHE SUL WEB DI SUPERFICIE – CHE MOSTRA

LE STATISTICHE DI ACCESSO AD ALCUNI SERVIZI DELLE DARKNET), I NUMERI DELLA CONTRAFFAZIONE E PIRATERIA EVIDENZIANO CHE IL MAGGIOR TERRENO FERTILE NEL WEB E' QUELLO C.D. "DI SUPERFICIE" DOVE, GRAZIE AI MOTORI DI RICERCA, ALLA PUBBLICITÀ NELLE PAGINE WEB, ALLE EMAIL DI SPAM, NONCHÉ AI SOCIAL NETWORK, SI RIESCE A RAGGIUNGERE LA QUASI TOTALITÀ DEI CYBER-NAVIGANTI.

PARTENDO PROPRIO DALL'ESPERIENZA INFO-OPERATIVA DELLE NOSTRE UNITA' SPECIALI POSSIAMO POTER AFFERMARE, IN LINEA CON QUANTO GIA' EVIDENZIATO NEL CORSO DELL'AUDIZIONE, CHE, AD OGGI, IL FENOMENO NELLA "DARKNET" E' SICURAMENTE CIRCOSTRITTO, SIA IN TERMINI DI VARIETA' DEI BENI OFFERTI (PRINCIPALMENTE IL SETTORE DEL "FASHION"), SIA NEL NUMERO DELLE PROPOSTE DI VENDITA, AL PARI DI QUELLO DEI SERVIZI O PRODOTTI PIRATATI.

IN OGNI CASO, LA POTENZIALITA', IN TERMINI DI DIFFUSIONE DELL'ILLECITO OFFERTO DAL "DARK WEB", DEVE FAR MANTENERE ALTO IL LIVELLO DI ATTENZIONE, SPECIALMENTE SUL TEMA DELLA CONTRAFFAZIONE, LADDOVE LA "DARKNET" POSSA (E VENGA UTILIZZATA) PER TRANSAZIONI TRA "GROSSISTI".

NON E' UN CASO CHE IN ALCUNI "POST" DI OFFERTA DI PRODOTTI CONTRAFFATTI PRESENTI NEL "DARK WEB", SI RICHIEDA, PER FINALIZZARE L'OPERAZIONE DI ACQUISTO, UN QUANTITATIVO MINIMO DI PRODOTTI.

DUNQUE, UN QUADRO D'ASSIEME PARTICOLARMENTE COMPLESSO E IN CONTINUA TRASFORMAZIONE, OVE L'INCREMENTO DELLE OPPORTUNITÀ È ACCOMPAGNATO DA UN PARALLELO INCREMENTO DELLE VULNERABILITÀ, TANTO DA RICHIEDERE UNA SEMPRE MAGGIORE CONSAPEVOLEZZA ED ATTENZIONE DA PARTE DI TUTTE LE ISTITUZIONI INTERESSATE.

NE CONSEGUE L'IMPORTANZA DI ADOTTARE, A LIVELLO NAZIONALE E INTERNAZIONALE, UNA STRATEGIA UNITARIA E TRASVERSALE, CHE CONSENTA DI SUPERARE OSTACOLI NORMATIVI E BUROCRATICI, COSI' DA CORRISPONDERE ALLA MINACCIA CON AZIONI EFFICACI ED ADEGUATE, COME DIMOSTRANO LE RECENTI VICENDE GIUDIZIARIE BALZATE AGLI ONORI DELLA

40

CRONACA.

ILLUSTRATO, SIA PUR SINTETICAMENTE, IL QUADRO DI SITUAZIONE, IL COL. GIOVANNI PARASCANDOLO, COMANDANTE DEL NUCLEO SPECIALE FRODI TECNOLOGICHE PROCEDERA' A COMMENTARE IL VIDEO PREDISPOSTO SUL MONITORAGGIO DELLA "DARKNET".

17STC0027940