UNODA Occasional Papers
No. 32, October 2018

The Trade in Small Arms and Light Weapons on the Dark Web

A Study

by Giacomo Persi Paoli

UNODA
United Nations Office for Disarmament Affairs

United Nations

UNODA

United Nations Office for
Disarmament Affairs

UNODA Occasional Papers

No. 32, October 2018

The Trade in Small Arms and Light Weapons on the Dark Web

A Study

by Giacomo Persi Paoli

United Nations

The United Nations Office for Disarmament Affairs (UNODA) Occasional Papers are a series of ad hoc publications featuring, in edited form, papers or statements made at meetings, symposiums, seminars, workshops or lectures that deal with topical issues in the field of arms limitation, disarmament and international security. They are intended primarily for those concerned with these matters in Government, civil society and in the academic community.

The views expressed in this publication are those of the author and do not necessarily reflect those of the United Nations or its Member States.

Symbols of United Nations documents are composed of capital letters combined with figures. These documents are available in the official languages of the United Nations at http://ods.un.org. Specific disarmament-related documents can also be accessed through the disarmament reference collection at www.un.org/disarmament/publications/library.

Author

Dr. Giacomo Persi Paoli is the Associate Director of the Defence, Security and Infrastructure Research Group at RAND Europe. Since joining RAND Europe, Giacomo led several research projects in the defence and security domain for both national governments and international organizations. He is a conventional arms control specialist, with extensive track record in the field of small arms and light weapons. In this area, he has performed high-profile work for the United Nations and the European Commission. He also has experience in other fields of conventional arms trade regulation, particularly in relation to the implementation of the Arms Trade Treaty and other international instruments regulating trade in, or procurement of, conventional weapons or other defence materiel. He received his PhD in economic theory and institutions from the University of Roma Tor Vergata (Italy).

RAND Europe is a not-for-profit policy research organization that aims to improve policy and decision-making in the public interest through objective research and analysis. Its clients include national governments, militaries, multilateral institutions and other organizations with a need for rigorous, independent, interdisciplinary analysis. Part of the global RAND Corporation, RAND Europe has offices in Cambridge, United Kingdom, and Brussels, Belgium.

This publication is available from
www.un.org/disarmament

UNITED NATIONS PUBLICATION
Sales No. E.19.IX.1
ISBN 978-92-1-130357-5
eISBN 978-92-1-047465-8

Printed at the United Nations, New York

Contents

Figures

Tables

Preface

The potential role of the dark web in facilitating trade in firearms, ammunition and explosives has gained increased public attention following recent terrorist attacks in Europe and other criminal activities worldwide. In fact, the hidden and obscured parts of the web are used by criminals and others to access a worldwide market where it's possible to procure or sell a wide range of weapons and associated products through encrypted marketplaces and vendor shops.

While the use of these platforms as enablers for the illicit drug trade has increasingly been the subject of academic research, to date, no systematic investigation has been undertaken of the role of the dark web in relation to the illegal arms trade, drawing on the insights offered by primary data.

Following the outcomes of the Third United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, which acknowledged the importance of considering new challenges and opportunities arising from new forms of illicit trafficking, this document summarizes the main findings and implications of the first empirical study investigating the scale and scope of arms trafficking on the dark web.

The full study was conducted by RAND Europe and the University of Manchester, and was funded by the United

Kingdom Partnership for Conflict, Crime and Security Research under the theme of transnational organized crime.

For more information about this report or the full study, please contact:

Dr. Giacomo Persi Paoli
Research Leader, Defence, Security and Infrastructure
RAND Europe
Westbrook Centre, Milton Road
Cambridge CB4 1YG
United Kingdom
Tel. +44 (1223) 353 329
gpersipa@rand.org

Executive summary

Study background and context

There is an ongoing debate over the extent to which online black markets on the so-called "dark web", the part of the Internet not searchable by traditional search engines and hidden behind anonymity software, facilitate arms trafficking. Details have emerged in the media following the Munich shooting in 2016 linking the weapons used by the attacker to vendors on dark web marketplaces (also known as cryptomarkets). Some media reports have also linked the Paris terrorist attacks in November 2015 to these platforms. While these reports appear to have raised concerns about the role of such dark web markets in arms trade, evidence on the subject is largely anecdotal, based on secondary data as reported after events such as terrorist attacks or successful law enforcement operations.

Following the outcomes of the Third United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, which acknowledged the importance of considering new challenges and opportunities arising from new forms of illicit trafficking, this document summarizes the main findings and implications of the first empirical study investigating the scale and scope of arms trafficking on the dark web, which was conducted by RAND Europe and the University of Manchester from September 2016 to July 2017.

Summary of methodology, caveats and limitations

The project team employed a mixed-methods approach that included the following:

- **Review of relevant literature**, including peer-reviewed academic literature, grey literature sources from official, government and other relevant organizations and, particularly relevant for this study, web-sourced contributions from respected commentators and independent researchers within the dark web community .
- **Review of clear web resources**, including websites used to identify marketplaces and provide information and commentary on recent developments related to cryptomarkets as well as **discussion forums**.
- **Crawling, scraping and analysis of cryptomarket data** in the form of "digital traces" left in connection to marketplace transactions. The data was obtained using a software tool specifically designed to crawl and scrape cryptomarket data.[1]
- **Consultation with policy and law enforcement experts** through an expert workshop and individual interviews.

Limitations

Some caveats and limitations on the methodology should be considered in the interpretation of the results. These are summarized as follows:

- The primary data collection was conducted from 19 to 25 September 2016 and represents a snapshot of cryptomarkets at the time (i.e., the project team did

[1] DATACRYPTO is a tool designed by one of the authors in collaboration with David Décary-Hétu at the University of Montreal (Décary-Hétu & Aldridge 2013) specifically for collecting the unique sales-related data available on cryptomarkets.

not conduct a continuous monitoring of the activity on cryptomarkets).

- Dark web markets that fall into the vendor shop category do not provide information that can be used to estimate sales generated; therefore, the estimates presented in this study refer exclusively to the analysis of data from cryptomarkets, potentially resulting in an underestimation of the overall size and value of the trade.
- The assessment of gross revenue generated by dark web sales on cryptomarkets used feedback left by buyers as a proxy for confirmed sales; this comes with some limitations, as no obligation exists for buyers to leave feedback (i.e., feedback is under-representing sales), or vendors could use techniques to inflate the number of feedback entries (i.e., over-representing sales).
- Image analysis was not conducted on listed products due to the inability to scrape images using the available tool; this may have had an impact on the information generated through the qualitative analysis and on the ability to cross-check through visual analysis the accuracy of the information included in the description of the listings.
- Given the impossibility to determine with certainty the nature of a vendor (scammer, law enforcement or real vendor), the results are likely to include listings that do not correspond to real vendors.
- Information on vendor location is based on the analysis of the (self-reported) "Ship from" field of each listing, complemented by the analysis of additional information obtained from product descriptions across cryptomarkets. However, information on the locations of buyers is exclusively based on vendors' stated willingness to ship to certain locations. When vendors are willing to ship worldwide, the data available does not allow the identification of the specific destination.

Summary of key findings from the analysis

The project team built the evidence base on three main pillars: (a) size and scope (e.g., what is available on the market and in what quantities); (b) value (e.g., what are the dark web market prices of the products offered and how much is the dark web arms trade worth); and (c) shipping routes and techniques (e.g., where are vendors shipping from, where are vendors willing to ship to—or, if possible, where are buyers located—and how are these items shipped). Within the constraints described above, this section summarizes the main points that emerged from the study related to these three pillars and their implications, mapping them along the study research questions.

Question 1: How can firearms and related products be purchased and sold on the dark web?

- There are, at present, two types of marketplaces found on the dark web where firearms and related products are offered and sold: cryptomarkets and vendor shops. Several clear web sources exist to guide interested users in locating and choosing marketplaces of both kinds on the dark web, as well as to support buyers in identifying reliable vendors.

  Cryptomarkets bring together multiple sellers, known as "vendors", managed by marketplace administrators in return for a commission on sales. Cryptomarkets provide third-party services that afford a degree of payment protection to customers: escrow (in which payment is released to vendors only after customers have received and are satisfied with their purchases) and third-party dispute adjudication. Cryptomarkets use cryptocurrencies for payment and allow customers to provide feedback connected to their purchases, with scores aggregated and displayed by the marketplace to guide customers in selecting reliable vendors and highly rated products.

Vendor shops, also known as "single-vendor markets", are set up by a vendor to host sales for that vendor alone. These vendors sell directly to customers willing to make purchases without the third-party services provided on cryptomarkets. In this way, vendors can avoid the commissions on their sales charged by cryptomarkets and avoid the financial risk entailed by cryptomarket "exit scams". Vendor shops tend to be more specialized and often trade on reputation track records earned via cryptomarket selling to generate customer trust. Many vendor shop owners trade simultaneously on cryptomarkets.

Once the online part of the transaction is finalized, the products purchased are normally shipped by post using special shipping techniques to minimize the risk of detection. In the context of firearms, these techniques often involve disassembling the weapon and shipping different parts in multiple packages.

Question 2: What is the estimated size and scope of the trade in firearms and related products on cryptomarkets?

(a) Number of dark web markets listing firearms and related products and services for sale and number of vendors

- There were 24 English/French-language cryptomarkets operating during our assessment period. Eighteen of these markets (75 per cent) were successfully accessed and inspected to ascertain evidence of arms-related selling. Of the 18 accessed markets, 15 (83 per cent) had rules explicitly allowing, or not explicitly prohibiting, arms sales. Nine markets (50 per cent) provided vendors with a dedicated "firearms" category into which vendors could place listings, while the others included firearms and related products into a general category (e.g., "other" or "miscellaneous").

- Sixty vendor accounts were identified for which firearms listings were held across all accessed markets. Using "Pretty Good Privacy" matching, the project team estimated that this translates to 52 unique vendors. The vast majority (88 per cent) sold on only one marketplace, with the remainder selling across two (8 per cent) or three (4 per cent) markets.

(b) Range and type of firearms and related products advertised and sold on cryptomarkets

- Of the relevant 811 listings identified by this study, firearms represented the most common category of product sold. Within the firearms category, pistols are by far the most common firearm type, followed by rifles and submachine guns. The majority of firearms offered for sale are live weapons, with the exception of the submachine guns, the majority of which are replicas. The condition of the firearm, new or used, does not appear to be an important feature, given that more than half of the listings do not provide information on this aspect.
- Ammunition is rarely sold in isolation and is more often sold in combination with the firearm, suggesting that vendors may have access to a wider supply base for the products they are offering. The same applies to parts, components and accessories.
- Particularly relevant is the fact that the second most common product category is represented by digital products. These include both manuals on how to manufacture firearms and explosives at home and 3D models to enable home-based printing of fully functioning firearms or their parts.
- From a quantitative perspective, the 811 listings identified as relevant for the purpose of this study represent only the 0.5 per cent of the total number of listings collected. This illustrates how, from a quantitative perspective, the use of

cryptomarkets to sell weapons is marginal when compared to other product categories.

- The evidence base does not allow determining the scale of dark web arms trafficking compared to its offline equivalent. On the other hand, from a qualitative perspective, dark web marketplaces seem to offer both a wider range and better quality of firearms than those normally accessible on the streets (despite the latter being to a certain extent country-specific).

Question 3: What is the estimated value of the trade in firearms and related products on cryptomarkets?

- Prices for firearms on cryptomarkets are generally higher than retail price, with some variations based on the make and model.
- Replica firearms appear to be significantly more expensive than retail price, sometimes even more expensive than real firearms.
- For pistols, condition (used or new) seems to have no significant impact on price, while for rifles, new items, as expected, cost more than used ones.
- Concerning sales, based on the estimates generated by this study, firearms (including their parts, components, ammunition and accessories), explosives and digital products generate 136 sales per month, with an estimated monthly gross revenue in the region of US$ 80,000. The majority of transactions and of gross revenue comes from pistols, which appear to be the most commonly traded product.
- From a quantitative perspective, the value of the monthly trade in firearms and related products on the dark web is marginal when compared to other products sold on cryptomarkets (e.g., Kruithof et al. (2016) estimated

that drug listings generated a monthly revenue of US$ 14.2 million) and to the legal arms trade. The evidence did not support a comparative analysis between the value of online and offline illicit trade in firearms and related products because no robust estimates of the latter exist.

- Concerning the volume of monthly transactions, in the absence of a benchmark, it is difficult to establish how 136 sales per month on cryptomarkets relate to the wider context of arms trafficking. Nevertheless, from a risk assessment perspective and in consideration of the potential impact that arms trafficking can have on internal security, the volume can be considered sufficiently high to be cause for concern for policymakers and law enforcement agencies.

Question 4: What are the main shipping routes and most common shipping techniques?

A large portion of shipping origins and destinations remain undetermined. However, some key observations can be drawn from the evidence:

- The United States appears as the dominating source country in terms of both number of listings and number of monthly transactions.
- The overwhelming majority of listings appear to be open to worldwide destinations, making it difficult to identify where buyers are located. Where data is available, Europe appears to be a key recipient of firearms sold on the dark web.
- The data suggests that the majority of the dark web arms trade is international rather than domestic.
- Firearms are normally disassembled and shipped in multiple parcels hidden in other "consumer electronics castings", such as printers or car stereos, to avoid or minimize the risk of detection.

Implications and considerations

On the basis of the findings outlined above and acknowledging the limitations of our methodology, it is possible to summarize the main implications and considerations as follows:

Question 5: What is the potential impact of dark web–enabled arms trafficking on the overall black market, with particular emphasis on market dynamics and market actors?

- The dark web is both an enabler for the trade of illegal weapons already on the black market and a potential source of diversion for weapons legally owned.
- The scale of the market remains limited, making it a more viable and attractive option for individuals and small groups than for larger criminal groups or armed actors engaged in conflict.
- The dark web enables illegal trade at the global level, removing geographical barriers between vendors and buyers and increasing their personal safety through a series of anonymizing features protecting the identity of individuals involved.
- The veil of anonymity provided by some key technical features of the dark web, combined with its relative ease of access, also removes most personal barriers, making the dark web an attractive option for a wider range of types of individuals who may not be affiliated to, or inspired by, terrorist or criminal organizations.

Question 6: What are the potential implications of dark web–enabled arms trafficking for law enforcement agencies and policymakers, at both the national and international level?

- Law enforcement agencies are facing a series of operational challenges related to the main intervention strategies. While some of these challenges are inherent to the technical features of the dark web, others could be overcome through the active involvement and support of the policymaking community, both at the national and international level.
- At the national level, policymakers should ensure that the threat posed by illegal arms trafficking on the dark web is recognized and adequate resources are mobilized to ensure that law enforcement agencies are staffed, trained and equipped to respond effectively. In addition, policymakers should also consider longer-term strategies focusing on education and prevention as a form of soft intervention.
- The response to dark web–enabled arms trafficking starts with the rigorous implementation of already existing international instruments designed to tackle the general issue of arms trafficking by providing a range of control measures to limit the diversion of legally owned firearms to the black market or to trace illegal firearms back to the last known legal owner, providing an investigative lead into the point of diversion to the black market.
- Current international instruments regulating various aspects of the trade in firearms, their parts, components and ammunition are offering an already solid base to respond to the threat posed by dark web–enabled arms trafficking, but a more detailed analysis should be performed to identify areas that may require updating or further development.

- Key international legal instruments, such as the Organized Crime Convention, the Firearms Protocol and the Arms Trade Treaty provide a solid legal basis to frame national and international responses to dark web–enabled arms trafficking. However, slow transposition and implementation of the international legal framework at the domestic level, as well as the fact that certain key market players identified in this report are not yet States parties to the instruments identified, limit the extent to which tools and measures provided by such instruments can be used in practice.

Conclusions

This study has demonstrated that meaningful insights can be obtained by using empirical analysis methodologies to investigate dark web–enabled arms trafficking. Despite its limitations, described throughout the report, this study represents the first systematic, evidence-based assessment of trafficking in firearms (including their parts, components, accessories and ammunition) and explosives.

The findings generated by this study highlight the global nature of this threat and reinforce the importance of several key points included in the recently released outcome document of the Third United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects.[2]

In addition to the general principles and actions targeting the overall issue of arms trafficking, which are also applicable and relevant to dark web–enabled arms trafficking, some of the specific articles in the forward-looking part of the outcome document (i.e., implementation of the Programme of Action for the period 2018-2024) also resonate with the findings of this

[2] United Nations General Assembly (2018).

study. A selection of such articles and related study findings is illustrated in further detail in table 7.1 on pp. 76-77.

Additional research would be necessary to further develop the understanding of the market characteristics (i.e., size, scope and value of the dark web arms trafficking), the products available and the actors involved (e.g., buyers, vendors, administrators and others).

In particular, in order to generate a more robust understanding of the role of the dark web in enabling arms trafficking, a more continuous monitoring activity should be implemented. This would involve repeating and refining the data collection and analysis presented in this report over time in order to generate historical data that can be used to analyse trends. This would also enable a more rigorous assessment of the validity and applicability of current national and international counter-arms trafficking regimes including policies, laws and regulations, actors and resources.

I.

Introduction

> *[Lyburd] said buying the Glock was like "buying a bar of chocolate".*
>
> Report on Liam Lyburd, an 18-year-old who plotted a massacre at his former school in Newcastle
> BBC News, 30 July 2015[1]

> *[Robert Heimberger, head of Bavaria's criminal police] said it was likely the Glock pistol—which had been reactivated—was bought on the "dark net".*
>
> In reference to the 2016 Munich shooting where David Sonboly, 18, killed nine people
> BBC News, 24 July 2016[2]

There is an ongoing debate over the extent to which online black markets on the so-called "dark web"[3] facilitate the sale of firearms, weapons, explosives and banned digital materials. Public details have emerged in the media following the 2016

---

[1] "Liam Lyburd guilty of Newcastle College mass murder plot", British Broadcasting Corporation (BBC) News (30 July 2015). Available from https://www.bbc.com/news/uk-england-33718094.

[2] "Munich shootings: Police arrest 16-year-old Afghan", BBC News (25 July 2016). Available from https://www.bbc.com/news/world-europe-36880606.

[3] The dark web contains hidden pages of the Internet, which are not accessible to the everyday user. For a detailed explanation of the dark web, see section 2.1 and Figure 1.

Munich shooting linking the weapons used by the attacker to vendors on dark web "cryptomarkets";[4] while this has not been confirmed by public authorities, media outlets have reported that the dark web may have played a role even in the Paris terrorist attacks in November 2015.[5] Despite a perceived high level of concern in European communities following the attacks,[6] the majority of public information available on the subject is anecdotal, based on secondary data as reported after terrorist events or successful law enforcement operations. Very little is known about the sale of weapons on cryptomarkets from an empirical research perspective.[7] This report aims to fill the current gap in knowledge by using primary data to analyse the size, scope and value of the arms trade on the dark web.

Objectives and overview of the methodology

The overarching goal of this study is to provide law enforcement agencies and policy and decision makers with an

---

[4] A cryptomarket is defined as a "marketplace that hosts multiple sellers or 'vendors', provides participants with anonymity via its location on the dark web and use of cryptocurrencies for payment, and aggregates and displays customer feedback ratings and comments." (Barratt & Aldridge 2016).

[5] See, for example, Bender and Alessi (2016) and HNGN (2015).

[6] The German broadcaster ARD produced a series of investigative reports on the dark web in the wake of the 2016 Munich shooting, which "strengthened [the common] view" of "the dark net as the haven of evil" where weapons, drugs and child pornography are traded (Tagesschau 2017). As reported by German news magazine FOCUS Online, the journalist attempted to buy a Kalashnikov for $800 in Bitcoin, only to be scammed by the vendor (Pawlak 2016).

[7] Early attempts to study the longitudinal evolution of cryptomarkets gathered data on the "weapons" category of cryptomarkets. In the published analysis, the low volume of weapons traded was collapsed into the "other" category, along with drug paraphernalia, electronics, tobacco, sildenafil and steroids (Soska & Christin 2015). Independent researcher Gwern Branwen reported that gun sales up until June 2015 were "miniscule", where he cites 2011-2013 research from Silk Road, which "does not include any entry relating to them" (cited in Hullinger 2016).

evidence-based understanding of arms trafficking on the dark web in order to support wider national and international efforts aimed at tackling illegal trafficking in firearms and related products.

More specifically, this study seeks to provide evidence-based answers to the following research questions:

1. How can firearms and related products be purchased and sold on the dark web?
2. What is the estimated size and scope of the trade in firearms and related products on cryptomarkets, including the following:
   (a) Number of dark web markets listing firearms and related products and services for sale and number of vendors.
   (b) Range and type of firearms and related products advertised and sold on cryptomarkets.
3. What is the estimated value of the trade in firearms and related products on cryptomarkets?
4. What are the main shipping routes and most common shipping techniques?
5. What is the potential impact of dark web–enabled arms trafficking on the overall black market, with particular emphasis on market dynamics and market actors?
6. What are the potential implications of dark web–enabled arms trafficking for law enforcement agencies and policymakers, at both the national and international level?

To answer these questions, the project team employed a mixed-methods approach that included the following:

- **Review of relevant literature**, including peer-reviewed academic literature, grey literature sources from official, government and other relevant organizations, and, particularly relevant for this study, web-sourced

contributions from respected commentators and independent researchers within the dark web community.

- **Review of clear web resources**, including websites used to identify marketplaces and provide information and commentary on recent developments related to cryptomarkets as well as **discussion forums**.
- **Crawling, scraping and analysis of cryptomarkets data**, in the form of "digital traces" left in connection to marketplace transactions. The data was obtained using a software tool specifically designed to crawl and scrape cryptomarket data.[8]
- **Consultation with policy and law enforcement experts** through an expert workshop and individual interviews.[9]

Limitations

Some caveats and limitations on the methodology should be considered in the interpretation of the results. These are summarized as follows:

- The primary data collection was conducted from 19 to 25 September 2016 and represents a snapshot of cryptomarkets at the time (i.e., the project team did not conduct a continuous monitoring of the activity on cryptomarkets).
- Dark web markets that fall into the vendor shop category do not provide information that can be used to estimate sales generated; therefore, the estimates presented in

[8] DATACRYPTO is a tool designed by one of the authors in collaboration with David Décary-Hétu at the University of Montreal (Décary-Hétu & Aldridge 2013) specifically for collecting the unique sales-related data available on cryptomarkets.

[9] All engagements with experts were conducted under the Chatham House Rule. When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of either the speaker(s) or any other participant, may be revealed.

this study refer exclusively to the analysis of data from cryptomarkets, potentially resulting in an underestimation of the overall size and value of the trade.

- The assessment of gross revenue generated by dark web sales on cryptomarkets used feedback left by buyers as a proxy for confirmed sales; this comes with some limitations, as no obligation exists for buyers to leave feedback (i.e., feedback is under-representing sales), or vendors could over-represent sales using techniques to inflate the number of feedback entries.
- Image analysis was not conducted on listed products due to the inability to scrape images using the available tool; this may have had an impact on the information generated through the qualitative analysis and on the ability to cross-check through visual analysis the accuracy of the information included in the description of the listings.
- Given the impossibility to determine with certainty the nature of a vendor (scammer, law enforcement or real vendor), the results are likely to include listings that do not correspond to real vendors.
- Information on vendor location is based on the analysis of the (self-reported) "Ship from" field of each listing, complemented by the analysis of additional information obtained from product descriptions across cryptomarkets. However, information on the locations of buyers is exclusively based on vendors' stated willingness to ship to certain locations. When vendors are willing to ship worldwide, the data available does not allow the identification of the specific destination.

II.

How dark web markets function to facilitate illegal trade

This chapter introduces the dark web and describes two of its main types of markets: cryptomarkets and vendor shops. It also provides an overview of the mechanics associated with conducting business on the dark web: from finding the right marketplace to making a payment and receiving the purchased good. The purpose of this chapter is to provide the reader with a basic understanding of how the dark web can be used to conduct illicit trade in goods and service before presenting, in the following chapters, findings specifically related to arms trafficking.

What is the dark web?

The Internet can be conceptually broken down into three layers. The first layer is the open, freely accessible and searchable Internet, which we call the "clear web". Users typically use search engines (e.g., Google, Yahoo) to find indexed websites and content they want to visit and consume. Users typically interact with the clear web when surfing the web on computers or mobile devices.

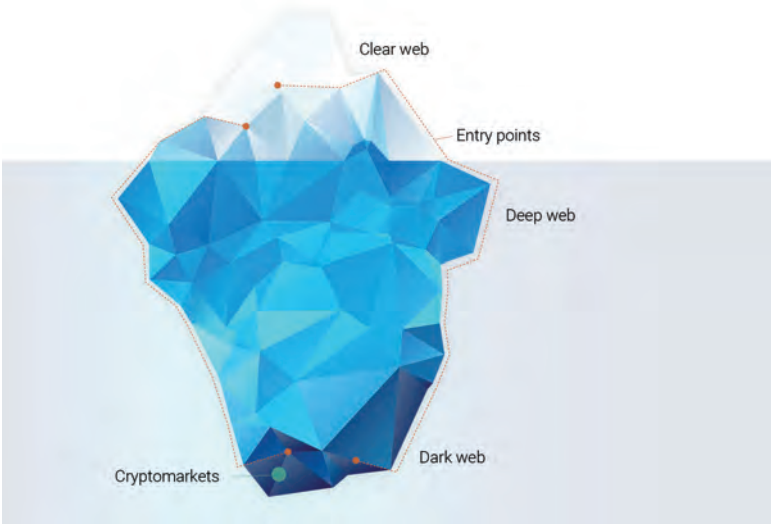
The second layer is the "deep web", containing all the unsearchable parts of the Internet (i.e., unindexed by search engines) and local intranets (e.g., business and home local area networks). The layer hosts web content that often requires

membership logins, such as for online banking services, medical records, membership-only databases (e.g., academic databases) and company intranets. Visibility of, and access to, the content of the deep web is restricted to users with special permissions and privileges.

The "dark web" is the unindexed, unsearchable portion of the deep web that requires specific software packages to navigate. Such software packages (e.g., Tor and I2P) enable access to the dark web while concealing the user's identity and online activity from surveillance and traffic analysis. Accessing and browsing the dark web is not illegal per se as the illegality is focused more on its use.

A common way of illustrating the nature of the web is through the visual representation below (see figure 1).

Figure 1. **The location of clear, deep and dark webs, and cryptomarkets**



Source: Persi Paoli et al. (2017, p.11)

Types of marketplaces on the dark web

Illegal trading on the dark web is enabled by technologies that allow buyers and sellers to interact and transact with near anonymity.[1] Dark web markets enable payment with cryptocurrencies (e.g., Bitcoin, Litecoin or Monero) so transactions are obfuscated and difficult to trace. The combination of anonymizing technology and using cryptocurrencies for payment obscures the link between real-world identities and the personas adopted on dark web marketplaces. These two technologies enable the trade of illegal goods and services, effectively in plain sight of law enforcement.

There are, at present, two principal types of marketplaces found on the dark web:

1. Cryptomarkets
2. Vendor shops, also known as "single-vendor markets"

In the following sections, the functions of both types of dark web markets are described, as well as how they enable the trade in illegal goods and services, with a focus on firearms-related selling.

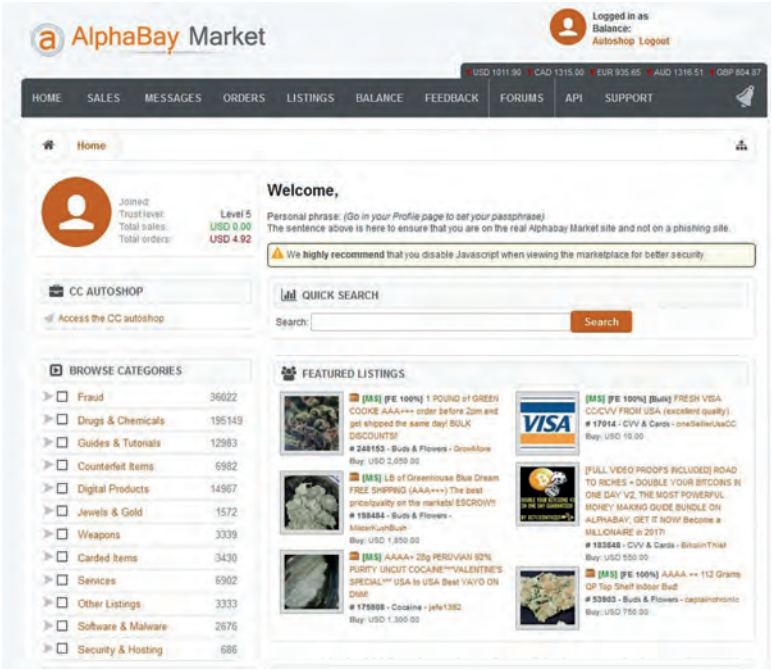
Cryptomarkets

Cryptomarkets look similar to legal online marketplaces like eBay or Amazon. Customers typically must set up accounts to view the marketplace and access the homepage once logged in (see figure 2). Marketplaces have a set of pre-defined categories into which sellers, known as "vendors", can categorize their listings to allow customers to quickly locate the type of product or service they are looking for. Although not all cryptomarkets sell firearms (see chapter III), the markets that stock weapons often provide a unique category, such as that used by Alphabay and shown in figure 2 below. Customers can also use a search facility to identify relevant listings.

[1] Barratt et al. (2017).

The marketplace homepage provides links to information and services supported by the marketplace. These typically include account information, a messaging system enabling direct communications between cryptomarket users and a discussion forum for open discussion of issues concerning the marketplace community. Sections typically include guides for vendors and customers on using the marketplace; discussion connected to the products typically sold on cryptomarkets (e.g., drugs, fraud-related items and weapons); discussion connected to minimizing the risk of detection by law enforcement agencies; and a "scam reports" section, where buyers and vendors can report problems with transactions and enlist marketplace administrators to intervene and adjudicate disputes.

Figure 2. **Screenshot of the homepage for the Alphabay cryptomarket**



Source: Persi Paoli et al. (2017, p.12)

Users of dark web markets benefit from encryption by virtue of the location of these markets on the dark web, but anonymity may still be compromised when direct communications between buyers and vendors involves incriminating information, such as names and addresses of customers, with external hacks and marketplace closures by law enforcement resulting in de-anonymization.

Cryptomarkets generally have sections on their sites listing rules for vendors and buyers related to transactions and associated security measures.

Vendor shops

Vendor shops, by comparison, generally have a much simpler visual interface, as with many legal online shops set up by individuals or businesses to sell their own products and services. Because vendor shops host sole-trading vendors that specialize in particular products, these markets have fewer listings when compared with cryptomarkets.

While some listings of vendor shops are categorized similarly as those of cryptomarkets, other vendor shops list all their products on their homepages. Vendor shops have a limited functionality compared to cryptomarkets, appropriate to their business structure in selling directly to customers, but links will typically be available for customers to register and log in, for seller contact information and sometimes for frequently asked questions.

Buying and selling on dark web markets

Finding dark web markets

As already described, web pages located on the dark web are not indexed by clear web search engines like Google, and so—by design—cannot be identified this way. To access a dark web market, therefore, customers must already know of the existence of the market and have its URL (Uniform Resource

Locator).[2] Unlike clear web URLs that use an intuitive format (e.g., www.businessname.com), dark web market URLs cannot be guessed, are not intuitive and are not designed to be memorable. Users must therefore first locate the market's URL on the clear web, and then copy and paste the link into a suitable dark web browser. For example, one such aggregator of dark web markets is found at Aggregarma.com.[3]

For potential buyers, finding cryptomarkets is easier, in relative terms, than identifying a reliable and trusted vendor to purchase goods from. While cryptomarkets have proliferated after the shutdown of Silk Road 1, customer and vendor trust has been challenged as a result of fraud by marketplace owners as well as by law enforcement operations.[4]

Payment on dark web markets

There are certain similarities between purchasing goods and services on the clear web and how transactions occur on dark web markets. Buyers, after identifying a product they wish to purchase, click the familiar "Buy now" button on the product listing page. Like purchases on legal clear web shops, buyers must register with the marketplace and have sufficient funds to complete the purchase.

A salient difference between clear and dark web markets is the form of payment. On dark web markets, payments are made with cryptocurrencies. The first, best known and still most commonly used is Bitcoin, although increasingly popular alternatives ("altcoins") include Monero, Ethereum, Ripple

---

[2] Barratt & Aldridge (2016).

[3] The name of this website has been changed as part of efforts to ensure responsible dissemination of information. In his Agenda for Disarmament, the Secretary-General made the commitment to encourage responsible innovation of science and technology, as well as the responsible dissemination of knowledge, in conformity with the principles and objectives of the United Nations.

[4] Zetter (2013); Aldridge & Décary-Hétu (2016a).

and Litecoin. Transactions made using cryptocurrencies are not necessarily linked to the real-world identities of buyers and sellers, and this makes it difficult for law enforcement to trace illegal transactions. But obtaining cryptocurrencies presents a number of challenges for buyers, with much dark net community discussion suggesting that working out how to buy Bitcoin was the trickiest part of dark web purchasing. In addition, buying cryptocurrencies to make illicit purchases, or selling them to "cash out" into local currencies, creates additional security risks for users.

Having obtained sufficient funds in a cryptocurrency accepted on a cryptomarket, the buyer initiates a transaction by clicking "Buy now". However, payment is not immediately received by the vendor, but instead held in deposit by the marketplace or by a third actor, known as payment escrow. Once the order is received and the buyer is satisfied, the buyer returns to the marketplace to "finalize" the order, at which point payment is released from escrow and transferred to the vendor's account.

Shipping and receiving goods

Because many products sold on dark web markets are digital products (e.g., stolen credit card or identity information, e-book guides, or 3D-printing files) sending and receiving purchases can be fairly straightforward. Without the need for orders to be shipped through postal systems, the risks associated with orders being intercepted by handlers, including post office employees and customs officials at borders, is reduced. Buyers receive their digital product delivery directly in the marketplace upon payment.

For physical products, such as drugs, ammunition and weapons, vendors must rely on postal services to ship orders to customers. Dark web markets provide vendors with an opportunity to transact with customers across a wider

geographical reach than is possible with conventional illegal markets, and the postal system is an enabler in this process.[5]

Research suggests that cryptomarket users identify these "offline" activities of dark web transactions as the primary source of risk of detection and apprehension by law enforcement.[6] For vendors, these activities include sourcing packaging materials and making drop-offs into postal systems. For buyers, receiving deliveries is identified as a risky aspect of cryptomarket purchasing.

A range of strategies are shared on cryptomarket discussion forums and used by vendors to reduce the risk that postal shipments will be intercepted and traced back to them.[7]

Using marketplace forums, vendors share advice obtained from government-published criteria used by law enforcement agencies for profiling suspect packages. Stealth techniques for drug dealers are widely shared online,[8] despite some clear web forums prohibiting the discussion of techniques.[9]

Researchers found that customers face heightened risks of detection and arrest while receiving their deliveries.[10] Vendors often advise customers on certain names to use for delivery in order to increase the chances for parcels to escape detection by the authorities, including undercover law enforcement agencies. Vendors sometimes alerted customers to the risks associated with shipment tracking[11] beyond those from signing for deliveries, given the ability of law enforcement agencies to

---

[5] Aldridge & Décary-Hétu (2014); Christin (2013); Mounteney et al. (2016).
[6] Aldridge & Askew (2017).
[7] Ibid.
[8] Vendors described methods for removing their fingerprints from packages, thereby limiting evidential ties to them in the event of parcel interception. For example, "stealth" packaging strategies by drug vendors were aimed at reducing suspect visual cues of package contents.
[9] The subreddit rules for r/DarkNetMarkets instruct users to not "post stealth details".
[10] Aldridge & Askew (2017).
[11] Tzanetakis et al. (2015).

conduct large-scale international investigations and audit postal records to track vendors.

Dead drops

Postal or parcel services are still seen as "the major bottleneck in the system".[12] A recent development known as "dead drops", allowing dark web market sellers to avoid postal systems, has been described in recent research in connection to drug selling on cryptomarkets:[13]

> The dead drop delivery model involves a "dropman" hiding a consignment of pre-packaged and labelled drug deals, purchased from a vendor offering the service, in a number of suitably discreet offline locations … Customers making a purchase in this way … pick up the deal, with funds released to the vendor—and commission to the dropman—from escrow once pick-up is confirmed. At least one cryptomarket currently allows vendors this delivery option, but it is unknown how widespread take-up is at present. The risk that a dropman may be undercover law enforcement is possible, but a marketplace offering this delivery option contends that the risk is small.

The extent to which dead drops are used for delivery by cryptomarket vendors is not yet known, but this particular innovation should be further monitored in connection with firearm selling on dark web markets, where the challenges and risks of the postal delivery for firearms and bulky weapons seem greater than small, lightweight and stealthy drug deliveries via the post.

---

[12] Mounteney et al. (2016, 7).
[13] Aldridge & Askew (2017).

III.

Dark web–enabled arms trafficking: Estimating the size and scope of the market

This chapter presents the study findings related to the size and the scope of the arms trade via the dark web. This is based on analysis of the supply side of the market, which sheds light on the volume and range of products offered for sale. Each section includes a description of the specific methodology used to investigate each aspect as well as a presentation and discussion of the findings. It is important to note that the findings presented in this chapter are subject to the caveats and limitations illustrated in chapter I.

Identifying dark web marketplaces trading firearms, ammunition and explosives

The first resource considered for identifying relevant hidden markets was Aggregarma. The list provided by Aggregarma distinguishes cryptomarkets from sole-trading vendor shops.[1] At

[1] The dark web market listing provided by Aggregarma, while highly regarded and widely used by customers and researchers to identify marketplace URLs, excludes markets that do not specifically request to be included, as well as markets whose owners make the request but are turned down because they do not meet specific requirements. The project team was therefore unable to collect data from any cryptomarkets not included in the list. The impact of being unable to access—or even to

the time of data collection (September 2016), no vendor shops listed on Aggregarma sold arms-related products.

For cryptomarkets, the project team identified all available marketplaces using the Aggregarma markets list in September 2016 and attempted to gain access to each market using the following strategies to identify those relevant for the purpose of this project:

- **Marketplace-dedicated "arms"-related category**. Product categories were inspected to identify cryptomarkets with dedicated arms-related categories available for vendors to classify the items they listed for sale.
- **Keyword search for arms-related listings**. This strategy allowed the team to identify arms-related listings even in markets without a dedicated category.
- **Marketplace restrictions**. Cryptomarkets typically have rules for marketplace conduct, with some restricting particular products and services. These rules were examined for each marketplace to determine if arms were explicitly prohibited or allowed.

Table 3.1 below shows the findings from the scan of the 24 English/French-language[2] cryptomarkets operating during our assessment period.[3]

know of the existence of—cryptomarkets excluded from the Aggregarma list is considered minimal, as most excluded markets were likely to be very small and/or have limited functionality.

[2] Four cryptomarkets were Russian, and we were unable to secure a Russian-language speaker to assist us in examining these markets.

[3] Two markets had closed in the interim.

Table 3.1 **Cryptomarkets listed on Aggregarma: numbers classified as selling arms**

	n	% of 18
Cryptomarkets listed on Aggregarma	24	
Markets we were able to access and inspect	18	
Markets allowing (or not explicitly prohibiting) firearms sales	15	83%
Markets with dedicated categories for firearms	9	50%
Markets where we identified firearms listings through searching	8	44%

Note: Data refers to the list accessed on 19 September 2016.

Discussion

The majority of cryptomarkets assessed had rules in place consistent with allowing arms sales. This suggests that most cryptomarkets present a potential channel for access to firearms. However, the fact that only half of the markets provided vendors with categories to use when placing their listings suggests that firearms sales were not sufficiently common to warrant a dedicated category on the marketplace homepage. Vendors may therefore have resorted to "miscellaneous" or "other" product categories to place such listings. Conversely, three markets had weapons categories, but our search identified no firearms-related listings within these categories.

Together, these findings suggest that even cryptomarkets facilitating firearms sales may attract relatively few vendors listing such items for sale in comparison to those selling more popular products and services on these marketplaces (i.e., drugs and fraud-related items).

Our keyword searches identified that just under half of the markets had active arms-related listings. Nevertheless, it should be noted that the assessment is not based on continuous monitoring of marketplaces, but on a single snapshot. Therefore, it is not possible to exclude the possibility that more active firearms listings may be shown in the future, if a longer time frame is considered.

Vendor shops

To identify vendor shops specializing in firearms, the project team solicited the help of a dark web expert (who wished to remain anonymous) to analyse dark web discussion forums and provide the project team with a list of vendor shops specializing in weapons. In addition, the project team supplemented this list with additional reading on relevant subreddit discussions in the Reddit online community.

Using these methods, the project team collated a list of 15 vendor shops thought to specialize in arms-related products. The team was able to access 13 of the shops (more information on these is provided below) and, in doing so, identified eight then listing arms-related products.

Discussion

The inaccessibility of certain vendor shops for which URLs were available suggests a number of possibilities. First, niche specialization may hamper vendor shop longevity. It may be difficult for vendors specializing in arms-related products to create sufficiently profitable enterprises that enable longevity; in comparison, for example, specialist drug vendors, whose reputations are strengthened through cross-market selling on dark web markets, are likely to generate a greater volume of sales. Second, the non-accessible markets may struggle with the uptime of their servers, for a range of technical reasons. Finally, they may simply have ceased trading.

This non-accessibility provides for only a minimal understanding of the role that vendor shops have in hidden market arms sales.

Estimating the size and scope of the dark web–enabled arms trade

To estimate the size and scope of the dark web–enabled arms trade, data was collected directly from cryptomarkets in

the form of the "digital traces" left in connection to market transactions.[4]

The collection of primary data through a specifically designed crawler and scraper was conducted once, in late September 2016. As this implies, the project team had only visibility of the products available for sale at the time the crawling was conducted. The data should therefore be considered as a snapshot rather than the result of a continuous monitoring. This may impact the analysis performed on the size, scope and overall value of the market.

Data collection took place between 19 and 25 September 2016. The resulting dataset spanned 12 cryptomarkets and generated 167,693 listings, of which 811 were identified as relevant for the purpose of this study.

Table 3.2 lists the specifically named cryptomarkets from which data was collected and, for each market, the total number of listings, the number of listings that were arms-related and the proportion expressed as a rate per 1,000 listings.[5]

Table 3.2 **Cryptomarkets selling arms-related listings from which data was collected**

	Total number of listings	Number of arms-related listings	Rate (per 1,000 listings)
Alphabay	36,906	414	11.2
Clowdsito[a]	64,625	173	2.7
Valhalla (Silkkitie)	19,939	114	5.7

[4] Décary-Hétu & Aldridge (2015).

[5] It should be noted that since the date of the crawling, many of the listed cryptomarkets are no longer operating. Some have been taken down by law enforcement agencies (e.g., Alphabay, Hansa-market and Valhalla), others have closed operations. However, it should be noted that this is quite a common phenomenon and other markets have emerged since then. At the time of writing this Occasional Paper (October 2018), the open source portal Aggregarma.com reports 26 live markets and vendor shops.

	Total number of listings	Number of arms-related listings	Rate (per 1,000 listings)
Hansa-market	22,151	49	2.2
Paradizorm[a]	11,932	29	2.4
Serpintonarm[a]	7,377	14	1.9
Toxmarche[a]	1,312	8	6.1
Barterepon[a]	1,596	4	2.5
Nervogormar[a]	697	3	4.3
Polacrolis[a]	253	2	7.9
Ockatrad[a]	277	1	3.6
Lodisocar[a]	628	0	0.0
Total	**167,693**	**811**	**4.8**

[a] The name of this website has been changed as part of efforts to ensure responsible dissemination of information. In his Agenda for Disarmament, the Secretary-General made the commitment to encourage responsible innovation of science and technology, as well as the responsible dissemination of knowledge, in conformity with the principles and objectives of the United Nations.

The dataset of 811 listings included listings of the same product by the same vendor across a number of cryptomarkets. This is not uncommon and while these listings might be understood as "duplicate" listings, it is critical that they are not deleted, for a number of reasons. First, multiple listings for the same product across markets may be variously tailored by vendors for purposes specific to that marketplace. For example, the same listing on different marketplaces may provide different available shipping destinations. This was particularly helpful in identifying shipping routes (see chapter V). The second, and perhaps more important, reason relates to the meaning attached to a listing. A listing should be understood only as an advertisement placed for sale and should not be read to imply anything about the available supply of products. A vendor may have multiple listings across marketplaces for the one and only gun that vendor has available to sell. Alternatively, a vendor may have only one listing on one marketplace but hold 20

guns in stock. Hence listings do not necessarily correspond in a meaningful way to available products.

Finally, cryptomarkets generate digital traces of transactions connected to a particular listing. A vendor holding ostensibly duplicate listings on different marketplaces will generate sales connected to those separate listings. Removing duplicate listings would therefore remove the transaction data contained on these listings, compromising the utility of our data for understanding the size of the cryptomarket trade.

High-level product analysis

For the purpose of this study, the 811 listings were manually coded into the following categories:

- Firearms
- Ammunition
- Parts and components (e.g., slides, frames, barrels)
- Accessories (e.g., scopes)
- Explosives (e.g., grenades)
- Digital products (e.g., "do-it-yourself" guides for home explosives, 3D models of firearms or their parts)
- Other weapons (e.g., modified stun guns/tasers, knives, batons)

Table 3.3 lists the frequency of listings placed for sale across the scraped cryptomarkets.

Table 3.3 **Frequency of arms-related product categories**

Product	n	%	n	%
Firearms	339	42		
Digital products	222	27		
Other weapons	178	22		
Explosives	6	1		
	sold alone		+ in combination	
Ammunition	54	7	98	12
Accessories	8	1	66	8
Parts and components	4	<1	8	1
Total	**811**	**100**		

Discussion

Firearms listings (42 per cent) were most common, followed by digital products (27 per cent) and other, non-firearm weapons (22 per cent). When vendors sold ammunition separately, this comprised only 7 per cent of listings. However, when vendors sold ammunition in combination with firearms, the number of listings including ammunition nearly doubled (12 per cent). Only eight listings offered accessories only, but this figure jumped to 66 (8 per cent) when sold in combination with other products. Parts and components were rarely sold, either separately (four listings) or in combination with other products (eight listings, or 1 per cent).

Several observations can be made from the distribution of weapons listings described above. First, ammunition and accessories are listed alone, but also as part of a "package deal" with firearms. This suggests that vendors have access to firearms as well as access to ammunition and/or accessories. Vendors might be reselling personal firearms and related products already in their possession or they might have a network of contacts (either as part of the dark net community or offline) as part of their supply chain. Finally, offering package deals could

be a simple marketing choice by vendors to increase the appeal of their products.

With respect to parts and components, despite the existence of cases where buyers were assembling their firearms by purchasing individual parts from different vendors at different times,[6] their market share appears to be small. This might be a result of this particular crawl (i.e., a crawl conducted at a different moment in time may have produced a very different result) or it could imply that, despite some exceptions, the "build-your-own" approach represents a very niche part of the market, with the wide majority of buyers interested in purchasing fully assembled and functioning firearms.

Firearm types

The project team categorized each firearms listing on the basis of three criteria:

- **Firearm type**. This referred to a simple categorization based on three different weapons types: pistols (excluding full-automatic), submachine guns (and full-automatic handguns) and rifles.
- **Live, replica, deactivated or converted**. This was used to identify the status of the firearm and included the distinction between live firearms and replicas/alarm/signalling guns, as well as deactivated or converted firearms.
- **New or used**. This referred to the condition of the firearm, where specified.

Table 3.4 provides descriptive detail on the types of firearms listed for sale across the 12 cryptomarkets.

[6] RAND expert workshop, 20-21 March 2017.

Table 3.4 **Firearms types listed for sale, by replica and new/used**

	Pistols (n = 284)	Submachine guns (n = 22)	Rifles (n = 33)	Total (N = 339)
Total	84%	6%	10%	100%
Live firearms	82%	41%	91%	81%
Replicas	17%	59%	9%	19%
New	19%	9%	12%	18%
Used	27%	14%	21%	25%
Not specified	54%	77%	67%	57%

Discussion

Pistols were the most commonly listed firearm (84 per cent), followed by rifles (10 per cent) and submachine guns (6 per cent). Replicas accounted for a minority of listings placed by vendors for pistols (17 per cent) and rifles (9 per cent); nearly 6 in 10 (59 per cent) submachine gun listings, in contrast, were replicas. Moreover, the coding scheme was designed to identify, in addition to live guns and replicas, converted replicas, deactivated firearms and reactivated firearms. No vendors were found describing their product listings in ways consistent with these classifications. This might be due to the fact that these kinds of firearms could simply be sold as "used" without necessarily providing information to this level of detail.

The condition of the majority (57 per cent) of listings across all the three firearms types was unspecified. For the remaining 43 per cent, used firearms were more frequent than new ones, accounting, respectively, for 25 per cent and 18 per cent of the total number of firearms listed. Though the project team did not analyse the images associated with each listing, this could have provided additional information related to the condition and minimized the number of "unspecified" cases.

Regarding the types of firearms being sold, pistols represent the clear majority. Consulted law enforcement

officials[7] highlighted that that could be related to the relative ease of concealing handguns in parcels (even if disassembled) compared to achieving the same result with bigger firearms. Another reason might be related to the characteristic of the market whereby pistols are more common than submachine guns and long rifles. Therefore, they would be expected to be more dominant in terms of both supply and demand.

Finally, a particularly interesting point from an arms control perspective relates to markings. The serial numbers, markings and manufacturer engravings on small arms, light weapons and their ammunition allow for their provenance and heritage to be traced. The tracing of weapons based on unique serial numbers is only possible with the cooperation of States and manufacturers that maintain databases of registered weapons. Changes in ownership are logged in documentary records. Weapons with a defaced or removed serial number cannot be identified uniquely. Knowing the ownership history of a weapon allows it to be traced for an accurate determination of when it diverted into an illicit sphere.

Of all firearms listings (n = 339), only a small fraction commented on the markings of weapons:

- It was common for serial numbers to be removed (9)
- Quoting the verbatim serial was rare (2)
- One vendor stated that they would remove markings on weapons at the buyer's request

As already described earlier in this report, the project team did not conduct a visual analysis of the images associated with each listing due to technical limitations of the tool used to do the crawling. Therefore, the only source of information for markings was the text in the description, but it is likely that more information on markings could have been obtained from the images.

[7] RAND Europe Expert Workshop, 20-21 March 2017.

Makes and models of firearms

For the purpose of this study, a second layer of analysis was conducted to understand what makes and models are most commonly offered on cryptomarkets. Of the 339 firearms listings, make and model information was specified for 300. Instances where only makes were specified accounted for about 10 per cent of the total, while in fewer circumstances, even if the model was specified, the information provided was sufficient to determine the make. This was the case, for example, with some models that have been produced by different manufacturers over the years. Without information on the year of manufacture, and without access to the image which could provide visual identification of the manufacturer, determining the make was in some cases not possible. A detailed list of the number of firearms offered by make is provided in appendix A.

For only those makes with more than 10 listings (excluding the 39 listings in which the make was not specified), table 3.5 provides the models associated with each make.

Table 3.5 **Firearm models (n) for firearm makes listings > 10**

Make	Model
Glock	19 (17); 17 (14); 26 (8); 19Gen4 (4); 22 (2); 23 (2); 37 (2); 42 (2); 43 (2); Unspecified (2); 18 (1); 21 (1); 23 Gen4 (1); 27 (1); 42Gen4 (1)
Colt	1908 (5); 1911 (5); Government M1911 (3); Officer (3); SAA 3rd Gen (3); 1903 (1); 3rd Gen Storekeeper (1); AR-15 (1); Buntline Scount 5905 (1); Camp Perry (1); King Cobra 6 (1); MKIV (1); MKIV Gold Cup (1); SAA 125th Ann. (1); SAA 38-40 (1); Unspecified (1)
Sig Sauer	M400 (1); P210-6 (1); P210 Legend (1); P210-1 (2); P210-6 (1); P226 (3); P229 Legion (1); P229 Scorpion (4); P320 Compact (1); P938 Nitron micro (2); Pro 2022 (2)
Beretta	70 (1); 92A1 FDE (1); 92FS (3); M9 (2); M9A1 92FS (6); PX4 (1); PX4 Storm (2); Unspecified (2)
Ekol-Voltran	Aras Magnum Hp (1); Arda Starter-K9 (1); ASI (2); Dicle 8000 (2); Firat Compact 92 (2); Major (1); P29 (3); Sava Magnum (1); Special 99 V85 (2); Viper (2); Viper 2.5 (2); Viper 6 (1)

Make	Model
Ruger	22/45 Mark III (1); Bisley Vaquero (1); Black Hawk (2); LCP Mod 3725(1); Mini 14 (1); MK II (1); P85 (1); P89 (3); Red Hawk (1); Single Six (1); SP-101 (1); Speed 6 (1); SR40 (1); Unspecified (2)
Smith & Wesson	338 FPS (1); Body Guard (2); M&P Shield (2); M&P22 (1); Mod 3000 (1); Mod 4006 (1); Model 57 (4); SD9VE (1)

Note: This table reports the models listed as for sale for each make with ten or more listings. The number in brackets shows the frequency of each specific model. The models are reported in this table in the same way as they were included in the title and/or description of the listings. No further analysis has been done to rectify inaccuracies or combine variations of the same model.

The table illustrates the wide range of the most common makes and models available for sale on the analysed cryptomarkets at the time of the crawling. As previously stated, these results are related to one crawl in September 2016 and were not generated through a continuous monitoring. Therefore, they should be considered as a snapshot at one given moment in time. Nevertheless, as further described in the section entitled "Impact on the illicit firearms market" in chapter VI, the evidence and the expert opinions gathered through this study seem to suggest not only that the range of products available on cryptomarkets is significantly wider than what would be available in any single location at the street level, but also that the quality of the products seems higher.

Digital products

Particularly relevant for the purpose of this study is the availability of, and trade in, digital products. This is due to the fact that with digital products, the entire transaction, including the delivery, happens in the virtual space, with little to no "real-world" involvement. When exploring digital products, the project team focused on two categories in particular: e-books/manuals providing a wide range of instructions (on topics from home-made explosives, to manufacturing and/or modifications of firearms, parts, components and ammunition); and 3D models

to support additive manufacturing (i.e., 3D printing) of firearms and/or their parts.

The digital products category was the second most common, with 222 listings (27 per cent of the total). The vast majority of these (n = 208) were e-books providing instructions for the manufacture of explosives or firearms. Eleven listings were digital files for 3D printing of firearms. Five of these listings contained a file for printing only one firearm, with the remaining six providing files for printing of a larger number of different firearm models and components. The box below contains an extract from one of these listings. The remaining three listings we classified as digital promises, selling information on where to buy firearms.

Sample e-book listing (the first 10 of 35 named parts and components)

This pack is a collection of the newest FOSSCAD CAD files:

Rifles/AK-47_Stock-Shanrilivan
Rifles/AKM_75_Round_Drum_Magazine_Yee_v0.2-nils
Rifles/AR-10_Nephilim_Reinforced_Lower_Receiver_v1.1-WarFairy
Rifles/AR-15_Bumpfire_Stock_v2-Disruptive_Solutions
Rifles/AR-15_Carbine_Handguards-WarFairy
Rifles/AR-15_CMA_Stock_v1.1.1-shadowfall
Rifles/AR-15_FOSSCAD_Israel_75rd_Drum_Magazine-nils
Rifles/AR-15_Hanuman_Bullpup_v1.0-WarFairy
Rifles/AR-15_Minimalist_Stock-WarFairy
Rifles/AR-15_Orion_PDW_Stock-WarFairy

Discussion

As mentioned earlier in this section, the trade in arms-related digital products is particularly relevant due to the additional challenges it poses. While guides and manuals on how to make bombs at home were illegally circulating on the web well before the establishment of cryptomarkets, the level of accessibility provided by these platforms represents reason

for high concern among policymakers and practitioners.[8] In addition to explosives, these guides can provide tutorials for a wide range of illegal actions, ranging from the conversion of replica/alarm guns into live weapons, to the full manufacture of home-made guns.

The availability of 3D models for additive manufacturing of parts, components or full firearms has been recognized by the international community as a major source of concern.[9] With the improvement of commercially available 3D printers (e.g., increased accuracy, better quality of materials used for printing), the possibility of producing at home viable substitute parts to replace, for example, those bearing identification markings on a firearm may hamper the ability of tracing illegal firearms back to their last legal owner, identifying the point of diversion. That being said, the use of home-made parts through additive manufacturing depends on a range of other factors, including the accuracy of the 3D model, the quality of the printer, the quality of the material used for the print and, finally, the skills of the person who has to do the final assembly and replacement of parts and components; the margins for technical or human errors remain significant even with the improvements in the available technology.[10] Nevertheless, the implications deriving from the easy availability of these files should not be underestimated.[11]

[8] Ibid.
[9] United Nations General Assembly (2014).
[10] King & McDonald (2015).
[11] RAND Europe expert workshop, 20-21 March 2017.

IV.

Dark web–enabled arms trafficking: Estimating the value of the market

This chapter focuses on the financial element of the dark web–enabled arms trade, with specific focus on both prices and transactions. Like chapter III, each section includes a description of the specific methodology used to investigate each aspect, the presentation of the findings and a discussion of their meaning. It is important to note that the findings presented in this chapter are subject to the caveats and limitations illustrated in chapter I.

Price of arms-related products available for sale

A price analysis was conducted on the entire dataset of 811 listings both to identify the market value of certain type of weapons and as a first step towards the estimation of the gross revenue generated by arms trade on the dark web. A careful analysis of each priced listing was necessary to eliminate possible intentional distortions. Cryptomarket vendors sometimes increase the price of a listing by an order of magnitude—temporarily—to discourage customers from making a purchase: the vendor may, for example, be out of stock or unavailable to process transactions.

All 811 listing descriptions were reviewed for explicit reference to holding prices and none was found. Only one listing had an unfeasibly high price (US$ 99,999) and it was

removed from any price analyses. Table 4.1 illustrates for each product category the number of listings, the mean, minimum and maximum price, and the standard deviation. For firearms, both live and replicas, the project team captured the prices for both those products sold alone and those sold in combination with other products (e.g., ammunition, spare parts and/or accessories).

Table 4.1 **Price per unit by product type listed for sale**

	n	Mean	Min	Max	Standard deviation
Live firearms					
Sold alone	178	$1,187	$179	$10,264	1,133.97
+ bundled with other product(s)[a]	95	$1,457	$225	$13,500	1,636.57
Replica firearms					
Sold alone	58	$132	$35	$468	70.83
+ bundled with other product(s)[a]	7	$551	$45	$886	318.50
Ammunition	51	$84	$9	$555	98.38
Explosives	6	$210	$100	$210	158.04
Other weapons	175	$68	$3	$650	85.70
Digital products	222	$3	<$1	$90	6.62

Note: Table excludes listings categorized exclusively as: parts and components (4) and accessories (8). Six listings without a price were excluded from the analysis ("other weapons" = 3; "ammunition" = 3).

[a] Some firearms listings were sold bundled with other products (ammunition, parts and components, accessories). The elements of the listing were not separately priced, and so prices here are for the bundle of products combined.

A more detailed look into the price structure of live firearms is provided in Table 4.2 where prices are provided for each category of firearm both when sold alone and when sold in combination with other items. For both of these sub-categories, prices are further broken down based on the stated condition of the firearm.

Table 4.2 **Price per unit of live firearms listed for sale**

	n	Mean	Min	Max	Standard deviation
Pistols sold alone					
New	24	$705	$245	$2,728	476.73
Used	45	$1,079	$218	$2,195	545.8
Unspecified	78	$865	$179	$2,200	530.59
Pistols sold with[a]					
New	24	$1,118	$324	$4,000	911.41
Used	30	$1,427	$225	$4,950	1,159.42
Unspecified	32	$1,115	$300	$3,400	803.42
Sub-machine guns sold alone					
New	0	–	–	–	–
Used	1	$2,495	$2,495	$2,495	–
Unspecified	4	$5,006	$3,058	$10,264	3,510.5
Sub-machine guns sold with[a]					
New	0	–	–	–	–
Used	2	$2,400	$700	$4,100	2,404.16
Unspecified	2	$3,775	$3,700	$3,850	106.07
Rifles sold alone					
New	3	$3,749	$2,000	$7,046	2,857.32
Used	4	$771	$329	$1,250	394.97
Unspecified	18	$2,272	$1,000	$4,000	1,019.69
Rifles sold with[a]					
New	1	$13,500	$13,500	$13,500	–
Used	3	$1,966	$1,200	$2,500	680.56
Unspecified	1	$1,047	$1,047	$1,047	–

[a] Some firearms listings were sold bundled with other products (ammunition, parts and components, accessories). The elements of the listing were not separately priced, and so prices here are for the bundle of products combined.

The final level of price analysis was conducted for the most common makes of live pistols (i.e., those with more than 10 listings) to provide a more accurate reference point for price comparisons between the dark web-based market value and either the offline (black) market value or the manufacturer's suggested retail price (MSRP)/recommended retail price (RRP).

Table 4.3 illustrates the price range of the six most common live pistol makes, both when sold alone and when sold in combination with other products.

Table 4.3 **Price per unit of live pistols listed for sale for the most common makes**

	n	Mean	Min	Max	Standard deviation
Glock	28	$1,189	$245	$2,200	623.62
+ bundled with other product(s)[a]	30	$1,557	$370	$4,017	1,033.37
Colt	21	$853	$424	$2,011	439.29
+ bundled with other product(s)[a]	8	$1,063	$950	$1,852	318.87
Sig Sauer	8	$705	$390	$1,500	333.48
+ bundled with other product(s)[a]	9	$761	$500	$1,500	305.96
Ruger	16	$752	$314	$1,700	471.33
+ bundled with other product(s)[a]	2	$1,090	$399	$1,780	976.51
Beretta	7	$1,027	$419	$2,000	624.76
+ bundled with other product(s)[a]	11	$615	$299	$2,000	599.16
Smith & Wesson	9	$799	$179	$1,850	469.97
+ bundled with other product(s)[a]	2	$900	$800	$1,000	141.42

[a] Some firearms listings were sold bundled with other products (ammunition, parts and components, accessories). The elements of the listing were not separately priced, and so prices here are for the bundle of products combined.

Discussion

Table 4.1 provides a general overview of the price range for different product types offered on the cryptomarkets analysed by the project team at the time of the crawling. While a comparison across different categories would not be

particularly meaningful, some key observations can be derived for each category. For firearms, the range of prices observed is due to the fact that Table 4.1 combines all firearms types and conditions. Nevertheless, it is relevant to note that, in some circumstances, replica firearms are offered at a higher price than live firearms. This is particularly interesting as, in general, replicas are significantly cheaper than equivalent live firearms. For instance, in the United States, replica guns tend to cost about one tenth of the price of an equivalent/comparable live gun (e.g., a blank-firing replica 9 mm Magnum revolver costs about US$ 80,[1] compared to a live Smith & Wesson Model 66 Combat Magnum® costing US$ 850).[2]

Cryptomarkets have the effect of raising the cost of replicas, which have been advertised to cost as much as US$ 468 when sold alone. This may suggest that a premium is paid for anonymity even for replica guns that could be bought legally and for a fraction of the price through authorized dealers. This may be due to the fact that in certain national legislation, certain types and models of replica/alarm/signalling guns are regulated in the same way as live firearms, making their purchase subject to the same set of rules and authorizations.

Evidence (see table 4.2) also suggests that, when sold alone, the condition of a pistol (i.e., new or used) does not have a significant impact on the price. In fact, the mean price for used pistols is higher than the mean for the new (or condition-unspecified) ones, although the maximum price of a new pistol sold alone is roughly 20 per cent higher than the maximum price for a used one. This may suggest that, for pistols, the condition is not necessarily a highly valued parameter for determining the market price, but that other factors (e.g., make, model, package deals) might be more important. This trend does not seem to apply for rifles, where the price of new products is significantly higher than the price of used ones. No observations can be made

[1] Armory.net (2017).
[2] Smith & Wesson (2017).

on submachine guns (and full-automatic pistols) as there were no listings of new products in this category.

As mentioned above, table 4.3 can be used as a reference to determine the price difference between the dark web market value and either the offline (black) market value or the MSRP/RRP. In both cases, the prices will depend on the location of the buyer. Black market as well as retail prices are likely to vary depending on the location (e.g., an RRP for a Glock in the United States might be different from an RRP for the same gun in a European country).

For illustrative purposes only, by checking online retail prices of a few different makes and models, it is possible to determine that the maximum prices of pistols sold alone on cryptomarkets are significantly higher than the retail price. Considering mean prices instead, the difference is a lot smaller and a premium seems to apply only to certain makes. For example, the retail price for new Glocks in the United States can vary between US$ 459 and US$ 749, depending on the model.[3] On cryptomarkets, the maximum price is roughly three times higher than the maximum retail price, while the mean price is about 50 per cent higher. A similar example is provided by Beretta pistols, whose online retail price varies between US$ 349 and US$ 900 depending on the model (and excluding special editions).[4] For other makes (e.g., Smith & Wesson), the mean price appears to be more aligned with the retail price.

As stated above, these examples should be considered for illustrative purposes only, as a full and rigorous investigation of the legal market in different countries would be necessary to compare cryptomarkets' prices to different offline retail prices.

Concerning other types of products, prices for ammunition range from less than US$ 10 to over US$ 500. This discrepancy can be caused by various factors. First, as ammunition is

[3] GlockStore.com (2017).
[4] GunBroker.com (2017).

generally sold in packages, and not with individual rounds, the different listings might offer different quantities (e.g., 50 rounds of ammunition). Second, the calibre of the ammunition offered might have an impact on the price, with those calibres more difficult to procure legally, depending on national regulations, being offered at a higher price.

Finally, the digital products have the lowest price of the whole dataset of 811 listings. While this is not surprising, when combined with the fact that digital products were the second most common arms-related product offered on cryptomarkets (after pistols), their low price reinforces the observations made in the section entitled "Digital products" in chapter III around the risks deriving from the increased availability of usable 3D printing files.

Cryptomarket sales for arms-related products and services

Assessing the supply side of the market and conducting a price analysis of the products available for sale does not provide information on the real value of the arms trade on the dark web. This is because not all products and services listed by vendors generate sales. Dark web markets that fall into the vendor shop category do not provide information that can be used to estimate numbers of sales generated; therefore, the estimates presented in this study refer exclusively to the analysis of data from cryptomarkets, potentially resulting in an underestimation of the overall size and value of the trade.

Table 4.4 details the number of listings for selected product types that were "active"—that is, listings that had generated at least one transaction at the time data collection was conducted—alongside the total number of transactions and gross revenue generated, estimated on a per month basis.

For the purpose of this study, gross revenue (or turnover) connected to a particular listing or for a vendor is calculated

using listing price multiplied by our estimated measure of monthly transactions.[5]

Table 4.4 **Active listings, transactions and gross revenue by product type**

Product type	N active listings	%	Transactions (per month)	Gross revenue (per month)
Firearms (N = 339)	44	14	56	$74,733
Ammunition (N = 54)	32	59	35	$2,954
Explosives (N = 6)	3	50	2	$541
Other weapons (N = 178)	75	42	101	$3,616
Digital products (N = 222)	50	23	41	$212
Total[a]	**209**	**26**	**237**	**$83,288**

[a] Total includes categories excluded from the table: listings categorised exclusively as: parts and components (4) and accessories (8).

Given the specific focus of this study, further analysis of sales was conducted for different firearms types and conditions. Table 4.5 illustrates the results of this analysis.

[5] For each listing, the project team calculated the number of days between the date of data collection for each market and the date of the listing's oldest feedback. The number of feedbacks for each listing was then used to calculate the rate of feedbacks per day. This rate was multiplied by 30 to provide an estimate of monthly transactions.

Table 4.5 **Estimated monthly transactions and gross revenue by firearm type**

	Pistols (n = 284)	Submachine guns (n = 22)	Rifles (n = 33)	Total (N = 339)
Live guns	(52) $64,224	(1) $2,586	(3) $7,923	**(56)** **$74,733**
Replicas	– –	– –	– –	– –
New	(29) $28,527	– –	– –	**(29)** **$28,527**
Used	(9) $12,762	– –	(1) $423	**(10)** **$13,185**
Not specified	(14) $22,934	(1) $2,586	(2) $7,500	**(17)** **$33,021**
Total	**(52)** **$64,224**	**(1)** **$2,586**	**(3)** **$7,923**	**(56)** **$74,733**

Note: This table reports the models listed as for sale for each make with 10 or more listings. The number in brackets shows the frequency of each specific model. The models are reported in this table in the same way as they were included in the title and/or description of the listings. No further analysis has been done to rectify inaccuracies or combine variations of the same model.

Discussion

Overall, based on the data available, the value of arms trade on the 12 cryptomarkets analysed in this study can be estimated in the region of US$ 80,000 per month when excluding the category of "other weapons", which falls outside of the scope of this study. This figure is certainly dwarfed in comparison with recent estimates of the legal trade in small arms, which is measured in the order of billions.[6] Nevertheless, it provides a useful starting point for future investigations. While generating annual estimates would require a more continuous monitoring of the sales on cryptomarkets, the evidence suggests that the number of transactions per year could potentially be in the order

[6] The Trade Update 2016 estimated that international small arms trade by top and major exporters is worth at least $5.8 billion (Pavesi, 2016).

of hundreds for firearms and ammunition, while being more limited for explosives.

Monthly estimates of both the actual value and volume of the arms-related trade on the dark web are likely to be underestimates, for the reasons already mentioned: inability to estimate the value and volume generated by single-vendor markets; inability to crawl all cryptomarkets; and limitation of the methodology (e.g., one-off snapshot, use of feedback as proxy for transactions).

On average, 26 per cent of arms-related listings had generated at least one transaction, but there was substantial variation within product type, with ammunition listings most likely to be active (59 per cent) and firearms least likely (14 per cent). Nevertheless, firearms listings generated more estimated monthly transactions (56) than ammunition listings (35). Listings for explosives were few, and generated only two transactions per month. Gross revenues (transactions multiplied by listing price) were highest for firearms, reflecting the relatively high price for this category of product. In fact, firearms generate nearly 90 per cent of all gross revenue generated by vendors selling arms-related products.

As reflected in table 4.5, the majority of firearms sales were generated by pistols, not only in absolute terms, but also when compared to the number of listings (roughly 18 per cent of pistols listed were sold, compared to 5 per cent for submachine guns and 10 per cent for rifles). This confirms that pistols have a dominant role in firearms trade on cryptomarkets not only on the supply side, but also on the demand side. The relatively high demand for firearms compared to other weapons may also be one of the factors pushing the price up (in comparison with retail price), as discussed in the previous section.

When looking at the condition or status of the firearm, the first observation is that while listings for replicas were not uncommon, they generated no sales in the period of the measurement. It is worth noting that the review of open-source

literature suggests that converted replica guns can be obtained through cryptomarkets (see, for example, the Munich shooting where the crime weapon was a converted theatrical prop). This may suggest that these types of replicas/alarm/blank-firing guns are possibly sold already converted, even though the qualitative analysis of each title and description did not identify any listing clearly stating this type of firearm.

While, as described earlier, the condition of the firearm has only a limited impact on the price range, the firearms listings explicitly identified as "used" by vendors generated less than half of estimated monthly transactions and gross revenue compared to firearms explicitly described by vendors as "new". Within the pistols category, those specified as new by vendors generated the most sales, but listings in which new/used status was unspecified by vendors, overall, generated similar numbers of sales across firearm types.

These results could be reverted or reinforced if more information was available on those firearms where the condition was not specified in the title or description. The most immediate solution, which was not implemented for technical reasons, would be to conduct a visual analysis of the images associated with each listing.

Finally, it should be noted that transactions were conducted, even if in small numbers, also for other firearms types including submachine guns and rifles. Assuming that such transactions are real and not the result of fake feedback, this would illustrate that demand also exists for more powerful firearms and that buyers are willing to take on the risk of receiving a bigger, bulkier item (possibly delivered through multiple parcels).

V.

Dark web–enabled arms trafficking: Assessing shipping routes and techniques

This chapter focuses on the shipping and handling of firearms offered or sold on the dark web. It includes an analysis of shipping routes as well as of shipping and handling techniques based on the data gathered from the listings and from the consultation with experts. As in the previous two chapters, each section includes a description of the specific methodology used to investigate each aspect, the presentation of the findings and a discussion of their meaning. It is important to note that the findings presented in this chapter are subject to the caveats and limitations illustrated in chapter I.

The challenges of estimating shipping routes

Cryptomarket listings provide information on the countries or regions from which vendors indicate they ship, as well as countries or regions to which they are willing to ship their products. Previous research used the "ship from" data on cryptomarket listings to indicate a vendor's country of operation, but this approach has a number of limitations.[1] First, the "ship from" information that vendors place on listings is only an imperfect proxy for country of vendor operation.

[1] Décary-Hétu et al. (2016); Van Buskirk et al. (2016).

There is evidence, for example, that some Dutch cryptomarket vendors may ship drugs via intermediaries in other countries or by travelling to neighbouring countries to make the shipments themselves.[2] This strategy may be used to reduce the risk of package interception in destination countries that specifically target Dutch packages for screening due to the role of the Netherlands in drug production and its location on international drug trafficking routes.[3] In relation to firearms, the project team was not able to access any evidence supporting these types of behaviour from vendors; however, the general principles of using intermediaries or travelling to other countries could, potentially, apply to firearms as well. A second limitation of the "ship from" information on listings is that vendors do not always list a specific country and instead indicate a region or other large area (e.g., "Europe") from which they say products will be shipped. Many vendors are unwilling to provide any geographically identifying information in this connection, for example indicating that they ship from "Worldwide".

Although vendors indicate on their listings the countries to which they are willing to ship their products, cryptomarket data cannot always tell the customer location associated with a transaction. Destination countries for purchases generated in connection to a vendor listing that ships worldwide, for example, cannot therefore be determined. However, listings placed by vendors that restrict their sales only to customers in one country or region do provide an indication of destination.

Bearing these caveats in mind, the country-based analyses included in this section used this "shipping" location information on listings. This information was also aggregated at region and continent levels using a list published by the United Nations.[4] When listings indicated products would be shipped worldwide, or to multiple regions that spanned the categorization scheme,

[2] Kruithof et al. (2016).
[3] Ibid.
[4] UNSTATS (2013).

these were coded as "Worldwide/multiple regions". Where the origin or destination of listings could not be determined, listings were categorized as "Unknown".

The tables produced as part of the analysis by country will of necessity involve some double counting of vendors. For example, a vendor with one listing that "ships from" the United States and another listing that "ships from" the United Kingdom will be counted twice. For this reason, summing would provide totals that would exceed the number of vendors estimated to be in the sample. The possibility that vendors can list different "ship from" locations for different products is an illustration of the limitation of using this data as a proxy for vendor location. Although it seems likely that most vendors will accurately list their location (not least to avoid deception and potentially negative feedback from customers arising from this), there may be valid reasons vendors list "ship from" locations that do not coincide with their location.

Estimating where firearms are shipped from

Cryptomarkets give the opportunity to vendors to specify, in a specific field of the listing, the location from which the products they are offering will be shipped. Since datasets can be in the order of tens, hundreds or thousands of listings, this data is used only as a reference for estimating the products' location at the time of shipping. This comes with the limitations described in the section above.

In the context of this study, given the relatively small size of the dataset, counting 811 listings, the project team reviewed each listing to identify other clues (e.g., in the text of the description) that could be used to increase the accuracy or level of confidence in assessing the "ship from" country or region.

To make this assessment, the project team employed the following criteria (in order of priority):

1. The country of origin as specified in the listing description
2. The self-attested "ship from" of each listing
3. The "ship from" country on other listings by the same vendor
4. The "ship from" country of a vendor on other cryptomarkets
5. The "ship to" category, where a single destination country is specified
6. The most prevalent "ship to" destination, from the same vendor over many cryptomarkets
7. Analysing the "supplier ID" for an indication of the country of origin (e.g., "balkanweapons", "dutchmarket" and "USuser")

The criteria above were used, from the first to last, to identify the most specific reference to the country or region the product was shipped to. For example, if a listing reported in the "ship from" field "North America" and the description included specific reference to shipping from the United States, the listing was coded with the most specific of the two (in this case, United States). Table 5.1 illustrates the number of listings generating sales, the estimated monthly transactions and estimate gross revenue for each "ship from" location.

Table 5.1 **Firearm listings where vendors state products are shipped from: listings generating sales, estimated transactions per month and estimated gross revenue location (ordered by monthly gross revenue)**

Country	N listings	N active listings	Transactions (per month)[a]	Gross revenue (per month)
Multiple/unknown	40	16	7.7	$29,526
United States	201	16	30.5	$24,987
Netherlands	8	3	4.5	$8,088
United Kingdom	5	1	6.0	$5,043

Country	N listings	N active listings	Transactions (per month)[a]	Gross revenue (per month)
Germany	18	4	4.1	$3,453
Europe	8	4	2.2	$2,514
Australia	11	2	0.6	$1,121
Austria	1	0	0.0	$0
Canada	2	0	0.0	$0
Denmark	44	0	0.0	$0
Slovenia	1	0	0.0	$0
Total	**339**	**46**	**55.6**	**$74,733**

Note: Where an individual country or single identifiable region could not be ascertained in a listing, this appears in the table as 'multiple/unknown'.

[a] The following method was used to calculate our transaction variable: number of feedbacks for each listing divided by the number of days between the date of data collection for each market and the date of the listing's oldest feedback; this generated the rate of feedbacks per day, which, multiplied by 30, provided an estimate of monthly transactions.

Concerning possible destinations, the data available from cryptomarkets did not allow the team to identify where products were actually shipped unless the country or region to which a vendor was willing to ship a product matched the location of the vendor (e.g., vendor stating clearly "Shipping only to Country X"). Vendors, however, often indicated multiple countries and regions to which they were willing to ship. In some cases, vendors including "Worldwide" as a destination also included specific countries or regions (despite them being naturally part of "Worldwide"). This might be a random choice, or it could be a tactic (a) used to increase the visibility of the listing when users use search criteria or filters to navigate cryptomarkets, or (b) potentially based on the vendor's assumption of where buyers might be more interested in receiving their products.

Estimating where firearms are shipped to

By cross-checking data on transactions with data on shipping destinations, the project team estimated the volume (transactions per month) and gross revenue associated with each shipping destination. Table 5.2 summarizes the results of this analysis.

Table 5.2 **Available shipping destinations for firearms: listings generating sales, estimated transactions per month and estimated gross revenue location (ordered by monthly revenue)**

Country	N listings	N active listings	Transactions (per month)[a]	Revenue (per month)
Worldwide	307	38	49.2	$68,561
Europe	9	4	4.3	$4,154
United States	7	1	0.8	$1,042
Germany	2	2	1.0	$813
Australia	4	1	0.1	$163
Multiple	3	0	0.0	$0
North America	3	0	0.0	$0
Northern Europe	1	0	0.0	$0
Oceania	3	0	0.0	$0
Total	**339**	**46**		**$74,733**

[a] The following method was used to calculate our transaction variable: number of feedbacks for each listing divided by the number of days between the date of data collection for each market and the date of the listing's oldest feedback; this generated the rate of feedbacks per day, which, multiplied by 30, provided an estimate of monthly transactions.

An additional level of analysis allowed the project team to cross-check data on locations from which firearms are shipped and possible destinations. The analysis produced two types of estimated shipping routes. The first consists of the "potential" shipping routes (i.e., those that consider the entire dataset of 339 listings for firearms and their information on origin of the merchandise and available destinations). The second estimate

of shipping routes includes exclusively those listings (46) that generated sales/revenue. While the first estimate includes all the potential countries of origin of the shipment and associated destinations, the second refers only to those countries of origin that generated sales and for which the destination was known. Tables 5.3 and 5.4 summarize the results of this analysis.

Table 5.3 **Available shipping routes for all firearms (n = 339)**

Route	Listings
United States ⇨ Worldwide	188
Denmark ⇨ Worldwide	44
Multiple/unknown ⇨ Worldwide	40
Germany ⇨ Worldwide	13
Netherlands ⇨ Worldwide	8
United States ⇨ United States	7
Europe ⇨ Europe	5
United Kingdom ⇨ Worldwide	5
Australia ⇨ Australia	4
Australia ⇨ Worldwide	4
Australia ⇨ Oceania	3
Europe ⇨ Worldwide	3
Germany ⇨ Europe	3
United States ⇨ Multiple	3
United States ⇨ North America	3
Canada ⇨ Worldwide	2
Germany ⇨ Germany	2
Austria ⇨ Northern Europe	1
Slovenia ⇨ Europe	1
Total	**339**

Table 5.4 **Shipping routes used for firearms listings generating sales (n = 46)**

Route	Listings	Estimate monthly revenue
Multiple/unknown ⇨ Worldwide	16	$29,526
United States ⇨ Worldwide	15	$23,946
Netherlands ⇨ Worldwide	3	$8,088
United Kingdom ⇨ Worldwide	1	$5,043
Germany ⇨ Europe	1	$2,455
Europe ⇨ Europe	3	$1,699
United States ⇨ United States	1	$1,042
Australia ⇨ Worldwide	1	$958
Europe ⇨ Worldwide	1	$814
Germany ⇨ Germany	2	$813
Germany ⇨ Worldwide	1	$186
Australia ⇨ Australia	1	$163
Total	**46**	**$74,733**

Understanding shipping techniques

The qualitative analysis of individual listings allowed the project team to extract information on packaging and stealth techniques as well as on delivery and shipping options. A key element of shipping firearms and related products is the packaging.

In fact, the packaging of firearms, explosives and other weapons must be sophisticated in order to disguise the consignment from customs and postal service screening. Only a small portion of listings specified packaging and stealth instructions in the description. There were a number of reoccurring features in delivery and shipping:

- Shipping in multiple packages (often 2-3 parcels)
- Stealth and concealment were reassured by suppliers

Less frequently, there were nuanced instructions on the intended methods of packaging firearms. These instructions offer reassurance to prospective buyers that their purchases will evade detection by customs' or postal operators' security scans. On the clear web, some sites discourage the discussion of stealth techniques.[5] The qualitative analysis of the listings provided an initial indication of some of the techniques used to conceal weapons (or their parts):

- For instance, some vendors shipped firearms in "consumer electronics castings" such as printers or TV sets, or in a "music instrument case with a false hard bottom".
- Shipments of grenades were limited to three a parcel (i.e., "more grenades would result in a large and heavy packet…").
- One vendor was offering to ship firearms with illicit drugs in a bulk order for a discounted shipping rate.
- To justify not shipping internationally, one vendor expressed the additional step of "unnaturally breaking up guns" to pass customs, which would affect the durability, accuracy and quality of the weapon. This is likely to be an excuse to ship within a specific country (e.g., Australia or the United States) or region (e.g., Europe) to reduce the likelihood of packages being intercepted, as firearms can easily be disassembled and re-assembled without compromising their technical integrity.

An article in the popular media echoed the anecdotal evidence of smuggling firearms into the United Kingdom.[6] According to the article in *The Telegraph*, weapons are broken down into their component parts and sent in multiple packages with different parcel couriers. This intends to reduce

[5] The subreddit rules for r/DarkNetMarkets instruct users to not "post stealth details".

[6] Freeman (2016).

the likelihood of the package being seized by authorities.[7] Moreover, it allows the recipient to re-assemble the component parts into a functioning weapon without compromising its quality.

More generally, disassembling firearms into multiple parts and shipping them separately might also be a method to leverage loopholes in national legislation, as different countries regulate the sale of firearms parts and components in different ways. While shipping a full handgun might be illegal without the required licences, shipping in multiple parcels containing individual parts that per se are not illegal could be a way around controls.[8]

Discussion

Table 5.1 suggests that the large majority (almost 60 per cent) of the firearms listings are associated with the United States as their "ship from" location. The United States is followed by a selection of European countries which, in aggregate, account for roughly 25 per cent. Unspecified locations of origin account for roughly 12 per cent. This distribution refers to all firearms listings (339), but a very different picture is provided by the evidence when referring to listings generating sales. In this case, the distribution is significantly more balanced, with the United States and "Worldwide" accounting for 35 per cent each, followed by European countries at 25 per cent.

In terms of number of monthly transactions, evidence suggests that the firearms shipping from the United States are the most commonly purchased. The data indicates that the number of monthly transactions originating from the United States is almost double the number of those originating from Europe. Even assuming all the "Worldwide" transactions are

[7] Ibid.

[8] The extent to which individual parts and components are considered regulated goods requiring specific licences and authorisations to be traded and/or shipped can vary significantly among countries.

all non-US-based, this would not alter the perception that the United States appears to be the most common source country for firearms traded on English-language cryptomarkets.

Interestingly, comparing the average price per transaction, results of this study suggest that the United States has the lowest price compared, for example, to the average price-per-transaction in European countries taken individually or in aggregate. This could suggest that (a) most the firearms shipping from the United States are pistols/handguns, with a lower unit price compared to heavier firearms; and/or that (b) the market price for the same firearm type in the United States is significantly cheaper than elsewhere.

Regarding possible destinations, the evidence available is less accurate as the vast majority of vendors indicated they would ship worldwide, and the overwhelming majorities of both transactions and revenue were associated with this shipping option. As described at the beginning of this section, it is not possible to determine where vendors actually ship their products unless they clearly restrict their "ship to" criteria to just one region or country. From the limited data available, it is possible to observe that, in relative terms, Europe is a much more active recipient market than the United States, generating revenue about five times higher.

Analysing shipping routes (i.e., cross-checking "shipping from" against "shipping to" data), has provided some insight into how cryptomarkets are, at least potentially, an enabler for international arms trafficking. In fact, looking at the entire set of 339 firearms listings, only 4 per cent seem associated with domestic trade (i.e., shipping from and to the same country). It should be noted that the uncertainty of actual destinations within "Worldwide" makes it difficult to estimate the proportion of domestic versus international trade as the shipping option "Worldwide" covers both. Nevertheless, it is reasonable to say that, in principle, the overwhelming majority of vendors are willing to ship outside of their national borders. Even if

we include “Europe to Europe” as part of domestic trade, the percentage goes up by only 1 per cent.

Looking instead at the shipping routes associated with confirmed transactions, the domestic trade accounts for approximately 9 per cent of the total when looking exclusively at “same country”, and 17 per cent when considering also trade within Europe. This finding is in contrast with results of empirical cryptomarket analysis in the area of illicit drugs, where most revenues were generated intracontinentally rather than intercontinentally.

VI.

Overarching implications

This chapter extracts some of the emerging themes from the analysis of the findings. The purpose is to characterize how the dark web is changing, or has the potential to change, the features of arms trafficking and the planning assumptions that policymakers and law enforcement agencies have used traditionally to tackle this form of crime.

Impact on the illicit firearms market

Dark web arms trafficking: global in nature, small in scale

The emergence of the dark web has the potential to take the concept of the globalized arms trade to a different, potentially disruptive, level. The illegal arms trade on the dark web removes geographical barriers (among others) between supply and demand, as evidence clearly indicates (see chapter V). This in turn enables illegal trade at a global scale where buyers and vendors, potentially located on different sides of the world, are just a few clicks away from connecting and conducting illicit business.

While the results presented in chapters III and IV show that the actual scale of dark web–enabled firearms trade is relatively small compared to other types of products (e.g., drugs), there

was general consensus among the workshop participants that its potential impact on security could be significant.[1]

Concerning the scale of the dark web–enabled arms trafficking, the results of this study suggest that it is limited in terms of both volume and value compared to other forms of arms trafficking. This is true not only at the aggregate level, but also at the single-transaction level. The data illustrates that while "bulk orders" exist, they are limited to a smaller number of weapons (usually between two and six), which are in any case shipped in multiple packages to minimize the risk of detection. As mentioned by experts consulted as part of this study, to date, dark web arms traffickers have dealt in parcels, not shipping containers.[2]

This factor, in combination with the dependence on certain infrastructure and services, implies that the dark web is unlikely to become the method of choice to provide weapons that will be used in armed conflicts, both because arms are not traded at a large-enough scale and because of the potential limitations on infrastructure and services in a conflict zone. On the other hand, several law enforcement representatives believed that the dark web has the potential to become the platform of choice for individuals (e.g., lone-wolf terrorists) or small groups (e.g., gangs) to anonymously obtain weapons and ammunition behind the anonymity curtain provided by the dark web.[3]

---

[1] RAND Europe–United Nations Office for Drugs and Crime seminar, Vienna, 23 May 2017.

[2] RAND Europe expert workshop, 20-21 March 2017 (Representative of law enforcement agency).

[3] RAND Europe expert workshop, 20-21 March 2017 (Representatives [3] of law enforcement agency).

Cryptomarkets facilitate illicit trade in small arms and digital products

The results of this study show that almost all firearms sold on cryptomarkets fall under the category of small arms.[4] While heavier types of weapons, including rocket-propelled grenades (most commonly referred to as RPGs), have been identified on single-vendor shops, the impossibility of estimating transactions on such platforms and the lack of tools to estimate their "legitimacy"[5] suggest that small arms are the dominant product range available over the dark web.

This causes several control issues as many types of small arms are legally available for purchase in many countries, delaying the identification of those shipped illegally. This also relates to the trade in parts and components, which, again, is regulated in different ways across different countries. Assembling a firearm by purchasing parts and components individually, perhaps from different countries, is also a new possibility enabled by the dark web.

While purchasing firearms and their parts or ammunition implies the combination of the "virtual" and "real" world (i.e., buy "virtually" online/receive "physically" in the post), the results of this study suggest that the second most common

---

[4] "Small arms" are, broadly speaking, weapons designed for individual use. They include, inter alia, revolvers and self-loading pistols, rifles and carbines, submachine guns, assault rifles and light machine guns. They differ from "light weapons", which are, broadly speaking, weapons designed for use by two or three persons serving as a crew, although some may be carried and used by a single person. They include, inter alia, heavy machine guns; hand-held under-barrel and mounted grenade launchers; portable anti-aircraft guns; portable anti-tank guns, recoilless rifles, portable launchers of anti-tank missile and rocket systems; portable launchers of anti-aircraft missile systems; and mortars of a calibre less than 100 mm. (United Nations General Assembly (2005)).

[5] The word "legitimacy" or "legitimate" is used in opposition to "fake" or "scam" and does not imply the endorsement by the project team of the type of activity performed by the vendor.

arms-related products bought on the dark web are digital files. As already discussed, these may include tutorials to build explosives and bombs at home or convert blank-firing firearms into live ones (or semi-automatic into full-automatic), but can also include 3D models of firearms or their parts. In the case of digital products, the entire transaction happens online, making it even more difficult to trace.

This is a cause of particular concern. The proliferation of guidelines and 3D models, in combination with the increasing quality of commercially available 3D printers, may result in more untraceable weapons as users become increasingly able to manufacture fully functioning weapons. Or, most likely, original parts and components bearing identification markings, on an already existing firearm, could increasingly be replaceable by parts and components manufactured using 3D printers (see the section entitled "Digital products" in chapter III).

Finally, as previously mentioned, the results presented in chapters III and IV seem to suggest that cryptomarkets allow buyers to get better value for money: better-performing, more recent firearms for the same, or lower, price than would be available on the street. Where firearms control measures are implemented effectively, it is likely that the availability of firearms on the street-level black market will be limited both in terms of quantity and in terms of quality. In the United Kingdom, for example, firearms typically available on the black market are antiques that are subject to a different, less strict, regulation.[6] With the dark web, the inventory available to buyers is not affected by this type of limitation. In a competitive environment such as that of cryptomarkets, where multiple vendors compete with each other to sell their products, the value that buyers can get for their money can potentially be much higher.

[6] RAND Europe expert workshop, 20-21 March 2017 (Representatives [2] of law enforcement agencies).

Impact on market actors

The dark web removes typical barriers between vendors and buyers

The most evident implication of dark web arms trafficking in relation to people is the almost complete removal of barriers between vendors and buyers: vendors can instantly access a global client base, and buyers can, similarly, instantly access a global supplier base. Protected by the anonymity of their online personas, buyers and vendors can use cryptomarkets to interact instantly, directly, freely and safely, without requiring any form of introduction or "vetting", which arms dealers would normally expect before conducting business in the "offline" world.[7]

The level of Internet literacy and technical skills required to actively engage with the dark web can vary substantially depending on the level of anonymity that users are seeking to achieve. However, given the numerous step-by-step guidelines and tutorials available on the web, it is reasonable to assume that anyone able to browse the Internet and with a basic level of understanding of, and familiarity with, the modalities of purchasing goods and services online can successfully engage with marketplaces on the dark web. In very simple terms, anyone interested in buying a firearm illegally and possessing the information technology skills described above—or the basic skills required to search and consult online resources and tutorials—can connect to a cryptomarket and within minutes have access to tens of different vendors offering their products. While it is acknowledged that some of these vendors might be fake (e.g., scammers or law enforcement honeypot vendors), the ability for all kinds of individuals to connect to an international network of vendors, extrapolated from the business to consumer (B2C) principle of e-commerce, deeply changes the way individuals can procure firearms.

[7] Ibid.

The perceived anonymity of cryptomarkets may attract specific types of individuals

Another implication at the individual level is the profile of person who might engage in this type of arms trafficking. Both official and media reports have associated the use of the dark web to terrorist cells and organized criminal groups, as well as lone-wolf terrorists or individual criminals, which have used such platforms to source weapons and ammunition. However, interviews with law enforcement representatives indicate that the people involved in this type of crime can also include individuals not affiliated with terrorist or criminal groups, without prior criminal records and with no reason to be flagged by authorities.[8] This can include vulnerable or fixated individuals affected by mental conditions, minors and other categories of individuals who would not necessarily be willing or able to purchase a weapon or ammunition on the streets.

Trust is a key element behind the functioning of cryptomarkets, just as it is in the traditional black market. The difference is that on cryptomarkets, behind the veil of anonymity, trust is built primarily on business-worthiness and reputation, as vendor or buyer, and less on other subjective considerations related to the individuals behind the pseudonyms. Therefore, by design, no discrimination is made on cryptomarkets based on age, gender, ethnicity or any other factor that does not have a direct impact on the transaction (e.g., feedback history, quality of description, quality of the photo). The only exception to this rule may be represented by language: whether English or any other language, cryptomarkets are built on the assumption that users can interpret their contents.

An additional consideration, presented as a reasoned conjecture only, is that the dark web may provide a possible solution for those who could be defined "occasional vendors". While acknowledging the difficulty of selling a product without

[8] RAND Europe interview with law enforcement representatives (3).

having any reputation as a vendor, the dark web provides, in theory, the opportunity to any individual to anonymously dispose of firearms (e.g., personal items or inherited items sold for untraceable profit). This complicates even further the task for law enforcement agencies to monitor and identify vendors involved in dark web arms trafficking, as their activity on such platforms might be sporadic, and because the pool of potential vendors enlarges to encapsulate individuals who might not be known to the authorities.

Cryptomarkets introduce a new set of actors

In addition to vendors and buyers, there are at least three key actors who are involved in dark web–enabled arms trafficking (or any other illegal trade conducted through cryptomarkets). These key actors can be grouped as follows:[9]

- **Administrators** have an executive management role on the marketplace and fulfil the role of treasurer; they sit at the top of cryptomarkets and receive a commission for each sale finalized through the marketplace
- **Developers** are commissioned to carry out web design (and maintenance)
- **Moderators** are marketplace members of staff, sometimes receiving a salary for their services, which include assisting with site maintenance and customer support

These types of profiles/functions are quite common in the online world, but how they relate to the actors of the offline arms trade (e.g., brokers) remains to be analysed and normalized.

[9] Kruithof et al. (2016, 104).

Law enforcement and policy implications

Law enforcement agencies face a series of operational challenges

Previous RAND research identified four main strategies or intervention types that law enforcement can deploy to tackle dark web–facilitated trafficking.[10] While these strategies were analysed in relation to the drug trade, their general principles and associated challenges can be adapted and transposed to the context of arms trafficking. Table 6.1 provides an overview of these four strategies and associated barriers for law enforcement adapted, if necessary, to the context of firearms trafficking on the basis of the project team's consultation with experts.

Table 6.1 **Summary of law enforcement intervention strategies and related barriers**

Strategy/intervention type	Description	Barriers
Traditional investigation techniques	Techniques used to target the phases of the supply chain where online and offline meet (e.g., shipping and delivery of products). Examples include surveillance, use of informants, controlled deliveries.	High costs and potentially low benefits given the variety, and high number, of potential buyers; even if buyer is apprehended, it remains difficult to obtain identifying information or evidence on the vendors given the anonymity veil of cryptomarkets.

[10] Kruithof et al. (2016).

Strategy/intervention type	Description	Barriers
Postal detection and interception	Methods to track and trace parcels and monitor progress; scanning of suspicious parcels	High number of parcels processed on a daily basis puts large burden on postal systems and customs; difficulty in identifying reliable criteria to apply selective screening to parcels; competing priorities between commercial operators (speed and reliability of service) and law enforcement (identification of illegally shipped weapons); use of stealth techniques by vendors including the use of multiple parcels
Online detection and monitoring	Combining different data sources, tools and techniques using big data analytics and machine learning to connect different data sources and eventually de-anonymize cryptomarket actors Continuous monitoring of dark web market places Monitoring and tracking Bitcoin transactions through "block chain" analysis	Encryption: even if a server hosting a cryptomarket is seized, identifying users and/or locations remains very difficult Attribution: attributing specific activities to specific individuals is difficult due to the extensive use of software like Tor Fluctuation: the rapidly changing nature of cryptomarkets and their users makes it difficult to rigorously document illegal activity, making it difficult to successfully prosecute crimes
Online disruption	Infiltrating cryptomarkets to conduct operations that undermine the trust around anonymity and reliability (e.g., by increasing the number of scams) Taking down marketplaces	Migration of vendors and buyers to other cryptomarkets (displacement) Creation of new cryptomarkets (substitution) Enhanced security measures implemented by administrators

Source: Adapted from Kruithof et al. (2016).

In addition to the specific barriers associated with different types of intervention strategies, this study also identified some overarching challenges faced by law enforcement agencies that resonate with existing literature. These include the following:

- **Resources and skills**. Investigating and prosecuting dark web–enabled arms trafficking requires technical skills and resources. One interviewee noted that these might not be available as the level of understanding of the dark web, as well as the perception of the threat it may represent, varies considerably between policymakers and law enforcement agencies.[11] Workshop participants argued that linking novel investigation technologies and techniques with more traditional investigation techniques can prove challenging without adequate training and financial resources to support adequate staffing and equipment.[12]
- **International cooperation**. As the findings of this study illustrate, dark web–enabled arms trafficking appears to be more international than domestic. This makes effective international cooperation essential in responding to this type of criminal activity. Nevertheless, although consulted law enforcement representatives indicated a good level of cooperation,[13] there might be some practical obstacles due to different jurisdictions, or due to national legislation that may differ with respect to what can be sold legally (e.g., parts, components, ammunition, blank-firing guns).[14] In addition, cooperation between law enforcement agencies and public or private postal/courier service providers is key to ensuring that, once information allows for the identification of either a suspicious package or its sender or recipient, mechanisms are in place to swiftly intervene. The international nature of the dark web firearms trade

[11] RAND Europe interview with policy representative.
[12] RAND Europe expert workshop, 20-21 March 2017.
[13] Ibid.
[14] Kruithof et al. (2016).

implies that such public-private interfaces often cross several jurisdictions, requiring the cooperation of multiple law enforcement agencies in different countries and, potentially, multiple economic operators.

- **Legal restrictions on interventions**. Law enforcement agencies have to consider and comply with relevant legislation (including in a third country should international legal assistance be necessary) regulating privacy rights, data and information protection and other legal restrictions relevant to monitoring online behaviour or conducting online operations, as well as to screening parcels or conducting traditional surveillance.[15]

Policy action at the national level is necessary to overcome operational barriers

Although consulted law enforcement representatives referred to a number of successful operations covering the entire range of intervention strategies illustrated in table 6.1 above (e.g., Operation Onymous), they also highlighted that to achieve sustained efforts and long-lasting results, a strong political commitment including a clear recognition of the threat is a necessary step.[16] For example, the United Kingdom has committed in its National Security Strategy, *Strategic Defence Security Review 2016*, to tackle the criminal use of the dark web by establishing a new "Dark Web Intelligence Unit".[17] The creation of the unit is to enable the analysis of multiple data sources, coordinate with multiple agencies and deal with issues at scale. This type of commitment is critical to mobilize the

[15] Kruithof et al. (2016); intervention by national delegation during the open briefing of the United Nations Counter-Terrorism Committee on preventing terrorists from acquiring weapons, held at United Nations Headquarters, New York, on 17 May 2017.

[16] RAND Europe expert workshop, 20-21 March 2017 (Representatives from law enforcement and policymaking community).

[17] Her Majesty's Government (2016).

necessary resources and ensure that law enforcement agencies receive the required "top-cover" for conducting their operations.

Second, the previous sections highlighted the challenge that law enforcement agencies face with respect to legal restrictions. Therefore, policymakers should also ensure that policies and regulations are in place to empower law enforcement agencies to investigate and prosecute dark web–enabled arms trafficking while ensuring respect of civil rights and democratic principles.

Finally, at the national level, policymakers may also achieve impact through different types of interventions beyond the realm of law enforcement operations. Similar to what the literature suggests with respect to drugs,[18] prevention and education might be another intervention strategy. This might entail building on existing initiatives such as the gun violence prevention strategy led by the United States National Institute of Justice, which encompasses a combination of different programmes tailored to local communities,[19] or initiatives promoted by organizations like the American Psychological Association focusing on prevention (e.g., spotting warning signs in youth) and education.[20] This "soft" measure may be considered as complementary to law enforcement operations, and it would be more forward-looking with its design taking into account the new generation of digital natives.[21]

However, the international policy community will also need to take action and adapt to this new phenomenon

The proliferation of and trafficking in small arms have been acknowledged as a global security threat for a few decades,

---

[18] See for example, Christin (2013).

[19] For more information see National Institute of Justice (2017).

[20] For more information see American Psychological Association (n.d.).

[21] Oxford Dictionaries defines a *digital native* as "A person born or brought up during the age of digital technology and so familiar with computers and the Internet from an early age."

with the first official milestone set by the United Nations in 2001 with the adoption of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects.[22] Since then, several instruments have been created at all levels to support national and international efforts against small arms proliferation. More recently, reducing arms trafficking has been included by the United Nations in the new Sustainable Development Goals, with Target 16.4 stating: "By 2030, significantly reduce illicit arms flows".[23]

Dark web–enabled firearms trafficking fits in the wider context of illicit trade in small arms and light weapons, and the majority of the policy challenges and enablers related to the wider category still apply (e.g., reducing and preventing arms proliferation and misuse, reducing and preventing armed violence, reducing economic and social cost of small arms proliferation). Similarly, the dark web can function as an enabler and facilitate the circulation of illegal weapons, but it requires weapons to be available. Thus, compliance with already-existing international instruments to prevent and combat the illicit trade, including effective control measures to limit the availability of illegal weapons, are, and will remain, key in addressing this issue.

These measures include, for example, efficient marking and record-keeping practices; effective international cooperation mechanisms for tracing illegal weapons; good physical security and stockpile management practices; and reliable licensing and authorization processes, including background checks.

---

[22] United Nations (2001).

[23] Sustainable Development Goal 16: "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels". The full text of Target 16.4 reads: "By 2030, significantly reduce illicit financial and arms flows, strengthen the recovery and return of stolen assets and combat all forms of organized crime". (United Nations General Assembly (2015b))

While a full review of all international and regional instruments falls outside of the scope of this study, the findings of this first investigation into dark web–enabled arms trafficking, combining the data collected with the views of the experts consulted in this study, identified specific elements that may challenge existing instruments, in addition to the more general concern over availability of fully functioning firearms:

- **Trade in parts and components**. Definitions of parts and components, as well as rules regulating their trade, are not standardized
- **Trade in digital products**. Despite some initial acknowledgement of the potential threat posed by the diffusion of 3D-printing technologies, trading in digital products that can be used for the production of complete firearms or individual parts remains a grey area with little to no harmonized practice
- **Trade in replica, deactivated or other non-live guns**. While no confirmed sale of non-live firearms was available during the period of observation for this study, the data collected in this study confirms their availability on cryptomarkets. This, combined with the availability of guidelines and tutorials on how to modify and convert non-lethal weapons to live firearms, also documented by this study, increases the risk of conversion. Conversion of firearms is a common practice and an acknowledged threat, which cryptomarkets make even more complex to address.[24]

In addition, as described in the section above entitled "Cryptomarkets introduce a new set of actors", the use of digital platforms to conduct illegal trade in small arms and light weapons both increases the types of actors that are directly or indirectly involved in facilitating the illegal transaction and

[24] King (2015).

blurs the lines around attribution and accountability, potentially creating new legal loopholes for criminals to exploit.

Existing arms control instruments should not necessarily be considered obsolete for application to cryptomarkets, but their validity should certainly be tested against these emerging trends to assess the need for developing the necessary amendments or to suggest how to translate existing provisions to new types of crimes. In this regard, the Global Firearms Programme of the United Nations Office on Drugs and Crime (UNODC) prepared an analysis of three international legal instruments based on the results of this study with a view to identifying how or to what extent the already existing international legal framework provides an adequate and effective response to dark web arms trafficking. This analysis reviews three legally binding instruments at the international level that are of particular relevance to this study:

- The United Nations Convention against Transnational Organized Crime (Organized Crime Convention)
- Its supplementary Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition (Firearms Protocol)
- The Arms Trade Treaty

These three instruments have been reviewed by the UNODC to identify those provisions that may support policymakers and law enforcement agencies in their efforts to tackle dark web–enabled arms trafficking. Based on its analysis of the international legal framework, the UNODC identified the following high-level policy considerations:[25]

- The three international legal instruments reviewed provide a highly relevant framework as States parties develop and implement approaches to address illicit trafficking in firearms, their parts and components and ammunition on

[25] For the full analysis please refer to Persi Paoli et al. (2017, Annex)

the dark web. While the Organized Crime Convention is almost universally applicable, it is noteworthy that several States figuring prominently in the present research might have signed the Firearms Protocol, but are not State parties to it. There are also several States that have not yet adhered to the Arms Trade Treaty. Further efforts towards universalization of the legally binding instruments are therefore required.

- As all three instruments provide for legal and operational measures that can contribute to addressing illicit trafficking in firearms, their parts and components and ammunition on the dark web, a comprehensive approach to tackle the phenomenon in the context of a changing criminal environment should take into account the modus operandi used in web transactions and pay particular attention to those occasions when criminals need to leave their anonymity behind.
- Taking into account the personal and geographical anonymity challenges that transactions on the dark web bring, States should increase their efforts to follow through on commitments relating to speedy and reliable international police and judicial cooperation and information exchange.
- While some vendors might only transfer their legally held items, there is a high risk that criminals use cryptomarkets to transfer illicitly possessed items. By strengthening control, preventive and security measures over firearms, their parts, components and ammunition, stakeholders can reduce the risk of those items entering the illicit market. Stakeholders should therefore increase their efforts to fully transpose and implement the international legal framework at the domestic level in an efficient and comprehensive manner, including through preventive and security as well as enforcement measures.

Finally, dark web–enabled arms trafficking is a hybrid threat in its nature, combining the "real world" issues of arms trafficking with the challenges posed by information and communications technology (ICT) and the cyberspace. This will require a cross-sector, multi-agency approach to ensure that effective measures are implemented and best practices are identified and shared. For example, in consideration of the high level of unfamiliarity that the dark web still represents for many stakeholders, particularly relevant is the work conducted by the 2015 United Nations Group of Governmental Experts on developments in the field on information and telecommunications in the context of international security, which recommended 11 voluntary, non-binding norms of responsible State behaviour in the use of ICT, which called for cooperation and information exchange, including that "States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect."[26] While the dark web was not specifically mentioned in this 2015 document, which was more focused on more general cybersecurity issues, illegal trade in firearms on the dark web today would fall into the above-mentioned criminal use of ICT.

[26] United Nations General Assembly (2015a, para 13d); United Nations General Assembly (2015c).

VII.

Conclusions

This study has demonstrated that meaningful insights can be obtained by using empirical analysis methodologies to investigate dark web–enabled arms trafficking. Despite its limitations, described throughout the report, this study represents the first systematic, evidence-based assessment of such trafficking in firearms (including their parts, components, accessories and ammunition) and explosives.

The findings generated by this study highlight the global nature of this threat and reinforce the importance of several key points included in the recently released outcome document of the Third United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects.[1]

In addition to the general principles and actions targeting the overall issue of arms trafficking, which are also applicable and relevant to dark web–enabled arms trafficking, some of the specific articles in the forward-looking part of the outcome document (i.e., implementation of the Programme of Action for the period 2018-2024) also resonate with the findings of this study. A selection of these articles and related study findings is illustrated in the table below.

[1] United Nations General Assembly (2018).

Table 7.1 **Relevance of study findings for selected provisions of the Programme of Action implementation guidelines for 2018-2024 included in the outcome document of the Third Review Conference**

Category	Excerpts from the Programme of Action implementation guidelines for 2018-2024	Observations based on study findings
Legislative measures	To establish or strengthen, as appropriate, national laws, regulations and administrative procedures for the coordinated national implementation of the Programme of Action and other relevant instruments, including legally binding instruments, to which a State is a Party. To ensure that relevant national laws, regulations and administrative procedures prohibit, in the areas under the State's jurisdiction and control, the illicit trade in small arms and light weapons conducted through the internet.	Arms trafficking on the dark web poses several legislative challenges adding further sensitive and intractable issues (related to cyberactors and cybercrime) to the already variable legislative landscape relating to arms control.
Cooperation and capacity building	To encourage States, relevant United Nations offices, the International Criminal Police Organization (INTERPOL) and the World Customs Organization to enhance coordination, and share best practices and lessons learned. To take account of recent developments in small arms and light weapons manufacturing, technology and design in the implementation of the Programme of Action and the International Tracing Instrument, including additive manufacturing, and to strengthen cooperation between law enforcement agencies so as to prevent unauthorized recipients, including criminals and terrorists, from acquiring small arms and light weapons. To share information with other States, in accordance with national legal frameworks, as appropriate, on successful prosecutions, incidents of diversion, illicit international transfers and brokering, trafficking routes and techniques, and good law enforcement practices, including risk management methods and processes, related to the illicit trade in small arms and light weapons.	The findings illustrate the transnational nature of arms trafficking on the dark web with recent cases reported to have spanned multiple countries in different regions. Therefore, cooperation is key to addressing this phenomenon.

Category	Excerpts from the Programme of Action implementation guidelines for 2018-2024	Observations based on study findings
Control measures	To take all effective measures to prevent and combat the illicit online trade in small arms and light weapons taking place within the areas of jurisdiction of concerned States, including measures to ensure effective control over their export, import and transit. To prevent the illicit manufacturing, reactivation and conversion of small arms and light weapons	The dark web provides additional means and opportunities for criminals to illegally trade firearms and undermines the effectiveness of current arms control measures. In addition, by providing easy access to instructions and tutorials, the dark web increases the risk of illicit manufacturing, reactivation or conversion.
Awareness raising	To encourage initiatives that raise the awareness of possible risks associated with certain recent technological developments in the manufacture and sale of small arms and light weapons, while also acknowledging the opportunities offered by such technologies. To promote, at all levels, a culture of peace through education and inclusive public awareness programmes on the problems of the illicit trade in small arms and light weapons in all its aspects.	The dark web lowers or removes most geographical, physical and personal barriers to accessing the black market either to buy or to sell illegal firearms or related products. At the same time, the dark web is constantly evolving and so are the dynamics and characteristics of its illicit markets. Therefore, a long-term intervention strategy that goes beyond disruption by law enforcement and security forces is necessary, particularly in the field of education and prevention, targeting, in particular, the new generation of digital natives.

Additional research would be necessary to further develop the understanding of the market characteristics (i.e., size, scope and value of the dark web arms trafficking), the products available and the actors involved (e.g., buyers, vendors, administrators and others).

In particular, in order to generate a more robust understanding of the role of the dark web in enabling arms trafficking, a more continuous monitoring activity should be implemented. This would involve repeating and refining the data collection and analysis

presented in this report over time in order to generate historical data that can be used to analyse trends. This would also enable a more rigorous assessment of the validity and applicability of current national and international counter–arms trafficking regimes including policies, laws and regulations, actors and resources.

Firearms make breakdown

Make	Pistol	Submachine gun (and full-auto pistols)	Rifle	Total
Armsel	0	0	1	1
ASM	1	0	0	1
ATC	1	0	0	1
Auto-Ordnance	2	0	0	2
Barrett	0	0	1	1
Beretta	18	0	0	18
Bruni	1	0	0	1
Caesar Guerini	0	0	4	4
CKK Arms	1	0	0	1
CMMG	0	0	1	1
Colt	29	0	1	30
Coonan Classic	1	0	0	1
Custom-made	1	2	2	5
CZ	4	0	0	4
Derringer	1	0	0	1
Dreyse	1	0	0	1
Ekol-Voltran	18	2	0	20
Feinwerkbau	0	0	1	1
Flobert	0	0	1	1
FN	4	0	1	5
Franchi	0	0	4	4
Glock	59	1	0	60
H&K	6	0	1	7
Hi-Point	1	0	0	1
IMI	1	4	0	5
Ithaca	5	0	0	5
Iver Johnson	1	0	0	1

Make	Pistol	Submachine gun (and full-auto pistols)	Rifle	Total
Kel-Tec	3	0	0	3
Kimber	6	0	0	6
Kimber Custom	1	0	0	1
Luger	2	0	0	2
M&P	1	0	0	1
MAADI	0	0	2	2
Magnum Research	1	0	0	1
Mauser	1	1	0	2
Metro Arms	2	0	0	2
Mossberg	0	0	1	1
Nighthawk Custom	1	0	0	1
Para USA	1	0	0	1
Ratzeburg	2	0	0	2
Rossi	1	0	0	1
Ruger	18	0	0	18
Russian	1	0	0	1
Sig Sauer	18	0	1	19
Smith & Wesson	12	0	1	13
Springfield	5	0	0	5
Steyr	0	1	0	1
Steyr Aug	0	0	1	1
STI	1	0	0	1
Taurus	8	0	0	8
Tuna	2	0	0	2
Umarex	0	1	0	1
Unspecified	25	8	6	39
VCougar	1	0	0	1
Volga	1	0	0	1
VZ	0	1	0	1
Walther	9	0	0	9
Webley	1	0	0	1
Winchester	0	0	1	1
Zastava	1	0	2	3
Zoraki	3	1	0	4
Total	**284**	**22**	**33**	**339**

References

Aldridge, J., & R. Askew. 2017. "Delivery Dilemmas: How Drug Cryptomarket Users Identify and Seek to Reduce Their Risk of Detection by Law Enforcement." *International Journal of Drug Policy* 41: 101–109. doi:10.1016/j.drugpo.2016.10.010

Aldridge, J., & D. Décary-Hétu. 2014. *Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation*. SSRN. As of 27 June 2017: http://ssrn.com/abstract=2436643

———. 2016. "Cryptomarkets and the Future of Illicit Drug Markets." In *Internet and Drug Markets, EMCDDA Insights*, edited by EMCDDA, 23–30. Luxembourg: Publications Office of the European Union.

Armory.net. 2017. "Modern Pistols." Armory.net. As of 27 June 2017: http://armory.net/replica-guns/modern-pistols

Barratt, M. J., & J. Aldridge. 2016. "Everything You Always Wanted to Know about Drug Cryptomarkets* (*But Were Afraid to Ask)." *International Journal of Drug Policy* 35: 1–6.

Barratt, M. J., J. Aldridge, & A. Maddox. 2017. "The Darknet." In: *Sage Encyclopedia of the Internet*. London: Sage.

Bender, R., & C. Alessi. 2016. "Munich Shooter Likely Bought Reactivated Pistol on Dark Net." Wsj.com, 24 July. As of 27 June 2017: https://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686

Christin, N. 2013. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." *Proceedings of the 22nd International World Wide Web Conference*, ACM: 213-244.

Décary-Hétu, D., & J. Aldridge. 2013. "DATACRYPTO: The Dark Net Crawler and Scraper." Software program.

———. 2015. "Sifting Through the Net: Monitoring of Online Offenders by Researchers." *European Review of Organised Crime* 2(2): 122–41.

Décary-Hétu, D., M. Paquet-Clouston, & J. Aldridge. 2016. "Going International. Risk Taking and the Willingness to Ship Internationally Among Drug Cryptomarket Vendors." *International Journal of Drug Policy* 35: 69–76.

Freeman, C. 2016. "How Criminals on the Dark Web Are Smuggling Weapons into Britain." *The Telegraph*, 12 April. As of 27 June 2017: http://www.telegraph.co.uk/news/2016/04/12/how-criminals-on-the-dark-web-are-smugglingweapons-into-britain/

GlockStore.com. 2017. "Glock Factory Handguns." GlockStore.com. As of 27 June 2017: http://www.glockstore.com/Handguns/Glock-Factory-Handguns

GunBroker.com. 2017. "Beretta 92 FS." GunBroker.com. As of 27 June 2017: https://www.gunbroker.com/Beretta-92FS/Browse.aspx?Keywords=Beretta%2092%20FS&BuyNowOnly=1&Sort=4&Tab=2

Her Majesty's Government. 2016. *National Security Strategy and Strategic Defence and Security Review 2015. First Annual Report 2016*. As of 27 June 2017: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/575378/national_security_strategy_strategic_defence_security_review_annual_report_2016.pdf

HNGN. 2015. "Paris Attacks: Weapons Allegedly Bought on Darknet from Germany (REPORT)." HNGN.com, 27 November. As of 27 June 2017: http://www.hngn.com/articles/154606/20151127/paris-attacks-weapons-darknet-germany-report.htm

Hullinger, J. 2016. "Do People Really Buy Guns on the Dark Web?" FastCompany.com, 1 July. As of 27 June 2017: https://www.fastcompany.com/3055187/do-people-really-buy-guns-on-the-dark-web

King, B. 2015. *From Replica to Real – An Introduction to Firearms Conversions*. Small Arms Survey Issue Briefs, Number 10, February. As of 27 June 2017: http://www.smallarmssurvey.org/

fileadmin/docs/G-Issue-briefs/SAS-IB10-From-Replica-to-Real.pdf

King, B., & G. McDonald. 2015. *Behind the Curve; New Technologies, New Control Challenges*. Small Arms Survey Occasional Paper, Number 32, February. As of 27 June 2017: http://www.smallarmssurvey.org/fileadmin/docs/B-Occasional-papers/SAS-OP32-Behind-the-Curve.pdf

Kruithof, K., J. Aldridge, D. Décary-Hétu, M. Sim, E. Dujso, & S. Hoorens. 2016. *Internet-facilitated Drugs Trade. An Analysis of the Size, Scope and the Role of the Netherlands*. Santa Monica, Calif.: RAND Corporation. As of 27 June 2017: https://www.rand.org/pubs/research_reports/RR1607.html.

Mounteney, J., A. Bo, & A. Oteo. 2016. *The Internet and Drug Markets*. Luxembourg: Publications Office of the European Union.

National Institute of Justice. 2017. "Gun Violence Prevention." Nij.gov, 16 February. As of 27 June 2017: https://www.nij.gov/topics/crime/gun-violence/prevention/Pages/welcome.aspx

Pavesi, I. 2016. *Trade Update 2016. Transfers and Transparency*. Small Arms Survey, June. As of 18 June 2017: http://www.smallarmssurvey.org/fileadmin/docs/S-Trade-Update/SAS-Trade-Update.pdf

Pawlak, C. 2016. "Beckmann will Kalaschnikow im Darknet kaufen - doch das Experiment geht schief." ["Beckmann Wants to Buy Kalaschnikow in Darknet – But the Experiment Goes Wrong."] Focus.de, 18 May. As of 27 June 2017: http://www.focus.de/kultur/kino_tv/tv-kolumne-beckmann-beckmann-will-kalaschnikow-im-darknet-kaufen-doch-das-experiment-geht-schief_id_5542330.html

Persi Paoli, Giacomo, Judith Aldridge, Nathan Ryan, and Richard Warnes. 2017. *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web*. Santa Monica, CA: RAND Corporation. As of 05 August 2018: https://www.rand.org/pubs/research_reports/RR2091.html.

Smith & Wesson. 2017. "Model 66 Combat Magnum." Smith-wesson.com. As of 1 June 2017: https://www.smith-wesson.com/firearms/model-66-combat-magnum

Soska, K., & Christin, N. 2015. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem." *24th USENIX Security Symposium*, 33–48. As of 27 June 2017: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska.pdf

Tagesschau. 2017. "Darknet - Mythos und Realität Reise in den digitalen Untergrund." ["Darknet – Myth and Reality. Journey into the Digital Underground."] Tagesschau.de, 8 January. As of 27 June 2017: http://www.tagesschau.de/inland/darknet-reise-in-die-digitale-unterwelt-101.html

Tzanetakis, M., G. Kamphausen, B. Werse, & R. von Laufenberg. 2015. "The Transparency Paradox. Building Trust, Resolving Disputes and Optimising Logistics on Conventional and Online Drugs Markets." *International Journal of Drug Policy* 35: 58–68.

United Nations. 2001. *Report of the United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects, New York, 9-20 July 2001*. A/CONF.192/15. As of 27 June 2017: https://digitallibrary.un.org/record/447095/files/A_CONF.192_15-EN.pdf

United Nations General Assembly. 2005. *International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons*. A/60/88. As of 27 June 2017: http://www.unodc.org/documents/organized-crime/Firearms/ITI.pdf

———. 2014. *Recent Developments in Small Arms and Light Weapons Manufacturing, Technology and Design and Implications for the Implementation of the International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons*. Report of the Secretary-General. A/CONF.192/BMS/2014/1. 6 May. As of 27 June 2017: http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.192/BMS/2014/1&referer=/english/&Lang=E

———.2015a. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. 22 July. A/70/174. As of 30 August 2018: http://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf

———. 2015b. *Transforming our World: The 2030 Agenda for Sustainable Development*. Resolution 70/1, 25 September. A/RES/70/1. As of 27 June 2017: https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf

———. 2015c. *Developments in the field of information and telecommunications in the context of international security*. Resolution 70/237, 23 December 2015. A/RES/70/237. As of 30 August 2018: http://digitallibrary.un.org/record/815989/files/A_RES_70_237-EN.pdf

———. 2018. *Outcome document of the Third United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects*. Annex to "Report of the Third United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects". Advanced unedited version. A/CONF.192/2018/RC/3. 2 July. As of 05 August 2018: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/07/2018-07-06-Final-report-RevCon3_Approved-by-President.pdf

UNSTATS (United Nations Statistics Division). 2013. "Methodology: Standard Country or Area Codes for Statistical Use (M49)." Unstats.un.org. As of 27 June 2017: https://unstats.un.org/unsd/methodology/m49/

Van Buskirk, J., S. Naicker, A. Roxburgh, R. Bruno, & L. Burns. 2016. "Who Sells What? Country Specific Differences in Substance Availability on the Agora Dark Net Marketplace." *International Journal of Drug Policy*. 35: 16-23. As of 27 June 2017: http://www.ijdp.org/article/S0955-3959(16)30226-2/fulltext

Zetter, K. 2013. "How the Feds Took Down the Silk Road Drug Wonderland." Wired.com, 18 November. As of 27 June 2017: http://www.wired.com/threatlevel/2013/11/silk-road/

———. 2014. "New "Google" for the Dark Web Makes Buying Dope and Guns Easy." Wired.com, 17 April. As of 27 June 2017: https://www.wired.com/2014/04/grams-search-engine-dark-web/

ISBN 978-92-1-130357-5

18-16522