Dark Web & Bitcoin: Global Terrorism Threat Assessment

When Terrorist Groups can anonymously communicate and move untraceable Money

Lars Hilse, April 2013

V 1.1 (November, 2013)

Lars Hilse – Web Strategy & E-Business Development Consultants
Eichstrasse 10 B | 25767 Bunsoh | Germany
+1 (949) 208 4181 | +49 4835 9513027 | +44 845 5089559

WWW.LARSHILSE.COM

Table of Contents

Date of Initial Publication: April, 2013

1. Executive Summary

The years of the Post-9/11-Era have proven repeatedly, that some of the most important instruments in Counterterrorism are the interception of communication between suspects and the ability to determine conspicuous transfer of funding through the global banking-system.

What if these possibilities were taken from the intelligence community and law enforcement?

Our research has revealed that a part of the Internet, the so called Dark Web, enables criminals and terrorists to communicate in absolute anonymity through highly encrypted Email, Instant Messaging, and even entirely untraceable VOIP-calls. During these calls, both parties remain unidentifiable and their actual geo-location undeterminable.

Due to the anonymity it provides, the Dark Web is mainly used for criminal activities, a list of which we will outline in this paper.

The reason for such things as the Terrorist Finance Tracking Program (TFTP) to be initiated was to unveil conspicuous movements of money, enabling the Intelligence Community to associate these suspicious funds to individuals, which could then be flagged and/or investigated further.

Bitcoin, the Internet's digital currency, can be transferred globally between individuals (peer-to-peer), is absolutely untraceable and circumvents regulatory instruments like the TFTP, as it does not underlie any institutional control of financial authorities.

If Islamists, or other (cyber-)terrorist groups, due to increasing pressure by the Intelligence Community, harness these benefits to their advantage, law enforcement and the intelligence community will immediately lose the ability to investigate suspects using these methods.

We have come to the conclusion, that when the aforementioned instruments are utilized, a terror attack, significantly superseding the magnitude of 9/11 can be orchestrated and funded in absolute secrecy and without raising any flags until such a time, at which it is executed.

2. Dark Web

Like the World Wide Web (WWW) we use to communicate online, the Dark Web is a part/protocol of the entire Internet.

To access the Dark Web, third party software is necessary, but can be obtained legally on the WWW.

These access programs were invented to give political dissidents and other oppressed groups unmonitored and entirely anonymous access to the WWW.

To provide this level of anonymity, every connected client computer inside this network makes their IP available to other users, through which the encrypted traffic is routed, so that the actual user retrieving the content (illegal or not) cannot be identified or determined.

Like the WWW, the Dark Web offers the opportunity to provide content through servers inside these closed networks.

Other than on the WWW, the server operators and content providers remain anonymous, just like the client users retrieving and consuming this content.

2.1. Problems for the Intelligence Community

The aforementioned communication instruments present law enforcement and even the intelligence community with a variety of difficulties and disadvantages, the most prominent of which we will outline in the below categories.

2.1.1. Frequent Changes in Addresses and no Search Engines

According to an outdated study, less than 0.05% of the entire internet is indexed by search engines.

In this gigantic, un-indexed part lies the Dark Web.

And while there are search engines on the Dark Web, they hardly return any relevant results for content the submitting party intends to retrieve.

The more common way to obtain information on the Dark Web is by so called link lists and directories, which are manually updated; further, they are shared from person to person through anonymous email or IM services.

The manual updating of content is necessary because of the frequently changing addresses, a result of the content often being moved around different servers to reduce the risk of exploitation.

Unlike the WWW with its commonly known and easily identifiable address structure (http://www.fbi.gov), the Dark Web presents a more cryptic approach.

Some addresses do have parts of the website name in them (http://silkroad2eipagnk.onion – points to Silkroad, an online drug market place) yet still have parts of address name encrypted.

The fact that some of the crucial, updated addresses are given only to known insiders makes it very difficult for law enforcement to obtain them; even if the addresses are found, there is hardly any way to infiltrate the organizations running these operations.

2.1.2. Anonymous and Encrypted Communication Services

We've pointed out the technical similarities of the Dark- and the WWW earlier and because they are so alike, the Dark Web is not limited to websites being served.

Pretty much any form of communication available on the WWW is available on the Dark Net; the only, but very crucial difference is, that on the Dark Web we can't

- intercept or monitor communications taking place between two or more individuals
- categorize or associate it with an actual individual

due to the nature of the infrastructure, as all data is encrypted and routed through several nodes across the globe.

2.1.3. Anonymous and Untraceable Telephony

One of the advantages Law Enforcement and the Intelligence Community rely most heavily on is the possibility to intercept telephone conversations and Internet traffic between suspects, particularly those in organized crime and terrorist groups.

But not only the content of the conversations is crucial to building a case.

Pinpointing and tracking the location of individual suspects has become possible through triangular locating services by utilizing mobile broadcast towers, GPS or the technology in satellite telephones.

Certain Dark Web services allow individuals to circumvent all of these advantages, even on mobile devices.

1. Telephone conversations are encrypted from peer to peer
2. These conversations cannot be identified as VOIP calls
   a. They will appear as conventional, encrypted data-traffic in the ISP's protocols
3. Because this encrypted traffic is relayed through several nodes across the planet and the nodes are frequently changed
   a. The location of an individual can be deliberately masked and
   b. Their actual location will remain untraceable

2.1.4. Other Means of Anonymous and Untraceable Communication

In a recent paper several Intelligence Services came to the conclusion that the interception of conversations led through Apple's iMessage service appeared to be difficult.

Like the surface web (WWW), the Dark Web offers a variety of services that were built with the intent to make it impossible for communication to be intercepted.

In the case that the encryption is broken, the conversations cannot be associated to an individual.

Among these services are:

- Market Places
  Very much like Ebay and Amazon on the WWW only that these are used for drug/arms/information exchange (feature seller ratings, escrow, etc.); purchases are made anonymously through Bitcoin (see later section in this paper) and merchandise is sent through regular mail services. Recipient can deny to accept package if intercepted
- Email Services
  Features are very similar to conventional email services used on the WWW; providers of such services remain in the Dark Web and cannot be forced to give up suspicious accounts because the people running the services are indeterminable
- Instant Messaging
  Services feature same usability as WWW IM services only that the accounts are untraceable and cannot be associated to an IP address
- Peer-to-Peer (P2P) file exchange
  Platform similar to the torrent platform on the WWW only that data-traffic cannot be associated with an individual
- Forums/Message Boards
  Are technically very similar to those being operated on the WWW but accounts cannot be associated to individuals or their IP address/mobile account

3. Bitcoin

3.1. Technical Explanation

Bitcoin is a decentralized digital currency based on an open-source, peer-to-peer internet protocol. It was introduced by a pseudonymous developer named Satoshi Nakamoto in 2009.

Internationally, Bitcoin can be exchanged by personal computer directly through a wallet file or a website without an intermediate financial institution.

In trade, one Bitcoin is subdivided into 100-million smaller units called satoshis, defined by eight decimal places.

Bitcoin does not operate like typical currencies: It has no central bank and it solely relies on an internet-based peer-to-peer network.

The money supply is automated, limited, divided and scheduled and given to servers or "Bitcoin miners" that verify Bitcoin transactions and add them to an archived transaction log every 10 minutes.

The log is authenticated by ECDSA digital signatures and verified by the intense process of bruteforcing SHA256 hash functions of varying difficulty by competing "miners."

Transaction fees may apply to new transactions depending on the strain put on the network's resources.

Each 10-minute portion or "block" of the transaction log has an assigned money supply.

The amount per block depends on how long the network has been running.

Currently, 25 Bitcoin are generated with every 10-minute block.

This will be halved to 12.5 BTC during the year 2017 and halved continuously every 4 years after until a hard limit of 21 million Bitcoin is reached during the year 2140.

Bitcoin is the most widely used alternative currency: As of March 2013, the monetary base of Bitcoin is valued at over 400 million US dollars.

The large fluctuation in the dollar value of a Bitcoin has evoked criticism of Bitcoin's economic suitability as a currency.

Source: Wikipedia, retrieved on March 15th, 2013

3.2. Problems for the Intelligence Community

3.2.1. No Controlling Instances

One of the key advantages of money that is transferred through the conventional financial system is that it can be traced and in many cases associated or traced back to an individual, for instance through the American TFTP.

Because Bitcoin is transferred peer-to-peer, the traceability aspect is lost to Law Enforcement and the Intelligence Community.

Further, Bitcoin doesn't underlie the conventional banking system and is therefore out of the realm of financial authorities like Central Banks.

Even if the money would flow inside the global banking system, it could not be associated to an individual because the Bitcoin "Wallets" are kept encrypted like an anonymous Swiss, numbered account.

3.2.2. Assets cannot be Frozen or otherwise Seized

Because the Bitcoin system doesn't operate in the conventional banking system, assets traded therein cannot be seized or frozen, as there is no controlling instance to execute such orders.

This presents a major problem to Law Enforcement and the Intelligence Community.

If a terrorist/criminal group or an imminent terror attack were identified it could not be stopped by cutting the funding of such a group.

Bitcoins can be stored on a USB thumb drive or – for instance – stored on a server on the internet.

Unlike transporting large amounts of anonymous cash through airports/customs, with Bitcoin the amount of money transported is irrelevant to the size of the drive.

One Bitcoin takes up as much space as 1.000.000+ Bitcoins and customs officials would not know what they were looking for because USB drives have become one of the most commonly seen gadgets with every traveller.

3.2.3. Bitcoin can be "Laundered"

The Bitcoin system is in itself anonymous, yet presents a few, minute opportunities to identify funds obtained through criminal activity.

To eliminate this risk entirely, the Dark Web has a service providers specializing in laundering Bitcoin.

Like in the real world, funds are taken and replaced with Bitcoins with a clean history against a small fee for the service provider.

The fees charged for laundering Bitcoin is significantly smaller than laundering conventional currency.

3.2.4. Empowers untraceable Funding for (Cyber-)terrorism

The US Terrorist Finance Tracking Program (TFTP) offered some relief of tracking the assets of individuals believed to be engaging in – more or less – conventional terrorism.

However, with the age of cyber terrorism and cybercrime come new challenges, and among the most threatening is the creation of an untraceable Internet currency, entirely eliminating the possibility to track the movement of assets between individuals and organizations and revealing patterns of unusual movements of assets internationally.

Currently, the total Bitcoins in circulation amount to an estimated market value of about 400 million US Dollars and a lot of them are in possession of individuals.

With advances in technology, the 'mining' of Bitcoin will grow exponentially in the next couple of months, offering a much higher supply to the market.

Due to the ultimately fixed number of Bitcoins, the value of Bitcoin assets will increase in the future, a trend of which can be foreseen by the speculation-segments of the Bitcoin marketplace and exchanges.

Because it is entirely anonymous and absolutely untraceable, it has already become the number one asset in 'The Dark Web', an also entirely anonymous part of the Internet where a lot of the illegal activities are planned which are later executed on the surface web, the Internet you are aware of, the most prominent and widespread of which were the DOS-attacks following the freezing of assets in the Assange/Manning/Wikileaks case.

While the possibility of research into the Dark Web is limited, it has revealed numerous, generally illegal and terrorist-related activities.

Unlike the surface web, it doesn't offer any proper, consistent indexing through search engines because its infrastructure is much more dynamic through frequently changing servers and resource-addresses.

Facing ever-growing scrutiny through conventional surveillance and infiltration technology by law enforcement and the intelligence community, it is only a question of time until fundamental groups with hostile intentions will discover this network and enable them to communicate in absolute privacy.

Like the surface web, the dark web offers anonymous and encrypted email services, message boards, P2P file exchange and other means of communication, all of which are untraceable to the intelligence community and law enforcement bodies.

With the introduction of Bitcoin, it is now possible for these individuals and groups to transfer assets around the globe anonymously, funding operations in other parts of the world where the Bitcoin will be liquidated into other, more widely accepted currency like the US Dollar or the EURO.

3.2.5. Allows an absolutely uncontrollable Black Market

The recently uncovered Abdul Qadeer [AQ] Khan Network was probably the most prominent and staggering example of how a black market can function and remain hidden for decades under the eyes of the world.

It has to be kept in mind, that most communication between the involved parties were conducted through unencrypted PSTN, mobile networks and email.

Funds were transferred in ‘conventional’ US Dollar in exchange for blueprints, which were handed over on paper.

These traces allowed the intelligence community to ‘unwrap’ the Khan network to a certain extent, once the first strike was made.

If the Khan network had made use of the dark web for communications through encrypted email and used Bitcoin as the method of payment it would have been impossible to reveal at all and still in operation today.

Currently, the dark web is being used largely for

- The exchange of
  - Child-, animal- and other illegal pornography
  - Illegal substances (amphetamines, hashish, heroin, cocaine, etc.)
  - Compromising information of individuals
  - Hacked email and Social Media accounts
  - Scammed Credit Card numbers and Bank Account Information
- Preparing illegal 'hacktivist' operations (post-Assange-arrest DOS attacks on diverse financial institutions)

All of which are being paid for in absolute anonymity through Bitcoin.

3.2.6. Enables absolutely plausible deniability of foreign Governments and Institutions for involvement in 'Cyber-Attacks'

IP-tracing revealed that the recent cyber-attacks on military and government network infrastructures originated in China, but not even 'specialized' private companies were able to determine individuals or organizations and hold them accountable for these activities.

If these hackers had concealed their identity through a VPN or a chain of proxy-servers masked those efforts by using the tor-network (dark web entry-point) it wouldn't have been possible to even remotely associate these attacks to China.

In fact, the IP addresses which did show up as the source of these hacking-activities, which have drastically increasing both on government and private networks, could have already been 'spoofed' (masked) to point to China, granting another entity actually conducting these operations plausible deniability.

One of the problems with hacking has always been the 'finger-print' (in form of an IP address or similar traces) left behind when conducting such activity.

That was the reason industrial espionage was seldom conducted by means of hacking into networks, but rather through ‘social engineering’.

Current network flaws as the ones pointed out above, however, make it possible for the contractor of such activity to plausibly deny their involvement, and in more advanced cases even deflect attention from such activity towards unwanted competition in their field of business.

4. Examples of Crimes currently being committed

During our preliminary yet extensive research into the Dark Web we found an array of criminal activity.

We also found that when law enforcement agencies currently speak about ‘the dark side of the web’, they are often actually referring to publicly available websites.

Cautious reports estimate damages of cybercrime to the financial industry to be no less than 2 trillion USD annually; with a significantly increasing tendency.

The websites and infrastructure currently under scrutiny by law enforcement worldwide is merely the ‘retail’ hub for that specific field of business.

On these websites, credit card numbers are sold for upwards of 50 USD while the actual dark web offers them for a fraction of the costs in bulk.

4.1. Terrorism

Our research didn’t unveil a very large number of sites related to (Islamic) terrorism.

The ones we did find were in Arabic and mainly asking for donations.

Some, however, went as far as actively recruiting new members for ‘Jihad’ and shared ideological information (beheadings, IED attacks, etc.).

The problem will become imminent, when larger numbers of extremists will be forced underground by the increasing pressure put upon them through surveillance of law enforcement and the intelligence community.

It is only a matter of time until the benefits of anonymous communication and untraceable fund transfer will make it to these groups, thereby making them entirely invisible and impenetrable to observation and surveillance techniques.

Also, we found numerous extremist websites offering training manuals and instructions to obtain and build weapons, explosives and how they are best transported/smuggled across international borders.

4.2. Financial Fraud

The damage of cybercrime inflicted upon the financial industry is estimated to exceed 2 trillion US Dollars annually.

The Dark Web offers plenty of opportunities to purchase stolen credit card numbers or bank account information (including CVV, personal background information like DOB, SSN, Name) in lots.

Some of these cards are then individually sold out to novice buyers on the WWW, which will use them in minor fraud cases to purchase lifestyle or other items.

The larger scale frauds remain in the Dark Web, and are entirely anonymous.

One of many is to purchase Bitcoins, which are laundered multiple times and then anonymously turned into other, real-life commodities like gold and silver, which again are converted to entirely clean cash currency in an entirely different part of the world.

The ingenuity in these frauds is astounding and yet so simple, that the aforementioned 2 trillion US Dollar loss represent the tip of the iceberg.

4.3. Money Laundering of Conventional Currency

While the Dark Web provides numerous services to launder Bitcoin currency there are also outlets specializing in money laundry for conventional currency.

Several online-shops (most of which are primarily platforms for international drug trades and shipments) offer large quantities of US-Dollars, EUROs and other major currencies in exchange for Bitcoin.

These bundles of cash are then shipped to the recipient, mostly in another country where they will be brought into circulation.

Because the aforementioned deal was conducted in absolute anonymity, the purchaser of the cash cannot reveal the identity of the seller.

Conventional currency is thereby washed and untraceable while the seller trades his Bitcoins for clean currency in his home country.

4.4. Superior Counterfeits (Documents and Money)

Counterfeit bills are available in bundles on the Dark Web and can be purchased for a fraction of their price on the conventional black market.

The bills are purchased anonymously, paid for in Bitcoin and sent through the mail to the purchasing party.

The entire deal remains entirely anonymous and untraceable for law enforcement agencies and – if the distribution is on a larger scale – the intelligence community.

Further, counterfeit passports and a wide array of fraudulent national ID cards are available.

Most of them are created out of stolen identities of existing individuals so that they easily pass ID checks, for instance when crossing international borders.

4.5. International Drug Trade

And beside many other platforms on the Dark Web that specialize in mail-drug distribution, the most prominent is called "The Silk Road".

It offers all the conveniences and security features (escrow, customer reviews of products, etc.) that a surface web counterpart like Ebay would present its customers with.

While most of the products they sell are illegal drugs (from prescription medication over hashish and cocaine up to heroine and other opiates), they also have other categories for weapon trade, counterfeit currency and documents, illegal software download, etc.

The packages with the substances are sent anonymously through conventional mailing or courier services and without the sender leaving their address (or any other indicator as to their true identity) on the package.

In most countries, the recipient can deny to accept the package without the ability of the law enforcement agencies to charge the perpetrator, creating a very difficult legal scenario.

4.6. Arms Trade

Our research revealed multiple online marketplaces selling anything from handguns, over assault rifles and launchers for rocket-propelled grenades up to military grade plastic explosives.

The selection of weapons was rather limited on the more general marketplaces and getting to the more 'exquisite' pieces does require quite some dedicated searching.

However, the mere availability of such untraceable weapons, which are shipped throughout the world, leads the current debate about banning military grade weapons in the USA ad absurdum.

As pretty much all the other goods on these portals, the weapons are purchased against Bitcoin.

The total amount is usually held in escrow by the portal until such a time that the buyer confirms the receipt of the weapon to the portal.

Most of the weapons are usually shipped through postal or courier services in the smallest possible parts because single packages don't raise attention of automatic scanners.

Other, more obvious weapons and parts are delivered through more covert operations, some of the senders making use of more anonymous measures like ships and harbors.

The weapons are then taken into custody of a handler who delivers the weapon to the recipient.

4.7. Child (and other illegal) Pornography

Because of the increased surveillance of pedophiles on the WWW a lot of the scene has gone underground, exchanging their goods through services, a lot of which can be found on the Dark Web.

Probably one of the most visited and best earning platforms there is 'Lolita City', which shelters several 100GBs of child pornography.

Much more disturbing than the graphic content being exchanged on this and others sites are the questions being asked, which actually lead to a vivid exchange between individuals registered on the platform.

Among those are "how do I apply chloroform to my 11 year old niece", etc.

But the Dark Web doesn't stop here.

The content available goes over sodomy and ends at snuff video where people are killed for sexual pleasure of others.

4.8. Extortion (of Law Enforcement Personnel)

One case in Germany showed just how far criminals will go to silence opponents.

A senior officer, who was involved in the investigation of a group in organized crime, found himself confronted with a case in which the organization had infected his private computer with a Trojan.

They had then uploaded child pornographic images and – ironically – made an anonymous tip to his unit who had to initiate an investigation on him.

The case found itself before court because the group had meticulously removed all traces of their infiltration.

During the trial neither he, nor the forensics department, could prove that the files had been uploaded by anyone else but him.

This presents a major risk to law enforcement work around the globe in particular.

If running investigations can be so roughly sabotaged and influenced by measures this 'simple', a lot of future cases will have to be dropped when a majority of its staff is suspended or otherwise inhibited.

4.9. Contract Murder

Ordered hits are advertised on the Dark Web for as low as 5.000,– British Pounds.

Depending on the mark, these prices vary greatly but even high-ranking, public figures can be 'eliminated', according to several websites offering these services.

Based on the quality of some, we have to assume that a certain quantity of these services are fake and that their issuers are copycats.

However, an ever-increasing amount of service offerings and advertisements offer independent escrow services to secure the transaction for the purchaser.

Usually, the 'hit-man' requires a 50% advance payment for which he will purchase the weapon and execute the hit; further, the contractor has to provide proof that the other 50% of the funds are at his disposal, usually through a photo or screenshot of the Bitcoin-wallet on their computer.

After the liquidation has been performed, the hit-man receives the final payment.

Throughout the deal, neither the identity of the person having issued, nor the identity of the person having executed the hit have been revealed to each other nor any third party.

All correspondence, the payment and the people involved remain entirely anonymous during the entire process.

4.10. Human Trials

Proof that the Dark Web offers services beyond imagination was a group offering four anonymous warehouses for 'medical trials'.

These illegal trials would be performed on "people society would not miss" and it can be assumed that this reference was made towards homeless people.

This website claims to have performed

- starvation and water/fluid restriction
- vivisection/pain tolerances
- infectious diseases and organ effects
- transfusions
- drug trials
- sterilization
- neonate and infant tolerances to x-rays, heat, and pressure

- fetus tolerance to bleach
- etc.

and that these, or any other thinkable medical experiments, could be conducted at their facility.

The provided warehouses are rented out along with aforementioned "trial patients".

4.11. Human Trafficking

Forum threads with titles like "searching for Asian sex-slave" are common and heavily discussed on message boards dedicated to serving distinct sexual preferences.

Contact details are exchanged from where the conversations resulting thereof become untraceable.

However, discussions following the above lead us to assume that these exchanges actually take place and that humans are trafficked throughout the world to satisfy these demands.

Definitely worth mentioning is that the perpetrators in this scene are not dominantly male, but that there is a fairly high number of women operating in these circles.

This was revealed when the hacktivist group "Anonymous" published the names and email addresses of several thousand registered Lolita City users in 2011.

4.12. Content Piracy

Direct content piracy is currently not as far spread due to the technical limitations implied upon users on the Dark Web.

Because the access points only provide limited bandwidth, network speeds are often too slow to download large-sized files.

Increasing pressure of law enforcement on web users downloading pirated content has led marketplaces like Silk Road to offer download services.

Third parties download the desired content and deliver it through postal services.

In some cases, the content made available for download on an anonymous server where the purchasing party can download it, after the agreed payment is conducted.

This makes the pointing out of individuals conducting copyright related offences nearly impossible.

5. Conclusions

Due to the fact that our research has revealed the first terrorist groups communicating anonymously through the Dark Web and asking for donations for their cause in untraceable Bitcoin it is safe to assume, that these groups will spread the word about the benefits.

In spite of the ever-increasing pressure on these groups by Law Enforcement and the Intelligence Community, it is only a matter of time until these instruments become widely accepted among individuals engaging in terrorist or other criminal activity.

The most imminent threat is that even prolonged communication between individuals cannot be intercepted.

This would allow even the most complex terrorist attacks to be orchestrated and funded in absolute secrecy for months and years without the Intelligence Community standing a chance to find any clues until the attack has been successfully carried out.