INNOVATION REPORT

# ANONYMOUS NETWORKS & DARKNET

INTERPOL Innovation Centre

18 Napier Road

Singapore 258510

INTERPOL Global Complex for Innovation

INTERPOL

INNOVATION CENTRE DIRECTORATE

# INNOVATION REPORT:

# ANONYMOUS NETWORKS & DARKNET

September 2018

## EXECUTIVE SUMMARY

The Internet has provided an enormous opportunity for the global economy and social prosperity, but presents some significant challenges for law enforcement. Network anonymisation and the Darknet are used for legitimate reasons by people wishing that their privacy is maintained, but the Darknet is also used to camouflage illicit activities. The challenge for police investigators is to work through the myriad of technology and encryption capabilities to uncover the intent and extent of criminal activities. This investigative analysis has seen significant disruptions in criminal activity on the Darknet, including the taking down of Silkroad and AlphaBay markets. Police have witnessed the resilience of criminal conduct and operations in this environment. Countering this resilience requires a concerted effort from global law enforcement to mitigate the risks of illegal vendor shops and marketplaces, the "crimes as a service' economy, child abuse, extremist and radicalisation and other Darknet related crimes. To prepare law enforcement for the current threat and the future of cyber enabled crimes, it is recommended that Chiefs of Police consider:

1. Hiring and training technical experts on Internet, Deep web and Darknet capabilities;
2. Investing in tools such as web crawling, data mining and cryptocurrency analytical tools; and
3. Reporting and sharing cybercrime instances with other agencies to develop universal capabilities across law enforcement agencies.

The INTERPOL Innovation Centre is fostering global efforts to facilitate the above goals by providing support, expertise and coordination.

## 1. INTRODUCTION

Technology, in general, has created enormous opportunities in economic and social prosperity but has also triggered massive challenges for law enforcement as criminals can easily use them to conduct their illicit actions while evading attribution. Network anonymisation techniques are one such example. They enable users worldwide to communicate and exchange information securely. Allowing journalists, human rights advocates, political dissidents and law-abiding citizens that are concerned about their privacy to avoid censorship and freely communicate. However, despite the lawful use of these technologies they are perceived as a double-edged sword as they are also used extensively by criminals for their illegal endeavours. Creating a haven, called Darknet, for various illicit activities and groups away from the eyes of Law Enforcement Agencies (LEAs), in particular the trading of illicit goods and services (including drugs, firearms, credit card or account details, falsified documents, stolen goods, etc.), terrorism communications, crime-as-a-service, cybercrime software solutions, child exploitation material dissemination, money laundering, etc.

Darknet is described as a camouflaged/encrypted communication network that sits on top of the normal internet (aka. A Network of networks). To access the Darknet, specialised anonymity software and browser configurations are needed. These allow users to communicate, exchange information and goods facilitating the ultimate goal of committing crimes in a digitally concealed medium, uncontrolled by central authorities, governments and regulators with minimal constraints and efforts to access.

In the context of policing, we often encounter investigators focusing their efforts on the analysis of Darknet markets where illicit goods and services are traded. These investigations have had some significant outcomes for law enforcement thwarting criminal networks. Examples include the take-down of Silk Road 1.0, Silk Road 2.0, AlphaBay and the Hansa markets. Despite the numerous takedowns, an increasing number of Darknet markets and forums are appearing and facilitating more diverse types of illegal operations, such as Hackers for hire, Bio-terrorism guidelines, etc. Apart from the vast increase in the number of Darknet markets and forums as well as their illicit services and goods traded, the law enforcement community has also witnessed a significant increase in the sophistication and manner that criminals conduct their operations and cyber security activities in these environments. Presenting additional challenges and limitations for law enforcement to trace and track these activities within these Darknet markets and forums to real world criminal entities.

## 2. Analysis and Background Information

### INTERNET

The Internet is the global infrastructure which interconnects various networks and electronic devices through the use of standardised communication protocols such as the Internet Protocol (IP) and computer languages such as HyperText Markup Language (HTML); it is a ‘network of networks’. Through the Internet, an individual can access and use a number of applications, amongst them:

- Communication Platforms – Online chat and instant messaging between users. This is enabled by software programs such as the Internet Relay Chat (IRC), MSN Messenger, WhatsApp, etc.

- E-mail Platforms – electronic messages sent from one user to one or more recipients. Software such as Mozilla Thunderbird which facilitates creation, sending, receipt and viewing of these messages.
- Web Sites – Consisting of a set of related HTML documents and other scripting artefacts collected together under a single domain name (for example: www.interpol.int).[1] A site typically contains a mixture of text and multimedia content for a particular purpose (For example: a banking website which enables customers to access their account, discover services offered by the bank etc.).
- Online Gaming Platforms – Electronic games played over a local network of computers (LAN) or the Internet which enables two or more players to participate simultaneously from different locations.
- Social Media Sites and platforms – Applications that enable an individual to create and share content, or participate in social interactions, with other individuals.
- Cloud storages – Remote data storage facilities which allow its users to save their valuable data safely online. The data is then physically hosted inside server farms of large data storage providers throughout the world.

An individual uses an electronic device such as a computer, smartphone or a tablet computer to access these applications. Historically, a computer-based user would access the above services via his/her Internet browser (Internet Explorer, Firefox, etc.) to connect to the provider's domain name (website, i.e., www.facebook.com). Nowadays, a typical end user would use an application on his smartphone to interact with these services. Some service providers don't even offer a website based service anymore (i.e., there is no website to play a Candy Crush game). To do so, users load and save various software programs/applications to their electronic device which enables them to access specified services provided through these applications (for example: an e-mail client to access e-mails, a WhatsApp client to chat with other WhatsApp users).

The electronic device connects to the Internet via an Internet service provider (ISP).


*Figure 1 How an individual accesses the Internet via an ISP*

An individual pays a subscription fee to the ISP to be able to use the ISP to access the Internet. The ISP provides the internet access via an electronic device known as a modem (aka a "box") and a family of Digital Subscriber Line (DSL) technologies. Currently, ISPs typically deliver Internet access via standard telephone copper cables, Cable TV lines or optical fibre cabling. A dedicated modem for each of these types is required.

## ANONYMOUS NETWORKS

Being a network of networks, the Internet consists both of open, public and private networks. When an individual accesses an application on an open network, their identity is not typically concealed, and a third party can track their online activity. This means that the websites they visit, things they discuss via IRC, or the content they access can be identified and/or monitored. However, the possibility of being tracked is reduced or disguised for an individual who accesses an anonymous network.

Although anonymous networks cannot provide an individual with complete obscurity, they give an individual more significant opportunities to hide their online activities. This is because information and content are anonymously shared and possibly encrypted, disguising an individual and their online activities, and making it harder for third parties (such as law enforcement agencies) to identify the individuals and monitor activities. Anonymous networks are often considered to be locations which are used to facilitate illicit online activity because there is less likelihood of detection and disruption than if the same activity was conducted on an open Internet network.

### Deep web

Some companies scan the web to index contents making it readily searchable in a central location for internet users to find (i.e. Google, Bing, Yandex, DuckDuckGo, etc.). These "search engine" companies use *spiders/crawlers/robots (*dedicated pieces of software) to scout the web in search of data to index. These tools are limited in their scanning of data within anonymous networks, restricted access and private areas of the internet.

Research studies estimate that standard search engines do not index approximately 96% of the data on the Internet. The contents of the Deep Web are not indexed by these search engines so that data within these environments are not easily identified or uncovered through conventional systems and processes.

The Deep Web is not illegal. It is basically the storage of online information that people do not want to share publicly and includes material from universities with classified research, police restricted information, industrial secrets, hospitals with medical records, etc. Typically anything that requires an account and credentials to gain access to it falls within the scope of the Dark Web.

### Darknet

Although the Deep Web is not illegal in most jurisdictions, the Darknet (which is a subset of the Deep Web) facilitates a high volume of illicit activities. To access the Darknet, you need to use a specified protocol. They include:

- Freenet
- Invisible Internet Project (I2P)
- Loopix

- The Onion Router (TOR)
- Decentralized or Blockchain DNS (B-DNS) – Peername.com registrar for Namecoin, Emercoin, NXT and Ethereum domain names
- Alternative DNS (often referred to as Rogue DNS) – OpenNIC, Cesidian Root or NewNations

These anonymous networks are separate and not affiliated or linked to one another. Each anonymous network requires a dedicated program to access them (for example: an individual needs one particular program to access Freenet, another to access Loopix etc.). To do so, an individual accesses the Internet via an ISP then executes an anonymous network program to access the respective anonymous network. TOR is the most widely used protocol by criminals for accessing and establishing Darknet Market Places (DMP) or Hidden Services (HD).

After accessing an anonymous network, users can open and use applications similar to those which they would use on an open Internet network. For example, an individual can connect to an IRC and then can use web sites or applications from within this program, but applications on an anonymous network are not openly accessible outside of that specific environment. To get access to that environment an individual will require permission from the anonymous networks operator, or an endorsement from an existing user.

### *An example of the anonymous network: TOR*

*TOR is a network and an open source software initially developed in the 1990s by the United States Naval Research Laboratory to protect sensitive government intelligence communications. Currently, it is a non-profit project established in the United States, with various contributors, personal donors and sponsors.*

*"TOR is a distributed-trust, circuit-based low latency anonymous communication network". Anonymous communication systems were initially seen as systems relying on a mix of nodes to exchange messages at two levels: message content and message flow. High-latency systems represent, for example, the message-based systems/email systems (not requiring swift responses) and low-latency systems the connection-based ones (web applications, instant messaging, etc.).*

*TOR is the most customary anonymisation software used to access the Darknet, which directs Internet traffic through a free volunteer network consisting of approximately 7000 relays. It is being used for web surfing, chat and instant messaging by a very wide variety of people for both legal and illegal aims. According to live metrics found atTorproject.org, there are, at the time of this research, about 2 million direct TOR users.*

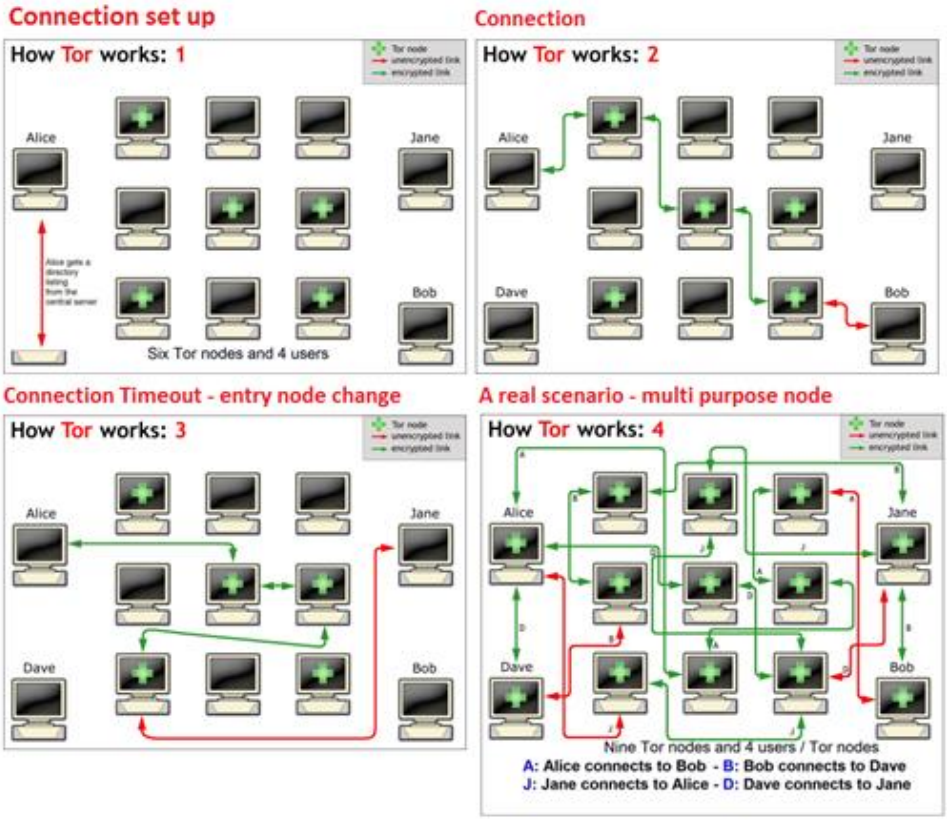


*Figure 2. TOR Routing*

*TOR periodically creates virtual circuits, and the traffic is sent from router to router along the circuit, ultimately reaching an exit node at which point the 'cleartext' packet is available and is forwarded on to its original destination. Viewed from its destination, the traffic appears to originate at the TOR exit node. No further details of the route (circuit) and original machine involved are available beyond the exit node.*

*All the data sent is protected with multi-layers of encryption over the TOR network during its transition from point A (Entry Node) to point B (Exit Node). While travelling over the network, the message goes through a series of decryptions and hops over different nodes that were chosen as part of the specified "circuit" in charge of channelling the message from an end to another.*

- *TOR Browser Bundle*

  *TOR Browser Bundle is an application based on a dedicated Firefox Browser crafted explicitly to resemble any other TOR client to minimise the chances of being identified and tracked based on technics known as machine fingerprinting. The TOR Browser Bundle implements the necessary Onion Routing protocol allowing users to access the TOR network. All requests made by the user via this dedicated Firefox Browser are forced to flow via the TOR Network.*

- **.ONION*

  *TOR protocols permit users to conceal their locations and connect to the Hidden Services (HS), each without knowing the other's network identity. The TOR HS protocol extends the*

*anonymity protection to all nodes, including servers. ".onion" is a special-use top-level domain name complemented with a unique 16-character alpha-semi-numeric hash, e.g., TORCH (one of Tor's search engine) has an HS domain and URL of http://xmh57jrzrnw6insl.onion. There is no authoritative central database to record all the existing hidden services. In the open internet, the ICANN and the registrars serve as authoritative entities to register domain names that are in turn allocated IP addresses. An open internet browser queries a Domain Name Services (DNS) Server to translate a URL to a domain name to an IP serving that web content. On Tor there is no IP address or central registry, the Hidden Service is resolved by the Tor protocol which establishes the circuit to reach it. The Tor client machine never knows where the HS server is.*

## 3. Crime Types Related To Darknet

A number of crimes are benefiting from anonymisation techniques and fostering their illicit businesses in the Darknet. The following areas are the most often seen crimes facilitated by the Darknet:

### Vendor shops/marketplaces

Some HS (website) are online-commerce stores virtually anyone can use to advertise services and sell various items. On TOR, such marketplaces are predominantly used to sell illicit drugs, firearms, counterfeit pharmaceutical medications, stolen identification data or documents, credit card details, etc. These stores are hosted in different locations around the world and are typically defined either as a vendor shop or an online marketplace.

A vendor shop typically receives and processes their transactions then fulfils orders directly to consumers themselves (for example, Brand X hosts its own store to sell only Brand X products to consumers).

Some contemporary examples of vendor shops operating on anonymous networks are:

- CharlieUK (aka CharlieUKontor, selling Cocaine)
- GammaGoblin (aka GG or Pushing Taboo, selling Lysergic acid diethylamide, LSD)
- The French Connection (aka FC, selling Heroin, Ecstasy and Methamphetamine)
- ToYouTeam (selling multiple illicit products)

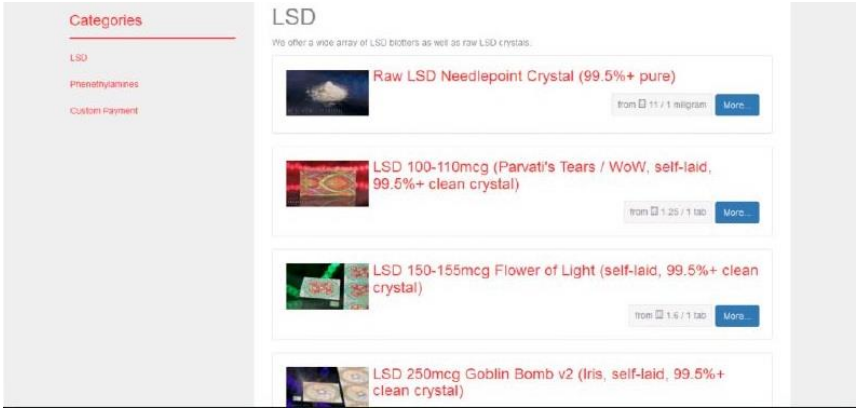


*Figure 2: An example of LSD for sale on a vendor shop on an anonymous network*

Figure 2 above, shows one example of a vendor shop offering various types of lysergic acid diethylamide (LSD) for sale to prospective customers.

A contemporary example of Darknet Market Place (DMP) operating on the anonymous network is:

Dream Market (aka DM, nearly 130000 listings as of August 2018, selling just about any service and goods under several categories: digital goods, drugs, services and "other"), table 1 below shows the number of listings under each of the categories as of 24 August 2018.

| Digital Goods 55582 | Drugs 61555 | Drugs Paraphernalia 276 | Services 5913 | Other 5966 |
|---|---|---|---|---|
| Data 2475 | Barbiturates 48 | Harm Reduction 54 | Hacking 842 | Counterfeits 3023 |
| Drugs 417 | Benzos 2877 | | IDs &Passports 998 | Electronics 227 |
| E-Books 13867 | Cannabis 18822 | | Money 978 | Jewellery 1239 |
| Erotica 2972 | Dissociatives 2464 | | Other 834 | Lab Supplies 102 |
| Fraud 4154 | Ecstasy 10345 | | Cash out 1513 | Miscellaneous 350 |
| Fraud Related 8996 | Opioids 3882 | | | Defence 489 |
| Hacking 2302 | Prescription 3152 | | | |
| Information 14510 | Psychedelics 3967 | | | |
| Other 1559 | RCs 738 | | | |
| Security 573 | Steroids 2807 | | | |
| Software 1275 | Stimulants 10175 | | | |
| | Weight loss 158 | | | |

*Table 1 Number of listings under each category on Dream Market*

From the above table, it is interesting to note that – contrary to common beliefs - major Darknet marketplaces such as Dream Market do not necessarily have listings for explosives, firearm, ammunition or illicit goods such as dangerous chemicals, lethal drugs or CBRN materials. These types of listings can be found on the Darknet but on less advertised Market Places that are more volatile.

## Crime as a Service (CaaS)

Besides the market for trading illicit goods, the "crime-as-a-service" economy is currently flourishing, making law enforcement actions more strenuous. Such CaaS includes hacking services and malware traffic, criminal consulting, trade of information on human trafficking, human experiments and torture methods, money laundering services, financial information (FULLZ, CVVs, DUMPs) and doxing (Researching and broadcasting an individual's personally identifiable information to cause damage).

## Child Abuse

Another crime facilitated under the anonymity of the Darknet is the dissemination of child abuse material and the discussion of actual exchanges and meetings. Remarkably, from an investigative point, this type of activity is usually not associated with monetary revenue, but instead, criminals operate as an organised community that exchanges illegal material.

## Extremism and Radicalization

Australian Transaction Reports and Analysis Centre (AUSTRAC) published a risk assessment for South East Asia and Australia related to Terrorism Financing[2]. This report studies the risks of raising, moving and using terrorism funds.

This report recommends urgent actions are needed:

- The overall risk for self-funding terrorism from legitimate sources is quoted HIGH. We can interpret there is a need for such potential donors to find an easy and anonymous way to donate their funds. Virtual Currencies are a very likely candidate channel.
- The overall risk for cross-border movement of funds is HIGH. Again we can anticipate here that terrorist networks will likely be willing to limit their risk of losing cash transports and move towards dematerialised fund transfers, i.e. Virtual Currencies
- The report quotes as the most likely use of terrorist funds to be: A/ Personnel mobility and travel, B/ Weapons and explosives material procurement. Both of these can be facilitated by services found on Darknet Market Places (fake documents, credit cards, weapons and ammunition). Regarding travel arrangements, one may acquire a plane ticket directly via btctrip.com or destinia.co.uk. Both accept payments in Bitcoins, Destinia also accepts Bitcoin Cash (BCH).

After AliPay, PayPal, Apple Pay and many other dematerialised payment systems, UATP a payment processing partner for over 260 airlines announced in 2015 an agreement with Bitnet (now UpHold) to facilitate payments in virtual currencies[3]. It is currently unclear if this project has been implemented.

The Financial Action Task Force (FATF) Emerging Terrorist Financing Risk report 2015[4], gives a large number of actual cases to support its arguments as it covers all aspects of fundraising and fund usage. On page 35, this report it touches on Virtual Currencies and quotes a case dated 28 August 2015 in

which a suspect was convicted and sentenced to 11 years in prison. Amongst other active support, this individual admitted to using Twitter (he had 4000 followers) providing instructions on how to use bitcoins to help fund ISIL and its supporters.

A US Treasury Department study[5] Reports that bitcoin could be used to fund terrorism but says the actual risk posed remains uncertain. This statement is a claim to do scientific research to ascertain the role of virtual currencies in funding or facilitating terrorism.

Hong Kong Financial Services and Treasury published a "money laundering and terrorism financing risk assessment"[6]. P103 (§9.9): No evidence of "Social Media, Virtual currencies, online payment systems, prepaid cards, crowdfunding or other new payment methods" used to fund terror organisations (in Hong Kong). According to the report, an interesting fact was found that Hong Kong suffered losses of 1.83 Billion HK$ in 2015 related to technological crime, 1.37 Billion HK$, i.e. 75% of total losses is attributed to corporate email scams.

The Institute on Counter-Terrorism has published a short but in-depth analysis of publicly advertised Virtual Currency financing campaigns by individuals or groups supporting radical terrorist groups[7]. Some cases mentioned are more likely individuals taking advantage for personal benefits (INTERPOL found that one of the self-proclaimed fundraising campaign managers was using the same Bitcoin address to receive donations and for payments of his gain on just-dice.com).

The ICT report also shows that the overall amounts raised remain very little (under 16000 Euros); however, the tendency is clearly increasing.

### Other Darknet Related Crimes Mentioned

- Counterfeit money (e.g. SuperDollars)
- Match-fixing and gambling
- Gaming credentials
- Hitmen
- Money Laundering
- Death records and suicide methods (e.g., "Church of Euthanasia's Guide to Suicide with Helium")
- Incentivizing murder (users compete for financial prizes by guessing the dates when famous people die)
- Scammers and hoax (phishing and cloned sites)

## 4. Payment Systems in Darknet

The Darknet and its ambitions for anonymity could not exist without a means for anonymous payments and trading: the preferred medium is virtual currencies and quite specifically cryptocurrencies. Both the vendors and the customers expect to maintain their anonymity throughout

the process including payment. For this, they rely heavily on virtual currencies. Virtual currencies are digital or "dematerialised" means of payment which are transacted online without the need for trust or material support. The validity of transactions relies on the integrity of a shared ledger.

There are several technologies for running a ledger and its cryptocurrencies. According to CoinMarketCap.com, as of August 2018, there are 1901 cryptocurrencies (BitCoin, Ethereum, Monero, ZCash, etc.).

Some cryptocurrencies may be traded against real-world services. For instance, https://www.btctrip.com accepts Bitcoin payments for plane tickets. At the time of writing this report, CoinATMRadar (Figure 3, below) registers 9818 geographical locations in the world where bitcoins can be traded for or against cash, credit cards, services or goods.

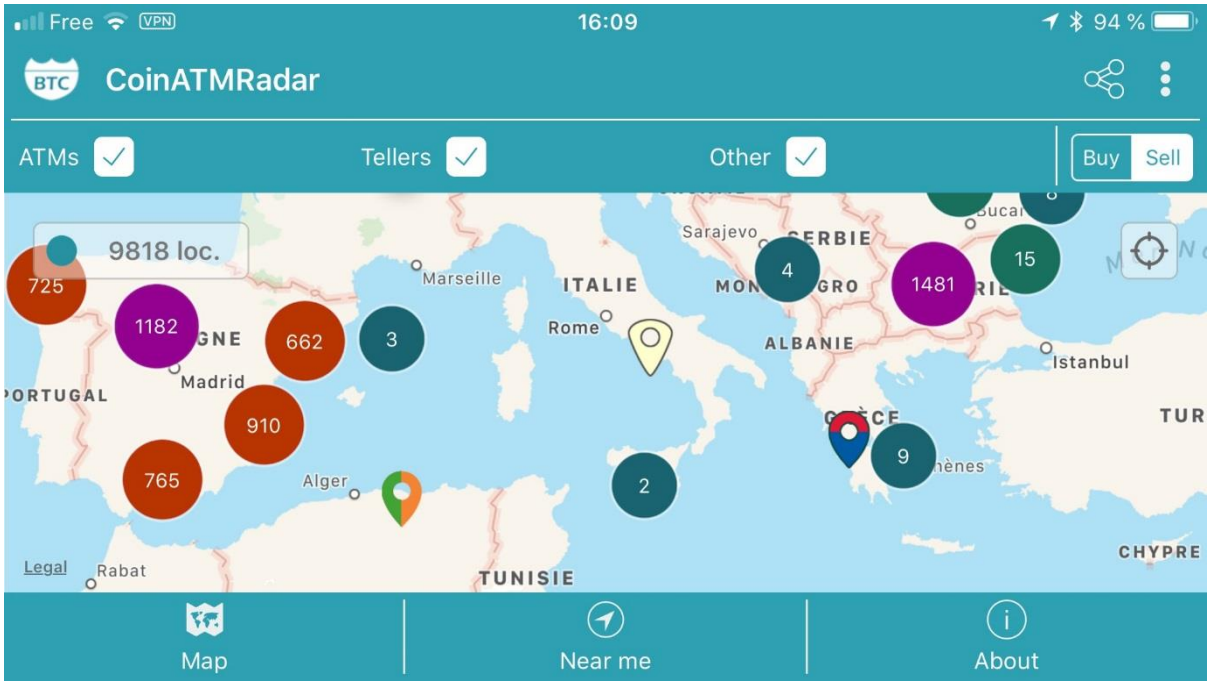


Figure 3 CoinATMRadar user interface, 9818 geographical location where BTC may be traded in the physical world

Cryptocurrencies are very common on Darknet Market Places, but a lot of other dematerialised payment systems exist. According to World Pay Global 2017 report[8], in a country like Ghana, up to 70.7% of all e-Commerce transactions are concluded via alternative payment systems such as Airtel, PayPal, iWallet, TxtnPay. While Credit or Debit Cards as we know them only account for 11.2% of the same transactions. Effectively, in countries where the physical banking infrastructures are challenging to deploy, the GSM data networks (3G/4G) are replacing banking cards and cash systems with mobile payment systems (SMS based micropayment systems) such as the popular M-PESA or Orange Money.

Finally, the Cryptolockers or ransomware families of malware have also been infamous for requesting payments via dematerialised and anonymous payment systems such as Paysafecards (includes the former Ukash) and MoneyPack.

## 5. Potential Opportunities and challenges for Police

Although Darknet is posing a huge challenge to law enforcement, opportunities also arise for investigating these illicit domains. Despite the fact that Darknet markets/forums are not easily accessible they still exist on the internet, and they contain critical information for investigators that can be collected and analysed to identify the administrators and users of these illicit platforms. Although technology might be evolving rapidly, users/humans are error-prone, leaving virtual traces that can be collected and analysed for tracing real identities.

### CHALLENGES

A number of challenges exist for law enforcement when investigating the Darknet. They include:

#### Unindexed Information / Accessibility

One of the major problems is that the information in the Darknet is unindexed meaning that you cannot easily locate information by using search engines. It allows criminals to hide on this part of the internet where law enforcement cannot easily search for keywords or websites. Although standard indexing services (search engines such as Google, Yandex, Bing, etc.) do not work on the Darknet, a number of Darknet search engines (e.g. Ahmia, Torch, NotEvil, SearX, etc.) exist and index a vast amount of these Darknet websites contents.

On the Darknet, this lack of exhaustive search engine is compensated by numerous blogs or chat forums where users may ask, share and rate their findings within the Darknet, these can be exploited by law enforcement to refine and target their activity.

#### Heavy Encryption at Rest and Transit

Anonymity is mutually inclusive with the deployment of robust encryption algorithms for protecting information. Most of the Darknet markets enforce a high level of encryption both at transit (on the datalinks transferring information) and rest (when stored on memory). It creates a challenge for law enforcement as it is not possible for investigators to analyse the information transferred between criminals or the information that is stored on the servers hosting the websites.

#### Decentralised Darknet Markets

Centralized architectures for hosting illicit markets have long been considered a single point of failure, enabling law enforcement to take advantage of their architecture, for locating and disrupting them. Therefore, criminals have been seeking decentralised architectures both for hosting and for naming their web server. Criminals can make use of peer-to-peer hosting solutions (e.g. OpenBazaar) and of decentralised domain name services (e.g. PeerName registration) for naming their website and ensure it is easily remembered and found (as opposed to the complicated .onion domain name).

| Internet domain | Typical TOR domain name | Typical Blockchain DNS: Namecoin (PeerName registrar) | Typical Invisible Internet Project (I2P) domain name |
|---|---|---|---|
| Wikileaks.org | suw74isz7wqzpmgu.onion | Wikileaks.bit | Wikileaks.i2p |

*Table 2 Fictitious comparison of domain names demonstrating the difficulty of remembering a TOR address*

The is a proliferation of options and services is posing a massive challenge to the law enforcement community as the investigators are investigating systems that are hosted in different places around the world, which operate under different laws surrounding data storage and exchange. Each system is maintained and operated by various actors with no relation to each other, making it extremely difficult to track or specifically disrupt a targeted criminal platform.

## Advanced Cyber-Security Infrastructure

Right after the takedown of Silk Road, we have seen a continuous advancement of the cyber-security practices of criminals, reaching unprecedented levels of anonymity and data protection. With more advanced methodologies introduced every month to protect their clientele from scammers, law enforcement and other miscellaneous threats. Such examples are the introduction of two-factor authentication[9], captcha deterrents[10], PGP keys for authentication and encryption, the enforcement of complex passwords, use of pin numbers to authorise purchases, warnings concerning best security practices, guidelines on how to avoid social engineering, and so on. They all have assisted criminals significantly decrease the number of mistakes made on the Darknet, which ultimately led criminals to conceal their identity more elaborately.

## Bullet Proof Hosting

Although it may be possible to identify the IP address of a server hosting a Darknet market/forum and reveal its location, it is highly likely that it would be hosted in a jurisdiction that does not enforce the needed cyber-laws to take it down, allowing criminals to operate in safe heavens uninterrupted.

## Dynamic/Versatile Websites

Darknet is well known for its versatile nature both in terms of the physical location of Darknet servers changing as well as entire Darknet markets/forums disappearing and then resurfacing (in some occasions) after some time. Due to the illicit nature and composition of the Darknet itself, the availability of the information is not guaranteed. Often a large number of Darknet websites/forums are lost within a few minutes/hours, with some of them resurfacing on other domain names, where others are lost forever along with critical information for investigators. Furthermore, in a lot of cases, it has been observed that Darknet websites change their physical location, so law enforcement is not able to keep up with tracing them hence evading attribution due to the long time needed to coordinate with law enforcement from other countries. A study conducted between 2011 and 2015 by Gwern Branwen[11] shows that out of the 87 documented TOR and I2P English-speaking Darknet markets, only 10 survived longer than 2 years.

## Countering Darknet related crimes: Recommendations for Chiefs of police

Below, IC provides some recommendations on how law enforcement can enhance their capabilities on the analysis of Darknet related crimes.

### Hire and train Tech Experts

Technology, including Darknet, is multifaceted and extremely fast pacing, necessitating experts with an in-depth knowledge of various aspects, such as networking, protocols, IT security, programming, etc. It is extremely hard for an expert to master several domains at once. Experts in Darknet investigations will therefore often focus on specific topics and rely on each other's knowledge and expertise. Experts remain relevant together and co-evolve with the latest state-of-the-art technologies and methodologies. These experts should regularly receive hands-on training to ensure that they are updated with the latest forensic and analytical practices. CNTL relies on academia and private sector partners to provide a continually evolving set of knowledge and tools to our trainers.

### Web-Crawling Solutions

As indicated above, Darknet contains versatile information that is often lost, rendering investigations obsolete because of insufficiently documented gathered data or simply by the lack of the raw data. To avoid losing such data, software systems called web-crawlers (similar to those used by search engines) can be employed to automate the caching and/or indexing of the online data on a recurring basis. By doing so, the web-crawlers build a safe and historical repository of contents. The information will be retained locally despite the original website/forum being changed or taken down.

SCRAPY[12] is an open source project with a strong community of users and developers. Based on Python language it is a nice alternative to test if a team does not have the budgets required for a full-blown commercial Machine Learning crawler.

### Data Mining Tools

As Darknet is only a part of the internet, it is wise that investigators collect and correlate information from all over the internet. Data mining tools are used to query and make sense of huge datasets. The ability of the data mining tool to deliver the search results in a correlated and sense-making way will be critical for the investigators to identify new leads and relations. Doing the same investigative work manually would simply be impractical due to the sheer volumes of data involved.

Open source communities are very active in developing data mining tools. One such open source tool is "R"[13]. It became a programing language in itself for mining and rendering results. R is rather popular despite the fact that it is a programing language on its own and is difficult to learn and use.

Another tool "Orange"[14] is growing in popularity as it integrates Machine Learning modules and is based on the more widely used Python programing language. Other Data Mining tools include KNIME and RapidMiner.

### Cryptocurrency Analytical Tools

Cryptocurrency addresses can be a rich source of information. It is possible for investigators to use appropriate crypto-analytical tools that will enable them to trace the path of payments to identify other criminals related to the source of investigation or additional information (e.g. associated crypto markets/exchanges, real-world services, etc.) that can assist in providing attribution.

As many LE services did, INTERPOL has developed "bitcoin explorer" a tool for analysing the history of Bitcoin transactions. Tools evolve, and we now consider such tools to be trivial because they are readily available online on sites such as https://blockchain.info. INTERPOL, under the project TITANIUM, is building the Virtual Currencies (VC) analytical tools of tomorrow. Our INTERPOL working group of VC experts helps us define the functionalities of these future tools. INTERPOL are creating a tool that enriches the transactions with the gathered data from many sources so an investigator can be alerted when a transaction touched a real-world service. Using technologies such as tainting we can weigh the 'badness' of a wallet. Working with the University College London, we are aiming to implement this next generation of blockchain explorers across several ledgers so investigators may have an opportunity to follow Bitcoins earned selling drugs on the Darknet, then mixed in ZCash and spent back in Bitcoins in the real world.

## 6. Conclusion

Anonymous networks and the Darknet, exist and are ever present and being utilised by organised crime groups and other persons with an illicit intent. Law enforcement in many respect is playing a game of catch up, to get ahead of the criminals that are using this technology to exploit the innocent. Traditional investigations skills will not be effective in identifying and tracking cybercrime through the Internet. A new high tech criminal investigator is required that can work and collaborate with others law enforcement officers across the virtual environment, and adapt their methods and tools to the ever changing technological challenges within this environment. Cybercrimes, cyber enabled crime are with us and will be more prevalent in our future as new emerging crimes are developed on the foundation of this technology. Global law enforcement must position ourselves for our new reality so that we can maintain the level of public safety and security that our communities expect.

## 7. INTERPOL – Innovation Centre

The Innovation Centre is creating strategic partnerships with law enforcement, academia and private industry on a global, regional and national level. These collaborations support INTERPOL in developing innovative solutions to policing threats and challenges. This paper is an initial draft of a dynamic and developing concept and we encourage you to be involved as we develop these ideas into the future. Interested parties are invited to contact the Innovation Centre edgci-ic@interpol.int.

## 8. References

[1] Internet, Oxford Dictionaries, Website, https://en.oxforddictionaries.com/definition/website, viewed 21 March 2018

[2] http://www.austrac.gov.au/sites/default/files/regional-risk-assessment-SMALL_0.pdf

[3] http://cf.uatp.com/partners/processing-partners/bitnet.html

[4] http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

[5] http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

[6] https://www.fstb.gov.hk/fsb/aml/en/doc/hk-risk-assessment-report_e.pdf

[7] https://www.ict.org.il/images/Jihadists%20Use%20of%20Virtual%20Currency.pdf

[8] http://offers.worldpayglobal.com/rs/worldpay/images/worldpay-alternative-payments-2nd-edition-report.pdf

[9] A two-factor authentication requires the end user to log into a system using two "keys": an information he/she knows (typically a passphrase) and an information he/she possesses (usually a one-time password generated on demand and valid only once for a given short period)

[10] Captchas are one time images or audio recordings users need to transcript into a validation box to confirm they are humans and not an automated system.

[11] "Darknet Market Mortality Risks", https://www.gwern.net/DNM-survival

[12] https://scrapy.org or https://github.com/scrapy/scrapy

[13] https://www.r-project.org

[14] https://orange.biolabs.si or https://github.com/biolab/orange3