MEDI@4SEC

The Emerging Role of Social Media in Enhancing Public Security

D1.1 Report on State of the Art Review

Chapter on the Dark Web

Authors: S. Oggero and T. Verburgh (TNO)

Co-funded by the Horizon 2020 Framework Programme of the European Union

EXTRACT FROM THE FINAL DRAFT REPORT ON STATE OF THE ART REVIEW, AWAITING FINAL ACCEPTANCE BY THE EUROPEAN COMMISSION.

About the project

The MEDI@4SEC project focuses upon understanding the opportunities, challenges and ethical considerations of enhancing social media use for public security: the good, the bad and the ugly. The good comprises using social media for problem solving, fighting crime, decreasing fear of crime and increasing the quality of life. The bad is the increase of digitised criminality and terrorism with new phenomena emerging through the use of social media. The ugly comprises the grey areas where trolling, cyberbullying, threats, or live video-sharing of tactical security operations are phenomena to deal with during incidents. Making use of the possibilities that social media offer, including smart 'work-arounds' is key, while respecting privacy, legislation, and ethics.

Interested?

Are you interested? See http://media4sec.eu/publications/ for the complete report, follow us on Twitter (@MEDIA4SEC) or contact marijn.rijken@tno.nl.

Cover illustration courtesy of TNO

Contact: Marijn Rijken (Marijn.rijken@tno.nl)

Date: September 2016

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700281.

Dark web

The 2015 Internet Organised Crime Threat Assessment indicates that cybercrime is becoming more aggressive, hostile and confrontational on individuals and businesses. Instead of subterfuge and covertness, there is a growing use of extortion, which boosts the psychological impact of fear and uncertainty on victims. For this reason, cybercrime increasingly bears the signature of organized crime (Europol IOCTA, 2015). This chapter will discuss the Dark Web, one of the digital social spaces particularly facilitating the perpetuation of "high tech" (organized) cybercrimes. Knowledge obtained for this chapter is not only based on scientific and grey literature but included red and blue teaming knowledge as well.

What is the Dark Web?

The internet consists of several layers of accessibility. The first layer is called the Clear web or Surface web. This part is accessible through regular search engines, such as Google or Yahoo and is where social media platforms reside. The second layer, called the Deep web consists of all the data not indexed by traditional search engines; these data can range from bank transactions to closed WhatsApp groups.[1] A small part of the Deep Web is called the Dark web (DW). Here content has been intentionally concealed and users can surf anonymously. In order to reach the DW and to access its content, one needs to install a certain program whose function is similar to that of a web browser or search engine. The most commonly known program is The Onion Browser (TOR).[2]

In this document we refer therefore to DW as online criminal activities, which use a TOR or similar browser technology (e.g., I2P, Freenet) TOR browsers work differently from conventional browsers (Raeesi, 2015).[3]

1.1 The use of social media in the domain of public security and policing

1.1.1 Legal and criminal use of the TOR protocol

The TOR protocol is legally used for several legitimate purposes[4]: to avoid identity theft, for marketing tracking, to circumvent censorship and to perform research on topics that might be sensitive in certain countries. Typical examples of legit users of TOR are listed in the table below:

[1] It is estimated that the Deep web is approximately 4,000-5,000 times larger than the surface web (Finklea, 2015).

[2] Other programs are Freenet and the Invisible Internet Project (I2P) (Ciancaglini et al., 2015).

[3] Every TOR user becomes a node in the TOR network and all traffic bounces through at least three nodes before reaching its destination; only the previous node and the subsequent node are known by routing nodes. Therefore, past one step, the nodes are literally "in the dark" about other nodes on the network (Tapai & Shorter, 2015). Bitcoin is the currency which criminals on the DW use the most because of the anonymity feature it provides. It is a non-government-controlled peer to peer anonymous crypto-currency (van Hout & Bingham, 2013). It was created in 2009 as an unregulated, alternative method of exchange for online payments and it has been the topic of much media, internet and policy discussion (Wilson & Yelowitz, 2015).

[4] https://www.torproject.org/about/torusers.html.en, accessed in August 2016

Table 8-1: Legitimate users of the Dark Web

TOR User Group	Purpose of Beneficial Use
(Political) activists and whistleblowers	Operate anonymously in totalitarian regimes; expose business or government related injustices reducing the risk of repercussions
Journalists	Protect sources and themselves while publishing non-state controlled articles
Law enforcement agents	Receive truly anonymous tips, use the internet during surveillance, protect undercover staff
Businesses	Support corporate spying and market screening operations
The military	Share confidential data, protect the identity of field agents, gather intelligence

A seventh group of users can be added to these groups, namely criminals. Different sorts of criminal activities and services are exploited on the DW including, criminal trade, child Sex Abuse (CSA) and criminal services, such as murder for hire, human trafficking, hacking services (Ciancaglini et al., 2015; Raeesi, 2015; Tapai & Shorter, 2015; Biryukov et al, 2013; McCoy, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno, and Douglas Sicker, 2008; Chertoff & Simon, 2015).

Other "grey" services, not necessarily illegal can be exploited for illegal purposes, such as financial transactions – that may facilitate money laundering; the distribution of informative material – typically dealing with illicit content as the "making of a bomb"; fora and chat services, often used for communications that can facilitate the growth of violent extremisms.

Due to the intrinsic properties of TOR, a quantitative analysis of the use of TOR to establish a ratio between the legal and illicit use is very challenging. There is no academic agreement on this question, and no hard numbers are presented. (Biryukov et al., 2013) argues a 50:50 ratio between legal and illegal content.

In the following paragraphs, we focus on a few of the mentioned criminal activities that represent an example of how the "high tech (organized) crime" is nowadays exploiting the DW.

1.1.2 Use of the Dark Web for policing

The use LEA's make of the DW itself for investigations is mostly not specified in the openly available literature. It is nevertheless generally known that the activities on the DW are object of investigation (a.m., Bryant, 2014), within two operational contexts, as listed below.

Proactive investigation for intelligence, employing the use of TOR and often manual searches of the encountered content; in a few cases, LAE's are experimenting the use of novel automatic tools to crawl portions of the DW and index their content.[5]

[5] An example of such tool is the specialized search engine developed by TNO (Spitters et al., 2014). The challenge in this case lies in the difficulty of automatically uncovering new DW pages; the limit of content protected by login also requires a semi-automated approach and the risk to automatically download CSA content (the simple possession of CSA can be illegal in some countries) need to be accounted for.

Reactive investigations, for example to collect information on the DW on a suspect. These operations are again challenging, mainly because of the difficulty to de-anonymise digital traces on the DW.

The perpetuation and impact of concluded operations concerning the DW are instead often mentioned in the media and in official reports; the following sections will focus on these.

How policing the Clear Web influence the Dark Web.

Before looking into the policing measures on the DW, noteworthy is that the DW can be influenced by policing and law enforcement efforts on the Clear Web. An example is given by the Internet content regulation from a drug-policy perspective: measures such as the Australian compulsory Internet filtering regime to block drug contents on Clear Web websites would likely drive drug discussions to the Deep or the DW, where digital spaces are not affected by Internet filtering and where governments are actually unable to regulate TOR website content (Barratt et al., 2012).[6] On the other side, this measure might also push violent online extremism into the DW, where monitoring of content is much more difficult and less debate takes place (Hussain & Saltman, 2014; Saltman & Russell, 2014).

A general policing attitude towards the DW and policing challenges.

Very little policing studies discuss crime on the DW, let alone studies of the impact of policing measures. This might follow from the novelty of the technology, from the induced and unprecedented move of several crimes into a relatively new transnational context and from the technical challenge posed by the technology itself, not easily accessible for research as open data sources are, and rapidly changing and growing. The exponential growth of the crime specifically on DW market places, for instance, poses a formidable challenge for the foreseeable future, since DW sites proliferate at a rate far greater than law enforcement has been able to intervene. It might become difficult to justify the effort and cost of operations aimed at regulating the DW, especially when there are so many other forms of cybercrime equally deserving of attention (JCAT). All these elements make any LEA's action for monitoring, investigation or prosecution of criminals very challenging.

Despite cybercrime policing having a typical local characterization, when it comes to the DW similar attitudes appear across law enforcements worldwide: authorities tend to focus on attacking the offender (in the case of CMs, focusing on the supply-side, as discussed in 8.3.4) and on removing the illicit content (as discussed in 8.3.5). The effectiveness of this approach is questioned in the academic literature. Two points are also highlighted: the difference between various cybercrimes perpetuated through the DW might call for different type of measures (e.g., difference between illegal trade and CSA as mentioned earlier); moreover, measures developed to exercise control on

[6] Another example is the renaming and rebranding strategy adopted by groups banned from the Clear Web when accused of promoting controversial or violent content (e.g., AM network, Hussain). Government imposed filtering and blocking regulations for content under a specific organization's name often prove to be futile on the Clear Web itself –the same content is quickly re-proposed under a new name and website data and traffic information becomes no longer accessible for further investigation.

phenomena on the Clear Web might bring weak if not counterproductive effects if applied to the DW, as already mentioned in the previous section.

The DW also poses a "policing dilemma". Anonymity is sometimes a cover for people doing "good" and in need of the protection of technology in order to surf the Web. TOR can be seen as a neutral tool, used for either good or ill (Jardine, 2015). A few examples in literature make a distinction between the TOR technology and the TOR-enforced hidden services, strongly attacking the latter (Guitton, 2013) as promoters of mostly unethical content and calling for a stop to the development of TOR hidden services. Other academics argue that shuttering anonymity networks would not be a viable long-term solution, rather ineffective and damaging to those people that genuinely benefit from these systems. Jardine and Stevens speak about the need of a more active "social policing", to minimize the socially damaging costs of anonymity-granting technologies, while still allowing the benefits of such systems (Jardine, 2015). Countermeasures to perceived misuse of the DW should be as flexible and adaptable as the technology is, and social policy can provide more capacity for this than relatively "crude" technological regimes (Stevens, 2010).

In this context, it is also worth mentioning the operations of other actors who autonomously infiltrate, disrupt and eventually take down DW websites and services. A popular example is the self-named "Operation DarkNet" of the hacker collective Anonymous, which in October 2011 announced to have accessed a large DW website hosting CAM content and publicly released the login details of more than 1500 users[7]. A second example, again a campaign launched by Anonymous, is "Operation Paris", which took down hundreds of websites on the Clear Web associated with ISIS; as a consequence, ISIS's media outlet, Al-Hayat Media Center, posted a link and explanations on how to get to their new DW site (Weimann, 2016). These cases might be examples of the self-implementation of "social policing measures" (Jardine, 2015) by fractions of the population, who feel the criminal use of technologies might jeopardize the benefits introduced by such systems.

Focus: the use of cryptomarkets.

Cryptomarkets (CM), are a relatively new criminological concept, introduced to outline the contours of a new generation of online illicit marketplaces (Martin, 2014). They are a type of website that look similar to regular online market places, such as eBay or Amazon, by allowing their customers to search and compare products and rate vendors, but also employing advanced encryption to protect the anonymity of users. While logged onto a CM, the physical location and identity of all users are masked, creating a completely anonymous marketplace. As a consequence, CMs provide an ideal trading facility to offer and buy illegal good. They gained popularity between 2011 and 2013, with the rise of Silk Road 1, the first major CM on the DW; other popular online market places for illicit goods are Silk Road 2, Agora, Evolution and Alphabay.

Impact of cryptomarkets on illegal (offline) trafficking. Marketplaces create new cyber-hotspots serving as places where potential offenders can meet each other, interactions

[7] http://www.huffingtonpost.com/2011/10/22/anonymous-hacks-lolita-city_n_1026327.html; http://www.telegraph.co.uk/technology/news/8846577/Anonymous-hacktivists-target-child-abuse-websites.html

between supply meet demand and relations are built. As a consequence of the CM providing informational and managerial opportunities, today loosely-organized groups and even individuals can be as efficient as old traditional organized groups in drug trafficking, offer their services to a far broader public than traditionally possible (and cutting out several middlemen, if wanted).

Cryptomarket policing. LEA's efforts against illegal trades on the DW have generally been in place to track the criminal proceeds, to limit the profits of crime and to tighten the global anti-money laundering regime (Raeesi, 2015). This approach follows from the "traditional" line of censorship of drug-related information in online and Internet sources (Barratt, 2012). In this way, LEA's have completed several operations: the leading law enforcement actors in America and in Europe have taken down several large websites and the operators behind them, amongst which the famous Silk Road 1 and Silk Road 2 (Barret, Farret & Winstock, 2014; Ron & Shamir, 2013; Finklea, 2015; FBI, 2014) and several others within operation Onymous (Europol, 2014). These results were made possible mainly through infiltration operations, classical police investigations and postal interception (Martin, 2014).[8]

Focus: child pornography

Criminals who are present on the DW appear more comfortable offending and discussing their sexual interest in children than those using the Surface Web. The greater level of anonymity and strong networking may be favouring their sexual urges, which would not be revealed in any other environment lacking such features. Hidden services within the DW are therefore often used as a platform for the distribution of child abuse material (CAM). The nature of these services drives the abuse of new victims because the production of fresh material is demanded for membership on child abuse forums and it reinforces the status of the contributors. Furthermore, child abuse offenders are facilitated by many of the financial services and products used by more "mainstream" cybercriminals; a continuation of migration from traditional payment mechanisms to those offering a greater degree of anonymity, such as Bitcoin, is observed. (Europol, IOCTA 2015). This might be evidence that offenders with a sexual interest in children who produce and distribute CAM are becoming more entrepreneurial and "innovative", exploiting developing technologies.

This might ensure that LEA's apply questionable policing policies, which can be inducement for ethical, legal and privacy discussions on a global level. According to information leaked to media sources, the federal bureau of investigation (FBI) hosted a Child Porn hidden service for 13 days after obtaining control of the site. The operation allowed to gather IP addresses and deposit malware to collect data about the site's users to the FBI. A hurdle not only difficult for Law Enforcement Agencies but also for researchers trying to study CSA is the "share-to-join" rule some CSA hidden services use.

[8] Another example of successful operations have been achieved in the Netherlands within the project ITOM (OM NL, 2014). Thanks to the resources (economical and in terms of personnel), the focus on cryptomarkets investigation and the transnational integral approach setup by the project, three big drugs sellers have been identified. The operation allowed to recover more than 1 M €. The project does not present prospects on effective strategies for policing the DW; alternative (not social media related strategies) are mentioned such as the "Naming and Shaming" approach.

In order to join the site researchers need to obtain an invite from a member, often by proving themselves as paedophiles and providing material in order to join.

Focus: possible use for terrorists, violent and hate extremists

Often, especially in recent times, claims are made about the terrorist use of the DW. Violent extremists are believed to be using the DW in the same way as they were using the Clear Web, but with exploitation of "added capabilities" (Weimann, 2016). Among the examples, step-by-step instructions to guarantee anonymity and hindering of geolocations from counter terrorism agencies are made available on the DW; a secret network of communications on the DW have been used between leaders of al-Qaeda to plan attacks in 2013; a DW page promotes donations in bitcoins to support the jihad (Weimann, 2016). Several of the criminal uses mentioned in section "Legal and criminal use of the DW" can indeed apply to activities that can lead to terrorism, such as money laundering, cyber-attacks to collect funds, fund raising, and weapon trafficking.

Multiple authors also mention that the hidden ecosystem of the DW can be particularly conducive not just for financing, trafficking and planning, but also for propaganda and recruitment (Chertoff & Simon, 2015). The "cold" recruitment of new supporters by the hand of radical groups and the promotion of extremist ideas are activities likely to display their message in locations much more easy to find and access than the DW (Bryant, 2014).

On the other side, communication phases subsequent to a first "contact" might seek more secluded digital spaces, such as closed for a, apps and chat services on the Clear Web. With the tightening of policies that ban extreme violent ideological content and services from the Clear Web, as well as private citizens initiatives of hacking, see 8.2, fanatics particularly motivated are driven on to the DW, where they are even harder to track (Hussain, 2014). Few data analytics research studies have attempted to collect and analyse fora of extremist content (e.g., Zhang, 2010) to pose a base for law enforcement operations. The challenge in this field is the "ephemeral nature" of content: fora emerge quickly and in many cases seem to disappear by changing name and location but retaining much of the same content.[9]

1.2 The influence and impact of social media use in the domain of public security and policing

Very little policing studies discuss crime on the Dark Web, let alone studies of the impact of policing measures. This might follow from the novelty of the technology, from the induced and unprecedented move of several crimes into a relatively new transnational context and from the technical challenge posed by the technology itself, not easily accessible for research as open data sources are, and rapidly changing and growing. The exponential growth of the crime specifically on DW market places, for instance, poses a formidable challenge for the foreseeable future, since DW sites proliferate at a rate far

[9] There is therefore yet little ability to assess the extent of terrorism-related content on the Clear and on the DW (Stevens, 2010), hence subsequent policing interventions are still far away.

greater than law enforcement has been able to intervene. It might become difficult to justify the effort and cost of operations aimed at regulating the DW, especially when there are so many other forms of cybercrime equally deserving of attention (Reitano et al., 2015).

All these elements make any LEA's action for monitoring, investigation or prosecution of criminals very challenging.

Despite cybercrime policing having a typical local characterization, where it comes to the Dark Web similar attitudes appear across law enforcements worldwide: authorities tend to focus on attacking the offender (in the case of CMs, focusing on the supply-side, as discussed in 8.3.4) and on removing the illicit content (as discussed in 8.3.5). The effectiveness of this approach is questioned in the academic literature. Two points are also highlighted: the difference between various cyber crimes perpetuated through the DW might call for different type of measures (e.g., difference between illegal trade and CP as mentioned earlier); moreover, measures developed to exercise control on phenomena on the Clear Web might bring weak if not counterproductive effects if applied to the DW, as already mentioned in the previous section.

The DW also poses a "policing dilemma". Anonymity is sometimes a cover for people doing "good" and in need of the protection of technology in order to surf the Web. TOR can be seen as a neutral tool, used for either good or ill (Jardine, 2015). A few examples in literature make a distinction between the TOR technology and the TOR-enforced hidden services, strongly attacking the latter (Guitton, 2013) as promoters of mostly unethical content and calling for a stop to the development of TOR hidden services. Other academics argue that shuttering anonymity networks would not be a viable long-term solution, rather ineffective and damaging to those people that genuinely benefit from these systems. Jardine and Stevens speak about the need of a more active "social policing", to minimize the socially damaging costs of anonymity-granting technologies, while still allowing the benefits of such systems (Jardine, 2015). Countermeasures to perceived misuse of the DW should be as flexible and adaptable as the technology is, and social policy can provide more capacity for this than relatively "crude" technological regimes (Stevens, 2010).

1.3 Inventory of strengths, weaknesses, opportunities and threats

In the previous paragraphs we already mentioned the most relevant literature discussions concerning how the Dark Web can introduce elements of strength, weakness, opportunity or threat in the context of law enforcement policing. These elements are discussed in the following sections.

1.3.1 Strengths

For the goal of law enforcement online surveillance, the Dark Web is a digital space where LEA analysts and researchers can conduct investigation anonymously, without leaving an online footprint. For specific contexts, the use of the DW as a space favouring online trade and e-commerce might induce a better "quality" of products due to self-

regulation mechanisms of the market. Additionally, traders on the DW encounter less physical risks than if they would trade "on the street". These arguments are particularly relevant with respect to the drugs trade.

Linked to the previous point, the cryptomarkets on the DW might lead to a disruption of traditional local organized crime networks. For instance, loosely-organized groups or individuals become nowadays as efficient as old traditional organized groups. This can be seen as an element of strength for LEAs in the disruption of strong locally organized criminal networks.

1.3.2 Weaknesses

Various elements of strength, if exploited by criminals, become elements of weakness for law enforcement goals. For the LEA's goal of identifying criminals, for instance, anonymity and untraceability of the online footprint of criminal users definitely poses a challenge to investigation and policing.

The DW is also a relatively novel and very rapidly innovating (changing) technology, hence it requires faster and more automatized investigations than the current state of operations. The content on the DW is neither easily accessible nor findable, it is a strong transnational context and is not met by adequate cybercrime detection capabilities. Standard infiltration operations (e.g., moles operating in a hidden service) have proved weak and shown little impact.

1.3.3 Threats

The general threat of the Dark Web is that its anonymity favours criminal activities. In particular, it poses a threat to the society through the proliferation of trade of specific products (e.g., drugs, counterfeit medicines, weapons) and services (e.g., murder for hire, data theft, CP). Media narratives describing the DW as "a place for criminals" do not help to counter this threat, but may be rather driving a bigger number of outlaws to it.

Additionally, the DW is intrinsically an economically-regulated environment: the DW financial methods attract a lot of capital and crypto markets naturally show resilience to intervention from LEAs on the supply side. The proliferation of criminal DW sites proceeds at a higher rate than the actual interventions and strategies can do.

Finally, being the Dark Web based on a highly complex, innovative and creative technology, the effects of both its legal and illegal exploitation are generally unknown and unpredictable on the long term.

1.3.4 Opportunities

Policing proposals

The DW is challenging law enforcement and policing capacities in an unprecedented way, and demands a greater (transnational) cooperation, more effective investigations (Reitano et al., 2015) and better technology tools targeting issues as the traceability and

attribution of criminal transaction and criminal communications on the DW (Europol IOCTA, 2015).[10]

Christin (Christin 2012) suggests that an opportunity would lie in strategies focusing the "offense" of law enforcement and policing on the demand of DW products, instead of the supply. He mentions four strategies for intervention on DW crypto markets: disrupting the network; disrupting the financial infrastructure; disrupting the delivery model; or "laissez-faire", i.e. tackling the issue by detachment. He argues though that the first two would be technologically impossible, while the latter would be unlikely adopted by governments due to the existing normative agenda on the war on drugs.

Opportunities: technological research developments that can form a base for policing

The last ten years have seen a progressive growth in the technological research around the features characterizing the DW. We list below a collection of the most interesting research efforts that could lead to methodologies, techniques or tool to be used by the authorities to support policing choices. It is important to note that the efficacy of these efforts has not been tested in a policy context yet, but each potential opportunity springs from an element of weakness in the DW phenomenon.

Identify top–sellers in crypto markets. The crypto markets provide fora and spaces for customer feedback (such as reviews); this information, if automatically analysed, can provide an interesting base to assess the network of sellers and identify top-sellers – potentially "top targets" in an intelligence operation. Deep learning sentiment analysis (Li) seems to outperform other methods in the context of malware and carding sellers.

Disrupt the system of trust. The presence of reviews on sellers on the DW can also be exploited for a more pro-active intervention. LEAs might be able to interfere with the businesses on crypto markets by manipulating buyer reviews. The goal can be that of provoking the failure or the reduction of profitability of the seller. (Markopoulos, 2015) uses a game theoretic model to derive an optimal strategy for a LEA to achieve market interference.[11]

De-anonymise. A central question that would enormously support LEAs operation is the "attribution of identity" question on the Dark Web. To answer this questions, advanced data mining and analysis technologies are required to perform DW users profiling. To actually determine the identity of a trader on the Dark Web, it is firstly important to trace anonymous transactions; data mining techniques are a powerful method to analyse large payment systems and publicly available transaction graphs of the type

[10] An already ongoing initiative targeting the first mentioned need in the case of transnational cybercrime is J-CAT, a task force led by EU member states, facilitated by Europol's Cybercrime Centre and running prioritized joint investigations (Reitano et al., 2015). This initiative proposes its platform, its efforts to partner with the private sectors and with universities and its mechanism for trust and intelligence sharing (governed by the Europol body) as opportunities for a successful fight against cybercrime.

[11] Different variables are balanced in the research, e.g., the budget to be "injected" in the market, the risk of exposure of the LEA operator and the risk of counterproductive effects such as increase in the profit of the seller. Review manipulation is shown to be a highly promising method, if LEAs have accurate information on the cost structure of market participants, on the effectiveness of the review mechanism, as well as on the details and the effectiveness of potential review manipulation countermeasures set by the market operator.

provided by the Bitcoin scheme (Ron & Shamir, 2013). Linking of heterogeneous data across different sources to a certain cyber identity is then needed.[12]

The simultaneous analysis of the content of posts on the Clear and Dark web might pose clues for an identity connection, relevant for both CP content and violent extremism content. Methods based on the homophile principle (two individuals are as close as their interests are in common) in combination with network analysis (two individuals are as close as their reference networks overlap) can help determining if a profile on the Clear Web matches a user on the Dark Web (Cristani, 2015).

Exploit user's errors and TOR vulnerabilities. As mentioned above, LEAs can exploit inaccuracies or accidents on the use of the DW. Some researchers also believe that a lot of DW users still show a certain degree of "naivety" (Bryant, 2014), by using TOR through a web browser. Standard web browser might have a JavaScript running or cookies enabled; both elements would assist a digital forensics investigator, testing whether a suspect accessed illegal material (Bryant, 2014). It is estimated that over 90% of regular TOR users would be sending their traffic from a non-TOR IP location at least once (Hurley et al., 2013).

Other researchers argue that vulnerabilities of the TOR network can also be exploited (Bradbury, 2014). Examples can be "hacking TOR" by breaking cryptographic keys –not impossible with an older version of the TOR key, running an own TOR relay, analysing the (clear) text traffic entering and leaving the network. Since TOR is continuously innovating, the sustainability of such methods is not obvious. A maybe more sustainable option is proposed by the director of the TOR project himself. He pointed out that the authorities could just as easily monitor Internet communications with the complicity of major ISPs, which would enable them to watch those communicating with TOR nodes before their traffic reached the DW, or after it left (Bradbury, 2014).

8.3.3 Conditions for success

The main condition for success in the case of the Dark Web is a transnational LEA effort focusing on quickly adaptable innovations, at the same level of technological progress and with the same flexibility that the same technologies governing the Dark Web propose. Awareness and understanding of how the criminal processes and the economy facilitated by the DW are also essential perquisites.

1.4 Reflection and conclusion

Technology is more than a new handy tool. It alters the way we think, the way we see the world and the world itself (Chan, 2001). Historically, technology has revolutionized policing practices (Chan, 2001), but it did the same for criminal ones. Technologies developed on the Internet introduced a new spectrum of capabilities and features, in

[12] Technologies like text mining can be used to analyse the communication between traders and customers; the choice of words, subtle indicators of style and even systematic spelling mistakes can form a "textual fingerprint". Analyzing temporal patterns can provide additional information (Raaijmakers, 2016). Ultimately it is the incidental connections of the Dark Web with the Clear Web (or the real world) that can lead to effective identification of individuals. These connections are often based on inaccuracies or accidents, such as mentioning accidentally an email address, or unintended visible swapping bitcoins (Raaijmakers, 2016).

terms of volume, velocity, interactivity, transnationality and dynamical evolution (Stevens, 2010). Therefore, cybercrime has become increasingly sophisticated, both technologically and psychologically (Grabosky, 2014).

The world of cybercrime on the DW is in particular a rapid changing world in which professionalization and commercialization are being implemented at a high rate (Verburgh, 2016). This is both a consequence of the technology "features" named above, and of self-adaptation measures in response to policing strategies or law enforcement operations.

The rapid development of DW cybercrime creates difficulty for researchers to keep track of new innovations; past research might soon be out-dated due to the fluidity of cybercrime. Even greater is the difficulty of policy makers and law enforcements, to identify and apply proper and timely innovations, reducing the possible DW misuses but at the same time maintaining the benefits of this technology.

We list below a number of reflections emerged from the literature review and that should be taken into account in the discussion on policing against DW-facilitated crimes.

- Policies should rely on flexible and adaptable innovations, to avoid limited applicability in a cybercrime community that is instead capable to quickly develop countermeasures.
- No "size-fits-all" measures: strategies should differentiate between the types of crime (e.g., CP vs crypto markets vs violent extremism activities).
- No "total-block" strategies: policies should seek balance between freedom of speech and crime solving.
- In the case of crypto markets-related crimes, strategies should focus on the "economical game". Policies should be able to tackle the ecosystem, instead of single targets, and focus on the demand first, instead of the vendor's side only. Disrupting a full economical system can bring a bigger and more sustainable impact than taking down single operators.
- In the case of violent extremism, strategies should rather focus on the producers, rather than the consumers of extremist material. Empowering the "good" and the "grey" users with spaces for open debate allows extremisms to be blended and debated.
- In general, for all types of crimes, strategies should consider the potential of the "good side" of the community, a little explored DW policy direction, by empowering "good users" for positive counter actions and stimulating "social policing".
- The options of applying social media strategies from the Clear Web to the Dark Web might be explored, being aware of the differences between the two digital dimensions. If Clear Web strategies are technically not applicable or practically not effective on the DW, attention should be given to the differences and to the exploration of possibly new methods.

Strategies should build on the experience and awareness of initiatives such as ITOM and JCAT, where transnational collaboration, coordination of joint and simultaneous operations in different locations around the globe have successfully been tested.

References

Barrat, M. J., Ferris, J. A. & Winstock, A. R. (2013). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction, 109*, 774-783.

Barratt, M.J., Lenton, S. & Allen, M. (2012). Internet content regulation, public drug websites and the growth in hidden internet services. *Drugs: Education, Prevention and Policy, 20*(3), 195-202.

Biryukov, A., Pustogarov, I., & Weinmann, R. (2013). Content and popularity analysis of tor hidden services. *arXiv:* 1208.6768v2. Retrieved at 09-14-2016 via http://bit.ly/2capDgo.

Bradbury, D. (2014). Unveiling the dark web. *Network Security, 2014*(4), 14-17.

Bryant, R. (2014). Policing Digital Crime, chapter in: *Policing the Deep Web* (pp 207-209).

Buskirk, van, J., Roxburgh, A., Farrell, M. & Burns, L. (2014). The closure of the Silk Road: what has this meant for online drug trading? *TOC, 109*(4), 517-518.

Ciancaglini, V., Balduzzi, M., McArdle, R. & Rösler M. (2015). 'Below the surface: exploring the deep web'. *Trends Micro, 1*, 1-48.

Cristani, M., Burato, A., Santacá, K. & Tomazzoli, C. (2015). The spider-man behavior protocol: exploring both public and dark social networks for fake identity detection in terrorism informatics. *University of Verona.* Retrieved at 09-14-2016 via http://bit.ly/2cwB3a7.

Europol IOCTA. (2015). The Internet Organised Crime Threat Assessment. *Europol.* Retrieved at 09-14-2016 via http://bit.ly/1VplmpF.

Federal Bureau of Investigation (FBI). (2014b). Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court. *U.S. Attorney's Office*. Retrieved at 09-08-2016 via http://bit.ly/1uBfAnL.

Finklea, K. (2015). Dark web. *Congressional Research Service*, 1-18. Retrieved at 09-14-2016 via http://bit.ly/2c8rmy9.

Grabosky, P. (2014). The evolution of cybercrime, 2004-2014. *RegNet Research Paper*, 1-16.

Griffith, V. (2014). Tor growth rates and improving Torperf throughput. *Tor Tech Report.* Retrieved at 09-14-2016 via http://bit.ly/2cag5lv,

Guitton, C. (2013). A review of the available content on tor hidden services: The case against further development. *Computers in Human Behavior, 29*(6), 2805-2815.

Hout, van, M.C. & Bingham, T. (2013). Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy, 24*, 524-529.

Hurley, R., Prusty, S., Soroush, H., Walls, R.J., Albrecht, J., Cecchet, E., Levine, B.N., Liberatore, M., Lynn, B. & Wolak, J. (2013). Measurement and analysis of child pornography trafficking on P2P networks. Department of Computer Science of Univeristy of Massachusetts and Williams college. Retrieved at 09-13-2016 via http://bit.ly/2ctiNym.

Hussain, G. & Dr. Saltman, E.M.. (2014). Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it. *Quilliam.* Retrieved at 09-11-2016 via http://bit.ly/2c8qLMW.

Interpol. (2015). Pharmaceutical crime on the darknet: A study of illicit online marketplaces. *INTERPOL.*

Jardine, E. (2015). The Dark Web Dilemma: Tor, Anonymity and Online Policing. *Global Commission on Internet Governance.* Retrieved at 09-14-2016 via http://bit.ly/2cwxEIq.

Kruithof, K., Aldridge, J., Décary Hétu, D., Sim, M., Dujso, E. & Hoorens, S. (2016). Internet-facilitated drugs trade. *Brussels / Cambridge: WODC, RAND Europe.*

Lavorgna. A, (2014). Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics. *Trends in Organized Crime, 17*(4), 250-270.

Markopoulos, P., Xefteris, D. & Dellarocas, C. (2015). Manipulating reviews in dark net markets to reduce crime.

Martin, J. (2014). *Drugs on the dark net. How Cryptomarkets are Transforming the Global Trade in Illicit Drugs.* Palgrave Macmillan.

OM NL. (2014). Verantwoording aanpak georganiseerde criminaliteit 2014. *Project ITOM, OM.* Retrieved at 09-14-2016 via http://bit.ly/2cExXVd.

Raeesi, R. (2015). The Silk Road, Bitcoins and the Global Prohibition Regime on the International Trade in Illicit Drugs: Can this Storm Be Weathered? *Glendon Journal of International Studies, 8*, 1-20.

Reitano, T., Oerting T. & Hunter, M. (2015). Innovations in International Cooperation to Counter cybercrime. The Joint cybercrime Action Taskforce (J-CAT). *The European Review of Organised Crime, 2*(2), 142-154.

Ron, D. & Shamir, A. (2013). How did dread pirate roberts acquire and protect his Bitcoin wealth?. T*he Weizmann Institute of Science.* Retrieved at 09-07-2016 via http://bit.ly/2cwcv4p.

Saltman, E.M. & Russell, J. (2014). The Role of Prevent in Countering Online Extremism. *Quilliam.* Retrieved at 09-14-2016 via http://bit.ly/2cajdOE.

Soska, K. & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *USENIX, Washington, D.C.*

Spitters, M., Verbruggen, S. & Staalduinen, van, M. (2014). Towards a comprehensive insight into the thematic organization of the tor hidden services. *IEEE Joint Intelligence and Security Informatics Conference,* 221-223.

Stevens, S. (2010). Regulating the 'Dark Web': How a Two-Fold Approach can Tackle Peer-to - Peer Radicalisation. *The RUSI Journal, 154*(2), 28-33.

Tapai, M.G. & Shorter, J. (2015). Into the depths of the internet: The deep web. Issues in Information Systems, 16, 230-237.

Verburgh, T. (2016). Profiles of cryptomarket arrestees: an exploratory study. *Vrije Universiteit Amsterdam: Master Thesis*.

Weimann, G. (2016). Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism, 39*(3), 195-206.

Wilson, M. & Yelowitz A. (2015). Characteristics of Bitcoin Users: An Analysis of Google Search Data. *Applied Economics Letters*, 22, 1030-1036.

Zhang, Y., Zeng, S., Huang, C., Fan, L., Yu, X., Dang, Y., Larson, C.A., Denning, D., Roberts, N. & Chen, H., (2010, May). Developing a Dark Web Collection and Infrastructure for Computational and Social Sciences. *IEEE Xplore*.