Il *Deep Web* (Web sommerso o invisibile) è l'insieme delle risorse informative del *World Wide Web* non raggiugibili dai comuni motori di ricerca. Secondo Wired, il Web è costituito da oltre un trilione di pagine, mentre Google ne indicizza solo tre miliardi. La struttura dell'intero *World Wide Web* è spesso paragonata a quella di un iceberg, di cui solo una minima parte è visibile sopra il pelo dell'acqua. Poiché vi sono implementate numerose sotto-reti con accessi regolamentati da diversi livelli di sicurezza, esso è rappresentato tramite livelli successivi o strati, dal più esterno (quello visibile a chiunque) a quelli più interni e difficilmente accessibili.

di Maria Clara Colombini

LA RICERCA E L'ANALISI NEL DEEP WEB: I BLACK MARKET

Clara Maria COLOMBINI *è consulente Tecnico per la Procura della Repubblica per il sequestro, repertamento e analisi dei sistemi informatici. Collaboratrice alla ricerca per la Cattedra di Criminologia e Criminalistica presso l'Università degli Studi di Milano. Docente accreditato Eupolis Regione Lombardia. ACE – Accessdata Certified Examiner. Digital Forensic Expert – Cyber Intelligence Expert.*

In questi ultimi anni abbiamo assistito alla crescita imponente dell'utilizzo del *web* per la vendita online, cosa che ha facilitato l'espansione delle vendite sia dei prodotti legali sia di quelli illegali da parte di numerose organizzazioni criminali nazionali ed internazionali. Infatti, un numero elevato di malfattori sfrutta le potenzialità del web (in particolare l'assenza di confini nazionali definiti, la non tracciabilità, l'anonimità degli attori e quindi la loro non-punibilità) per creare delle aree non rintracciabili (il cosiddetto "*Deep Web*") e quindi eludere le inevitabili responsabilità penali.
Nella sua parte più sommersa, la cosiddetta *DarkNet*, sono attive tutta una serie di attività illegali, tra le quali la vendita di armi, esplosivi e soprattutto quella delle sostanze stupefacenti, articolata in negozi o supermercati online (i "*Black Market*") presso i quali è possibile acquistare ed eseguire transazioni in modo del tutto anonimo.

TOR

Una delle più popolari vie di accesso al Deep Web è TOR, un protocollo e una rete di tunnel virtuali che permette a chiunque di nascondere la propria identità e migliorare la privacy e la sicurezza su Internet. Il progetto Tor (acronimo di *The Onion Router*) è nato nel 1995 per merito della Marina Militare degli Stati Uniti allo scopo di garantire che le conversazioni governative (ordini e disposizioni d'impiego) non fossero intercettate da entità nemiche o da servizi d'intelligence stranieri. Sviluppato dal 2002 dalla *Electronic Frontier Foundation* sponsorizzata dalla *US Naval Research Laboratory*, è ora gestito da *The Tor Project*, un'associazione senza scopo di lucro.
TOR non solo permette di accedere ai servizi bloccati dai provider[1] Internet locali, ma ospita servizi nascosti che permettono agli utenti di pubblicare siti web e altri servizi senza dover rivelare la posizione attuale del sito e proteggere gli utenti dall'analisi del traffico attraverso una rete di router[2] (i c.d. *onion routers*), che rendono il traffico anonimo. Il funzionamento della rete Tor è concettualmente semplice: i dati che appartengono a una qualsiasi comunicazione non transitano direttamente dal client[3] al server[4], ma passano attraverso i server Tor che agiscono da router costruendo un circuito virtuale crittografato[5] a strati (a *cipolla*). Infine, tramite il protocollo "*onion*" fornito da Tor, è possibile accedere ai cosiddetti "pseudo-domini di primo livello" *.onion*, altrimenti invisibili ai comuni browser.

I2P

Una seconda e più occulta via di accesso al Deep Web è I2P, un'altra rete anonima, che implementa un maggior grado di sicurezza rispetto a TOR: ogni applicazione client ha un router I2P che costruisce "*tunnel*" in entrata e in uscita: una sequenza di peer che passano messaggi in una direzione (verso e dal client, rispettivamente). A sua volta, quando un client vuole inviare un messaggio ad un altro client, lo invia attraverso un tunnel in uscita, diretto verso uno dei tunnel in entrata dell'altro client, fino a raggiungere la destinazione. Ogni utente della rete decide la lunghezza dei tunnel, determinando così un compromesso tra anonimato, latenza

1 *Provider*: azienda di servizi che dispone di computer costantemente connessi ad Internet tramite linee speciali: ad essi, attraverso una normale linea telefonica e un modem, si possono collegare gli utenti abbonati, avendo così accesso alla rete.

2 Router: ispositivo che collega tra loro più reti scegliendo il percorso migliore per i dati e che all'occorrenza converte il protocollo di trasmissione.

3 Client: in una rete informatica, ogni computer collegato al server e in grado di scambiare dati con esso.

4 Server: computer di elevate prestazioni che in una rete fornisce un servizio agli altri elaboratori collegati, detti client.

5 Crittografia: scrittura convenzionale segreta, decifrabile solo da chi sia a conoscenza del codice.

e velocità di gestione, in accordo con le proprie necessità. All'interno della rete I2P, non vi sono limiti al modo in cui le applicazioni possono comunicare, e i contenuti inviati sono criptati tramite tre strati di crittografia: la «*garlic*» (verifica la consegna del messaggio al destinatario), la crittografia tunnel (tutti i messaggi che passano attraverso un tunnel vengono crittografati dal gateway[6] tunnel al tunnel), e la crittografia del livello di trasporto tra router.

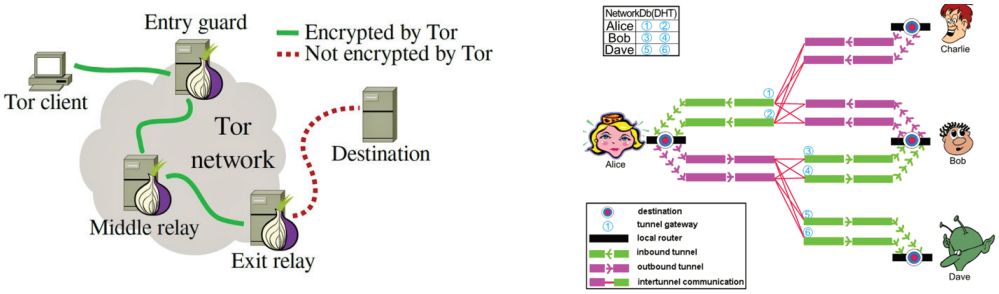

***Fig. 1** – Le strutture di Tor e di I2P.*

La ricerca nel Deep Web

Eseguire una ricerca dati nel Deep Web non è semplice proprio per le sue caratteristiche, volte alla protezione dell'anonimato e della non tracciabilità; sebbene siano stati implementati alcuni motori di ricerca interni, non ne esistono di evoluti come Google. Inoltre, i siti che svolgono attività illecite, nel mirino delle istituzioni di tutto il mondo e quindi soggetti a continui attacchi volti alla loro distruzione, devono spostarsi continuamente e implementare sofisticati sistemi di mascheramento per evitare di essere bloccati. Come trovarli, quindi?

Per inquadrare il problema possiamo brevemente analizzare lo scenario in cui si muove un comune spacciatore che, pur cercando di non farsi notare troppo, per svolgere la sua attività di scambio denaro-droga, deve accettare il rischio di esporsi, studiando nel tempo specifiche e diverse modalità di pubblicizzazione, allo scopo di farsi trovare dai possibili acquirenti, senza i quali non avrebbe ragione di essere. Allo stesso modo, un sito *online* di vendita di sostanze stupefacenti all'interno del Deep Web, e quindi protetto dalla sua struttura, per svolgere con continuità e nel tempo la propria attività commerciale (e stiamo parlando di enormi quantità di denaro), deve pianificare e realizzare un modo per permettere ai possibili acquirenti di:

- trovarlo dal web di superficie;
- farsi un'idea del suo funzionamento attraverso forum, blog o wiki che ne illustrano i prodotti;
- reperire e installare semplici tool per navigare nel Deep Web in sicurezza e anonimato;
- raggiungerlo tramite motori di ricerca intuitivi;
- iscriversi facilmente e in modo anonimo al market;
- essere accolto da un sito accattivante, sicuro e professionale;
- acquistarne quindi i prodotti in sicurezza.

La rete Tor offre anche un browser per la ricerca nel Deep Web con una sorta di indicizzazione, ma non offre l'accuratezza di Google, dovuta anche al fatto che i Black Markets non indicizzano le loro homepage. La ricerca inizia quindi dal Web di superficie, dove si possono trovare numerosi Forum, Blog e Wiki come Thehiddenwiki, Deepdotweb o Reddit, per fare solo qualche nome, che rimandano ai loro corrispettivi nel Deep Web, ove sono pubblicati gli elenchi aggiornati dei Black Market attivi a cui sono collegati.

Uno dei wiki più interessanti è *Onion Anonimity* (*32rfckwuorlf4dlv.onion*), che contiene diversi elenchi di URL[7] *.onion* suddivisi per argomenti e tipologia di servizio offerto. Esso offre, per ciascun collegamento, una descrizione del contenuto, i modi di accesso e un giudizio di "qualità e affidabilità" sulla "serietà" del servizio offerto, cosa che rivela l'esistenza di un'organizzazione che valuta e controlla i contenuti e le attività illecite del Deep Web censite. È interessante notare che, nonostante il sito ribadisca che vengono sistematicamente rimossi link a siti di narcotici, razzismo o attività criminali, ne riporta in realtà un gran numero.

***Fig. 2** – Onion Anonimity*

6 Gateway: programma o computer che regola la comunicazione e lo scambio di dati fra due o più reti con protocolli diversi.

7 Uniform Resource Locator o URL: sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet, tipicamente presente su un host server, come ad esempio un documento, un'immagine, un video, rendendola accessibile ad un client.

L'analisi del codice html[8] della pagina ha rivelato che essa contiene nei propri metadati le seguenti keywords: *islamic, state, islam, is, isil, isis, iraq, syria, califate, donate, help, money, weapons, jihad, holy war, mujahideen, sharia, Bitcoin*. Il servizio di ricerca di siti.*onion* "*Tor Hidden Service*" fornito da Ahmia (*www.ahmia.fi*) fornisce l'URL di origine: *http://kr4ypn2j34xinmtk.onion/* e la data di edizione (9 ottobre 2014 alle ore 9:40 a.m.). La presenza di una tale pagina in un Wiki di presunto orientamento "libertario" porta sicuramente a pensare a un collegamento molto stretto tra i mercati illeciti *online*, con l'enorme mole denaro occulto e incontrollato che gestiscono, e il terrorismo di matrice fondamentalista islamica.

I Black Market

I Black Market, veri e propri "supermercati dell'illecito", offrono al loro interno una vasta gamma di prodotti e servizi, tra cui un elevatissimo numero di sostanze illecite, dalla marijuana fino all'eroina, passando per tutta una serie di droghe sintetiche, senza peraltro tralasciare quei farmaci acquistabili solo tramite prescrizione medica (antidepressivi, stimolanti, antipsicotici, antidolorifici, sonniferi, ormoni, ecc.).
La moneta di scambio è il Bitcoin, acquistabile direttamente presso gli stessi mercati. Il Bitcoin è una moneta elettronica, creata nel 2009 da un anonimo conosciuto con lo pseudonimo di Satoshi Nakamoto, allo scopo ufficiale di alleggerire le transazioni finanziarie e commerciali dai pesi, dai balzelli e dai rischi che promanano dalle società d'intermediazione commerciale, ma nella realtà con il fine di consentire operazioni di acquisto/vendita in maniera veloce, poco costosa e soprattutto anonima. Il controvalore totale dell'economia Bitcoin è calcolato oggi in 80 milioni di unità in circolazione, raggiungendo il controvalore di più di 23 miliardi di dollari. A oggi il Bitcoin è valutato 212 Euro circa, ma, proprio per il suo valore puramente fiduciario, registra oscillazioni medie giornaliere pari a circa il 4 per cento, con punte di oltre il dieci.
La rete Bitcoin non utilizza un ente centrale, ma un database distribuito tra i nodi della rete, e sfrutta la crittografia per gestire gli aspetti funzionali consentendo il possesso e il trasferimento anonimo delle monete. Del trasferimento di Bitcoin non rimane alcuna traccia, proprio perché il sistema non è dotato di un server centrale, ma si limita a memorizzare una lista di tutti i trasferimenti la cui consultazione, però, è consentita ai soli partecipanti al network. Ciò rende impossibile per qualunque autorità, governativa o meno, di bloccare la rete, sequestrare bitcoin ai legittimi possessori o di svalutarla creando nuova moneta. Ne consegue che il Bitcoin è divenuto la moneta principe nelle transazioni illecite *online*, complemento perfetto di un assetto in grado di garantire l'anonimato più assoluto al criminale.

Silk Road

Forse il più conosciuto fra i Black Market, Silk Road, un sito di commercio elettronico raggiungibile fino allo scorso anno tramite Tor, si occupa della vendita *online* di svariati prodotti e servizi, per lo più illeciti, tra i quali tutta una serie di sostanze stupefacenti e psicotrope, che ne hanno fanno il più grande mercato mondiale di droga. Diretto dal 2011 da "*Dread Pirate Roberts*", pseudonimo sotto di cui si cela il proprietario, ricalca la struttura di Ebay, compreso un deposito di garanzia, per ridurre il rischio di truffe. Il 3 ottobre 2013 Silk Road viene chiuso dall'FBI e viene arrestato il sedicente direttore, Ross William Ulbrich, dal cui portafoglio virtuale vengono sequestrati più di **26.000 Bitcoin**, per un controvalore di circa **3,6 milioni di dollari**. Ai primi di novembre del 2013 è annunciata la riapertura di Silk Road da parte dello pseudonimo Dread Pirate Roberts, nonostante l'FBI abbia arrestato la presunta persona che si celava dietro a quel nome. I visitatori del nuovo Silk Road sono stati accolti da un messaggio di benvenuto da parte dell'amministratore del sito: «*è con grande gioia che vi annuncio un nuovo capitolo della nostra avventura*», ha scritto l'amministratore del sito, che ha usato il nickname di quello precedente, Dread Pirate Roberts: «*Silk Road è risorto dalle ceneri e ora è pronto ad accogliervi*».

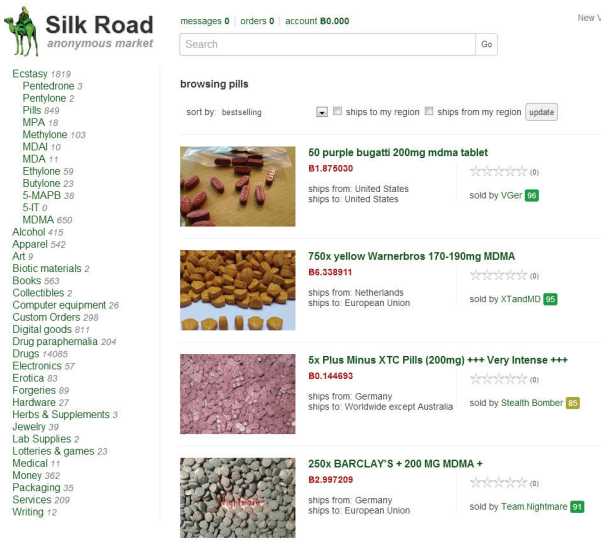

***Fig. 3** – Una Pagina di Silk Road 2.0.*

L'accesso avviene tramite registrazione: è sufficiente fornire un nome utente, una password, un codice identificativo per le transazioni e rispondere a un CAPTCHA[9] per accedere all'homepage e usufruire di tutti i servizi offerti e raggiungibili dall'homepage. Non tutte le pagine di Silk Road sono pubbliche: esistono, infatti, alcune pagine realizzate in modalità occultata denominata "stealth listings", di cui possono usufruire solo alcuni venditori, contattabili da una clientela selezionata solo attraverso messaggi privati in una specifica sezione ("Custom Orders", ordini personalizzati).

Silk Road si presenta come un intermediario, offrendo a venditori e acquirenti la propria struttura online allo scopo di condurre le transazioni in un ambiente sicuro, protetto, e soprattutto, anonimo. Sulla totalità dei prodotti offerti, che a ottobre 2014 consta di 14.095 differenti offerte, la maggior parte è composta dalla cannabis con il 18%, seguita dall'ecstasy e dagli stimolanti con

8 HyperText Markup Language (HTML): linguaggio di markup solitamente usato per la formattazione di documenti ipertestuali disponibili nel World Wide Web sotto forma di pagine web.

9 CAPTCHA "completely automated public Turing test to tell computers and humans apart": test fatto di una o più domande e risposte per determinare se l'utente sia un umano (e non un computer).

entrambi il 17%. A seguire troviamo psichedelici (15%) e farmaci (15%). Infine, con il 9% del totale, si trovano gli steroidi, con 4% sia i precursori sia gli oppioidi.

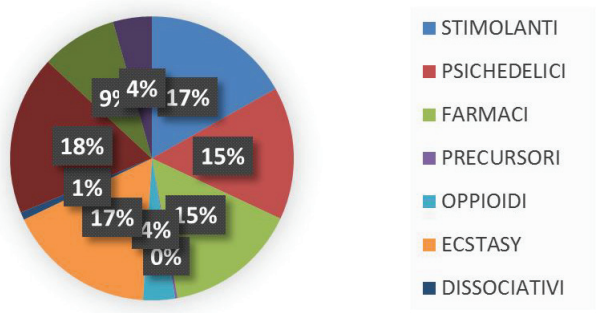

***Fig. 4** – Grafico delle percentuali sul totale delle droghe in vendita.*

In particolare la vendita di Cannabis, con i suoi sottoprodotti e preparazioni (526 diversi articoli), rappresenta, in data 1 novembre 2014, il maggior introito di Silk Road, coinvolgendo 192 venditori, di cui 162 dagli USA. La maggior parte di loro (152) vende al minuto, con quantità che vanno da un grammo fino al massimo di un etto di prodotto, per importi da 0,30 Bitcoin fino a due Bitcoin. 40 di loro invece vende anche all'ingrosso, offrendo quantità di merce da 1a 5 kg, con cifre che variano dai quindici ai 300 Bitcoin (per un controvalore al 13 novembre 2014 intorno ai 100.000 Euro). La maggior parte dei prodotti (131) è offerta al solo mercato statunitense, ventotto dagli USA a tutto il mondo, soprattutto le piante, e solo nove dagli USA verso il Canada. In data 1° novembre 2014, si contano 277 venditori di sostanze stupefacenti.
Per ognuno di loro è presente una pagina dedicata, che offre, al pari di un qualsiasi altro market online ben organizzato, tutte quelle informazioni che ne formano il profilo pubblico e che contribuiscono ad aumentarne la "reputazione". Essa è estremamente importante in una compravendita anonima basata unicamente sulla fiducia che il venditore riesce ad ottenere dal cliente e che gli permetterà quindi di espandere la propria attività. La pagina offre informazioni dettagliate su:

- profilo del venditore, le modalità di contatto, le valutazioni di gradimento oltre alle "news" sui prodotti e i servizi offerti;
- spedizione e pagamento:
  - *Packaging*: confezioni non appariscenti "business style" in busta a chiusura ermetica sottovuoto che garantisce l'integrità della merce e la mancanza di odori, resistente all'umidità a garanzia dell'arrivo a destinazione;
  - *Shipping*: spedizioni entro quarantotto ore senza spese di spedizione in tutto il mondo. Gli ordini superiori ai 200 dollari vengono spediti tramite i maggiori corrieri internazionali, come UPS; DHL, TNT , FedEx;
  - *Delivery time*: sono indicati i tempi medi per il ricevimento della merce per ogni paese (compresa la Città del Vaticano: interessante l'espressione "*you know you want it*"[10] riferita alla clientela);
  - *Refund*: modalità di rimborso in caso di non ricezione della merce;
  - *Privacy*: il venditore garantisce (?) che tutte le informazioni sull'identità dei clienti sono cancellate subito dopo transazione e spedizione andate a buon fine;
  - *Support*: è fornito un indirizzo email alternativo e una Chat in caso di non funzionamento del sito Silk Road. Inoltre viene fortemente raccomandato l'uso della crittografia in tutte le comunicazioni.

Una volta scelto il prodotto e inserito nel carrello personale, l'acquirente può passare al pagamento, unicamente tramite Bitcoin. Silk Road adotta il metodo del deposito di garanzia: il cliente non paga direttamente il venditore, ma deposita la cifra stabilita presso l'operatore del mercato che in tal modo controlla tutte le transazioni, trattenendo la propria percentuale e risolvendo eventuali dispute. Non sono permessi pagamenti diretti, pena l'espulsione. Silk Road avverte i clienti di effettuare acquisti solo presso venditori con feedback positivi e comunica che le commissioni saranno utilizzate per ripagare i clienti truffati, a riprova del "buon comportamento" della comunità di Silk Road.

Silk Road, come tutti i mercati *online* di prodotti illegali, allo scopo di garantire e garantirsi il più completo anonimato, protegge tutte le comunicazioni, dai messaggi email fino alle transazioni, tramite PGP (Pretty Good Privacy), metodo crittografico a doppia chiave. Esso si basa sulla generazione di una coppia di chiavi: una "segreta" e l'altra "pubblica". L'utente tiene al sicuro la propria chiave segreta mentre diffonde e rende disponibile la chiave pubblica. Ogni venditore possiede la sua coppia di chiavi crittografiche e comunica solo ed esclusivamente attraverso la propria chiave pubblica, che deve essere utilizzata dal cliente per criptare i propri messaggi verso di lui, firmandoli con la propria chiave privata, a garanzia della propria identità. È stato stimato che, nel caso di chiavi a 1024 bit, una rete di un milione di computer impiegherebbe $10^{\wedge 10}$ anni (un tempo pari all'età dell'Universo) per ricavare una chiave privata da una chiave pubblica

***Fig. 5** – Esempi di occultamento.*

10 "You know you want it": espressione inglese utilizzata nel gergo volgare col significato di: "sai di volerla, sai di averne bisogno".

Una volta che il cliente ha depositato il pagamento sul deposito di Silk Road, il venditore deve inviare la merce al cliente. Allo scopo di mantenere l'anonimato, è raccomandato di non utilizzare gli indirizzi privati delle abitazioni. Una volta ricevuta la merce, il cliente invia il feedback sul venditore, che riceve così il denaro sul proprio deposito.

A sostegno della "affidabilità" dei Black Market, esiste inoltre nel Deep Web un sito.*onion* denominato *"All Market Vendor Directory"* che offre una panoramica veloce sui principali market aperti, i loro venditori, e persino una pagina dedicata ai venditori estromessi dai mercati perché "compromessi" da un cattivo comportamento. A ogni venditore che vi aderisce, è dedicata una pagina in cui se ne riporta la reputazione, i market dove è presente e da quanto tempo, il nickname utilizzato, il numero di transazioni effettuate ed un recapito email.

Silk Road Reloaded

Il 6 novembre 2014 Silk Road 2.0 viene chiuso. Questa volta, a finire in manette, è stato **Blake Benthall, ventisei anni, soprannome Defcon,** residente a San Francisco, considerato il capo di Silk Road 2.0.
In data 12 gennaio 2014 il sito *reddit.com* riporta la notizia della nuova versione di Silk Road, accessibile non più da Tor ma da un'altra rete, I2P, che sfrutta un protocollo diverso e che permette la visualizzazione dei domini con estensione I2P.
La scelta della rete I2P sembra basata sul fatto che I2P offre un maggior grado di decentralizzazione, poiché implementata su svariati database distribuiti in rete in modalità peer-to-peer invece che sulle directory di Tor, ed anche, non meno importante, sul fatto che, mentre gli sviluppatori di Tor sono noti, i creatori di I2P restano anonimi. Un messaggio, con l'identico spirito di Silk Road 2, spiega: *"Chi siamo noi? Siamo quelli che hanno a cuore la vera libertà, l'autodeterminazione e l'autocontrollo. Che ci crediate o no voi siete i padroni di voi stessi. Che cosa significa esattamente? Molte cose, ma, prima di tutto che noi né nessun altro ha il diritto / privilegio di dirvi che cosa fare con la vostra persona, a qualsiasi livello, tranne / a meno che non danneggi un'altra persona o una sua proprietà ".*

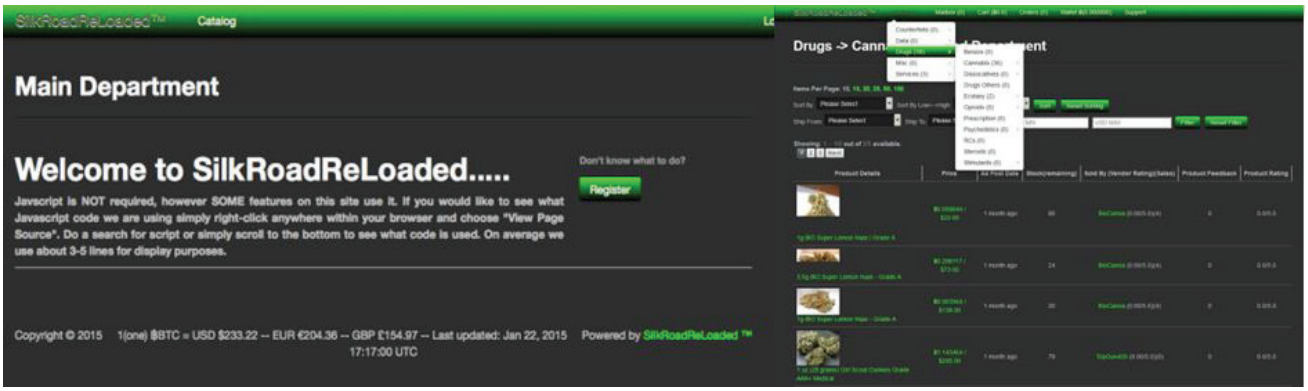

***Fig. 6** - Silk Road Reloaded sotto I2P.*

Silk Road Reloaded presenta un catalogo di svariate sostenze stupefacenti, denaro falso, false identità e tool per attacchi informatici. Supporta transazioni con diverse criptovalute convertendole in Bitcoin: gli *Anoncoin*, i *Darkcoin*, che a novembre sono stati ammessi come valuta su Nucleas, un bazar di Tor, i Dogecoin, i *Litecoin* e tutti gli otto tipi di *Altcoin*. I gestori del sito guadagnano una percentuale su ogni vendita e in questa nuova versione anche per ogni conversione di nuova valuta in Bitcoin.

Questo rilancio di Silk Road Reloaded dimostra che si possono implementare con relativa facilità innumerevoli alternative a Tor ed ai Bitcoin, azzerando in questo modo tutti gli sforzi fatti dalle forze dell'ordine per chiudere i Black Market nel Deep Web. Il fatto che Silk Road sia stato chiuso ed abbia riaperto subito dopo per ben 3 volte, porta a concludere che il sequestro dei Black Markets non sia un'azione da sola efficace nel contrasto alla vendita online di sostanze stupefacenti. Un affermato venditore di droga online (pseudonimo *Carlo Lopez*), intervistato tramite uno scambio di email criptate, da Kate Knibbs di Gizmodo nel luglio del 2014, afferma che Silk Road, come singolo mercato non è il futuro del contrabbando nel Deep Web: " *per qualsiasi sito web la longevità è di vitale importanza e secondo il mio pensiero, come fornitore serio e a lungo termine, i market vanno decentralizzati*".

I nuovi mercati peer-to-peer[11] della rete I2P non hanno un "Dread Pirate Roberts" al timone. Senza una figura centrale da arrestare e un data center posizionato su un unico server, ma distribuito invece su migliaia di macchine, diviene assai difficile per le forze dell'ordine individuare un Black Market con tale configurazione. Utilizzando questo modello si creano di fatto diversi mercati senza una locazione precisa e senza un amministratore centrale, e le forze dell'ordine dovrebbero gettare una rete molto più ampia per individuare e arrestare venditori e gli acquirenti. Un esempio di tale architettura distribuita è OpenBazaar, un mercato online destinato a divenire il rivale di Ebay, che rappresenta un interessante modello di sviluppo per le transazioni peer-to-peer a cui riferirsi per l'implementazione di una posizione più sicura per i Black Market.

11 Peer-to-peer: rete di computer o qualsiasi rete informatica che non possiede client o server fissi, ma un numero di nodi equivalenti (peer) che fungono sia da client che da server verso altri nodi della rete. Mediante questa configurazione qualsiasi nodo è in grado di avviare o completare una transazione. I nodi equivalenti possono differire nella configurazione locale, nella velocità di elaborazione, nella ampiezza di banda e nella quantità di dati memorizzati.

Conclusioni

Alla luce di quanto fin qui analizzato in ordine alla descrizione delle peculiarità della vendita di sostanze illegali dei Black Market, del profilo degli venditori e del loro modus operandi, è lecito concludere che solo un'attenta e specifica attività di sorveglianza della rete nel suo complesso può diminuire i rischi derivanti da tale incombente minaccia.
Gli analisti hanno la consapevolezza che l'intuizione della minaccia incombente e presente, insieme alla sua corretta comprensione, possono consentire l'elaborazione completa dei rischi da questa derivanti e lo studio delle ipotesi di contrasto e contenimento dei rischi stessi.

L'adozione di una Strategia di sicurezza interna U.E.[12] costituisce lo sforzo principale per raggiungere tali obiettivi; in tale contesto viene esaminato il SOCTA che è frutto del lavoro degli analisti di Europol. Il SOCTA, attraverso il modello europeo di analisi criminale (ECIM [13]) , elabora le informazioni provenienti dalle Forze di Polizia degli Stati Membri e non solo. Gli analisti di Europol osservano che la criminalità organizzata sta crescendo in dimensioni e complessità mantenendo un elevato traffico di droghe e delle sostanze chimiche essenziali per la loro produzione o complementari agli stupefacenti.
Le O.C. hanno diversificato l'offerta attraverso l'uso dei mezzi di comunicazione disponibili, *in primis* il web attraverso il *trade-on-line*, procurandosi in tal modo profitti eccezionali. Infatti il bacino dei consumatori europei di sostanze d'abuso resta in ogni caso un mercato con elevata disponibilità economica favorito dalla normativa interna all'Unione Europea che facilita le operazioni doganali determinando una grande vulnerabilità della regione.[14]

La disputa, quindi, sulla libertà della rete in tutte le sue declinazioni si scontra necessariamente con la tutela della privacy *versus* sicurezza nazionale e regionale.
Attualmente una possibilità dissuasiva nei confronti degli operatori commerciali che vendono beni o servizi illegali nella rete potrebbe essere una apposita previsione comunitaria secondo la quale gli autori di tutti i reati commessi attraverso l'uso di Internet, e quindi non solo quelli afferenti al tipico scenario di *cybercrime* o *cyberwar*, vengano colpiti da una aggravante della pena edittale del reato principale.

Tale proposta acquisirebbe un concreto valore dissuasivo solo quando le istituzione governative preposte alla prevenzione ed al contrasto della criminalità siano dotati di mezzi e strumenti in grado di poter effettuare il riconoscimento certo o la georeferenziazione del venditore e dell'acquirente. ©

Bibliografia essenziale

- Colombini Clara Maria, Tesi di Master:"*Profilazione ed analisi del fenomeno Black Market nel Deep Web per il contrasto alla vendita online di sostenze stupefacenti e psicotrope*" Master di 2° Livello in "Sistemi e Tecnologie Elettroniche per la Sicurezza, la Difesa e l'Intelligence", Facoltà di Ingegneria, Università di Roma Tor Vergata, 2015.
- Colombini Clara Maria, Colella Antonio, IISFA Chapter, *La Rete e le Informazioni*, 2011.
- Colombini Clara Maria, Colella Antonio, Mattiucci Marco, ARES 2012, *Network Profiling: Content Analysis of Users Behaviour in Digital Communication Channels*, Springer, 2012
- Colombini Clara Maria, Colella Antonio, Mattiucci Marco, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA): *Digital scene of crime: technique of profiling users*, 2012.
- Caradonna Mirna, *L'Europa, il crimine e gli scenari di rischio,* Rivista Trimestrale della Scuola di Perfezionamento per le FF.pp. Anno 2012, n.1-2. *Dragos Comaneci, Protecting Internet Anonymity with TOR* - The Onion Router Protocol, www.ixiacom.com.
- Europol, *The Internet Organized Crime Threat Assessment (IOCTA),* European Cybercrime Centre EC3, 2014.
- FBI - *Bitcoin Exchangers Plead Guilty in Manhattan Federal Court in Connection with the Sale of Approximately $1 Million in Bitcoins for Use on the Silk Road Website*, 2014.
- FBI, *Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website*, 2014.
- *Gianaroli Alessia, La risorsa HUMINT ed i sistemi tecnologici di ricerca informativa. Metodologie a confronto.* Tesi di Laurea Multinational Intelligence Studies Campus, AA 2013-2014.
- Marino Antonio, *Le nuove frontiere dell'illegalità a mezzo Internet*, 2013.
- Rapetto Umberto, *Cyberlaundering - Il riciclaggio del terzo millennio,* in Gnosis - Rivista italiana di Intelligence, n. 14/1999.
- Teti Antonio, *Bitcoin, la moneta del Cyberspazio*, Gnosis 2/2012.
- UNODC, World Drug Report 2013. ◊

12 Adottata dal Consiglio Europeo con provvedimento 5842/2/10 del 23/03/2010.

13 European criminal intelligence model.

14 Cfr. M. Caradonna "L'Europa, il crimine e gli scenari di rischio" Rivista Trimestrale della Scuola di Perfezionamento per le FF.pp. Anno 2012, n.1-2