CHALLENGES TO SAFEGUARDS FROM THE DARKNET

G. E. Christopher (grant.christopher@vertic.org)
The Verification, Research, Training and Information Centre (VERTIC)
London, United Kingdom

Abstract

Darknet and encrypted services are, at present, an unquantified challenge to safeguards and nonproliferation which should be expected to grow over time without mitigation. Darknet markets are frequented by scammers, fraudsters and individuals purchasing illicit services and goods. Darknet sites have also become popular locations for 'data dumps' including for financial information and website registration datasets. It may be possible that sensitive knowledge and data related to the nuclear fuel cycle could also be made available in a comparable manner. Moreover, the use of the darknet markets for connecting buyers and sellers of small goods will remain a challenge. The paper looks at potential new pathways of nuclear proliferation arising from uses of the darknet, and how these may impact the development of future IAEA Safeguards.

1. INTRODUCTION

The darknet is an infamous haven for criminal activity. The most well-known platforms on the darknet are the markets, such as Silk Road and Silk Road 2, which saw $100m per year of drug-dominated sales from 2011-2014 [1]. Since the takedown of Silk Road, new darknet markets, such as AlphaBay, have sprung up to continue its activities. If the darknet can facilitate illegal trade, then it may have a role in facilitating proliferation and transfer of sensitive goods or knowhow [2].

The darknet is also increasingly being used to host large volumes of hacked data, including sensitive personal data and leaked documents [3, 4]. This is relevant for safeguards implementation in two key respects: eventually a data dump may contain safeguards-relevant sensitive nuclear information or personal and organisational information of those responsible for safeguards implementation.

To consider the impact of the darknet as it continues to develop, we first provide a brief overview of the darknet in section 2: how it works, what distinguishes it from the regular internet, and what kinds of activity occur there. We then we review the potential proliferation threat of the darknet in section 3 and finally provide an overview with the four main risks identified for nonproliferation and safeguards in section 4.

2. OVERVIEW OF THE DARKNET MARKETS

The darknet is a subset of the internet that requires anonymising software to access. This section describes how anonymity on the darknet dictates behaviour and how this in turn impacts what is available on the darknet markets. We describe the physical and digital goods that are available and how these vary by forum. Finally, we provide a comparative snapshot of the AlphaBay market between 2015 and 2022.

2.1. Anonymity and the Darknet

How would you behave on the internet if you could act with fear of detection or reproach? The increasing use of encrypted communications (Signal, Telegram) and hidden services (the darknet) gives individuals more methods for long-distance private interactions. Activity enabled by this includes free political speech, the drugs trade, fraud and other serious crimes.

The internet has permitted the formation of millions of communities of the likeminded. Micro communities exist alongside massive international movements. On the internet, no hobby or interest is too niche to not be able to find fellow travellers: people can exchange ideas with people they would never otherwise have met. This coming together of the weird and wonderful extends to consumerism: for the right price it seems possible to buy anything every made if we want it enough and get it mailed to our doors. Some interests are not legal, so when netizens follow their desires, they must be mindful of the law, including engaging in restricted political speech or buying prohibited goods. To the average internet user, anonymity can be achieved on most websites by using an avatar or internet username that is unrelated to them, many high-profile users on sites such as Twitter have online notoriety, but the offline individual (IRL or in real life) is anonymous.

The more dangerous and prohibited the activity, the more the user must take care to separate their online identity from IRL. Maintaining operational security to prevent prying eyes is a complicated task. Accessing websites using standard means risks being observed by the internet provider or the website being visited. To reduce the risk of being observed by the internet provider a VPN can be used. To reduce the risk of being tracked by the website you a visiting a set of 'relays' can be used that mask the IP address (Internet Protocol) of the user. One such service is TOR (The Onion Router).[1] TOR is somewhat synonymous with the darknet but is itself a tool to anonymise internet users from websites.

The darknet is an anonymised offshoot of the internet. To access a darknet website (known as 'hidden services') a browser that anonymises the user, such as TOR, must be used. TOR can be used to access regular internet sites with enhanced security. The .onion websites require the user to use an anonymising web browser to access. Many regular internet or 'clearnet' websites have a .onion address counterpart to enhance the security, privacy for their users.[2]

2.2. Procurement on the internet

Goods and services on the internet are facilitated through many vendors. The business to business (B2B) and business to consumer sites (B2C) either provide direct sales from the inventory of a single business or are marketplaces or online 'supermarkets' such as Amazon or Alibaba where buyers can purchase from any listed consumer. Other sites are consumer to consumer (C2C) vendors sites, such as Ebay and Facebook Marketplace. Generally, commerce is regulated on these websites, both by tax paid to the government and confidence that the site will faithfully transfer payment from the purchaser to the seller after taking a cut. From both consumer protection laws and the credibility of the marketplace itself there is typically an assurance or guarantee of a replacement or refund if goods are damaged or low quality from either the manufacturer or vendor.

B2B procurement may be based on a long-term client relationship, an independent quality assurance from international manufacturing standards authorities or from consumer groups. Consumer interactions from B2C and C2C may be based more on brand awareness or product reviews. Finally, C2C transactions will not only be based on product quality reviews but the credibility of the seller; their track record for timely shipping of goods as listed without damage (excepting in transit). As the seller becomes smaller and less recognisable and as the marketplace becomes smaller (less numbers of transactions) the level of trust between the buyer and seller decreases.

Hidden service (darknet) websites, much like the regular internet, have variety of users and functions. The most notorious are the darknet markets.

2.3. Data dumps and darknet forums

Darknet hacking forums over the last decade have been the increasingly used for posting data breaches and large password dumps. Mass data breaches and password dumps are a consistent cybersecurity threat. The darknet forums are the go-to place for selling the data, which can be a lucrative forum for hackers. Data breaches have included government, local services [4], and large international service companies. Such data breaches can put a large volume of sensitive information in the public domain. Malware, ransomware, forged documents, are also frequently available on the forums [5].

2.4. Alphabay: A Darknet market snapshot

Alphabay was the most popular darknet market until it was taken down in 2017 by law enforcement in Operation Bayonet. This resulted in the arrest of the chief administrator Alexandre Cazes, and the takedown of the central server [6]. Another prominent Alpha Bay administrator, known as 'DeSnake' has built a new Alpha

[1] Others include I2P (Invisible Internet Project), and Freenet

[2] Facebook has an onion address at **facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion**

Bay which in 2022 reclaimed the position of the most popular Darknet Market by user numbers and estimated trade volume.

The website may seem like the Wild West, but the terms and conditions required to register on the new site are like any legitimate business, with some unusual riders. Doxing, terrorism, weapons, violence, pornography, fake or real Covid-19 vaccines/cures and hate speech are all banned. Interestingly, former CIS countries, including Russia, are not permitted to be included in any related activity for data dumps etc and the discussion, use or sale of Ransomware is forbidden.

Vendors and buyers are reliant on reputation to sell or make purchases – much like the relationship between buyers and sellers on legitimate online markets. For most goods and services, the seller must establish a good reputation for their product and shipping. Like legitimate online services where the vendor incurs risks with who they provide services to, such as Airbnb, the buyers also are rated and each user must maintain a ‘trust’ rating. Listings by category of the AlphaBay marketplace, for two comparative snapshots, in 2015 and 2022 are shown in Table 1.

TABLE 1. AlphaBay category listings in 2015 and 2022. Note n/a listings are as the category was not listed in the year given.

Listing	2015	2022
All listings	39115	39137
Fraud	7541	5984
Hacking & Spam	n/a	1026
Drugs & Chemicals	19406	35937
Services	1670	373
Security & Hosting	132	94
Guides & Tutorials	3459	2803
Software	376	785
Digital Items	2873	1384
Websites & Graphic Design	n/a	15
Jewels & Precious Metals	433	25
Counterfeit Items	1426	661
Carded Items	727	49
Automotive-Related Items	n/a	16
Legitimate Items	n/a	50
Other Listings	580	163
Weapons	436	n/a

The type of listings, and their popularity has remained remarkably stable between the two snapshots. By far the most popular listing is drugs, with notable interest in ‘Guides and Tutorials’, ‘Fraud’ and ‘Digital Items’. The Guides and Tutorials describe themselves as self-help for activities such as how to scam, use malware, or other fraudulent activities including eBooks on how to conduct fraud and operational security, but also Spotify, Netflix and Disney+ accounts for sale. Notably, under the new AlphaBay terms of use, weapons are no longer permitted to be sold through the site. Fentanyl is also banned under the terms and conditions, noting the risks to buyers.

3. THE DARKNET MARKETS: A PROLIFERATION THREAT?

3.5. Recent security literature on the darknet

Since the launch of the notorious market Silk Road in 2011, the darknet has become a focus of security-related research. Most of the academic literature on the darknet focuses on criminology and sociology of the darknet users, particularly with respect to terrorism and drugs [8, 9]. Other security-relevant literature has studied the trade of small arms [10-12] where a large active trade network is found to be facilitated by the darknet markets.

Blancke [13] and Christopher [2] provide two of the only studies to look at the nuclear relevance of the darknet. Blancke's 2018 snapshot of forum and market activity finds a small fraction of darknet users that demonstrate an interest in nuclear-related questions, but show a naivety, asking questions such as 'How to build a home-made nuclear reactor?' Blancke observes that the answers given on darknet forums show considerably more understanding than the questioner (and unusually for the example given above a descriptive link is provided to the Clearnet). Blancke examines the possibility of nuclear-security relevant trade, in items such as stolen americium, curium or plutonium. While no relevant cases are identified, both the possibility and the threat cannot be eliminated [13].

Christopher rules out the darknet markets facilitating strategic trade as a counterpart to the trade and procurement channels for Nuclear Suppliers Group listed items observed on Clearnet sites [14, 15]. Christopher finds no evidence of large-scale strategic trade on the darknet markets and makes similar observations to Blancke on nuclear security-related transactions. To explain this, Christopher offers several reasons. First, the darknet markets are inherently low trust because the state is not backing the trade. This means that the market, vendor and customer must demonstrate a reliable track record for successful sales of their main product. This depresses any market for costly one-off 'exotic' goods where no track record is present, and both the vendor and buyer expose themselves to high risk by conducting the transaction. Secondly, products are sent from the vendor to the buyer in only two ways: small shipments using postal services or digitally. The vendors on the darknet do not have the logistics in place to facilitate payment and shipment of large quantities of physical goods, limiting the ability to transfer.

3.6. What trends can we identify on the darknet markets?

The snapshot of the AlphaBay market shows that although there were some changes, the core product line offered by a darknet marketplace is remarkably stable. The three underpinning constants of darknet markets: payment, shipping and hosting/encryption are relatively stable, only undergoing slow evolution as the markets try to grow their customer base.

As was noted in the previous section, 'exotic' products are unlikely to be purchased by the typical user due to the low trust nature of the marketplaces. Given the reputation of the darknet markets, they will continue to attract low probability rare high-consequence transactions relevant to nuclear security. As such, small-scale transactions involving nuclear and radiological material remain possible. A persistent low-probability high-risk threat related to WMD terrorism, stemming from either stolen materials or manufacturing knowhow for sale on the darknet remains a concern for law enforcement [16, 17] as a regular flow of law enforcement operations, resulting in convictions for items such as ricin have shown [18, 19].

One notable trend on the darknet is the increasing appearance of large sets of hacked information, or 'data dumps'. The data may be obtained from opportunistic cyberattacks targeting companies with careless data security, or specifically targeted organisations by activist groups [3]. These dumps involve the personal data of millions of individuals, potentially putting anybody involved at risk of blackmail or fraud. A future data dump could include

3.7. An Aside: Encrypted Messaging Technology

Encrypted messaging is designed to prevent 3rd parties from being able to read private communications. The user base is very different from the darknet, with end-to-end encryption (E2EE) apps such as Telegram, WhatsApp and Signal saturating the smartphone app market.

While such applications have become popular with users, extremist groups have also taken up encrypted apps for running their networks [20]. Such technology would likely be central to any future proliferation network. While it is possible that Darknet communications could sustain a proliferation network or be the primary communications method between one or two nodes in the networks, direct E2EE would likely be the primary means of communications across a network due to the ease of use; trust in the platform and ability to securely share across the network.

4. CONCLUSIONS: THE FUTURE OF THE DARKNET AND NONPROLIFERATION

There are four risks associated with the darknet identified by this paper that will be relevant for safeguards:

1. Stolen or hacked data containing personal information of people relevant for safeguards;
2. Sensitive nuclear-related know-how published or offered on the darknet;
3. Sale of small quantities of nuclear or radiological material; and;
4. A proliferation network using darknet infrastructure to operate.

A fifth use of the darknet, for transfer of strategic trade goods, in quantities relevant for a nuclear fuel cycle, has been ruled out by previous research [2].

Of these four risks, the first, that personal information relevant to safeguards is posted on the darknet is expected to rise risk over time as large-scale data dumps become more common. The second risk, on the publication of sensitive know-how is relatively unknown. No systematic study, which has been made public, of the current extent and future risk of sensitive knowhow either offered as a service or published on the darknet. The third risk, on the availability of small quantities of radiological or nuclear material, will continue to be a persistent low-level threat. The fourth risk, for the darknet to facilitate a proliferation network, is increasingly obsolete after the rise of end-to-end encryption technology. While the darknet may facilitate some links between nodes of a proliferation network on the darknet, apps such as Telegram offer the same or higher levels or security whilst also offering ease of use.

BIBLIOGRAPHY

[1] ANDY GREENBERG. 2015. *Crackdowns Haven't Stopped the Dark Web's $100M Yearly Drug Sales* [Online]. Wired. Available: https://www.wired.com/2015/08/crackdowns-havent-stopped-dark-webs-100m-yearly-drug-sales/ [Last Updated 2015]..

[2] GRANT CHRISTOPHER, Strategic Trade and the Darknet Markets. *WorldECR,* (2019).

[3] KIM ZETTER. 2015. *Hackers Finally Post Stolen Ashley Madison Data* [Online]. Wired. Available: https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ [Last Updated 2015]..

[4] T. FLOYD, M. GRIECO & E. F. REID. Mining hospital data breach records: Cyber threats to U.S. hospitals. 2016 IEEE Conference on Intelligence and Security Informatics (ISI), 28-30 Sept. 2016 2016. 43-48..

[5] RODERIC BROADHURST, et al., Malware trends on 'darknet'crypto-markets: Research review. *Available at SSRN 3226758,* (2018).

[6] NATHANIEL POPPER. 2017. AlphaBay, Biggest Online Drug Bazaar, Goes Dark, and Questions Swirl. *New York Times*, 6 July..

[7] DANIEL MOORE & THOMAS RID, Cryptopolitik and the Darknet. *Survival,* 58 (2016) 7-38.

[8] GABRIEL WEIMANN, Going Dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism,* 39 (2016) 195-206.

[9] ALEXIA MADDOX, MONICA J. BARRATT, MATTHEW ALLEN & SIMON LENTON, Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society,* 19 (2016) 111-126.

[10] JACK FOYE, MATTHEW BALL, CHUXUAN JIANG & RODERIC BROADHURST, Illicit firearms and other weapons on darknet markets. *Trends and Issues in Crime and Criminal Justice,* (2021) 1-20.

[11] GIACOMO PERSI PAOLI. 2018. *The Trade in Small Arms and Light Weapons on the Dark Web: A Study* [Online]. UNODAAvailable: https://www.un.org/disarmament/publications/occasionalpapers/unoda-occasional-papers-no-32-october-2018 [2018]..

[12] GIACOMO PERSI PAOLI, JUDITH ALDRIDGE, NATHAN RYAN & RICHARD WARNES 2017. *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web,* Santa Monica, CA, RAND Corporation..

[13] STEPHAN BLANCKE, OSINT Snapshot: Dark web market trades illicit nuclear materials and knowledge. *Jane's Intelligence Review,* (2018) 1-4.

[14] CHARLES CLOVER. 2014. Alibaba: Weapons of mass ecommerce. *Financial Times*..

[15] G. CHRISTOPHER. 2015. *Open Source Information in Support of Safeguards* [Online]. International Atomic Energy Agency (IAEA).IAEA-CN--220 Available: http://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014_eproceedings_online.pdf http://inis.iaea.org/search/search.aspx?orig_q=RN:46076183 [2015]..

[16] EUROPEAN UNION. 2017. *Terrorism Situation and Trend Report* [Online]. European UnionAvailable: https://www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf [2017]..

[17] LASHA GIORGIDZE & JAMES K. WITHER. 2019. *Horror or Hype: The Challenge of Chemical, Biological, Radiological, and Nuclear Terrorism* [Online]. George C. Marshall European Center for Security StudiesAvailable: https://www.marshallcenter.org/en/publications/occasional-papers/horror-or-hype-challenge-chemical-biological-radiological-and-nuclear-terrorism-0 [2019]..

[18] BBC NEWS. 2015. Breaking Bad fan jailed over Dark Web ricin plot. *BBC News*..

[19] MATT ZAPOTOSKY. 2016. New York man sentenced to 16 years for trying to buy ricin on the 'Dark Web'. *Washington Post*..

[20] TECH AGAINST TERRORSIM. 2021. *Terrorist Use Of E2EE: State Of Play, Misconceptions, And Mitigation Strategies* [Online]. Tech Against TerrorismAvailable: https://www.techagainstterrorism.org/wp-content/uploads/2021/09/TAT-Terrorist-use-of-E2EE-and-mitigation-strategies-report-.pdf [2021]..