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

RESOCONTO STENOGRAFICO

79.

SEDUTA DI MARTEDÌ 13 GIUGNO 2017

PRESIDENZA DEL PRESIDENTE **MARIO CATANIA**

INDICE

PAGINA BIANCA

PRESIDENZA DEL PRESIDENTE MARIO CATANIA

La seduta comincia alle 14.35.

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

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso impianti audiovisivi a circuito chiuso e la *web-TV* del canale satellitare sul sito Internet della Camera.

(Così rimane stabilito).

Audizione del Segretario Generale della Federazione contro la Pirateria Musicale e Multimediale PFM, Luca Vespignani.

PRESIDENTE. L'ordine del giorno reca l'audizione del Segretario generale della Federazione contro la pirateria musicale e multimediale, Luca Vespignani. Il dottor Vespignani è accompagnato dal dottor Signorelli e dal dottor Pantaleo.

Il tema su cui abbiamo oggi l'audizione è, ovviamente, quello della contraffazione, correlata, da un lato, ai temi degli audiovisivi e dei prodotti musicali e, dall'altro, alla problematica sul *dark web*, relativamente alla quale il dottor Vespignani ritiene – così ci ha fatto sapere – di avere cose importanti da comunicare.

Do la parola al dottor Vespignani.

LUCA VESPIGNANI, *Segretario generale della Federazione contro la Pirateria Musicale e Multimediale FPM*. Innanzitutto grazie a tutti e buongiorno. Ho cose importanti nel senso che siamo arrivati a un punto in cui la tutela della proprietà intellettuale dei marchi ha raggiunto un livello di sofisticazione estremamente efficace. I risultati che abbiamo ottenuto nel mondo della musica, che rappresento qui, lo dimostrano. La crescita del mercato è dovuta all'esplosione del mercato legale, ma anche a efficacissimi interventi da parte delle forze dell'ordine e della magistratura, nonché, a livello normativo, ad alcune modifiche che hanno sicuramente aiutato.

Facciamo attenzione, però, perché adesso abbiamo il problema del *deep web* e del *dark web*. La storia della lotta alle violazioni del diritto d'autore e dei marchi è sempre stata una storia in cui le imprese sono sempre state in ritardo. Forse diventa opportuno, quindi, cominciare a pensare in anticipo alle potenziali strategie e agli strumenti da utilizzare per un fenomeno che oggi è ancora poco conosciuto, che è appunto quello del *deep web*.

Innanzitutto sfatiamo qualche mito. Quando si parla di *deep web*, si pensa a qualcosa di estremamente sofisticato, misterioso e inaccessibile. Paradossalmente, non lo è. Paradossalmente, il 95 per cento di Internet è *deep web*. Non è quello che vediamo. Quello che vediamo è una piccolissima parte.

Noi siamo cresciuti nell'ottica per cui Internet è il motore di ricerca e quello che digitiamo su Google e troviamo è il *web*. No, quella è una piccolissima parte del *web*. In realtà, il 90-95 per cento è composto di *deep web*, ossia di risorse che non possono essere raggiunte con i normali sistemi di navigazione. In fondo a questo *deep web* c'è un pezzettino, un 5 per cento, che è il *dark web*. Lì cambia ancora la prospettiva. Questo *web* continua a essere

inaccessibile e irraggiungibile da molti punti di vista, ma pone una serie di problemi anche molto seri.

Non sto a tediarvi con la definizione dei vari livelli, anche perché poi lascerò la parola a Marco Signorelli per una descrizione più tecnica. Il concetto sostanzialmente è che tutto quello che sta nel *deep web* consiste in risorse informatiche tradizionali – siti, *blog*, *forum*, documenti, immagini, *file* di qualsiasi genere – che non sono collegate fra di loro e sono contenuti dinamici, che non possono essere raggiunti da motore di ricerca. Di fatto, se non si hanno le chiavi per andare a trovare questi documenti, non si può intervenire.

Infatti, se andate a vedere la *slide* con la tabella, vedete che indicizzato e accessibile è Internet come noi lo conosciamo. Non indicizzato, ma accessibile volendo, è il *deep web*, in cui c'è una marea di documenti, perché ci sono documenti dell'amministrazione pubblica e altri documenti. Se guardate la pagina in cui c'è la raffigurazione del *deep web* come *iceberg*, notate che ci sono informazioni accademiche, risorse, documenti medici e documenti legali, tutti non linkati, ma potenzialmente accessibili, se si conosce la chiave per accedervi.

A parte tutte le risorse che vi ho detto, assolutamente legali ma non accessibili, da un dato punto in poi, in profondità, esiste il *dark web*, dove cominciamo a incontrare pedopornografia, vendita di armi, siti di organizzazioni terroristiche, prostituzione di tutti i tipi e droga, tantissima. Il *dark web* è diventato il principale sistema di smercio di stupefacenti. Non è più la strada, non sono più i canali tradizionali, ma è il *dark web*. Se vedete le immagini di fianco a questa raffigurazione del *web* profondo, notate che le vetrine a disposizione sono infinite.

Di contraffazione il *deep web* è pieno. Ho scelto alcuni esempi in maniera veramente casuale. Avrei potuto sceglierne decine e decine di altri. Vedete che alcuni dei principali *marketplace* del *deep web* nascono, vivono e si sviluppano soltanto per la vendita di materiale contraffatto. Vedete esempi sugli orologi e sull'abbigliamento, ancora esempi su abbigliamento e su accessori da abbigliamento con i più noti marchi.

Ho citato – lascerò poi la parola a Marco Signorelli – l'esempio più classico perché mi offre la possibilità di introdurre due o tre concetti fondamentali. L'esempio più classico è quello di *Silk Road*, ossia la Via della Seta, che una volta era la via per il commercio fra l'Impero cinese e Roma e adesso è diventata, invece, qualcosa di molto meno nobile e un contributo molto minore allo sviluppo delle culture e delle economie di imperi così distanti fra di loro. Era diventata il principale luogo di smercio di qualsiasi tipo di oggetto o sostanza illegale, ovviamente, su Internet.

Perché la cito ? Perché mi offre la possibilità di dire che occorre fare attenzione, perché tutti gli strumenti che abbiamo messo a punto fino a oggi non funzionano. Avrete sentito parlare di indagini delle forze dell'ordine con tracciamenti *online* degli IP, blocchi dei siti, sequestro dei siti, filtraggio dei nomi di dominio e sequestro dei nomi di dominio. Niente di tutto questo funziona sul *deep web*. Non si può intervenire in questa maniera. Paradossalmente, c'è una sorta di regressione. Si torna a forme di investigazione molto più tradizionali. Alla fine, infatti, ci saranno un paio di spunti su come poter intervenire. Mi riferisco alle cosiddette fonti OSINT.

Marco Signorelli sarà molto più chiaro. Gli lascio la parola perché è lui il tecnico.

MARCO SIGNORELLI, *Head of Anti-Piracy della Federazione contro la Pirateria Musicale e Multimediale FPM*. Per poter parlare di *deep web*, anche per affrontare le problematiche cui si va incontro nella fattispecie dell'*enforcement* e della tutela, bisogna comprendere esattamente come funziona questa comunicazione all'interno del *deep web*, nonché del *dark web*.

Le caratteristiche principali della comunicazione all'interno del *deep web* sono due, principalmente. Una è basata su un sistema di reti definite decentralizzate, le cosiddette reti *peer-to-peer*, in cui ogni nodo od ogni macchina che compone questa rete ha sia funzione di *client*, quando richiede i dati, sia funzione di *server*, quando fornisce i dati.

L'altra particolarità di questa comunicazione è che avviene tramite una cosiddetta crittografia simmetrica. La comunicazione viene effettuata attraverso lo scambio di una coppia di chiavi, chiave pubblica e chiave privata. Le due chiavi sono correlate matematicamente tra loro, ragion per cui i messaggi codificati con la chiave pubblica possono essere letti solo dalla corrispondente chiave privata.

C'è un esempio nella *slide* che ho riportato, senza entrare troppo nei tecnicismi, in cui si mostra come il messaggio di Alice, che deve comunicare a tale Bob, utilizzi la chiave pubblica di Bob e solo Bob, conoscendo la propria chiave privata, possa leggere questo contenuto.

Questi due princìpi fondamentali sono quelli che caratterizzano, nella *slide* successiva, il protocollo di comunicazione che viene utilizzato sul *deep web* e sul *dark web*, che è il TOR, che sta per *The Onion Router*. La caratteristica principale di questo protocollo è che comprende queste due particolarità, ossia si basa su rete distribuita *peer-to-peer* e crittografia simmetrica.

Perché The Onion Router ? Perché il messaggio viene impacchettato come se ci fossero dei *layer*. Vengono creati tanti *layer* quante sono le varie macchine attraverso le quali questo messaggio deve essere veicolato.

Nella *slide* successiva ho cercato di fare una rappresentazione il più schematica possibile di come avviene una comunicazione. Come vedete, sulla sinistra è rappresentato il mittente. Quando il mittente cerca di inviare un messaggio al destinatario, interroga la rete distribuita su TOR. Vengono individuati i nodi attraverso i quali il messaggio verrà inviato e per ogni nodo – i ruoli principali sono mittente, *entry-node*, *node*, *exit-node* e destinatario – che tratterà questo messaggio viene decriptata la parte di proprio interesse, che viene spedita al successivo nodo. Solo il destinatario finale vedrà il messaggio in chiaro.

Un'altra particolarità del servizio TOR sono i cosiddetti *hidden service*. Vado avanti in maniera molto semplice e pratica. Cosa sono gli *hidden service* ? Sono i siti *web*, sostanzialmente, tutti i servizi che vengono pubblicati all'interno della rete TOR, che si distinguono per l'estensione .onion. L'estensione .onion è stata così riconosciuta dall'*Internet Engineering Task Force* con l'RFC 7686 come un'estensione privata, che pertanto non deve essere assegnata e controllata dall'ICANN, l'ente che gestisce i nomi di dominio e le varie estensioni.

Di conseguenza, queste estensioni non vengono riconosciute nel mondo Internet normale. Se provo a navigare su un sito con estensione .onion, non ci riuscirò mai. Devo per forza e necessariamente accedere all'interno di TOR. I *software* che sfruttano TOR riescono a riconoscere questa estensione e, quindi, rimbalzano queste richieste all'interno della rete TOR fino ad arrivare al destinatario.

Uno degli aspetti che legano un po' quello che diceva prima Luca Vespignani sul fatto che all'interno del *deep web* e anche del *dark web* i contenuti non vengano indicizzati è molto chiaro quando si pensa che questi fenomeni vengono riconosciuti con dei siti *web*, con dei nomi a dominio con estensione .onion. Il nome dominio, però, non vi è riconducibile. Spesso è rappresentato semplicemente da caratteri alfanumerici e può cambiare nel tempo.

Come si fa a conoscere quali sono i siti all'interno del *deep web* ? Esistono degli aggregatori, dei motori di ricerca, nonché delle specie di Wikipedia – dopo vediamo un esempio – all'interno dei quali si può andare e trovare le informazioni, a meno di non entrare nelle comunità e nei *forum* chiusi e cercare le informazioni. Da lì vengono promossi i vari *marketplace*, quelli che abbiamo visto prima.

Che cosa occorre per navigare all'interno del *deep web* ? Occorrono sicuramente un TOR *browser*, che simula la connessione alla rete TOR, ed eventualmente altri strumenti specifici per TOR, come – ne cito alcuni – Freenet, I2P e Osiris. La moneta di scambio all'interno di queste comunità è il *bitcoin*, che ha anche una stessa caratteristica. È inutile spiegarlo qui. Penso sia ormai abbastanza chiara la definizione di *bitcoin*. Tale moneta sfrutta anch'essa le reti decentralizzate *peer-to-peer*. È completamente anonima e rapida,

nel senso che le transazioni hanno una velocità semplicemente data dal calcolo delle macchine: quando viene elaborata una transazione, nel tempo in cui arriva a destinazione la transazione è avvenuta.

Nelle pagine successive mostro un esempio molto pratico di navigazione sul *deep web*. Connettendosi nella rete TOR, viene assegnato un indirizzo IP all'interno di questa rete. La propria macchina diventa, in questo caso, un nodo della rete. Ho raffigurato un esempio del famoso Wiki nascosto, una sorta di enciclopedia in cui vengono elencati i principali *marketplace* della contraffazione e di tutti i vari materiali che possono essere venduti all'interno del *deep web*.

L'esempio successivo è una rappresentazione di *The Pirate Bay*. *The Pirate Bay* è abbastanza noto anche qui in Italia perché è stato inibito, inizialmente nel 2008, poi con Cassazione nel 2010. Ha subìto dall'Italia un'inibizione a livello IP e DNS. *The Pirate Bay* è un sito *Torrent*, un *tracker* di *Torrent* molto famoso a livello internazionale. L'Italia si è distinta qualche anno fa ed è riuscita a ottenerne l'inibizione dall'Italia, ovviamente chiedendo l'inibizione ai *service provider* italiani.

The Pirate Bay è stato uno dei primi portali per la musica pirata ad approdare anch'esso sul *deep web* proprio per evitare queste tipologie di censure. Nella rappresentazione che vedete si può notare che il nome di *The Pirate Bay* all'interno del *deep web* non è *The Pirate Bay*, ma un acronimo composto da una serie di caratteri alfanumerici.

È rappresentato in rosso il percorso che ha fatto il mio *browser*, in quel caso, per arrivare fino all'*onion site*, ossia fino al sito. Vedete che dal mio *browser* sono passato dalla Francia e due volte in Germania, oltre che per altri *relay*, che sono altri nodi della rete TOR, sempre per il concetto che spiegavo velocemente prima. Così si è arrivati a destinazione sul sito.

Le principali problematiche di *enforcement* in questo settore sono sicuramente la cifratura e l'anonimato, perché le comunicazioni avvengono in forma criptata. Compromettere l'anonimato in questo caso è molto più difficile, perché tutti i nodi coinvolti nella comunicazione dovrebbero essere complici e coordinati. Proprio per il motivo che spiegavo prima, ogni volta che passa la comunicazione all'interno di un nodo è comunque cifrata.

Si aggiunge la dinamicità degli eventi e degli stati, considerato che un sito TOR con estensione .onion può cambiare rapidamente. Anche questo determina delle problematiche. Un conto è dire che oggi il sito AZ2 si presentava in un dato modo. Domani AZ2 – sto sparando, ovviamente, esempi pratici – potrebbe non esistere più. Magari esiste su un altro nome a dominio.

Un'altra delle problematiche determinata dal fatto che sia tutto cifrato è l'individuazione degli *Internet service provider* coinvolti. Una delle metodologie *best practice* da utilizzare o da osservare per questa tipologia di fenomeno è rappresentata da un presidio di monitoraggio fisso, ossia da una costante osservazione del fenomeno.

Sicuramente è vero quello che accennava prima il dottor Vespignani, ossia che si torna un po' alle origini. Bisogna, infatti, incrociare l'investigazione da *web investigator* a quella classica da investigatore di strada. Perché ? Perché nelle informazioni che posso trovare all'interno del *deep web* ci possono essere dei dati e degli indizi che possono ricondurre al mondo reale. L'unione delle due metodologie di indagine e di osservazione è sicuramente una buona norma da seguire.

L'altro punto che avevo inserito riguarda le infiltrazioni. Potrebbe comportare, ovviamente, la commissione di reati, ma parlo dell'agente « sotto copertura ». Cosa vuol dire ? Si tratta di farsi invitare nei *forum*. Abbiamo parlato tanto di *forum* chiusi, di *forum* privati in cui si può vedere quello che c'è dentro solo se si viene invitati. Si devono, quindi, intrattenere dei rapporti con questi signori. Si parla di conversazioni con i *target* fino ad arrivare alle prove d'acquisto della merce.

Parlando di prove d'acquisto della merce, trovo interessante la collaborazione con gli spedizionieri, perché tutto quello che viene acquistato in questo mondo oscuro passa poi nel mondo reale. L'osservazione e la

collaborazione con gli spedizionieri e la raccolta delle informazioni presso questi potrebbero essere utili al fine delle indagini, fino ad arrivare al *follow the money*. Esistono già delle *best practice* anche in tema di criptomoneta che possono determinare i responsabili dell'illecito commesso all'interno del *deep web*.

LUCA VESPIGNANI, *Segretario Generale della Federazione contro la Pirateria Musicale e Multimediale FPM*. Tenete conto che il passaggio di *The Pirate Bay* al *deep web* è particolarmente significativo, perché *The Pirate Bay* è sempre stato il sito che ha anticipato le contromisure per sfuggire a qualsiasi tipo di *enforcement*. Oggi molti siti hanno già fatto un passo in più e sono passati dal *web* normale ai cosiddetti servizi CDN, ossia *CloudFlare* e servizi simili, che in qualche misura – non completamente – li proteggono da qualsiasi tipo di intervento. *The Pirate Bay*, non a caso, è già passato al *deep web*. Questo è il chiaro segnale che il futuro della contraffazione e di qualsiasi tipo di comportamento illecito sul *web* sarà quello.

Abbiamo provato a immaginare pochissimi punti che potrebbero essere la chiave per intervenire sul fenomeno nel futuro: formazione tecnico-informatica e investigativa e investimenti grossi in tecnologia. Chiunque si dovrà fare carico di andare a fare dei monitoraggi sul *deep web* e sul *dark web* si troverà a dover gestire una quantità di dati che non è neanche lontanamente paragonabile a quella che viene gestita oggi. Va introdotto, quindi, anche il concetto, per esempio, di *self-learning machine*. Diversamente, se non ci saranno dei sistemi che siano in grado di autoapprendere dai monitoraggi precedenti, sarà impossibile fare dei monitoraggi approfonditi.

Una piccola cosa è l'agente provocatore. Oggi, per esempio, nel mondo del *copyright* non si può utilizzare l'agente provocatore. Sarebbe un reato. Sul *deep web* è lo strumento principale di intervento. Senza l'agente provocatore, ossia quello che, come diceva il dottor Signorelli, si infiltra e fa parte della comunità, nel *deep web* non si riescono a ottenere risultati significativi dal punto di vista della tutela della proprietà industriale e intellettuale.

Se ci sono domande, siamo a disposizione.

PRESIDENTE. Intanto vi ringrazio per le cose che ci avete detto, che integrano un'audizione precedente che avevamo già fatto sul tema. La vostra documentazione, a una prima visione, mi pare molto utile, anche perché è intellegibile, ben ordinata ed esposta in modo logico.

Ho due domande veramente da uomo della strada. Con riguardo alla prima, abbiamo già ascoltato nell'audizione precedente, e voi ce lo riconfermate oggi, che il *deep web* rappresenterebbe il 90-95 per cento della movimentazione complessiva su Internet.

La domanda che vi faccio – scusate l'ingenuità – è la seguente: mi colpisce questo dato, perché nella percezione comune e nella vita comune conosco centinaia, o migliaia di persone che navigano su Internet e faccio fatica a conoscerne una che vada sul *deep web*. Com'è questa discrasia tra il mondo reale di chi naviga, le persone, noi tutti, e il dato del circolante ? Questa è la mia prima domanda.

Passo alla seconda domanda, che non ho fatto in tempo a fare l'altra volta. Nel *deep web*, dove peraltro non tutto è illegale – ce l'avete già detto; anzi, una parte della movimentazione non lo è – comunque è fondamentale questo sistema TOR, che è sostanzialmente il raccordo di tutta questa movimentazione.

La domanda che vi faccio, anche questa da uomo della strada, è: come nasce TOR, chi c'è dietro TOR, chi costruisce TOR ? Ci sono elementi del sistema che non possono venire dal basso. Devono avere avuto comunque un'impostazione – non voglio dire una regia – su cui poi magari dal basso si è costruito.

Do la parola agli auditi per la replica.

LUCA VESPIGNANI, *Segretario Generale della Federazione contro la Pirateria Musicale e Multimediale FPM*. Intanto rispondo alla prima domanda. Ovviamente, quando parliamo del 90-95 per cento, in-

tendiamo che il 90-95 per cento delle risorse, del materiale che costituisce il *web* nel suo complesso è *deep web* e *dark web*. È ovvio che ciò è inversamente proporzionale, come diceva giustamente il presidente, al numero di persone che accedono a quelle risorse.

Sono molte, molte meno le persone che accedono alle risorse del *deep web* e del *dark web*. Chi vi accede ? Vi accedono i professionisti in un determinato settore. Parlavamo prima, per esempio, dei documenti istituzionali, dei documenti medici e dei documenti legali, che sono nel *deep web* perché non devono essere di libero accesso. In quel caso saranno i professionisti di riferimento che vi accedono. Al *dark web* accede soltanto chi vuole commettere un crimine, fondamentalmente, ossia chi vuole vendere o acquistare materiale che non sarebbe liberamente vendibile.

Sulla questione TOR poi magari il dottor Signorelli vi fornirà una spiegazione più tecnica. È sempre il vecchio problema. A monte questa tecnologia è neutrale. C'è qualcuno che ha sviluppato un protocollo di comunicazione che potenzialmente avrebbe potuto essere usato per comunicazioni assolutamente legali. Nel caso di TOR il protocollo è già nato con la volontà di creare un sistema criptato che ufficialmente doveva tutelare in maniera estremamente accurata la *privacy* di coloro che comunicavano. In realtà, è nato già con l'obiettivo di sfuggire a qualsiasi tipo di controllo. A monte, però, rimane un protocollo di comunicazione neutro. Il problema è l'utilizzo che se ne fa.

MARCO SIGNORELLI, *Head of Anti-Piracy della Federazione contro la Pirateria Musicale e Multimediale FPM*. Quanto ai cenni storici, il protocollo TOR nasce agli inizi degli anni Novanta su mandato da parte del US Naval Research Laboratory per criptare le conversazioni che avvenivano all'interno dello scambio militare. Dopo gli anni Novanta il progetto fu portato avanti, sempre in ambito militare, con l'aiuto di altre fondazioni.

Nel 2006, se non sbaglio, nasce la Fondazione TOR Project, un'associazione privata che riceve fondi. Si tratta di liberi contributi da parte di chiunque, dei cittadini. La base era proprio un sistema di comunicazione per cifrare comunicazioni segrete militari di un ente militare americano.

PRESIDENTE. Faccio fatica a cogliere il meccanismo per cui questa fondazione privata riceve volontari contributi da privati cittadini. L'esperienza insegna che normalmente dietro ai meccanismi di questo genere, ma non solo, c'è sempre un utile. Qui dov'è l'utile ?

LUCA VESPIGNANI, *Segretario Generale della Federazione contro la Pirateria Musicale e Multimediale FPM*. Non sono solo privati cittadini. Sono anche aziende tecnologiche, talora rilevanti. L'utile, o comunque l'investimento, per queste aziende tecnologiche è comunque l'essere parte di un progetto che si suppone, o si spera, sia innovativo e diventi poi sfruttabile commercialmente nel futuro.

Ufficialmente la comunità di TOR nasce, o comunque si sviluppa e opera, semplicemente per garantire una sorta di Internet libero. Dopodiché, la storia ha dimostrato che molte di queste presunte associazioni per lo sviluppo di sistemi di comunicazione criptati, in realtà, consentivano dei guadagni a chi queste associazioni o queste fondazioni le gestiva. Ufficialmente il concetto è chiedere fondi per sviluppare una tecnologia che consenta il libero scambio di informazioni senza possibilità di censura o di intervento coercitivo.

PRESIDENTE. Pongo un'ultima domanda. Premesso tutto questo, cos'è che distingue il *dark* dal *deep web*, semplicemente il contenuto, la materia ? Per il resto si muovono esattamente allo stesso modo e dentro la stessa cornice. Quello che fa la differenza è soltanto il fatto che in un caso trattiamo di illeciti e nell'altro no, oppure ci sono anche ambiti diversi nell'ottica di Internet ?

LUCA VESPIGNANI, *Segretario Generale della Federazione contro la Pirateria*

Musicale e Multimediale FPM. Sicuramente la differenza sta nel contenuto, questo sicuramente. Nel *dark web* la grandissima maggioranza, se non la totalità, dei contenuti consiste in contenuti o materiali illegali. Cambiano anche, però, le modalità di accesso. Il *deep web* è semplicemente quello che dicevo all'inizio di questa presentazione: si tratta di documenti che non sono rintracciabili dai motori di ricerca. Tendenzialmente, sono legali. Nel *dark web* ci vuole qualcosa di più. Per accedere a quei siti è richiesto l'utilizzo di tecnologie complesse e i siti sono molto più protetti.

MARCO SIGNORELLI, *Head of Anti-Piracy della Federazione contro la Pirateria Musicale e Multimediale FPM*. Si può pensare al *dark web* quando ci sono dei *forum*, per esempio, dei *marketplace*, ossia dei mercati *online*, sempre all'interno, ovviamente, di questa fetta nascosta, che rendono visibile il contenuto solo agli utenti che sono stati iscritti. Sono comunità chiuse. Già lì si parla di *dark web*, perché quella comunità non è raggiungibile neanche al *deep web*. La si può vedere, ma poi, per accedere, si deve entrare in contatto, ricevere delle credenziali e accedere. Allora si parla di *dark web*. Poi, ovviamente, il contenuto è quello che differenzia anche questa definizione.

PRESIDENTE. Ho due domande. Sui *social* a volte ci sono dei sistemi ad accesso limitato. In questo caso possiamo parlare comunque di qualcosa di assimilabile o no ?

L'altra domanda che volevo fare in relazione alla sua risposta è la seguente: comunque il *dark web* si muove dentro il sistema TOR, o no ?

MARCO SIGNORELLI, *Head of Anti-Piracy della Federazione contro la Pirateria Musicale e Multimediale FPM*. Credo di poter rispondere a entrambe le domande con una risposta. La prima domanda era se alcuni *social network*, essendo anch'essi protetti da un accesso con credenziali, possano rientrare nel *dark web*, se ho compreso bene. No, perché si parla comunque di *dark web* e di *deep web* quando queste comunicazioni avvengono attraverso il protocollo TOR. Questa è la prima distinzione.

Con questa rispondo anche alla seconda domanda, ossia che è necessario l'utilizzo del protocollo TOR. È lo strumento di comunicazione utilizzato nel *deep* e *dark web*, in tutto ciò che è nascosto al mondo Internet.

PRESIDENTE. Bene. Credo sia stata una giornata molto utile, sicuramente a me, per la crescita nella comprensione di tutto questo tema, ma anche a tutta la Commissione. Vi ringrazio e dispongo che la documentazione prodotta sia allegata al resoconto stenografico della seduta odierna.

Dichiaro chiusa l'audizione.

La seduta termina alle 15.05.

Licenziato per la stampa
il 20 gennaio 2018

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

ALLEGATO

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

ROMA - 13 GIUGNO 2017

DEEP WEB: DEFINIZIONE, CARATTERISTICHE, PERICOLI, SFIDE

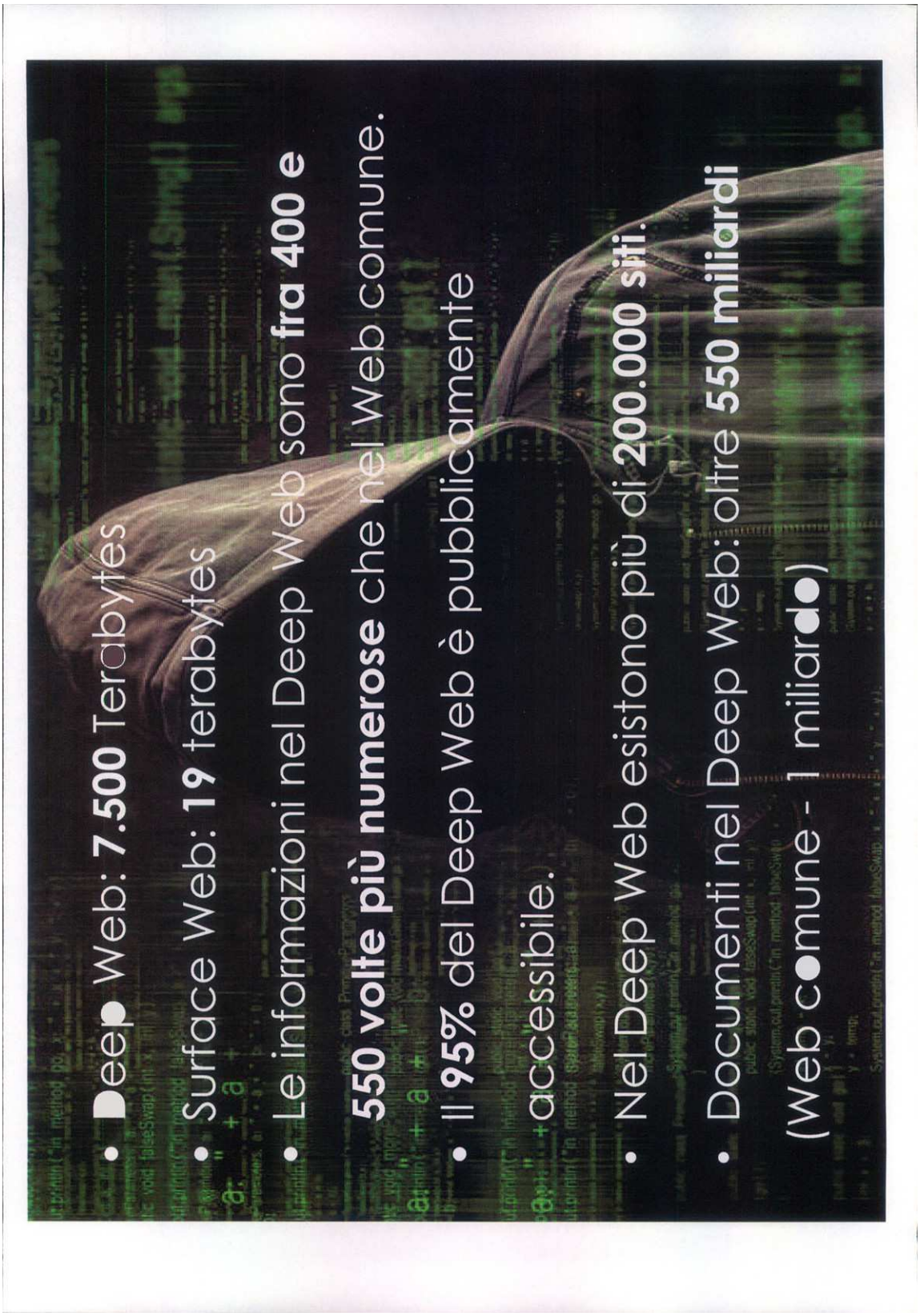
FPM
Federazione contro la Pirateria Musicale e Multimediale

digital content protection

FPM
Federazione contro la Pirateria Musicale e Multimediale
FPM (Federazione contro la Pirateria Musicale e Multimediale) viene fondata nel 1996 da IFPI (International Federation of the Phonographic Industry) e da FIMI (Federazione Industria Musicale Italiana) con lo scopo di proteggere i diritti di proprietà intellettuale dei suoi associati e di sensibilizzare le istituzioni e l'opinione pubblica sui rischi e i danni causati dal fenomeno.
digital content protection
DcP è una start up nata dall'esperienza ultra decennale di FPM nel settore della tutela dei diritti di proprietà intellettuale e industriale. DcP opera a protezione del diritto d'autore, dei marchi e dei diritti della persona, offrendo servizi professionali di alto profilo tecnologico nell'ambito della brand & content protection, della forensic e della web reputation.


Google
Bing
Wikipedia
DEEP WEB
Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information
Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.
Social Media
Multilingual Databases
Financial Records
Government Resources
Competitor Websites
Organization-specific Repositories
(DARK WEB)
A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. Deep Web Technologies has zero involvement with the Dark Web.
Illegal Information
Drug Trafficking sites

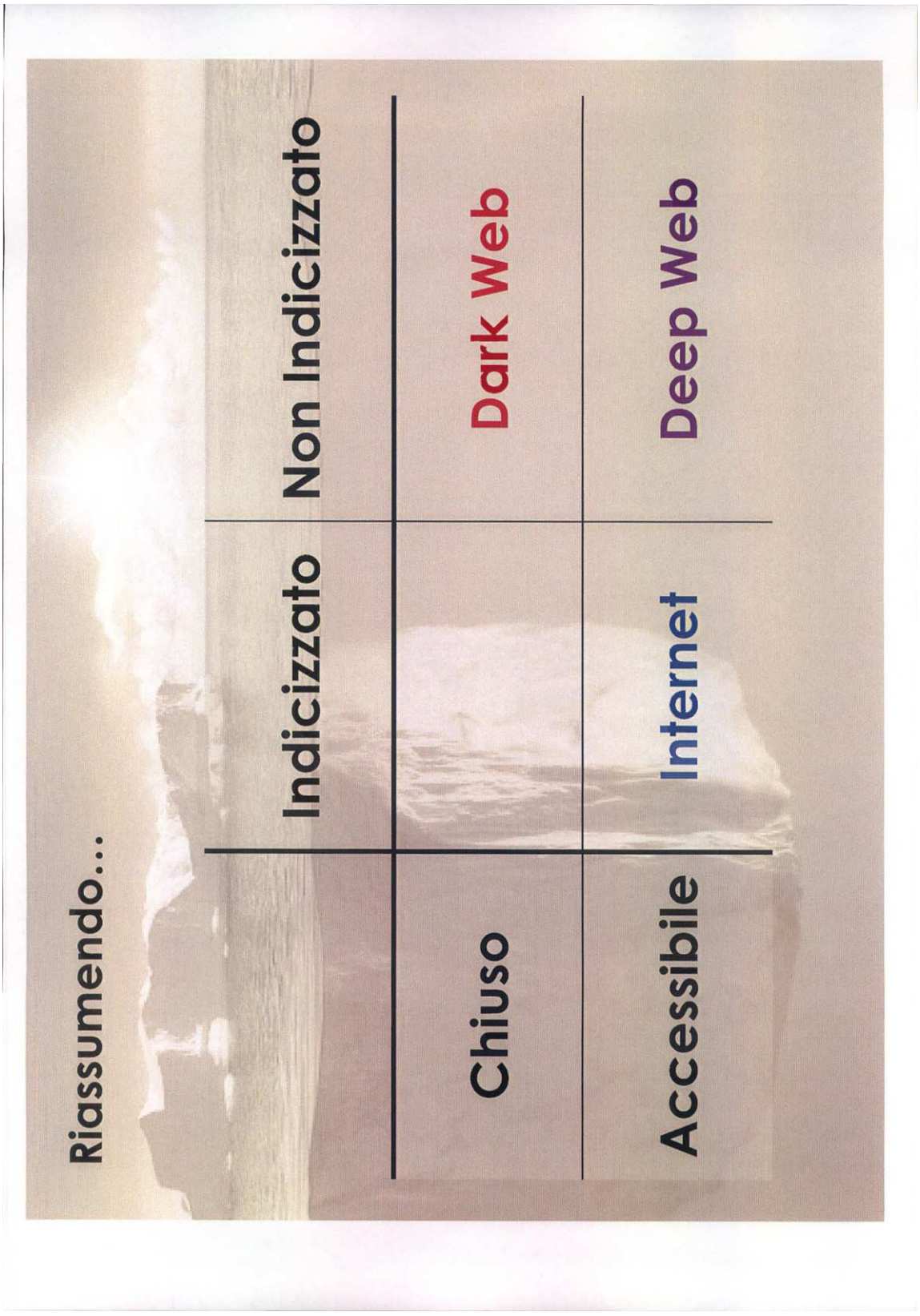
Livelli del Deep Web
Livello 1 – Web Comune: composto da siti che utilizziamo tutti i giorni e totalmente accessibili.
Livello 2 – Surface Web: dove operano server informatici e siti come Reddit
Livello 3 – Bergie Web: ultimo livello del Web accessibile senza uso di particolari strumenti o conoscenze. Contiene siti e risultati di ricerca nascosti da Google.
Livello 4 – Deep Web: stai entrando a tutti gli effetti nel Web Sommerso, a cui si può accedere attraverso la rete anonima TOR.
Livello 5 – Charter Web: contiene forum dedicati ad attività illegali dove gli scambi commerciali si effettuano con la moneta del luogo: il Bitcoin.
Livello 6 – Marianas Web: chiamato in questo modo in riferimento alla fossa delle Marianne, è la fonte delle più note leggende metropolitane della Rete e dicono che contenga l'80 % di tutto il Web.


• Deep Web: 7.500 Terabytes
• Surface Web: 19 terabytes
• Le informazioni nel Deep Web sono fra 400 e 550 volte più numerose che nel Web comune.
• Il 95% del Deep Web è pubblicamente accessibile.
• Nel Deep Web esistono più di 200.000 siti.
• Documenti nel Deep Web: oltre 550 miliardi
(Web comune - 1 miliardo)

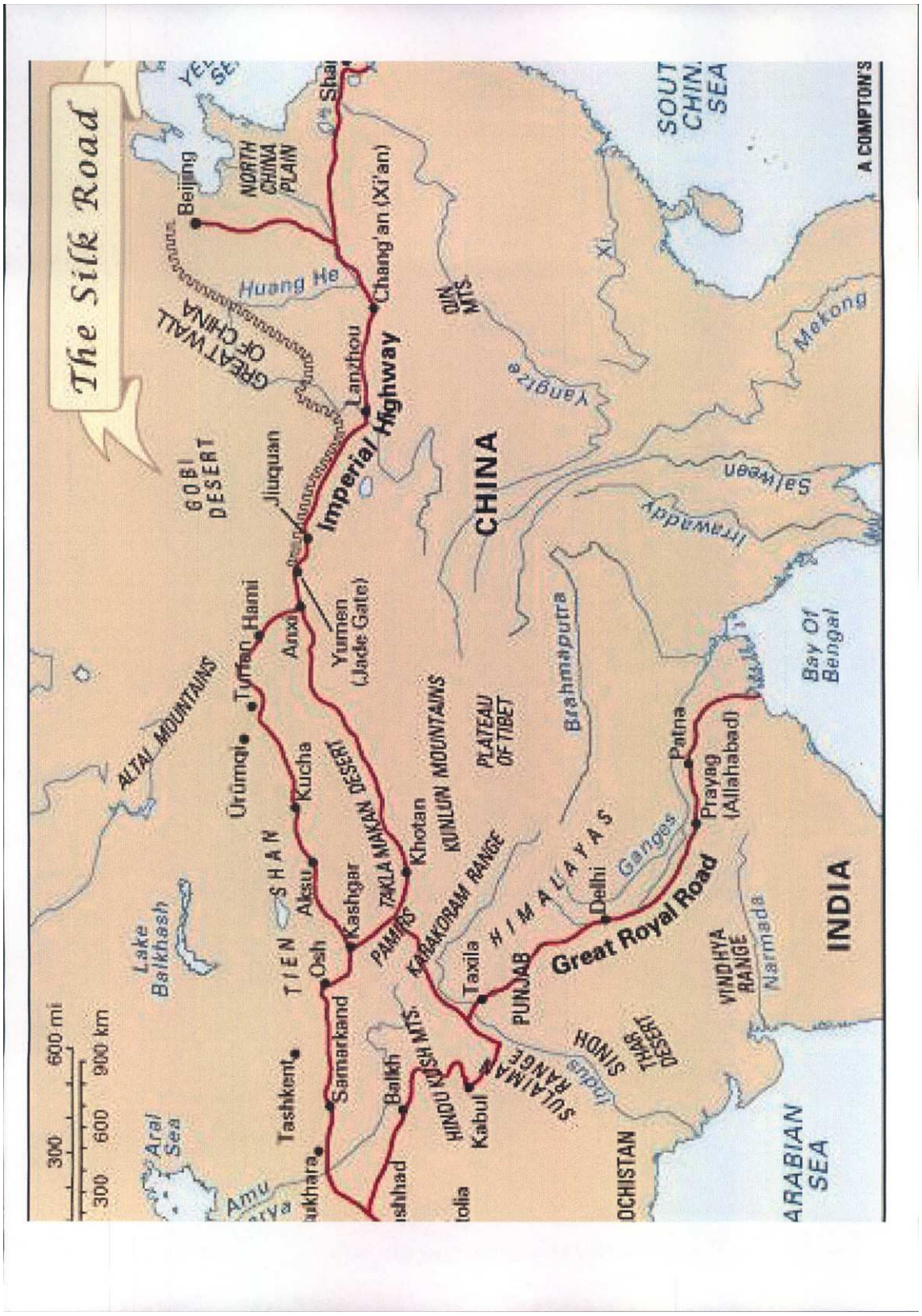
Un po' di storia...
• Internet degli inizi: solo pagine statiche facilmente raggiungibili tramite motori di ricerca
• A metà degli anni 90: introduzione delle pagine dinamiche accessibili via link e query
• 1994: Jill Ellsworth conia il termine "Web invisibile"
• 2001: Bergman conia il termine "DEEP WEB"
• Il DARK WEB si sviluppa parallelamente

Contenuti del deep web

•**Contenuti dinamici**: pagine web dinamiche, ovvero pagine Web il cui contenuto viene generato sul momento dal server, che possono essere richiamati solo compilando un form o a risposta di una particolare richiesta;
•**Pagine non collegate**: pagine Web che non sono collegate a nessun altra pagina Web. Se l'accesso non è impedito da adeguate impostazioni di sicurezza, il motore indicizza la parent directory del sito, che contiene non solo le pagine visibili, ma tutto ciò che è caricato nel server ospitante;
•**Pagine ad accesso ristretto**: siti che richiedono una registrazione o comunque limitano l'accesso alle loro pagine impedendo che i motori di ricerca possano accedervi;
•**Script**: pagine che possono essere raggiunte solo attraverso link realizzati in JavaScript o in Flash e che quindi richiedono procedure particolari;
•**Contenuti non di testo**: file multimediali, archivi Usenet, documenti scritti in linguaggio non HTML, in particolare non collegati a tag testuali (tuttavia alcuni motori di ricerca come Google sono in grado di ricercare anche documenti di questo tipo);
•**Contenuti banditi dai comuni motori di ricerca** perché illegali: di questa categoria fanno parte siti pedo-pornografico o snuff, commercio e produzione illegale di droghe e armi, siti sottoposti a censure governative, siti di warez e malware;
•**Software:** certi contenuti sono nascosti intenzionalmente al normale Internet, e sono accessibili solo con software speciali, come Tor, I2P o altri darknet software. Per esempio Tor consente ai propri utenti di accedere anonimamente a siti che utilizzano il suffisso .onion, nascondendo il loro indirizzo IP.


Riassumendo...
Indicizzato
Non Indicizzato
Chiuso
Accessibile
Internet
Dark Web
Deep Web


Cosa si trova nel Deep (Dark) Web?
You usually only see about 10% of what's on the internet.
What's on the Deep Web?
child pornography
guns
assassins
terrorism
prostitutes
sex
drugs
What is the Deep Web?
It's a part of the internet that is invisible. It began in 1994 as the Hidden Web, and was renamed Deep Web in 2001.
It offers anonymity and freedom to anyone posting there.
Searching google will not get you into the Deep Web.
The other 90% of the internet you don't see is the Deep Web
How do I get there?
These sites are locked down so tightly, you need a special browser to access them.
Tor (short for The Onion Router) is the main portal to the Deep Web. It encrypts the user's information a number of times, in layers like an onion, and sends it to a wide network of volunteer servers all over the world. This technique makes it almost impossible to track users or their information.
The WikiLeaks site operated in the Deep Web, before it went public.
The group Anonymous has used the Deep Web not only for direct actions but also to organize itself.
QMI AGENCY


The Silk Road
Beijing
NORTH CHINA PLAIN
Huang He
GREAT WALL OF CHINA
Chang'an (Xi'an)
Lanzhou
Jiuquan
GOBI DESERT
Imperial Highway
Yumen (Jade Gate)
Anxi
Turfan
Hami
Ürümqi
Kucha
Aksu
Kashgar
Khotan
TAKLA MAKAN DESERT
KUNLUN MOUNTAINS
PLATEAU OF TIBET
CHINA
GUN MTS.
Yangtze
Mekong
Xi
SOUTH CHINA SEA
Salween
Irrawaddy
Brahmaputra
Bay Of Bengal
ALTAI MOUNTAINS
TIEN SHAN
Lake Balkhash
Osh
Tashkent
Samarkand
Aral Sea
Amu
PAMIRS
KARAKORAM RANGE
HINDU KUSH MTS.
Balkh
Kabul
Taxila
HIMALAYAS
PUNJAB
Delhi
Ganges
Patna
Prayag (Allahabad)
Great Royal Road
VINDHYA RANGE
Narmada
SULAIMAN RANGE
Indus
SINDH
THAR DESERT
INDIA
ARABIAN SEA
OCHISTAN
300 600 900 km
300 600 mi
A COMPTON'S

Silk Road
anonymous market
messages 0 | orders 0 | account ฿0.00
Search
Go
Hi,
log
a few words
the Dread Pirate Rc
Shop by Category
Drugs 6,625
Cannabis 1,080
Dissociatives 190
Ecstasy 829
Opioids 382
Other 450
Precursors 59
Prescription 1,429
Psychedelics 828
Stimulants 1,079
Apparel 310
Art 114
Biotic materials 1
Books 858
Collectibles 1
Computer equipment 43
Custom Orders 60
Digital goods 590
Drug paraphernalia 247
Generic XANAX (Alprazolam 1mg): 400 pills Grade A+
฿1.52
Pure Oxycodone HCL Powder (OC, Roxy)- 1/4
฿0.53
TESTOSTERONE CYPIONATE 250mg/ml x 10
฿0.69
25x 130mg MDMA CAPS(FREE SHIPPING)
฿1.62
100 GR - MDMA 84%
Pack of Five (5) Suboxone (Buphrenorphine) 8mg/2mg
SALE SALE!!!!!! 250 grams METHYLONE!
MJ/Methylone
Bring on the Shadow People! New batch MDPV
News
Closing the Al
A brand new I Silk Road!
The gift that k giving
Who's your fa
Acknowledgin

Brevi cenni sulla vicenda Silk Road

Silk Road
anonymous market

- Nel 2011 appare un link a Silk Road su un forum nel Web Comune (richiesta informazioni per acquistare funghi allucinogeni) – **Tentativo di pubblicizzare il sito -** Nello stream di MSG compare un indirizzo di Gmail
- FBI e HSI iniziano a indagare e tramite richiesta di file di log a Google, risalendo all'utilizzo di una VPN in un internet cafè di San Francisco
- Iniziano appostamenti, indagini e pedinamenti che consentono di individuare Ross Ulbricht (Dread Pirate Roberts). Parallelamente iniziano indagini sulla presenza sui Social di Ulbricht
- Ulbricht commette una **serie di errori**:
  - Utilizzo di nickname riconoscibili
  - Tentativo di acquistare documenti falsi
  - Tentativi di assoldare un killer nel deep web
- **Errore** di configurazione di un captcha che rivela l'IP
- Hackeraggio?
- **Pedinamento finale fisico e digitale** – Ulbricht arrestato e poi condannato all'ergastolo

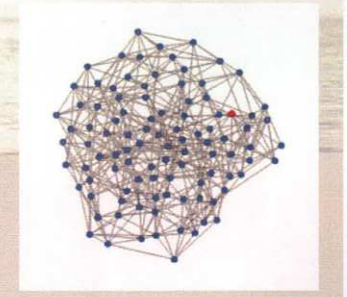

New seller accounts
silkroadvb5piz3r.onion
Startpage
THIS HIDDEN SITE HAS BEEN SEIZED
by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney's Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York


Indagine da molti punti di vista «tradizionale»
Fonti OSINT
THIS HIDDEN SITE
Southern District of New York
New seller accounts
silkroadvb5piz3r.onion
Startpage

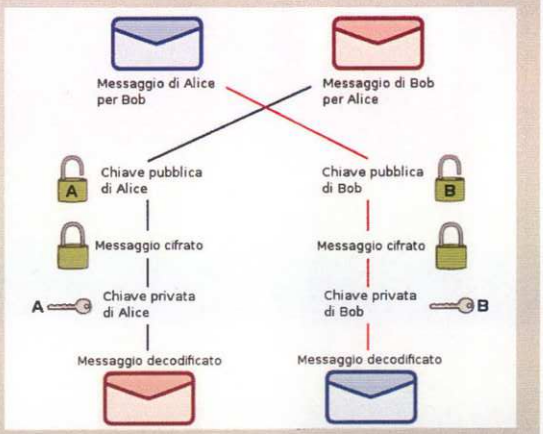
DeepWeb e la comunicazione cifrata (TOR)

Cenni fondamentali comunicazione TOR

- **(1)** Sfrutta la logica di comunicazione **P2P** (cd. peer to peer) dove non vi è una distinzione tra client e server, la rete si dice infatti paritaria in quanto tutti i computer che ne fanno parte si chiamano nodi ovvero hanno un ruolo sia da **client** (quando richiedono i dati) che da **server** (quando forniscono i dati)



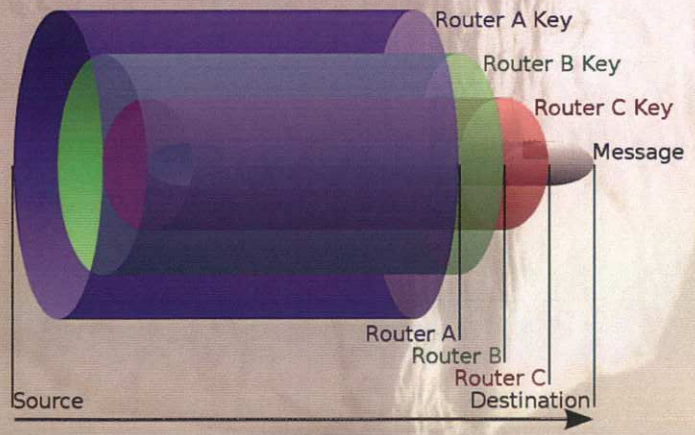
- **(2)** Comunicazione a **crittografia asimmetrica** ovvero su un sistema che utilizza una coppia di chiavi - una chiave pubblica e una privata. Le due chiavi sono correlate matematicamente, per cui i messaggi codificati con la chiave pubblica possono essere decodificati solo da chi possiede la chiave privata e viceversa. La forza di questo sistema è che anche conoscendo la chiave pubblica, non è possibile risalire alla corrispondente chiave privata



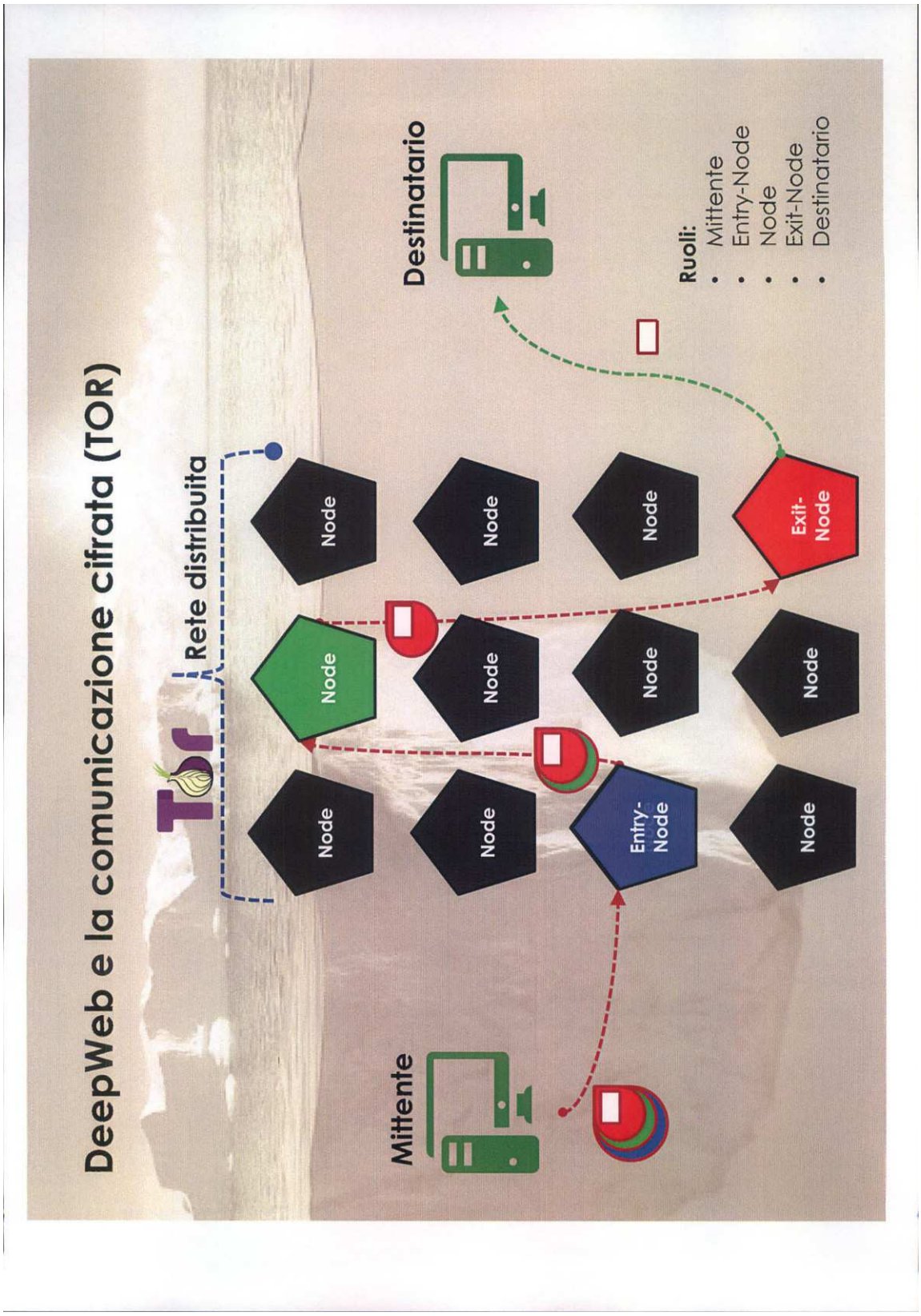
DeepWeb e la comunicazione cifrata (TOR)

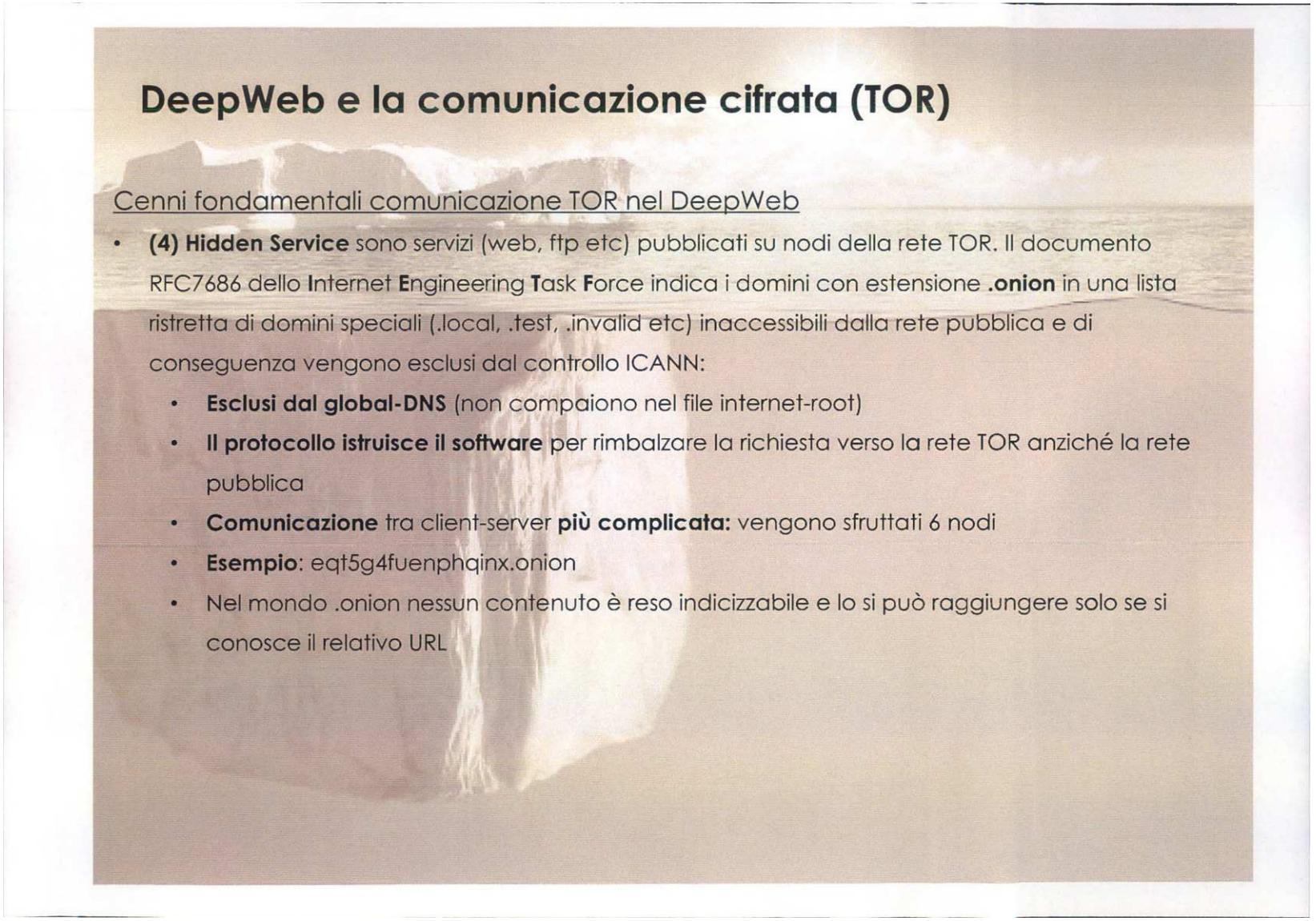
Cenni fondamentali comunicazione TOR

- **(3) TOR** (The Onion Router) è il protocollo di comunicazione utilizzato nel Deep Web. Risolve il problema dell'anonimato integrando la logica di rete **P2P** con la **crittografia asimmetrica**: ogni nodo che riceve il pacchetto di dati conosce solo il nodo precedente e quello successivo a cui spedirlo, inoltre i percorsi mutano continuamente e sono scelti in fase di invio.



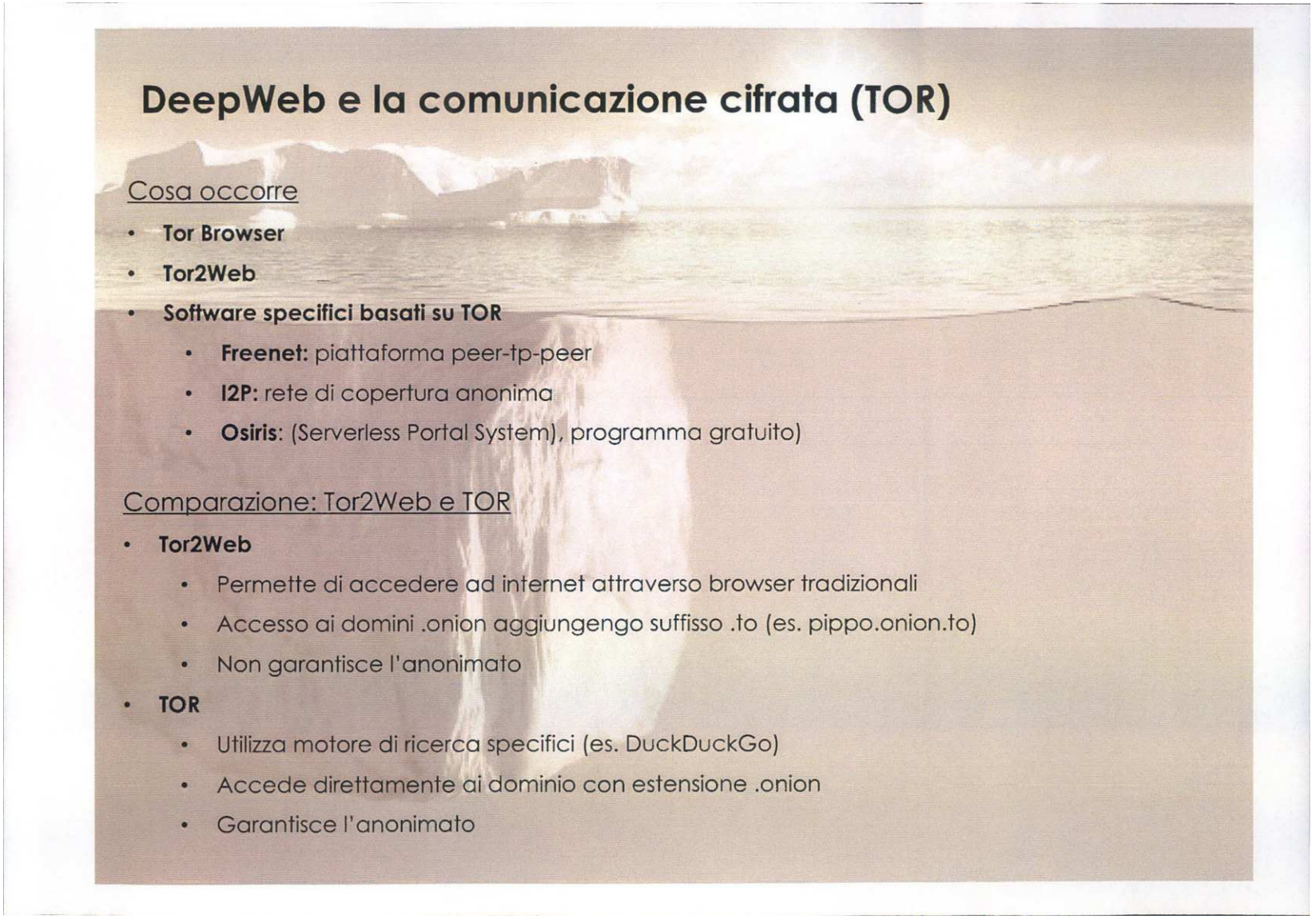
Fonte Wikipedia: E' un sistema di comunicazione anonima per Internet basato sulla seconda generazione del protocollo di rete di onion routing. Tramite l'utilizzo di Tor è molto più difficile tracciare l'attività Internet dell'utente; difatti l'uso di Tor è finalizzato a proteggere la privacy degli utenti, la loro libertà e la possibilità di condurre delle comunicazioni confidenziali senza che vengano monitorate


DeepWeb e la comunicazione cifrata (TOR)
Rete distribuita
Mittente
Destinatario
Ruoli:
Mittente
Entry-Node
Node
Exit-Node
Destinatario
Node
Entry-Node
Exit-Node


DeepWeb e la comunicazione cifrata (TOR)
Cenni fondamentali comunicazione TOR nel DeepWeb
• (4) Hidden Service sono servizi (web, ftp etc) pubblicati su nodi della rete TOR. Il documento RFC7686 dello Internet Engineering Task Force indica i domini con estensione .onion in una lista ristretta di domini speciali (.local, .test, .invalid etc) inaccessibili dalla rete pubblica e di conseguenza vengono esclusi dal controllo ICANN:
• Esclusi dal global-DNS (non compaiono nel file internet-root)
• Il protocollo istruisce il software per rimbalzare la richiesta verso la rete TOR anziché la rete pubblica
• Comunicazione tra client-server più complicata: vengono sfruttati 6 nodi
• Esempio: eqt5g4fuenphqinx.onion
• Nel mondo .onion nessun contenuto è reso indicizzabile e lo si può raggiungere solo se si conosce il relativo URL

DeepWeb e la comunicazione cifrata (TOR)

La pubblicazione di servizi tramite Onion introduce ulteriori layer di sicurezza per ottenere maggiore garanzia di anonimato e impossibilità di monitoraggio delle attività.


DeepWeb e la comunicazione cifrata (TOR)
Cosa occorre
Tor Browser
Tor2Web
Software specifici basati su TOR
Freenet: piattaforma peer-tp-peer
I2P: rete di copertura anonima
Osiris: (Serverless Portal System), programma gratuito)
Comparazione: Tor2Web e TOR
Tor2Web
Permette di accedere ad internet attraverso browser tradizionali
Accesso ai domini .onion aggiungengo suffisso .to (es. pippo.onion.to)
Non garantisce l'anonimato
TOR
Utilizza motore di ricerca specifici (es. DuckDuckGo)
Accede direttamente ai dominio con estensione .onion
Garantisce l'anonimato

DeepWeb e la comunicazione cifrata (TOR)

Come si paga

- Sistemi di pagamento anonimi, criptomonete (prevalentemente BitCoin, poi Monero, ZCash)
  - Sfruttano tecnologie P2P e operano con logiche che escludono il controllo centralizzato
  - Transazioni elettroniche condotte attraverso URI (Uniform Resource Identifier), facilmente sfruttabile attraverso QR codes e smartphone

Caratteristiche

- **Decentralizzata**
  - Assenza autorità centrale per il controllo – ogni macchina che fa parte del network macina Bitcoin e processa transazioni
- **Anonima**
  - Nessuna associazione a dati identificativi della persona (nome, indirizzo etc)
- **Rapida**
  - Le transazioni vengono elaborate velocemente e i pagamenti arrivano in pochi attimi: giusto il tempo necessario al network per elaborare la transazione

DeepWeb e la comunicazione cifrata (TOR)
Esempio navigazione DeepWeb
Tor Status
Connecting to the Tor network
Establishing a Tor circuit
Please wait while we establish a connection to the Tor network. This may take several minutes.
Open Settings
Quit
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with DuckDuckGo.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
Tor Browser User Manual »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »
Main Page
Welcome to The Hidden Wiki
Editor's picks
Introduction Points
Financial Services

DeepWeb e la comunicazione cifrata (TOR)
Esempio navigazione DeepWeb
Download music, movies, g...
uj3wazyk5u4hnvtk.onion
Search
New Identity
New Tor Circuit for this Site
Security Settings...
Tor Network Settings...
Check for Tor Browser Update...
Tor circuit for this site
(uj3wazyk5u4hnvtk.onion):
This browser
France (51.254.112.52)
Germany (83.169.6.12)
Germany (62.138.7.171)
(relay)
(relay)
(relay)
Onion site
The Pirate Bay
Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100
Pirate Search
Preferences
Languages
All Audio Video Applications Games Porn Other
Pirate Search
I'm Feeling Lucky
How do I download?
Login | Register | Language / Select language | About | Blog
Usage policy | TOR | Doodles | Forum
BitCoin: 129TQVAroeehD9fZpzK51NdZGQT4TqifbG

Problematiche di enforcement

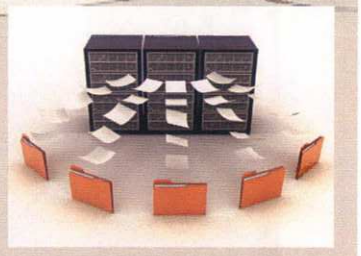
Le principali problematiche di enforcement del Deep e Dark Web

- **Cifratura** e **Anonimato**: le comunicazioni avvengono in forma criptata (vd. TOR). Compromettere l'anonimato è più difficile: tutti i nodi coinvolti nella comunicazione dovrebbero essere complici e coordinati
- **Dinamicità** degli eventi e degli stati: considerato che un sito TOR con estensione *.onion* può cambiare rapidamente il proprio indirizzo e che la comunicazione segue percorsi scelti randomicamente di volta in volta
- **Individuazione** degli ISP coinvolti

Metodologie di indagine

Metodologia

1. **Presidio e monitoraggio**: attività di osservazione costante, individuazione comportamenti e mappatura principali attori sia nel mondo "online" che "reale", attraverso big-data e machine-learning. . La prova viene raccolta e trattata come una normale evidenza su internet, seguendo le best-practice oramai consolidate
2. **OSINT**: raccolta informazioni e sviluppo degli indizi individuabili sia nel mondo deep/dark (es. indirizzi email, indizi contenuti nella cifratura PGP etc) che su internet (es. annunci Reddit etc)
3. **Infiltrazioni** (!! può comportare la commissione di reati !!), agente sotto-copertura:
   - Invito su forum/comunità chiuse
   - Conversazioni con i target
   - Prove di acquisto merce
- **Follow the money**: investigazioni su criptomoneta, blockchain etc
- **Collaborazione con spedizionieri:** dalla raccolta informazioni all'ispezione di spedizioni sospette



CALL TO ACTION
• **FORMAZIONE** tecnico-investigativa
• Investimenti in **tecnologia**
• Monitoraggi profondi
• Big data management
• Self-learning machine
• **Agente provocatore?**

FPM
Federazione contro la Pirateria Musicale e Multimediale
digital content protection
FPM - Federazione contro la
Pirateria Musicale e Multimediale
Via Leone XIII n. 14
20145 Milano
+39 02 76021377
www.fpm-antipiracy.it
DcP – Digital Content Protection S.r.l.
Via Leone XIII n. 14
20145 Milano
+39 02 76001356
www.dcpmail.it
Luca Vespignani
Segretario Generale
luca.vespignani@fpm-antipiracy.it
Luca.vespignani@dcpmail.it
Marco Signorelli
Direttore Strategie & Operazioni
Marco.signorelli@dcpmail.it
Marco.signorelli@fpm-antipiracy.it
Alcuni diritti