RAND EUROPE

Behind the curtain

The illicit trade of firearms, explosives and ammunition on the dark web

Giacomo Persi Paoli, Judith Aldridge,
Nathan Ryan, Richard Warnes

For more information on this publication, visit www.rand.org/t/RR2091

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

RAND Europe is a not-for-profit research organisation that helps to improve policy and decision making through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Support RAND
Make a tax-deductible charitable contribution at
www.rand.org/giving/contribute

www.rand.org

www.rand.org/randeurope

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. However, the hidden and obscured parts of the web are used also by criminals and other types of individuals 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 facilitators for illicit drug trade has increasingly been the subject of research by a number of academics, little has been done to conduct a systematic investigation of the role of the dark web in relation to the illegal arms trade, drawing on the insights offered by primary data.

To address this gap, and with a view to supporting policy and decision makers, RAND Europe and the University of Manchester designed this research project, funded by the UK Partnership for Conflict, Crime and Security Research (PaCCS) under the Transnational Organised Crime theme, which is led by the Economic and Social Research Council on behalf of the Partnership. This project was officially endorsed by the Global Firearms Programme of the United Nations Office for Drugs and Crime, which also contributed to the study by providing an independent assessment of the international legal framework's applicability to the subject of dark web-enabled arms trafficking. This assessment is attached to this study.

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

For more information 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

Table of contents

Figures

Boxes

Tables

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 2016 Munich shooting which link the weapons used by the attackers to vendors on dark web marketplaces. Some media reports have also linked the November 2015 Paris terrorist attacks 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. Little empirical evidence is available. 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.

The rise of scamming, heightened policing, and low volume of weapons sales on the dark web has spread caution in the dark web community, if not widespread doubt, about the viability of using dark web marketplaces to buy weapons on the dark web. Yet, recent cases documented by governmental agencies or reported by the media suggest that dark web arms trafficking is a real phenomenon.

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.

Today, as this study demonstrates, weapons are still offered on a number of cryptomarkets and purchased by individuals. Through the consultation with law enforcement representatives and the review of a number of cases, either reported by the media or documented in law enforcement (or other governmental agency) press releases, the project team identified three different high-level contexts relevant to dark web-enabled arms trafficking: terrorism, organised crime and vulnerable or 'fixated people'. All these cases contain instances of individuals or groups, albeit with differing intents, that have purchased or sold firearms on the dark web or attempted to do so.

Study purpose, objectives and methodology

The overarching goal of this study is to provide law enforcement, policy and decision makers with an 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. In addition, the project team seeks to contribute to the wider body of academic research exploring cryptomarkets.

In the context described above, this study has seven objectives:

General objectives

1. To understand the modus operandi of buying and selling firearms and related products on the dark web.
2. To consider the viability of dark web markets for firearms selling, and more specifically, the extent to which these sellers may engage in scamming by taking payment for products they do not deliver, or may not possess.

Market analysis

3. To estimate the size and scope of the trade in firearms and related products on cryptomarkets, including:
    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.
4. To estimate the value of the trade in firearms and related products on cryptomarkets.
5. To identify shipping routes and most common shipping techniques.

Analysis of implications

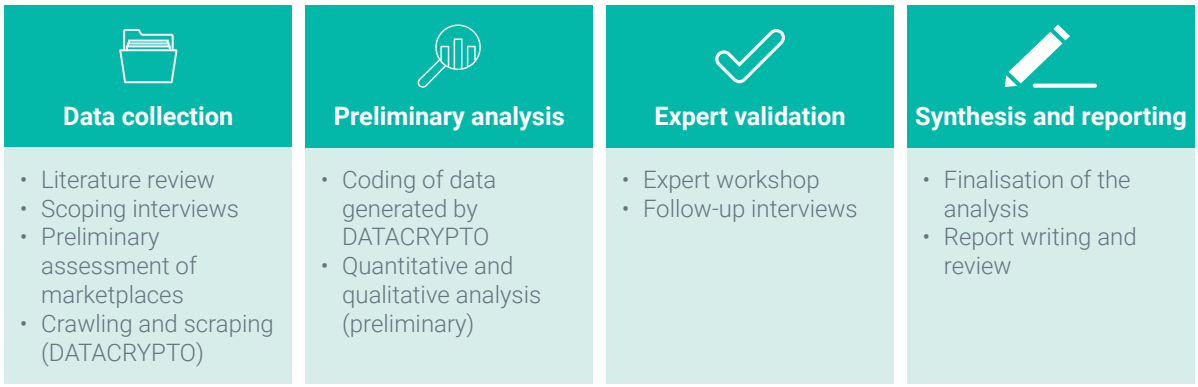
6. To identify the potential impact of dark-web enabled arms trafficking on the overall arms black market, with particular emphasis on market dynamics and market actors.
7. To identify the potential implications of dark web enabled arms trafficking for law enforcement agencies and policy makers, at both the national and international level, including implications for existing international legal instruments designed to tackle the issue of illegal arms trade and transnational organised crime.

To achieve these objectives, the project team employed a mixed-methods approach which included:

- Review of relevant literature including peer-reviewed academic literature, grey literature sources from official, government and other relevant organisations, and, particularly relevant for this study, web-sourced contributions from respected commentators and independent researchers within the darknet community.
- Review of darknet community clear web resources including websites used to identify marketplaces and provide information and commentary on recent developments related to cryptomarkets.
- Review of darknet community discussion forums to shed light on the question of scamming by firearms vendors.
- Preliminary investigation of cryptomarkets to identify those selling firearms. This included the identification of those having a dedicated product category as well as targeted searches to identify the presence of relevant listings in those cryptomarkets not having a dedicated product category.
- 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.
- Consultation with policy and law enforcement experts through an expert workshop and individual interviews.

Figure Ex.1 summarises the research approach for this study.

Figure Ex.1 Overview of the research approach



Limitations

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

- The data collection was conducted over 19–25 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 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 feedbacks (i.e. feedback is over-representing sales).
- Image analysis was not conducted on listed products, due to the inability to scrape images with 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 which 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 location 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: 1) size and scope (e.g. what is available on the market and in what quantities); 2) value (e.g. what are the dark web market prices of the products offered and how much is the dark web arms trade worth); 3) 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). This section summarises the main points emerging from the study related to these three pillars and their implications, mapping them to the study objectives.

General objectives

Objective 1: to understand the modus operandi of buying and selling firearms and related products on the dark web.

- 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. 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.

  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 specialised 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 finalised, the products purchased are normally shipped by post using special shipping techniques to minimise the risk of detection. In the context of firearms, these techniques often involve disassembling the weapon and shipping different parts in multiple packages.

Once the online part of the transaction is finalised, the products purchased are normally shipped by post using special shipping techniques to minimise the risk of detection.

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.

Objective 2: to consider the viability of dark web markets for firearms selling, and more specifically, the extent to which these sellers may engage in scamming by taking payment for products they do not deliver, or may not possess.

- There is contrasting evidence in relation to the prevalence of scamming in the context of firearms trade on cryptomarkets. While the general the perception among users is that vendors selling firearms are mostly scammers or law enforcement agencies, a number of recent cases suggest that real vendors also operate on cryptomarkets. The data available does not allow to determine in a rigorous way the extent to which scamming occurs.
- Analysing the metrics most commonly used by researchers to assess the probability of scamming, feedback ratings and life-span of listings, does not provide solid enough evidence to determine with confidence that listings for firearms and related products are mostly scams. For example, compared to drugs, the mean feedback for firearms is only marginally lower; in contrast, the mean feedback for ammunition is higher than the mean feedback for drugs. Looking at the life-span of listings, while it is true that firearms have the lowest life-span, in absolute terms the figures are comparable in scale and the difference in life-span may be due to the different nature of the products being sold.
- In conclusion, given the potential impact on security of even one weapon being sold through the dark web, the allegedly higher possibility of scamming should not be used as reason to dismiss or minimise the relevance of the issue. From a risk assessment perspective, as well as for policy making and operational planning purposes, it is recommended that, in absence of other sources of information, each listing and vendor are considered real while accepting that a portion of them may be scammers or law enforcement agencies.

Market analysis

Objective 3: to estimate the 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').
- 60 vendor accounts were identified for which firearms listings were held across all accessed markets. Using PGP 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 sub-machine guns. The

majority of firearms offered for sale are live weapons, with the exception of the sub-machine guns, where replicas are the majority. The condition of the firearm, new or used, does not appear as 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 permit the scale of dark web arms trafficking to be determined 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 firearms than what is normally accessible on the streets (despite the latter being, to a certain extent, country-specific).

> The use of cryptomarkets to sell weapons is marginal when compared to other product categories.

Objective 4: to estimate the 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 $80,000. The majority of both transactions and 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 both other products sold on cryptomarkets (e.g. Kruithof et al. [2016] estimated that drugs listings generated a total of monthly revenue of $14.2m) 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 as no robust estimates of the latter exist.
- Concerning the volume of monthly transactions, in 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 policy makers and law enforcement agencies.

Objective 5: to identify 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.

Implications and considerations

On the basis of the findings outlined above, and acknowledging both the limitations of our methodology and the potentially disruptive role played by scamming, it is possible to summarise the main implications and considerations as follows:

Objective 6: to identify the potential impact of dark web enabled arms trafficking on the overall arms 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 anonymising 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, removes also the majority of 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 organisations.

The United States appears as the dominating source country in terms of both number of listings and number of monthly transactions.

Objective 7: to identify the potential implications of dark web enabled arms trafficking for law enforcement agencies and policy makers, at both the national and international level, including implications for existing international legal instruments designed to tackle the issue of illegal arms trade and transnational organised crime.

- Law enforcement agencies are facing a series of operational challenges related to the main intervention strategies which exist to combat this problem. 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 policy-making community, both at the national and international level.

- At the national level, policy makers should ensure that the threat posed by illegal arms trafficking on the dark web is recognised and adequate resources are mobilised to ensure that law enforcement agencies are staffed, trained and equipped to respond effectively. In addition, policy makers 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 existing international instruments designed to tackle the general issue of arms trafficking. These instruments provide a range of control measures to limit the diversion of legally owned firearms to the black market and to trace illegal firearms back to the last known legal owner, providing an investigative lead into the point of diversion.
- 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 which may require updating or further development.
- Based on the analysis of the international legal framework conducted by UNODC (attached to this report), it appears that key international legal instruments such as the Organised Crime Convention, the Firearms Protocol and the ATT 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 (e.g. the US) are not yet State Parties to the instruments identified, limit the extent to which tools and measures provided by such instruments can be used in practice.

Final remarks

This study has demonstrated that significant value can be obtained by using empirical analysis methodologies to investigate dark web-enabled arms trafficking. Taking into account the caveats and limitations described throughout the report, this study represents the first systematic, evidence-based assessment of the trafficking in firearms (including their parts, components, accessories and ammunition) and explosives. However, based on the observations above, further research is necessary to further develop the understanding of the market characteristics (e.g. 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, more continuous monitoring activity should be undertaken. 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.

Acknowledgements

This report would not have been completed without the support of many organisations and individuals. We are grateful to the UK Partnership for Conflict, Crime and Security Research (PaCCS) for providing sponsorship of the study and in particular to Dr Tristram Riley-Smith for his continuous support.

We would like to express our gratitude to Simonetta Grassi and Mareike Buettner at the UNODC for contributing to the study through the authorship of an independent analysis of the international legal framework (attached as an annex to this report), and for their support in increasing the impact and visibility of this study through the organisation of two events in Vienna on the occasion of the Eighth Session of the Conference of the Parties to the UN Convention against Transnational Organized Crime (October 2016) and the 26th Session of the Commission on Crime Prevention and Criminal Justice (May 2017).

We are also particularly grateful to the UK Home Office, The UK National Crime Agency and the London Metropolitan Police for their expert input. In particular we would like to thank Steve Welsh from the National Crime Agency (Behaviour & Disruption, Intelligence Directorate – Commodities) and Nicholas Gray from the Home Office (Drugs & Firearms Policy, Strategic Centre for Organised Crime – Office for Security and Counter-Terrorism) for their intellectual contribution throughout the study and their support in the organisation of a very successful expert workshop (March 2017).

We would also like to acknowledge the support of David Décary-Hétu (University of Montreal) for his support with the primary data collection from cryptomarkets. Finally, we are very grateful to our senior quality assurance reviewers, Alexandra Hall and Stijn Hoorens, for their constructive feedback.

Abbreviations

AFP	Australian Federal Police
ATF	US Bureau of Alcohol, Tobacco, Firearms and Explosives
ATT	Arms Trade Treaty
B2C	Business-to-Consumer
BBC	British Broadcasting Corporation
BKA	German Federal Police (*Bundeskriminalamt*)
BMR	Black Market Reloaded
CCTV	Closed-circuit television
CEO	Chief Executive Officer
DHS	US Department of Homeland Security
DPR	Dread Pirate Roberts
EO	Executive Outcomes
EU	European Union
FBI	US Federal Bureau of Investigation
FE	Finalise early
FFLs	Federal Firearms Licensees
GFP	German Federal Police
ICT	Information Communication Technology
IP	Internet Protocol
IT	Information Technology
ISACS	International Small Arms Control Standards
ITU	International Telecommunication Union
MSRP	Manufacturer's Suggested Retail Price

NCA	UK National Crime Agency
PaCCS	Partnership for Conflict, Crime and Security Research
PGP	Pretty Good Privacy
PSNI	Police Service of Northern Ireland
RRP	Recommended Retail Price
SDG	Sustainable Development Goal
SHA512	Secure Hash Algorithm 512
SR1	Silk Road
TV	Television
UN	United Nations
UNGA	United Nations General Assembly
UNODC	United Nations Office for Drugs and Crime
URL	Uniform Resource Locator

1 Introduction

'[Lyburd] said buying the Glock was like 'buying a bar of chocolate'.'

Report on Liam Lyburd (18), who plotted a massacre at his former school in Newcastle.
BBC News, 30 July 2015

'[Mr 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

There is an ongoing debate over the extent to which online black markets on the so-called 'dark web'[1] facilitate the sale of firearms, weapons, explosives and banned digital materials. Public details have emerged in the media following the 2016 Munich shooting linking the weapons used by the attackers to vendors on dark web 'cryptomarkets'[2]; 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 November 2015 Paris terrorist attacks.[3] Despite a perceived high level of concern in European communities following the attacks,[4] 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

1 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 2.1.

2 A cryptomarket is defined as '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)

3 See, for example, Bender and Alessi (2016) and HNGN (2015).

4 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 darknet 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).

of weapons on cryptomarkets from an empirical research perspective.[5] 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.

1.1. The emergence of the weapons trade on the dark web and reported cases

The trade of firearms and weapons over the dark web emerged with the first cryptomarket, the Silk Road (SR1).[6] The cryptomarket's founding administrator – using the pseudonym Dread Pirate Roberts (DPR) – initially limited SR1's terms of service to preclude the sale of items or procurement of services causing third-party harms, effectively banning 'anything who's [sic] purpose is to harm or defraud, such as stolen credit cards, assassinations, and weapons of mass destruction.'[7] Approximately 12 months after opening SR1 in February 2011, 'The Armory' was spun off by DPR to enable vendors to list 'guns, ammo [and] explosives' on a separate cryptomarket, away from the illicit narcotics trade on SR1.[8] The trade of weapons over cryptomarkets caused widespread concern among the 'darknet community'[9] – long before public concern and prosecutions by law enforcement agencies – due to the increased attention from law enforcement agencies, the product category's high value and susceptibility to scamming, and the ability of weapons to inflict harm on third parties, counter to the libertarian value of harm reduction held by early crypto-anarchists.[10]

The rise of scamming, heightened policing and low volume of weapons sales on the dark web has spread caution in the darknet community, if not widespread doubt,[11] about the viability of using cryptomarkets and 'single-vendor shops'[12] to buy weapons on the dark web. Yet, recent cases documented by governmental agencies or reported by the media (see below for more details) suggest that dark web arms trafficking is a real phenomenon. Today, weapons are still offered on a number of cryptomarkets (11 of those identified by this study– Table 3.2). For a detailed account of the history of weapons trade on the dark web, see Appendix B.

Through consultation with law enforcement representatives and review of a number of cases, either reported by the media or documented in law enforcement (or other governmental agency) press releases, the project team identified three different high-level contexts relevant to dark web-enabled arms trafficking: terrorism, organised crime and

5 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 2011–13 research from Silk Road (SR1), which 'does not include any entry relating to them' (cited in Hullinger 2016).

6 Chen (2012).

7 Chen (2011).

8 Biddle (2012).

9 The darknet community refers to the administrators and users actively involved in the configuration, moderation and use of cryptomarkets and associated forums related to the dark web.

10 Munksgaard & Demant (2016).

11 Hullinger (2016); Vitáris (2016a).

12 Single-vendor shops are administered by one vendor, typically in a niche market, and may not offer escrow, customer feedback or dispute resolution services, which are often provided by cryptomarkets. See section 2.2 for a detailed definition of single-vendor shops.

> All these cases contain instances of individuals or groups, albeit with differing intents, that have purchased or sold firearms on the dark web, or have attempted to do so.

vulnerable or 'fixated' people.[13] All these cases contain instances of individuals or groups, albeit with differing intents, that have purchased or sold firearms on the dark web, or have attempted to do so. Some examples for each category are provided below, while more are available in Appendix C.

Terrorism

In the absence of any official public statement by the authorities, a lot of uncertainty still persists around how the terrorists involved in the November 2015 Paris attacks gained access to the assault rifles that were used. One theory emerged two weeks after the attacks, on 27 November 2015, when a man was arrested in Germany on suspicion of conducting illegal arms trafficking on the dark web, including of non-lethal weapons converted to fire live ammunition. On the same day the German newspaper *Bild*, on the basis of investigative documentation it claimed to possess, reported that the same dealer sold, on 6 November, the four assault rifles that were used in the attacks.[14] This theory, which was picked up and rapidly distributed by several international news agencies and media outlets, has yet to be confirmed by relevant authorities and remains, to date, an unconfirmed conjecture. However, whether or not this modus operandi will be confirmed in relation to Paris, this case highlighted the possibility of the dark web being used by terrorists to procure weapons.

Another case, which bridges the category of political extremism-inspired terrorism and that of vulnerable or fixated individuals, relates to the 18-year-old David Ali Sonboly, who, on 22 July 2016, shot and killed nine people at the Olympia Shopping Centre in Munich, Germany, before killing himself.[15] He appeared to be deliberately targeting teenagers and young people of Turkish or North African origin and was reported to be inspired by the 2011 Norway attack by far-right extremist Anders Breivik.[16] Sonboly, of Iranian background, was reported to suffer from depression and was receiving treatment for mental conditions.[17] One source reported that investigations by the German Federal Police (*Bundeskriminalamt* or BKA) identified that he had obtained the Glock 17 automatic pistol and 250 rounds of 9 mm ammunition from the dark web.[18] It is believed the handgun was a re-activated pistol, which had previously been used as a theatre prop. The weapon's provenance is difficult to trace since its serial number was removed; however, it is believed to have originated in Slovakia. Having identified that Sonboly visited Marburg, Germany, twice before the attack, the BKA managed to identify the dark web vendor and ran a 'sting' operation with undercover officers. Once arrested, the vendor became fully cooperative with the Federal Police, leading them

13 The term 'fixated' has been defined by Mullen et al. (2009) in a forensic psychiatry and psychology context to describe those people with 'an intense preoccupation with an individual, activity or idea.'

14 Solms-Laubach (2015); Huggler (2015); Vitáris (2015).

15 BBC News (2016).

16 Rothwell et al. (2016).

17 Rothwell et al. (2016).

18 Bender & Alessi (2016).

to a hidden weapons cache where they further recovered a sub-machine gun, four semi-automatic pistols and a quantity of ammunition.[19]

Crime

In a press release published on 31 May 2017 by the US DOJ (Department of Justice) Attorney's Office, Northern District of Georgia, details emerge of how four men[20] used dark web cryptomarkets to sell firearms to countries worldwide.[21] Using the pseudonyms 'CherryFlavor' and 'Worldwide Arms', the organised crime gang in Georgia, US, shipped over 50 parcels containing firearms hidden inside electronic goods. The gang had been acquiring firearms legally from the OutDoorTrader website and reselling them on cryptomarkets in order to circumvent federal firearm laws.[22]

Investigations by the US Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and other agencies began in June 2013, approximately four months prior to the arrest of DPR. The CherryFlavor group operated on the cryptomarkets Utopia and Black Market Reloaded (BMR), which experienced an influx of users after the shutdown of SR1 in October 2013, and Agora Market, which similarly received displaced users after Operation Onymous in November 2014.[23] A combination of methods led to the identification of the crime gang. Federal search warrants, coupled with trace interviews, showed the original purchases of the weapons were in the Atlanta area. Intelligence analysis and a massive international postal audit with 11 partner countries[24] involving several suspected US Post Offices, resulted in the identification of the CherryFlavor gang. Two of the men arrested have since entered guilty pleas before a federal grand jury, on 3 May 2017.[25]

> Using the pseudonyms 'CherryFlavor' and 'Worldwide Arms', the organised crime gang in Georgia, US, shipped over 50 parcels containing firearms hidden inside electronic goods.

Vulnerable or fixated individuals

During September 2015, Liam Lyburd, a teenager from Newcastle, UK, was allegedly planning an active shooter attack to massacre his former classmates at Newcastle College. The police were tipped off by a friend about Lyburd's messages on Facebook under the pseudonym 'Felix Burns', which hinted at his plans. As a result, they raided his home address and discovered a Glock semi-automatic pistol and nearly a hundred rounds of 'hollow-point' expanding ammunition. According to the British Broadcasting Corporation (BBC), the weapon had been obtained from the dark web,[26] on

19 Callimachi et al. (2016).

20 The indictment contains charges against Mr Sherman Jackson, Mr Brendan Person, Mr Gerren Johnson of Atlanta, Georgia and Mr William Jackson of East Point, Georgia.

21 US DOJ (2017a).

22 US DOJ (2017a).

23 Décary-Hétu & Giommoni (2016).

24 Countries involved in the massive international postal audit were Austria, Australia, Belgium, Canada, the United Kingdom, Ireland, Denmark, France, Germany, the Netherlands and Sweden.

25 US DOJ (2017a).

26 BBC News (2015).

the cryptomarket 'Evolution'.[27] He had also prepared a so-called 'kill bag' which contained home-made pipe bombs, boots, overalls and a mask. Lyburd was found guilty of plotting multiple murders at his former college and given a life sentence.[28] He described purchasing the Glock as 'like buying a bar of chocolate'.[29]

As the recent examples from the contexts of terrorism, crime and mental health demonstrate, the threat to community safety posed by individuals or groups is documented, evident and real. Similarly, the successful purchase of weapons using cryptomarkets has been an enabler for illegal activity in all the cases reviewed.

1.2. Objectives and overview of the methodology

As described above, anecdotal evidence and media reports suggest that firearms trafficking on the dark web is a real phenomenon, despite the presence of scamming and law enforcement sting operations.[30] However, limited systematic research exists to empirically substantiate such claims. This is particularly due to the lack of evidence-based appreciation of the scale, scope and volume of the illegal trade of weapons on the dark web.

The overarching goal of this study is to provide law enforcement agencies and policy and decision makers with an 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. In addition, the project team seeks to contribute

The overarching goal of this study is to provide law enforcement agencies and policy and decision makers with an evidence-based understanding of arms trafficking on the dark web.

to the wider academic research exploring cryptomarkets.

In the context described above, this study has seven objectives:

General objectives

1. To understand the modus operandi of buying and selling firearms and related products on the dark web.
2. To consider the viability of dark web markets for firearms selling, and more specifically, the extent to which these sellers may engage in scamming by taking payment for products they do not deliver, or may not possess.

Market analysis

3. To estimate the size and scope of the trade in firearms and related products on cryptomarkets, including:
    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.

27 Nichol (2015).

28 Gayle (2015).

29 BBC News (2015).

30 See Appendix B for the cases involving scamming on 'The Armory' and the speculation over the vendor account 'weaponsguy' being 'flipped' by US law enforcement agencies.

4. To estimate the value of the trade in firearms and related products on cryptomarkets.
5. To identify shipping routes and most common shipping techniques.

Analysis of implications

6. To identify the potential impact of dark-web enabled arms trafficking on the overall arms black market, with particular emphasis on market dynamics and market actors.
7. To identify the potential implications of dark web enabled arms trafficking for law enforcement agencies and policy makers, at both the national and international level, including implications for those already existing international legal instruments designed to tackle the issue of illegal arms trade and transnational organised crime.

To achieve these objectives, the project team employed a mixed-methods approach which included:

- **Review of relevant literature** including peer-reviewed academic literature, grey literature sources from official, government and other relevant organisations, and, particularly relevant for this study, web-sourced contributions from respected commentators and independent researchers within the darknet community.
- **Review of darknet community clear web resources** including websites used to identify marketplaces and provide information and commentary on recent developments related to cryptomarkets.
- **Review of darknet community discussion forums** to shed light on the question of scamming by firearms vendors.
- **Preliminary investigation** of cryptomarkets to identify those selling firearms. This included the identification of those having a dedicated product category as well as targeted searches to identify the presence of relevant listings in those cryptomarkets not having a dedicated product category.
- **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.[31]
- **Consultation with policy and law enforcement experts** through an expert workshop and individual interviews.[32]

Figure 1.1 summarises the research approach for this study.

More information on the methodology, and related caveats, used to collect and analyse primary data from the dark web is provided in relevant sections throughout the report. The following paragraphs provide further information on the other methodologies used in this study.

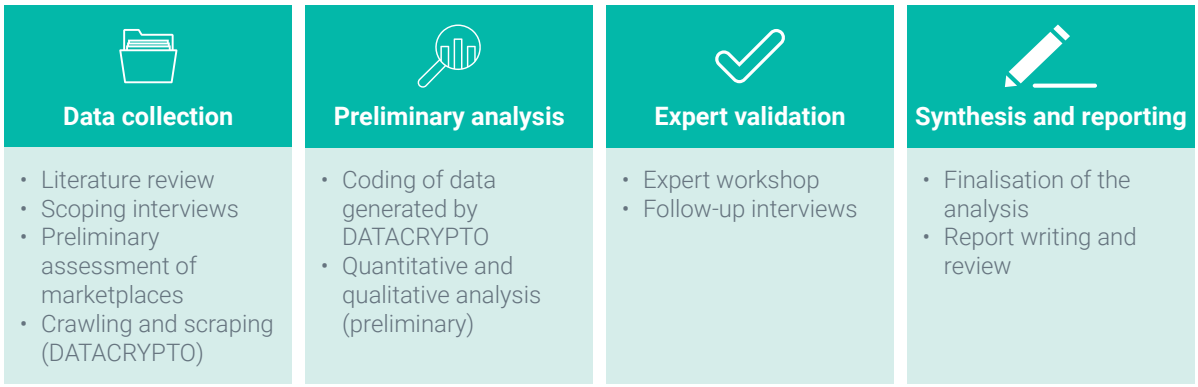
Literature review

The review of available academic literature was conducted in two different phases of the project. Initially, academic literature on the topic of cryptomarkets was consulted (i) to guide the framing of the problem and develop an initial understanding of the 'mechanics' of cryptomarkets; and (ii) to inform an initial assessment of

31 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. More information on DATACRYPTO is provided in Box 3.1.

32 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.

Figure 1.1 Overview of the research approach



the viability of cryptomarkets for arms trafficking based on existing research investigating the drugs trade on the same platforms.

On the basis of the preliminary findings from primary data and as a result of expert consultation, the project team also consulted additional academic literature specialised in the field of arms control in order to support the interpretation of the results and the rigour of the analysis.

In addition to academic literature, grey literature and media reports were also consulted throughout the project to capture as much information as possible on cases of arms trafficking involving the dark web. Priority was given to sources from prosecution files or court cases (including press releases), and when these were not available the study team consulted media sources, discussion forums and specialised blogs. These sources were then analysed longitudinally to extract information on the following elements: what weapons were purchased or sold, by whom and in what context, how the transaction took place and what type of intervention/response was implemented. The information collected was then used by the project team to complement (by challenging or corroborating) the results emerging from the dark web data in relation to the type of firearms being sold and the modus operandi.

Expert engagement through interviews and workshop

The project team consulted a range of experts throughout the study. At the onset of the study, before the analysis of the primary data, the project team conducted a series of scoping interviews with representatives of law enforcement agencies (3), policy makers (3) and a cryptomarket experts (1). These interviews were particularly relevant to complement the (limited) information available in the literature about dark web arms trafficking, allowing for a better framing of the problem and providing a direction for the initial analysis. The interviews with law enforcement agencies and policy makers were semi-structured and developed around the exploration of four main themes: how serious is the issue of dark web-enabled arms trafficking; how has it changed the arms trafficking picture (e.g. both in terms of people and merchandise); what type of responses are available; and what are the main challenges. The interview with the dark web expert was used to obtain an initial appreciation on the viability of the dark web firearms trafficking, including a preliminary assessment of scamming, and guidance on locating some dark web sites, particularly single-vendor shops.

After a preliminary analysis of the primary data, an expert workshop was organised to solicit

expert feedback on the validity of the analytical approach, on the nature of the results and on the potential implications. The workshop counted 16 external participants including, in addition to the project team, three representatives from the policy-making sphere, two academic experts, two representatives of regional law enforcement agencies and nine representatives of different national law enforcement agencies. The notes of the workshop were taken in accordance to the Chatham House Rule and further analysed by the project team. An agenda of the workshop can be found in Appendix E.

A final round of interviews (3) was conducted to further investigate specific themes that emerged from the workshop (e.g. scamming, conversion of non-lethal weapons and overarching policy implications).

1.3. Structure of the report

This introductory chapter provides the study context as well as an overview of the specific objectives. Chapter 2 provides an introduction to the dark web and associated terminology, and describes how it can be used to facilitate illegal trading in firearms, weapons and explosives. Chapters 3–5 include a detailed analysis of the findings of the study structured according to three main themes: size and scope, value, and shipping routes and techniques. Chapter 6 presents an overview of the overarching implications emerging from the analysis. Finally, Chapter 7 provides some overarching conclusions and a description of the way forward.

Annexed to this report is an analysis of the relevant international legal framework prepared by the Global Firearms Programme of the United Nations Office for Drugs and Crime (UNODC).

Finally, the report is complemented by a series of appendices providing the reader with further information on the following topics:

- Terminology (Appendix A).
- A brief history of firearms on the dark web (Appendix B).
- A review of open-source documents and media reports on recent cases involving firearms purchased or sold over the dark web (Appendix C).
- A breakdown of firearm makes offered on the dark web identified during the data collection (Appendix D).
- Expert workshop agenda (Appendix E).

2 How dark web markets function to facilitate illegal trading

2.1. What is the dark web?

The 'dark web' is a section of the internet not accessible to the everyday user. Armed with the correct software package and possession of a known dark web address, navigating to the dark web becomes as simple as surfing the internet. Anonymising software packages (e.g. Tor and I2P) enable users to hide their unique Internet protocol (IP) address while using applications to securely browse 'darknets'.[33] The term 'darknet community' is used throughout the report to refer to the group of networked individuals who are technically savvy and who participate in online discussion forms, both on the clear and deep webs (see Box 2.1).

> Armed with the correct software package and possession of a known dark web address, navigating to the dark web becomes as simple as surfing the internet.

There are a number of technical configurations a user can implement, test and monitor to anonymously browse the dark web to ensure a higher level of identity protection. Technical vulnerabilities are exploited by law enforcement agencies, sometimes with the assistance of university researchers,[34] in an attempt to de-anonymise users of the dark web, in particular on cryptomarkets.[35]

2.2. Types of marketplaces on the dark web

Hidden services are enabled by anonymity software; the most commonly used is Tor.[36] Tor anonymises internet users' IP addresses, and so makes it difficult to trace internet activity back to users. Illegal trading is enabled by technologies that allow buyers and sellers to interact and transact with near anonymity.[37] Dark web markets enable payment

33 In computer networking, 'darknets' are the technical term for an overlay network that can only be accessed with specific software, such as Tor and I2P. By using a combination of non-standard protocols and ports, with cryptographic controls to encrypt messages, users can communicate with anonymity (i.e. without revealing their unique IP address) and security (i.e. even if the traffic is intercepted, it cannot be read by a third party).

34 Cox (2016a).

35 Greenwald (2013).

36 Lewman (2016).

37 Barratt et al. (2017).

Box 2.1 A model of the clear web, deep web and 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 and DuckDuckGo) 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, for example 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 and it requires specific software packages to navigate. The Tor network enables access to the dark web – otherwise known as 'hidden services' – while concealing the user's identity and online activity from surveillance and traffic analysis. Entry points into the dark web can be found on the clear web through traditional search engines. These entry points make the dark web more accessible to the public than deep the web by providing URLs of dark websites.

Accessing and browsing the dark web is not illegal per se as the illegality is focused more on its use: for example, it is illegal to view, share and download illegal content (e.g. child pornography and pirated content) hosted on the dark web. A common way of illustrating the nature of the web is through the visual representation below (see Figure 2.1).

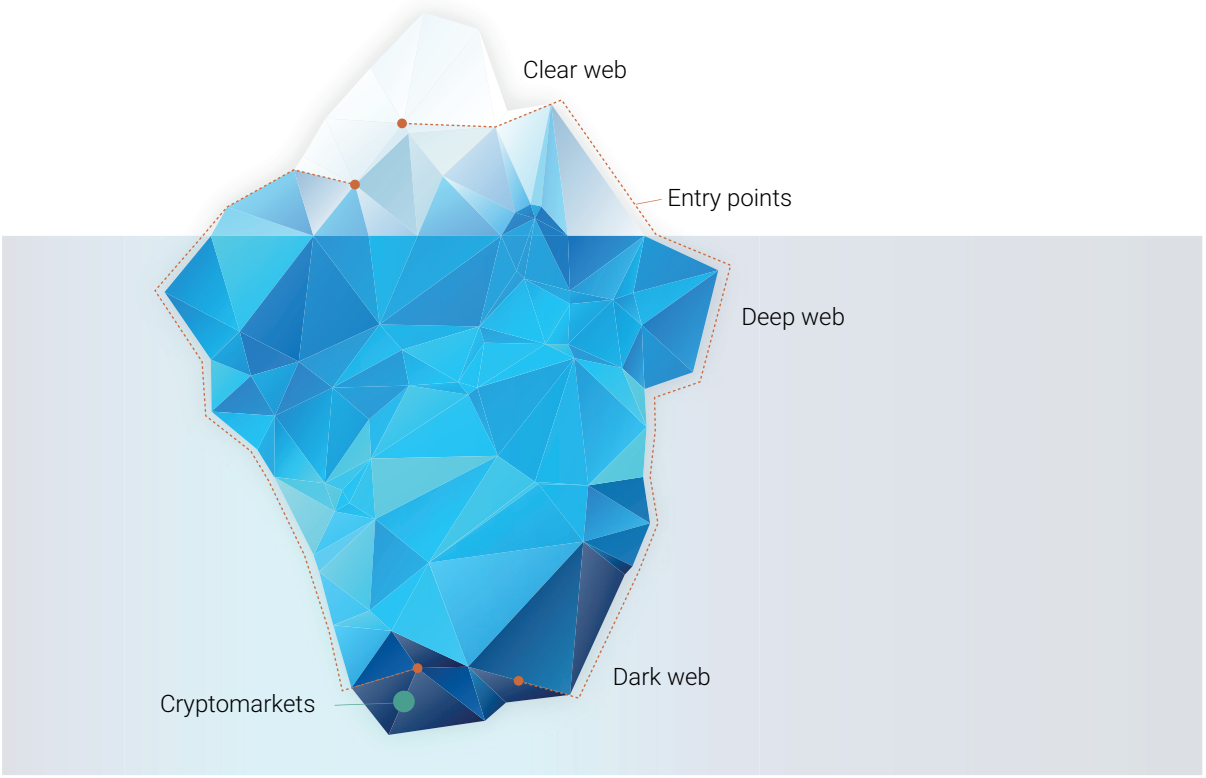
with cryptocurrencies (e.g. Bitcoin, Litecoin, Monero) so transactions are obfuscated and difficult to trace. The combination of anonymising technology and use of cryptocurrencies for payment obscures the link between real-world identities and the personas adopted on dark web marketplaces. These two technologies enable the trade of illegal goods and services, effectively in plain sight of law enforcement.

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

1. **Cryptomarkets** bring together multiple sellers, known as 'vendors', managed by marketplace administrators in return for a commission on sales, leading to comparisons with similar clear web legal markets like eBay or Amazon's marketplace.[38] 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

38 Barratt (2012).

Figure 2.1 The location of clear, deep and dark webs, and cryptomarkets



customers in selecting reliable vendors and highly rated products. Cryptomarkets tend to specialise foremost in illegal drugs[39] but also offer listings connected to fraudulent activities, including stolen credit card and identity information.[40] Other product types, firearms being one example, are less commonly available for sale.

2. **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, they can avoid the commissions on their sales charged by cryptomarkets and avoid the financial risk entailed by cryptomarket 'exit scams'.[41] Vendor shops specialise in particular products or services, and often trade on reputation track records earned via cryptomarket selling to generate customer trust. Many vendor shop owners trade simultaneously on cryptomarkets.

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

39 Aldridge & Décary-Hétu (2014); Christin (2013).

40 Kruithof et al. (2016).

41 'Exit scams' are executed by marketplace administrators when absconding with the funds held in user accounts and escrow services.

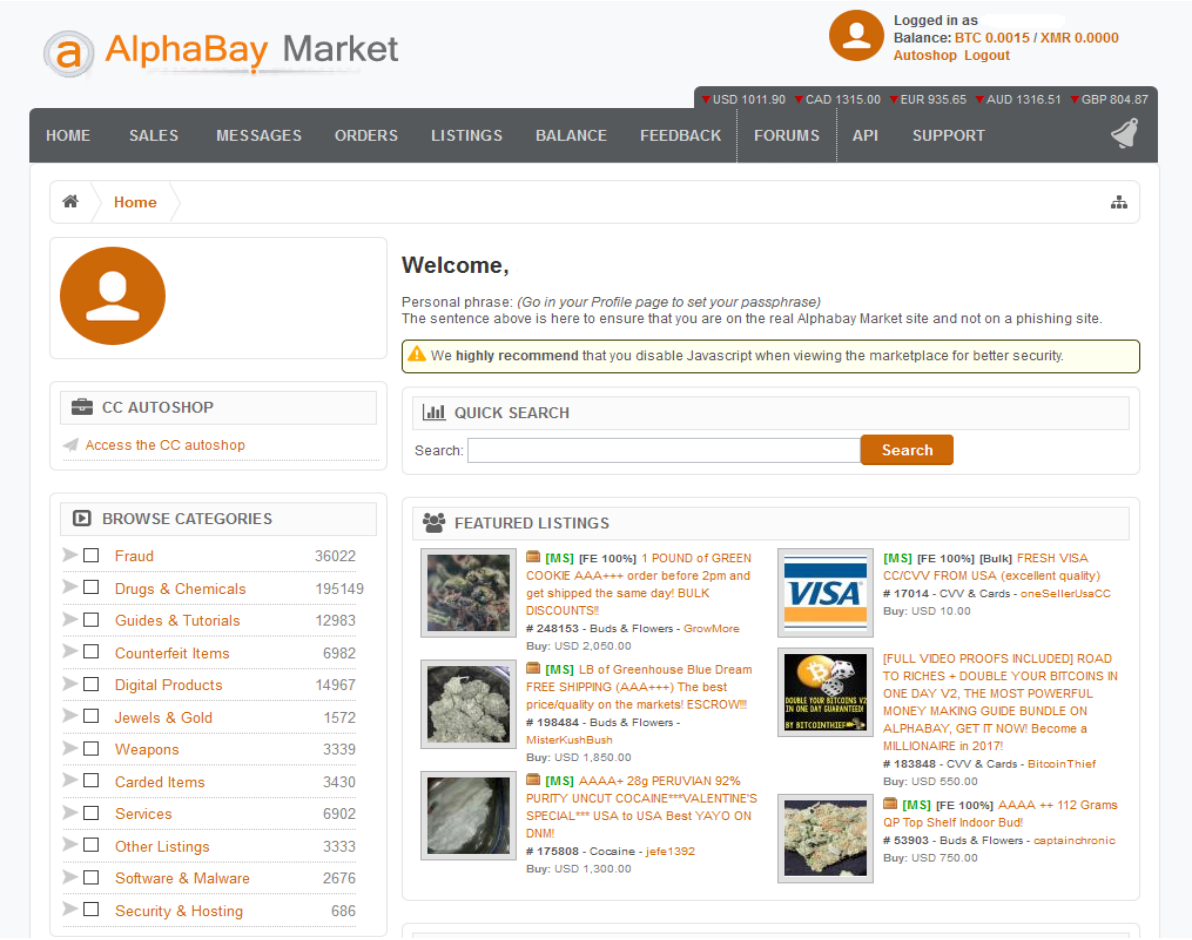
2.3. Appearance and services

2.3.1. Cryptomarkets

Cryptomarkets look similar to legal online marketplaces like eBay or Amazon. Customers typically must set up accounts to view the marketplace, and once logged in, access the homepage (see Figure 2.2). Marketplaces have a set of pre-defined categories into which sellers, known as 'vendors', can categorise 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 3), the markets that stock weapons often provide a unique category, such as that used by Alphabay and shown in Figure 2.2 below. Customers can also use a search facility to identify relevant listings.

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's community. Sections typically include: guides for vendors and customers on using

Figure 2.2 Screenshot of the homepage for the Alphabay cryptomarket



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

the marketplace, discussion connected to the products typically sold on cryptomarkets (e.g. drugs, fraud and weapons), discussion connected to minimising 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.

Dark web markets' users 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-anonymisation. Some vendors encourage or require direct messaging using PGP ('Pretty Good Privacy') software that provides end-to-end cryptographic privacy and authentication.[42] Use of encrypted communication was less common on the first cryptomarket, SR1, but external hacks leading to de-anonymisation have seen increases in the use of PGP since.[43]

Cryptomarkets generally have sections on their sites listing rules for vendors and buyers related to transaction and associated security measures. Researchers documenting these rules on ten cryptomarkets early in 2016 found that seven of the ten had such rules.44 Five marketplaces did not allow vendors to request that customers 'finalise early' (FE) (i.e. circumvent escrow) or allowed this only to those 'approved' to do so. Two marketplaces stated that too many customer reports of vendor scamming would result in the vendor's account being deactivated. One marketplace described systems to prevent marketplace exit scams. Some marketplaces had stated rules against blackmailing, or 'doxxing',[45] customers. Three marketplaces explicitly encouraged participants to use security and encryption practices, with one stating that marketplace adjudication would be unavailable to participants not employing such practices.

2.3.2. Vendor shops

Vendor shops, by comparison, generally have a much simpler visual interface, in common with many legal online shops set up by individuals or businesses to sell their own products and services. A screenshot example of the vendor shop Black Market Guns is provided in Figure 2.3 below. Because vendor shops host sole-trading vendors who specialise in particular products, these markets have fewer listings when compared with cryptomarkets.

While some vendor shops categorise their listings in a way similar to cryptomarkets, others list all their products on the shop's homepage. 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

42 Cox (2016b).

43 Aldridge & Askew (2017); Soska & Christin (2015).

44 Kruithof et al. (2016).

45 Doxxing (also spelled 'doxing') is the practice of releasing personal and private information, including home addresses and national identity numbers, against the person's wishes. (Barratt & Aldridge, 2016)

Figure 2.3 Screenshot of the homepage for the Black Market Guns vendor shop

information, and sometimes frequently asked questions.

2.4. Buying and selling on dark web markets

2.4.1. Finding dark web markets

Web pages located on the dark web, in contrast, are not indexed by clear web search engines like Google, and so – by design – cannot be identified this way.[46] To access a dark web market, therefore, customers must already know of the existence of the market and have its URL (Uniform Resource Locator).[47]

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. The defining feature of dark web URLs is the '.onion' suffix (i.e. similar to a '.com' and '.org' website address), which signifies the special-use domain of the Tor network. Users must therefore first locate the market's URL on the clear net, and then copy and paste the link into a suitable dark web browser.

One such aggregator of dark web markets is found at Deepdotweb.com. The frequently updated market list[48] is regarded in the darknet

46 Barratt et al. (2017).

47 Barratt & Aldridge (2016).

48 Deepdotweb (2017d).

For potential buyers, finding cryptomarkets is easier, in relative terms, than identifying a reliable and trusted vendor to purchase goods from.

community as the best single-source location for market information.[49]

The dark web market search engine 'Grams' was developed in 2014. It has been labelled the 'new Google' for the dark web, making 'buying dope and guns easy'.[50] After navigating to the Grams dark web URL, users may search for specific products across markets using relevant search terms. Then, Grams users can click resulting links to be taken directly to the cryptomarket. Presently, Grams only searches and links to some cryptomarkets and no single-vendor shops can be accessed in this way.

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 SR1, customer and vendor trust has been challenged more as a result of fraud by marketplace owners than by law enforcement takedowns.[51]

'Exit scams' by marketplace owners involve administrators locking escrow services, vendor and customer accounts without prior notice, and then shutting down the market and absconding with substantial sums of virtual currencies (such as Bitcoin and Litecoin).[52] A 2016 investigation by independent security researcher Gwern Branwen on dark web market closures reported that, where the reason for closure was known (77 markets), the most common reason (for 35 markets – 40 per cent) involved exit scams, and only seven closures resulted from law enforcement efforts.[53] The now known possibility of cryptomarket exit scams may in part account for the recent increase in the number of vendors setting up sole-trading vendor shops to reduce this risk.

With exit scams now a possibility that must be considered when selecting a market, buyers and vendors make use of clear web resources to inform their selection.[54] For example, Deepdotweb accepts reviews connected to dark web markets, which are aggregated and displayed to visitors. In addition to providing customers with hidden market URLs, Deepdotweb's 'Dark Net Markets Comparison Chart'[55] assembles relevant metrics to guide market selection. These include market review scores from users submitted via Deepdotweb, percentage uptime, reports of security issues and warnings, and market longevity. For vendors, relevant comparison chart metrics might guide their selection of markets on which to sell their products. For instance, the comparison table lists cryptomarkets' commission charge, the cost of the 'vendor bond' (i.e. the charge for setting up a vendor account), and escrow services provided by the marketplace.

---

49 For example, the Grams dark web search engine 'Market Comparison' page refers its users to Deepdotweb's list as even 'more detailed and up to date' than its own list (Grams 2017).

50 Zetter (2014).

51 Zetter (2013); Aldridge & Décary-Hétu (2016a).

52 Tzanetakis et al. (2015).

53 Reasons documented by Branwen (2013) for market closure: (i) shut down due to law enforcement; (ii) precipitated by a hack or de-anonymisation; (iii) a scam/theft by operators; (iv) voluntary (without known losses to users).

54 Tzanetakis et al. (2015).

55 Deepdotweb (2017a).

2.5. Establishing trust: how buyers and sellers choose one another

This section outlines how trust is fostered and encouraged on cryptomarkets between parties who never reveal their true identities. The study team draws on recently published literature by Tzanetakis et al. (2015), who provide a detailed explanation of building trust and resolving disputes on cryptomarkets, as well as Morselli et al (2017)., who investigated conflict management on cryptomarkets.

2.5.1. How buyers choose vendors

When selecting a vendor from which to make a purchase, cryptomarket buyers can be guided by the reputations that vendors accrue directly on the marketplace in connection to feedback provided by previous customers. After receiving an order, buyers are offered the opportunity to leave feedback for the vendor, and cryptomarkets aggregate and display these vendor reputation metrics, in a similar way to legal clear net marketplaces.[56] Marketplace administrators and vendors strongly encourage this practice, and research suggests that a majority of transactions – 88 per cent on SR1 in 2013 – result in customer feedback, although more recent estimates (71 per cent in January 2016) suggest feedback rates may be decreasing.[57]

Customer feedback does not represent a perfect guide for buyers in identifying reliable vendors. Feedback can be manipulated by vendors, who can create fake customer accounts through which to make purchases from themselves, thereby generating false feedback. Marketplace administrators generally have rules prohibiting this, and strategies to detect suspicious activities, but the practice cannot be eliminated.[58] Buyers can also consult the 'scam reports' sections of marketplace discussion forums, which alert them to vendors with unresolved or confirmed accusations of scamming. In the context of firearms vendors operating on cryptomarkets, the low volume of sales – compared to the high volume of sales by drug vendors – yields a reduced opportunity to solicit feedback from buyers.

> Feedback can be manipulated by vendors, who can create fake customer accounts through which to make purchases from themselves.

Scamming vendors reduce the profits generated by marketplaces that result from commissions, and reflect badly on the marketplace's reputation – and therefore the confidence of buyers in that marketplace.[59] Cryptomarket administrators, alongside a dedicated 'scam-watch team' comprising active cryptomarket community members, investigate claims of vendor scamming. Participants have multiple channels of resolving conflict, either privately on secure messaging platforms or more publically on forums. Administrators have the final word in dispute resolution, which is often expressed as 'policy in action' when they enforce the rules of the cryptomarket.[60]

Clear web discussion forums (e.g. Reddit's /r/Darknet and /r/DarkNetMarkets) and active

56 Tzanetakis et al. (2015).

57 Aldridge & Décary-Hétu (2014); Kruithof et al. (2016).

58 Deepdotweb (2017b).

59 Morselli et al. (2017).

60 Morselli et al. (2017).

> Buyers wishing to make purchases from vendor shops have less information to guide them in choosing a reliable vendor.

cryptomarket clear web subreddits (e.g. /r/AlphaBay and /r/ValhallaMarketplace/) can be consulted by buyers to identify trusted and reliable vendors, or to avoid suspected scammers and vendor accounts compromised by law enforcement agencies.[61] Reddit's darknet-relevant subreddits involve posters airing disputes as well as satisfactory transactions with named vendors, and Deepdotweb's review service offers similar crowd-sourced insights.

Buyers wishing to make purchases from vendor shops have less information to guide them in choosing a reliable vendor. Vendors operating sole-trader shops will not benefit from the third-partyvendor reputation metrics generated automatically on cryptomarkets in connection to that vendor's entire transaction history. While vendor shop owners may post testimonials from 'satisfied customers' on their websites, no third-party oversight is in place to prevent the exclusion of negative reviews, or indeed entirely fabricated reviews. However, because many vendors set up vendor shops trade on reputations earned on cryptomarkets – where many, but not all,[62] will continue to trade – buyers considering the possibility of transacting with vendor shops may be able to consult cryptomarket-generated vendor reputation metrics, where possible.

While some vendor shops refer to providing escrow services, the project team was unable to determine the veracity of these claims. Escrow is, by definition, a third-party service, and the project team was unable to identify any independent escrow services that serve illegal marketplaces. Vendor shops promising escrow-protected payments may, therefore, be scammers seeking to lure unwary customers.

> Buyers valuing good customer service in risky illegal markets may select vendors whose listings reflect this orientation.

Researchers have suggested that cryptomarket trading may provide a context for illegal market trading in which sellers may be more valued for good communications skills and customer service than might be the case in traditional offline markets.[63] The private messaging services on cryptomarkets facilitate this development. Buyers valuing good customer service in risky illegal markets may select vendors whose listings reflect this orientation. Previous analysis of listings placed by vendors on cryptomarkets yields for example the following[64]:

- 'Free shipping, fast service, fast communication'
- 'Look No Further: No Cut, No Crap, Great Communication, Speedy Service'
- 'I usually reply to customers within 4–5 hours. Do not hesitate to ask questions'.

61 See Branwen's (2015a, 2015b) speculation about 'weaponsguy' operating as ATF/FBI.

62 See Figure 2.3 for an example of a vendor shop rationale for not selling on cryptomarkets.

63 Aldridge & Décary-Hétu (2014).

64 Aldridge & Askew (2016).

Box 2.2 The risk of vendor scamming

There are a variety of techniques vendors can use to scam buyers. For instance, vendors may take payment but not deliver the purchased goods to the customer. This type of scam can be facilitated by requiring customers to FE and pay for the goods before they receive the order. FE bypasses the payment protection that cryptomarkets offer in the form of escrow services. The administrators of SR1 noted the prevalence of scamming that occurred outside of escrow.[65]

A second scamming strategy by vendors is less likely to lead to marketplace bans, which might be the result of scamming technique illustrated above. What is known as 'selective scamming' can be used by vendors even for escrow-protected transactions. Vendors are conscious of the risk of losing packages in the post, either through interceptions by customs or postal handling errors.[66]

A third variety of scamming exploits the good reputation of vendors by duplicating their pseudonym and fraudulently operating using the trust they have acquired in the darknet community. Vendors with good marketplace reputations can capitalise on this by scamming customers, but only if they do so infrequently. Customers who do not receive orders may report the vendor to administrators, but selectively scamming vendors with good marketplace reputation metrics can blame shipment loss to reduce the likelihood that cryptomarket administrators will label them as scammers.

Determining the extent of scamming by firearms vendors on cryptomarkets is as important to recognise as it is difficult to quantify. The scamming of firearms has occurred since the existence of the first weapons-only cryptomarket, 'The Armory'.[67] Currently active cryptomarkets (e.g. Alphabay) still post scam reports on clear web discussion forums today.[68] See Appendix B for a short history of firearms scamming on the dark web. Appendix C expands on section and documents and details a number of successful cases of firearms trafficking over the dark web, related to terrorism, serious and organised crime, and vulnerable and fixated individuals.

2.5.2. How vendors choose buyers

Although less widely documented in the literature, scamming can occur in the opposite direction too, i.e. a buyer having received an order may claim otherwise. Vendors' stated refund and reship policies illustrate the risk to profit entailed by parcel loss must be accepted to keep customers happy and continue to generate positive feedback. Still, vendors will be keen to minimise selling to customers who present a greater risk of claiming shipment loss as a scam. Vendors have a number of strategies at their disposal when choosing buyers with whom to transact. First, just as buyers have access to vendor reputation metrics, vendors can access a prospective

65 Christin (2013).

66 Décary-Hétu et al. (2016).

67 Deepdotweb (2017c).

68 See the subreddit /r/AlphaBay/ for examples of scam reports posted by vendors and buyers in order to resolve disputes.

> There are a variety of techniques vendors can use to scam buyers.

buyer's transaction history, and choose to avoid customers new to the marketplace, or refuse to sell to those with disputes associated with their transactions. Vendors can require potential customers they consider a scam risk to pay without escrow payment protection: vendors can therefore be paid upfront and ask buyers to FE. Third, vendors can specify a refund and reship policy that varies according to the purchasing track record of a potential buyer. Analysis of cryptomarket vendors' listings in previous research by Aldridge and Askew provides illustrative examples[69]:

- 'We have good stealth, and not had any orders not received. We know it is unlikely but if it happens, we will check your past stats and if they're good, you can choose 100% reship or refund.'
- 'Refunds: 50% of the price, but 75% refund for regular buyers. Customers with < 10 successful buys will get NO refund.'
- 'Reshipping only to folks with five or more previous buys and no returns. I will never ask you to finalise early, but please release the coins to me as soon as you receive the shipment. Fair's fair.'

2.6. 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. Similarly to 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 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 darknet 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, known as payment escrow. The vendor then packages the product and ships the parcel via postal services or private courier company. Once the order is received and the buyer is satisfied, the buyer returns to the marketplace to 'finalise' the order, at which point payment is released by the marketplace from escrow and transferred to the vendor's account. In this way, escrow provides protection for the buyer: if an order is not received or the product is not as advertised, the buyer declines to finalise the purchase, and the vendor is not paid.

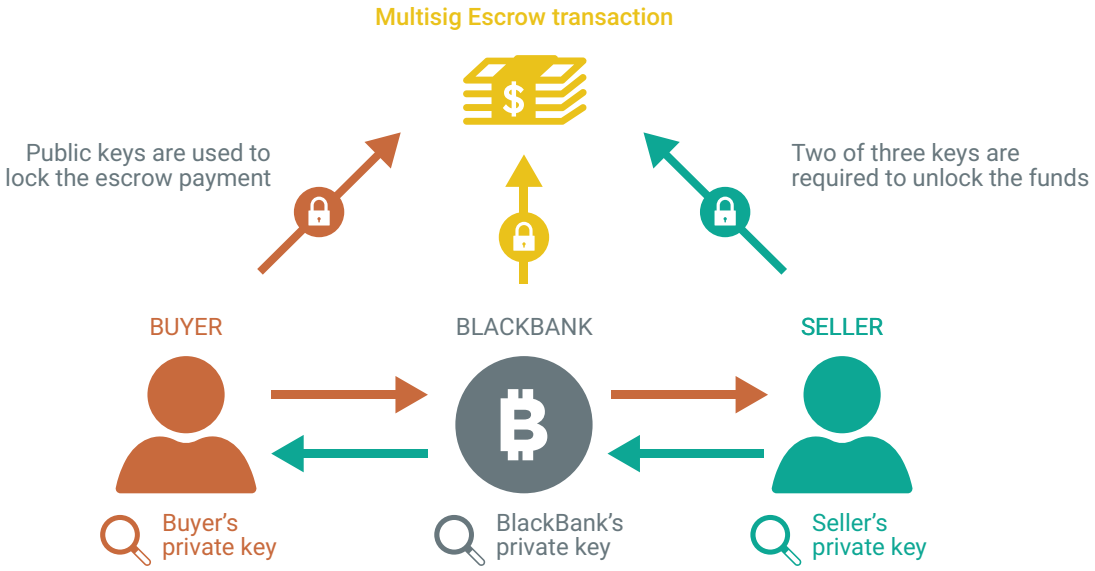
Some cryptomarkets now support multi-signature escrow transactions that require sign-off

69 Aldridge & Askew (2016).

Figure 2.4 Overview of payments using escrow services

Source: adapted from Kujawa (2014)

Figure 2.5 Overview of multi-signature escrow



Source: adapted from Deepdotweb (2014c)

from two out of three parties – the buyer, the seller, and the marketplace itself – to release funds.[70] Unlike the traditional, centralised escrow, it is impossible for one party alone to retrieve payment. The use of multi-signature on cryptomarkets appears to be catching on: 13 of the 21 markets in the Deepdotweb 'Market Comparison Chart' now offer multi-signature escrow.[71]

70 Cox (2016b).

71 Deepdotweb (2017a).

2.7. Shipping and receiving goods

Because many products sold on dark web markets are digital products (e.g. stolen credit card or identity information, eBook guides, 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.[72]

Recent 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.[73] 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: the selection of delivery drop-off locations at a distance from home or work; the rotation of drop-off points into postal systems; and avoiding entering post offices where they might be recorded by closed-circuit television (CCTV).[74]

> Using marketplace forums, vendors may discuss shipping techniques based on government published criteria for profiling suspect packages.

Using marketplace forums, vendors may discuss shipping techniques based on government published criteria for profiling suspect packages.[75] Such discussions take place more rarely on the clear web as dedicated forums usually prohibit this type of content.[76]

It has been identified by researchers that customers face heightened risks of detection and arrest while receiving their deliveries.[77] Vendors often advise customers to supply their real names for delivery. The use of fake names was believed to increase the chances that parcels would be identified as suspicious by post office employees and flagged for further investigation by authorities, potentially resulting in the 'controlled deliveries' by undercover law enforcement agencies that have been used to effect arrests.[78] Vendors sometimes alerted customers to the risks associated to their shipments being tracked,[79] – beyond signing for deliveries

72 Aldridge & Décary-Hétu (2014); Christin (2013); Mounteney et al. (2016).

73 Aldridge & Askew (2017).

74 Aldridge & Askew (2017).

75 Vajgert (1996).

76 The subreddit rules for r/DarkNetMarkets instruct users to not 'post stealth details'.

77 Aldridge & Askew (2017).

78 Branwen (2012).

79 Tzanetakis et al. (2015).

– given the ability of law enforcement agencies to conduct large-scale international investigations and audit postal records to track vendors (as shown in relation to the organised crime group CherryFlavor, noted in Chapter 1).

Dead drops

Postal or parcel services are still seen as 'the major bottleneck in the system'.[80] 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[81]:

> 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, and then making available the geo-coordinates alongside a short video for each 'dropped' deal. Only once deals have been dropped are listings with this delivery option offered to buyers. Customers making a purchase in this way can immediately access the location information and 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.

80 Mounteney et al. (2016, 7).

81 Aldridge & Askew (2017).

3 Dark web 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, the presentation of the findings and a discussion of their meaning.

3.1. Identifying dark web marketplaces trading firearms, ammunition and explosives

As detailed in this report (see section 2.1), dark web pages are not searchable through standard search engines. The first resource considered for identifying relevant hidden markets was Deepdotweb, following the lead of many cryptomarket researchers publishing in the scientific peer-reviewed literature who use it as a source. The list provided by Deepdotweb distinguishes cryptomarkets from sole-trading vendor shops.[82]

Market owners themselves request inclusion, with selection for the list granted only to cryptomarkets meeting stated requirements connected to market functionality, active vendors and review numbers.[83] For this reason, the Deepdotweb list is likely to exclude smaller cryptomarkets or those with limited functionality. In contrast, Deepdotweb's requirements for vendor shops present a higher bar for list inclusion: these market owners must have been active for over a year, and have high ratings (4.9 out of 5) on the cryptomarkets on which they also trade. According to a Deepdotweb administrator, firearm vendor shops are excluded from list inclusion typically because 'marketplace infrastructure and functionality are poor.'[84] At the time of data collection,[85] no vendor shops listed on Deepdotweb sold arms-related products.

82 The dark web market listing provided by Deepdotweb, 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 know of the existence of – cryptomarkets excluded from the Deepdotweb list is considered minimal, with most excluded markets likely to be very small and/or have limited functionality.

83 Deepdotweb (2017b).

84 Email correspondence with Deepdotweb administrator on 4 February 2017.

85 As of September 2016.

3.1.1. Cryptomarkets

For cryptomarkets, the project team identified all available marketplaces using the Deepdotweb markets list in 19 September 2017 and attempted to gain access to each market using the following strategies to identify those relevant for the purpose of this project:

1. **Marketplace-dedicated 'arms'-related category**. Product categories were inspected to identify cryptomarkets with dedicated arms-related categories available for vendors to classify the listings they placed for sale.
2. **Key word search for arms-related listings**. This strategy allowed the team to identify arms-related listings even in markets without a dedicated category.
3. **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 available cryptomarkets. There were 24 English/French-language[86] cryptomarkets operating during our assessment period.[87] Eighteen of these markets (75 per cent) were successfully accessed and inspected to ascertain evidence of arms-related selling according to the three criteria set out above. Of the remaining six, four were otherwise functioning markets that were temporarily down at the time of the scan, and two were unable to be accessed due to referral restrictions.[88]

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. Only for eight markets (44 per cent) was the team able to find arms-related listings through searching.

Table 3.1 Cryptomarkets listed on Deepdotweb: numbers classified as selling arms

	N	% of 18
Cryptomarkets listed on Deepdotweb	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

86 Four cryptomarkets were Russian, and the project team did not include a Russian-language speaker to support the analysis of these markets.

87 Two markets had closed in the interim.

88 Two markets were not accepting unsolicited members and were labelled 'referral only' markets.

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 selling was 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 listings. Conversely, three markets had weapons categories, but our searching identified no firearms-related listings within these categories.

Together, these findings suggest that even cryptomarkets facilitating firearms selling 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 key word 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 timeframe is considered.

3.1.2. Vendor shops

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

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

Discussion

The inaccessibility of certain vendor shops for which URLs were available suggests a number of possibilities. First, niche specialism may hamper vendor shop longevity. It may be difficult for vendors specialising 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 minimal understanding of the role that vendor shops have in hidden market arms sales. As detailed in sections 4.2 and 5.2, the absence of transaction information available on vendor shops makes it impossible to estimate the size of the trade, or even if vendor shops generate any trade at all.

3.2. 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.[89]

89 Décary-Hétu & Aldridge (2015).

Box 3.1 DATACRYPTO functioning

DATACRYPTO is a web crawler/scraper class of software that systematically archives websites and extracts information from them. Once a cryptomarket has been identified, DATACRYPTO is set up to log in to the market and download its contents, beginning at the web page fixed by the researchers (typically the homepage). After downloading that page, DATACRYPTO parses it for hyperlinks to other pages hosted on the same market and follows each, adding new hyperlinks encountered, and visiting and downloading these, until no new pages are found. This process is referred to as web crawling. DATACRYPTO then switches from crawler to scraper mode, extracting information from the pages it has downloaded into a single database.

One challenge connected to crawling cryptomarkets arises when, despite appearances to the contrary, the crawler has indexed only a subset of a marketplace's web pages. This problem is particularly exacerbated by sluggish download speeds on the Tor network which, combined with marketplace downtime, may prevent DATACRYPTO from completing the crawl of a cryptomarket. A number of researchers[90] have suggested that partial crawls were to blame for possibly misleading results published in Dolliver's 2015 article[91] in connection to Silk Road 2. A diagnosis provided by a group of researchers in a 2016 paper[92] were unable to replicate Dolliver's results using data collected from the same marketplace over a similar period. DATACRYPTO was designed to prevent partial marketplace crawls through its 'state-aware' capability, meaning that the result of each page request is analysed and logged by the software. In the event of service disruptions on the marketplace or on the Tor network, DATACRYPTO pauses and then attempts to continue its crawl a few minutes later. If a request for a page returns a different page (e.g. asking for a listing page and receiving the home page of the cryptomarket), the request is marked as failed, with each crawl tallying failed page requests.

DATACRYPTO is programmed for each market to extract relevant information connected to listings and vendors, which is then collected into a single database:

- Product title;
- Product description;
- Listing price;
- Number of customer feedbacks for the listing;
- The country or region from which a vendor ships the product;
- The country or regions to which the vendor placing the listing is willing to ship.

The data was obtained using the DATACRYPTO software tool (see Box 3.1). It should be noted that DATACRYPTO was not configured to extract data from vendor shops. Therefore, the estimates of the size and scope included in this chapter are, of necessity, restricted to that generated in connection to cryptomarkets.

90 Aldridge & Décary-Hétu (2015); Van Buskirk et al. (2015).

91 Dolliver (2015).

92 Munksgaard et al. (2016).

In addition, the design infrastructure of some cryptomarkets selling arms-related products and services prevented crawling using DATACRYPTO, likely due to programming anomalies within these markets rather than active crawling counter-measures put in place by marketplace administrators.[93]

The collection of primary data through DATACRYPTO was conducted once, in late September 2016. This implies that 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. Box 3.2 provides further details on our classification methodology.

Box 3.2 Identifying the arms-related listings for this study

To identify which of the 167,693 listings were relevant for the purpose of this study, the project team used a mixed methodology based on a combination of machine learning and manual investigation. The machine learning process was built in connection to a separate cryptomarket research project in which DATACRYPTO collected data from eight cryptomarkets in January 2016, generating a dataset of 106,348[94] listings. All listings were hand-coded by a team of seven research assistants who then classified each listing using the information provided by vendors in the product title and description. This first phase of 'learning' was then applied to successive DATACRYPTO data collections, automatically classifying new and uncoded cryptomarket listings, to a high degree of accuracy. The machine learning approach automatically classified as arms-related 560 of the 167,693 product listings across the 12 cryptomarkets.

To complement this automated process, manual searches were conducted on the remaining 167,133 listings to ensure that no relevant data was left out of the analysis. The search terms used for the manual searches were a combination of generic terms (e.g. rifle, ammunition) and manufacturer names (e.g. Beretta), alongside appropriate spelling variations (e.g. ammo). This process generated a further 3,756 listings. Product descriptions for each of these listings were then inspected individually to remove those inappropriately classified as arms-related. Most of those identified through searching[95] were discarded. Detailed analyses were based on the 811 arms-related listings that remained.

Table 3.2 lists the specifically named cryptomarkets from which data was collected using DATACRYPTO, 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.

93 Kruithof et al. (2016).

94 Kruithof et al. (2016).

95 Most listings incorrectly found through searching were actually drug listings. Examples include: a strain of cannabis referred to as AK-47; ecstasy pills branded as 'grenades'; 'gunpowder' heroin. Pornography-related listings often included actress names, one of which was Beretta.

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

Cryptomarket	Total number of listings	Number of arms-related listings	Rate (per 1,000 listings)
Alphabay	36,906	414	11.2
Dreammarket	64,625	173	2.7
Valhalla (Silkkitie)	19,939	114	5.7
Hansa-market	22,151	49	2.2
Oasis1	11,932	29	2.4
Python market	7,377	14	1.9
TheDetox market	1,312	8	6.1
Traderoute	1,596	4	2.5
Minerva	697	3	4.3
Acropolis	253	2	7.9
Tochka	277	1	3.6
Dark-net-heroes-league	628	0	0.0
Total	**167,693**	**811**	**4.8**

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 5). 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, to delete ostensible duplicates would assume – likely erroneously – that listings 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.

3.2.1. 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 & components	4	<1%	8	1%
Total	**811**	**100%**		

Note: n=number of listings

Discussion

Firearms listings (42 per cent) were most common, followed by digital products (27 per cent) and other, non-firearms 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 listing 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 – 1 per cent).

Firearms listings (42 per cent) were most common, followed by digital products (27 per cent) and other, non-firearms weapons (22 per cent).

> Pistols were the most commonly listed firearm (84 per cent), followed by rifles (10 per cent) and sub-machine guns (6 per cent).

Several observations can be made from the distribution of weapons listings described above. First, there is a considerable difference between ammunition and accessories sold alone, when compared against those sold as part of a 'package deal' with firearms. It suggests vendors have access to firearms as well as access to ammunition and/or accessories. Vendors might be re-selling personal firearms and related products already in their possession or they might have a network of contacts (either as part of the darknet 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,[96] 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.

3.2.2. Firearm types

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

- **Firearm type**: this referred to a simple categorisation based on three different weapons types: pistols (excl. full-automatic), sub-machine 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.

It should be noted that DATACRYPTO is not designed to download and store the images that are usually associated with listings. This implies that all findings are based on the textual analysis of the listings' titles and descriptions, and that the project team had no opportunity to derive any further characteristic of the item offered based on a visual analysis of the image (e.g. if a description reported the condition of a weapon as 'like new', the project team could not verify the statement by looking at the provided image).

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

Discussion

Pistols were the most commonly listed firearm (84 per cent), followed by rifles (10 per cent) and sub-machine 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 six in ten (59 per cent) sub-machine 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

96 RAND Europe expert workshop, 20–21 March 2017.

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

	Pistols (n = 284)	Sub-machine 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%

Note: n=number of listings per category. N=total number of firearms listings

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. Assuming that all 'unspecified' listings are either new or used would alter significantly the results of the analysis and no real evidence is available to support either choice. Though the project team did not analyse the images associated with each listing, this could have provided additional information related to the condition and minimised the number of 'unspecified' cases.

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.

Finally, regarding the types of firearms being sold, pistols represent the clear majority. Consulted law enforcement officials[97] highlighted that this 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 sub-machine guns and long rifles. Therefore they would be expected to be more dominant in terms of both supply and demand.

97 RAND Europe expert workshop, 20–21 March 2017.

Box 3.3 Information on 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 which 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.[98]

Of all firearms listings (n=339), only a small fraction (29 – 9 per cent) commented on the markings of weapons. In these 29:

- It was common for serial numbers to be removed (9);
- Quoting the verbatim serial was rare (2);
- One vendor stated they will 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. It is likely that more information could be obtained from the images.

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 number of firearms offered by make is provided in Appendix D.

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.

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

98 Bevan (2009).

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)
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 section 6.1, 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.

3.2.3. 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: eBooks/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.

Digital products were the second-most-frequent item, accounting for 222 listings (27 per cent of the total). The vast majority of these (n=208) were eBooks providing instructions for the manufacture of explosives or firearms. Eleven (11) listings were instead digital files for 3D printing 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. Box 3.4 contains an extract from one of these listings. The remaining three listings we classified as digital promises, selling information on where to buy firearms.

Box 3.4 Sample eBook listing (the first ten 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 policy makers and practitioners.[99] 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 recognised by the international community as a major source of concern.[100] With the improvement of commercially available 3D printers (e.g. increased accuracy, better quality of materials used for the printing), the possibility of producing at home viable substitute parts to replace, for example, those

99 RAND Europe expert workshop, 20–21 March 2017.

100 UNGA (2014).

> The availability of 3D models for additive manufacturing of parts, components or full firearms has been recognised by the international community as a major source of concern.

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.[101] Nevertheless, the implications deriving from the easy availability of these files should not be underestimated.[102]

3.2.4. Other weapons

The study team also collected and coded listings for 178 (22 per cent) other (i.e. non-firearms) weapons. The resulting breakdown is illustrated in Table 3.6.

Table 3.6 Weapon types (% based on 178 subsample)

	n	%
Stun guns/Tasers	57	32%
Knives	52	29%
Knuckle dusters/batons/clubs	20	11%
Combo packs	37	21%
Other	12	7%
Total	**178**	**100%**

101 King & McDonald (2015).

102 RAND Europe expert workshop, 20–21 March 2017.

4 Dark web 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. Similarly to Chapter 3, 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. When more information on the methodology is considered necessary, it is provided in a box.

4.1. 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.

This strategy is referred to as setting a 'holding price'.[103] The advantage for the vendor is that the listing can remain active, alongside all of its valuable customer feedback. While these extreme prices signal product unavailability to potential customers, vendors will often also modify the title or description of such listings to explain the function of the holding price explicitly (e.g. '*I'm on vacation for the next few weeks, so I've put a high holding price on until I get back.*').

If holding prices are treated as 'actual' market prices, any analysis that includes them will produce distorted estimates.

In general, researchers have dealt with the problem of holding prices in one of two ways. With smaller datasets, all high-price listings can be individually inspected by researchers for signs of holding prices and excluded from the analysis.[104] For datasets sufficiently large to make this process impractical, researchers have created a historical database of the prices of listings from previous crawls and scrapes of cryptomarkets made in previous months.[105] Then, instead of using the most recent price associated with a listing derived from our data collection, the median price is

103 See also: Kruithof et al. (2016, 14).

104 Aldridge & Décary-Hétu (2014).

105 Kruithof et al. (2016); Soska & Christin (2015).

used, thereby excluding occasional high prices collected for any one listing. Because the number of arms-related listings in this study was fairly small, the research team opted for the first method. All 811 listing descriptions were reviewed for explicit reference to holding prices and none was found. Only one listing had an unfeasibly high price ($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.

> If holding prices are treated as 'actual' market prices, any analysis that includes them will produce distorted estimates.

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	S.D[a]
Live firearms					
Sold alone	178	$1,187	$179	$10,264	1,133.97
+ bundled with other product(s)	95	$1,457	$225	$13,500	1,636.57
Replica firearms					
Sold alone	58	$132	$35	$468	70.83
+ bundled with other product(s)	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

[a] *Standard Deviation*

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

*** 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 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	S.D
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**					
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**					
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**					
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	-

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

*** 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 US replica guns tend to cost about 1/10 of the price of an equivalent/comparable live gun (e.g. a blank-firing replica

9 mm Magnum revolver costs about $80,[106] compared to a live Smith & Wesson Model 66 Combat Magnum® costing $850)[107]

Cryptomarkets have the effect of raising the cost of replicas, which have been advertised to cost as much as $468 when sold alone. This may suggest that a premium is paid for anonymity even for replica guns which could be bought legally and for a fraction of the price through authorised 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 authorisations.

> Cryptomarkets have the effect of raising the cost of replicas, which have been advertised to cost as much as $468 when sold alone.

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 on sub-machine guns (and full-automatic pistols) as there were not any 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 offline (black) market value or 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 US retail price for new Glocks can vary between $459 and $749, depending on the model.[108] 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 $349 and $900 depending on the model (and excluding special editions).[109] 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

106 Armory.net (2017).

107 Smith & Wesson (2017).

108 GlockStore.com (2017).

109 GunBroker.com (2017).

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 $10 to over $500. This discrepancy can be caused by various factors. First, as ammunition is 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 product offered on cryptomarkets (after pistols), the low price reinforces the observations made in section 3.2.3 around the risks deriving from the increased availability of usable 3D-printing files.

4.2. 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, 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 (see Box 4.1 for more details on how transactions were estimated).

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*	**209**	**26%**	**237**	**$83,288**

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

Box 4.1 Customer feedback as a proxy measure for transactions

Consistent with approaches taken by other researchers,[110] the project team used customer feedback as a 'proxy' measure for transactions. While leaving feedback is strongly encouraged on marketplaces, not all customers will leave feedback; this methodology therefore produces underestimates of actual sales. While it is not possible to know with certainty the proportion of actual transactions that generate customer feedback we can measure, this has been estimated by researchers as 88 per cent in September 2013 in connection only to drug sales and 71 per cent in January 2016 across all product categories.[111] The evidence is not sufficient to determine whether these gauges of the extent of underestimation apply in the same way to arms-related sales. Most sales on cryptomarkets are of drugs, which are consumable products, meaning customers are more likely to leave feedback in connection to a first-time purchase from a vendor, and less likely to do so when later making repeat purchases from the same vendor. This possibility has been offered as a partial explanation for customer feedback undercounts of actual sales. Because arms-related purchases seem unlikely to generate the same level of repeat custom as might be found for drugs, we suggest the possibility that customer feedbacks for arms-related cryptomarket buying may be somewhat closer to actual sales.[112] This possibility is offered as reasoned conjecture only. On the other hand, it is also possible that once a relationship is established between a vendor and a buyer, successive transactions could be arranged outside of a cryptomarket platform.

The following method was used to calculate our transaction variable. 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. It is important to understand, therefore, that our transaction variable is an estimate based on a one-off snapshot of the marketplaces at the time of our data collection and not the result of a continuous monitoring. The project team cannot ascertain actual transaction numbers in a way that is comparable across listings because the lifespan of listings varies; some will have been placed by vendors many months prior to data collection, and others will have been placed more recently, with correspondingly less time available to generate transactions. For listings placed days or a few weeks prior to data collection, the transaction rate is inferred based on more limited feedback data and may not accurately reflect the transactions the listing eventually generates. This is an inevitable limitation with cross-sectional data.

Finally, it should be noted that customer feedback can be manipulated: vendors can create user accounts through which to make purchases from their own vendor accounts, thereby generating feedback. Marketplace administrators generally have rules prohibiting this, and strategies to detect suspicious activities, but the practice cannot be eliminated. To the extent that this occurs, the estimates of sales volume in this report will be inflated accordingly.

110 Aldridge & Décary-Hétu (2014, 2016b); Christin (2013); Soska & Christin (2015).

111 Aldridge & Décary-Hétu (2014); Kruithof et al. (2016).

112 Kruithof et al. (2016).

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.

Table 4.5 Estimated monthly transactions and gross revenue by firearms types

	Pistols (n = 284)	SMGs (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**

This table provides a breakdown of the number of monthly transactions (in brackets) and associated gross revenue by weapons type (pistols, sub-machine guns and full-automatic pistols, and rifles). The upper part of the table illustrates the transactions and gross revenue for live weapons vs. replicas/alarm guns. The lower part of the table provides an overview of the transactions and gross revenues associated with different conditions. It is important to note that these results are based on a single snapshot of cryptomarkets and not on a continuous monitoring.

The final level of analysis with respect to sales relates to different makes. While in previous tables the analysis was limited to those makes having at least ten listings, in this case the results include all firearms makes generating sales (i.e. if at least one firearm of a specific make has been sold, then the make will appear in the table). Table 4.6 illustrates the number of active listings, transactions and gross revenue by make for all firearms listings generating sales.

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 $80,000 per month when excluding the category of 'Other weapons', which falls outside of the scope of this study. This figure certainly is dwarfed in comparison with recent estimates of the legal trade in small arms, which is measured in the order of billions.[113] 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,

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

Table 4.6 Active listings, transactions and gross revenue by make

Make	N active listings	Transactions (per month)*	Gross revenue (per month)
Glock	60	11.1	$24,882
Sig Sauer	19	13.2	$11,045
MAADI	2	1.9	$7,500
Zoraki	4	3.9	$5,051
Taurus	8	6.3	$4,860
CZ	4	1.2	$3,820
Smith & Wesson	13	3.6	$2,822
Colt	30	4.6	$2,574
Walther	9	2.7	$2,455
Zastava	3	1.4	$2,450
Steyr	1	0.6	$2,265
Ruger	18	0.5	$889
ATC	1	0.4	$597
Flobert	1	0.7	$423
Mauser	2	0.3	$422
Beretta	18	0.4	$349
Derringer	1	0.7	$303
Rossi	1	1.2	$269
Unspecified	39	1.0	$1,758

** 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.*

the evidence suggests that the number of transactions per year could potentially be in the order 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, compared to the 5 per cent of sub-machine guns and 10 per cent of 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

Pistols have a dominant role in firearms trade on cryptomarkets not only on the supply side, but also on the demand side.

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 how transactions were conducted, even if in small numbers, also for other firearms types including sub-machine guns and rifles. Assuming that such transactions are real and not the result of fake feedback, this would illustrate that demand exists also 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).

Box 4.2 Payment methods

Very few listings had instructions, notes or references regarding payment methods (n=23 – 3 per cent). There is an implicit assumption on cryptomarkets that financial transactions will involve an accepted cryptocurrency and use escrow services, and that parcels will be tracked, which might account for the low volume of instructions to buyers. Moreover, detailed instructions for conducting anonymous financial transactions using cryptocurrencies are readily available online. Despite the low number of qualitative indicators, there was a wide variety of instructions to prospective buyers:

- Listings stating full escrow services (7);
- A stated preference for money orders (3);
- For unsigned deliveries, FE is suggested by vendors (6);
- When shipping to a location where items are restricted, suppliers ask to FE (2).

Escrow services are one of the key mechanisms for enabling trust between anonymous parties on cryptomarkets (as described in section 2.6.).

4.3. Understanding firearms vendors

4.3.1.Where else they sell

To identify the vendor accounts that belong to the same individual or group, the project team compared the encryption keys[114] that vendors used to encrypt their communications. These encryption keys are by definition unique, and other researchers have used them as a way to identify different vendor accounts belonging to the same vendor.[115]

Through this methodology 60 vendor accounts were identified for which firearms listings were held across all 12 markets. Using PGP 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.

Several marketplaces prohibit weapons selling; firearms vendors may, therefore, have limited opportunities for cross-market selling.

The estimate of unique vendors assumes that vendors use the same PGP key across markets, and this may not be the case. However, vendors tend to employ cross-market selling to increase their exposure, with many explicitly stating the vendor alias names they use on other markets. Vendors seeking to build and sustain reputations have little to gain, therefore, by employing different PGP keys across markets.

Nevertheless, scamming vendors may take the opposite approach and seek to re-establish new identities to conceal scamming, and therefore be unable – or indeed unwilling – to establish selling track records and associated reputation. Table 4.7 illustrates the number of accounts held by vendors listing firearms for sale across marketplaces.

114 Vendors used PGP encryption keys, which are a standard in the security industry to encrypt messages.

115 Soska & Christin (2015).

Table 4.7 Firearm vendors and cross-market selling

		N	%
Vendor accounts across all markets		60	
Number of markets	One market	46	88%
	Two markets	4	8%
	Three markets	2	4%
Unique vendors		52	

4.3.2. Scamming by firearms vendors

Vendors can scam buyers for financial gain and the fraudulent practice has occurred since the emergence of cryptomarkets.[116] The weapons category might be predisposed to greater rates of scamming than other product categories, given its aggregate low volume of sales, the relatively high price of firearms and the known risks of interception when shipping weapons.[117] As further documented and cited in Appendix B, a number of notable cases support the view that scamming is a prevalent and persistent feature of the cryptomarket environment:

- Cryptomarkets could host dishonest, fraudulent or 'flipped' vendors[118]
- Cryptomarkets might exit scam, taking all funds held in escrow and users' wallets
- Single-vendor shops might be a scam.

Examples of scams include market exit scams (e.g. Evolution, Sheep and Project Black Flag), flipped vendors (e.g. speculation over the vendor account 'weaponsguy' being operated by US law enforcement agencies) and scam single-vendor markets (e.g. non-SR1-affiliated 'Armory' and 'Black Market'), not to mention vendors who simply scam buyers for their Bitcoins and/or altcoins.

In this section we aim to shed light on the question of scamming by firearms vendors. To assess the extent of scamming, we analysed customer feedback and listing lifespan of firearms and compared those to other types of products and product categories. In addition, we complement this analysis with a summary of the perceptions of members of the darknet community.

Assessing the relative likelihood of scamming using customer feedback ratings and age of listing

One possible indication of scamming can be found in connection to customer feedback ratings and lifespan of a listing. Vendors who scam customers may be more likely to receive low feedback ratings. Also, it is reasonable to believe that a vendor making a scam sale connected to a listing may be more likely to take

116 SR1, as the first modern cryptomarket, was not immune to vendor scams; it reportedly warned 'that buyers relying on out of escrow transactions "have been scammed"' (quoted in Christin 2012).

117 The cryptomarket Agora banned the sale of lethal weapons in July 2015, citing the difficulty of shipping firearms, their expense, the increased attention from law enforcement and prevalence of dishonest vendors (AgoraMarket 2015).

118 Flipped vendors refer to vendors' accounts which have been taken over by law enforcement agencies Branwen (2015b).

down the listing when the transaction is completed, in order not to draw attention to themselves. Listings placed by scamming vendors may therefore have a shorter lifespan than those placed by non-scamming vendors.

Using all the listings generated by scraping the 12 cryptomarkets, the project team compared average feedback scores and listing lifespans across four product categories: drugs, fraud, digital (non-arms-related) and arms-related. The latter category was further broken down into firearms, ammunition, other weapons and digital products (arms-related). Table 4.8 compares average listing feedback ratings and listing lifespan across product types.

Table 4.8 Mean customer feedback ratings and listing lifespan by product type

Product type	Customer feedback ratings		Listing lifespan
	n	Mean (out of 5)	Mean (days)
Drugs	29,250	4.86	148
Fraud	7,394	4.79	183
Digital (non-arms related)	9,631	4.81	185
Arms-related	209	4.73	153
> Firearms	46	4.51	112
> Ammunition	32	4.99	135
> Other weapons	75	4.65	169
> Digital (arms-related)	50	4.86	180
Statistically significant		P < .001	P < .001

Discussion

Compared to listings for other product types (drugs, fraud and non-arms-related digital products), arms-related listings had the lowest average customer feedback ratings. Going deeper into the arms-related listings, two product types appear to drive these lower ratings: (i) firearms and (ii) other weapons. Arms-related digital products received customer feedback ratings comparable to ratings for other digital products. Interestingly, listings for ammunition had the highest ratings of all (mean=4.99). However, customers purchasing firearms may be less satisfied with their purchases for reasons unrelated to scamming. Firearms are bulky items, so satisfaction may be related to packing and delivery problems less likely to affect smaller or digital products.

Listings for fraud and non-arms-related digital listings had the longest mean lifespans (183 and 185 days). The average lifespan for arms-related listings was much lower (153 days), but drug listings had the shortest average lifespan (148 days). However, comparing product types within arms-related listings, it is possible to note how firearms listings in particular have a much shorter average lifespan (112 days) than all other product types. There

are a range of other factors that may contribute to the lifespan of listings unrelated to scamming, however. Compared to other product categories such as drugs, firearms are expensive items for which sellers may be unlikely to hold substantial stock. Non-scamming vendors of firearms may be more likely to take down a listing immediately following a sale where stock holdings are limited, or for items with one-off availability. However, as discussed above, removing a listing right after the transaction is complete can also be associated with scamming behaviours. Therefore, these results should only be read as suggestive of the possibility that firearms vendors may be more likely to scam their customers than vendors of other products.

Box 4.3 Gauging the perception of firearm vendor scamming as evidenced in darknet community discussion

To assess the perceptions of scamming by firearm vendors in the darknet market community, the project team turned to relevant online darknet discussion in Reddit. These discussion threads were identified via Google search using the following search: 'reddit darknet market OR shop guns OR firearms OR weapons'. This procedure identified seven discussion threads, all of which were initiated by users asking for advice on locating dark web markets for buying firearms. A few posters responded to these requests by providing links to known vendor shops, but made clear that these were not offered as recommendations due to stated uncertainty connected to whether these shops were genuine. One vendor shop link was provided by the purported market owner.

The majority of ensuing discussion connected to these posts illustrated clear reservations about the legitimacy of vendors selling firearms. Although no users reported having been scammed themselves or knowing others who had, the perception that dark web firearms vendors were scammers dominated the discussion.

Cryptomarkets prohibiting the sale of firearms may do so due to the risk scamming poses for the marketplace, perhaps suggesting that risk-to-profit for marketplaces may be more important than ethical concerns about third-party harm. This observation is consistent with Agora's stated reason for removing lethal weapons listings, namely that weapons 'are expensive and stimulate both scamming by dishonest vendors and honeypot listings by [law enforcement] agencies…'[119] Moreover, Agora's administrators cited the low volume of sales in weapons and the fact that listing weapons 'would do more harm than good for our users.' Additionally, the reason for shutting down the SR1-affiliated weapons cryptomarket 'The Armory' was strikingly similar: 'The volume hasn't even been enough to cover server costs and is actually waning at this point.'[120]

Given the influence of the online darknet community in the form of crowd-sourced wisdom used to guide vendors and buyers, these perceptions of firearm vendor scamming – even if inaccurate or poorly informed – should be taken into consideration.

119 Deepdotweb (2015b).

120 BitcoinTalk (2012).

4.3.3. Motives and marketing techniques

During the analysis of the listings' descriptions, the project team captured a series of comments or expressions used by vendors as marketing messages. These included messages re-assuring potential buyers of the crime-free nature of the weapon (e.g. 'never used in crime or murder'; 'the gun is used but never shooting at somebody'); other vendors leveraged political sentiment (e.g.: 'buy now and feel safe again in your own country, you have right to that!') or personal attitudes (e.g. 'get one or two and carry more comfortably, walk more confidently.'); finally, some vendors seemed to leverage the cultural influence of the entertainment industry (e.g. videogames and movies) that glamorises killing to promote their products (e.g. 'has a godly rotating barrel that looks sweet when you're killing people.')

During the analysis of the listings' descriptions, the project team captured a series of comments or expressions used by vendors as marketing messages.

5 Dark web 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. When more information on the methodology is considered necessary, it is provided in a box.

5.1. 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.[121] First, the 'ship from' information vendors place on listings is only an imperfect proxy for country of vendor operation. 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.[122] 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.[123] 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

121 Décary-Hétu et al. (2016); Van Buskirk et al. (2016).

122 Kruithof et al. (2016).

123 Kruithof et al. (2016).

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.

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 UN.[124] When listings indicated products would be shipped worldwide, or to multiple regions that spanned the categorisation scheme, these were coded as 'Worldwide/multiple regions'. Where the origin or destination of listings could not be determined, listings were categorised 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.

5.2. 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. Normally, with datasets in the order of tens, hundreds or thousands of listings, the data is used by researchers as the only 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.

124 UNSTATS (2013).

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)*	Gross revenue (per month)
Multiple/unknown	40	16	7.7	$29,526
US	201	16	30.5	$24,987
Netherlands	8	3	4.5	$8,088
UK	5	1	6.0	$5,043
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'.

** 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. Box 5.1 contains a list of all countries/regions specifically referred to as shipping locations by vendors selling firearms. 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 could be a tactic (i) used to increase the visibility of the listing when users use searchcriteria or filters to navigate cryptomarkets, or (ii) potentially based on the vendor's assumption of where buyers might be more interested in receiving their products.

Box 5.1 Available shipping locations used by firearms vendors

Australia

Australia, New Zealand

Austria, Germany

Canada, United States, World

European Union

European Union, United States

Europe

Europe, Germany

Europe, World

Germany

North America, Europe, Asia, Oceania

UK, Europe

United States

United States, Europe, World

World

World, Cyprus, Germany, Monaco, United Kingdom

World, Europe, Asia, Oceania, Africa

World, Europe, Asia, Oceania, France

World, Europe, Asia, Oceania, United States

World, Europe, Europe, Peru, Austria

World, Europe, Finland, France, Germany

World, Europe, Jamaica, Finland, Germany

World, Europe, United States, United Arab Emirates

World, Europe, United States, United Kingdom, Australia

World, Finland, France, Germany, Greece

World, Germany

World, Haiti, United States, Germany, Macedonia

World, North America, Europe

World, North America, Europe, Asia, Oceania

World, North America, South America, Europe, Asia

World, South America, Europe, Asia, Asia

World, South America, Europe, Asia, Germany

World, South America, Europe, Asia, Oceania

World, South America, Europe, Asia, United States

World, South America, Europe, Europe, Germany

World, South America, Europe, Finland, Germany

World, South America, Europe, France, United Kingdom

World, United States

World, United States, United Kingdom, United Arab Emirates

World, World, South America, Europe, Asia

5.3. 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 summarises the results of this analysis.

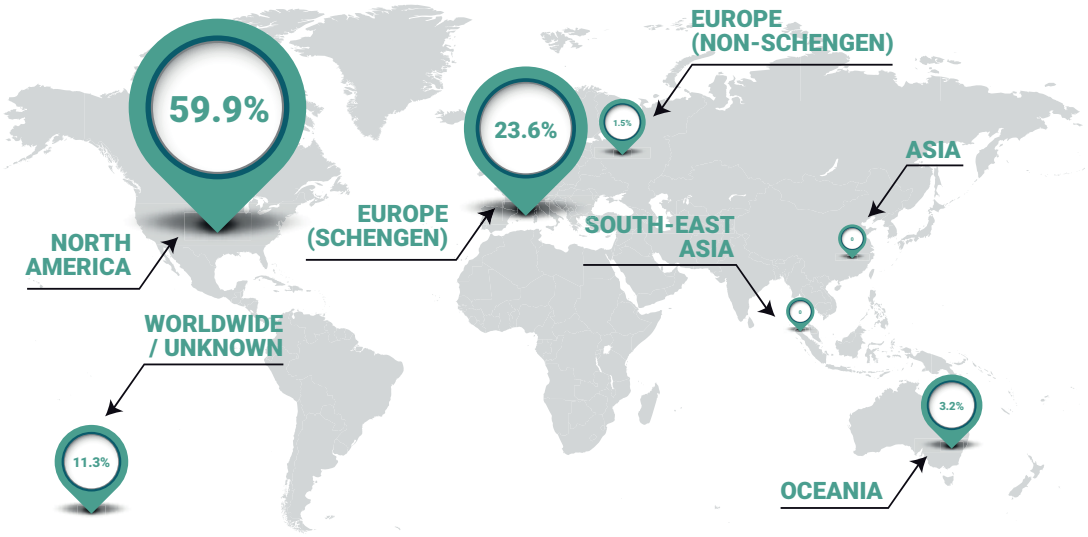
Table 5.2 Available shipping destinations for firearms: listings generating sales, estimated transactions per month and estimated gross revenue location (ordered by monthly revenue)

Country	N Listings	N active listings	Transactions (per month)*	Revenue (per month)
Worldwide	307	38	49.2	$68,561
Europe	9	4	4.3	$4,154
USA	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**

** 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 different 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 origins that generated sales and for which destination was known. Table 5.3 and Table 5.4 summarise the results of this analysis.

Figure 5.1 Worldwide distribution of arms vendors by region (n=339)



Source: RAND Europe

Figure 5.2 Available shipping routes for all firearms listings (n=339)

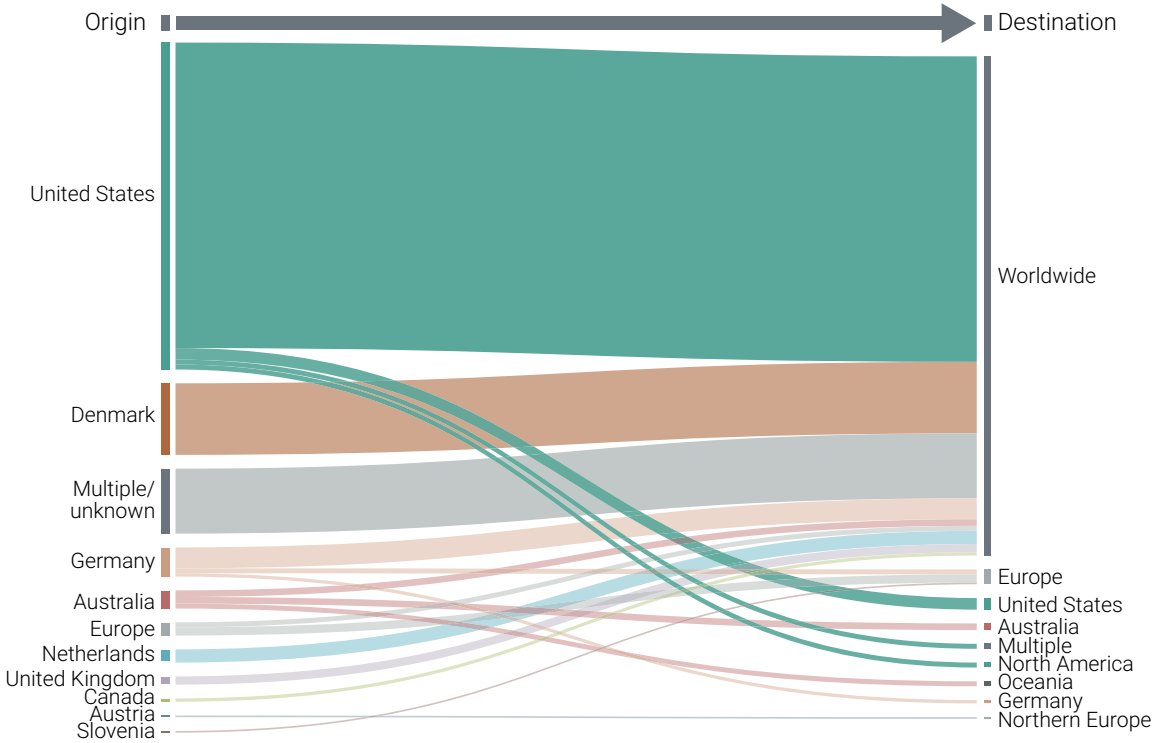


Table 5.3 Available shipping routes for all firearms (n=339)

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**

5.4. 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 and, where available, vendors' refund and reship policies.

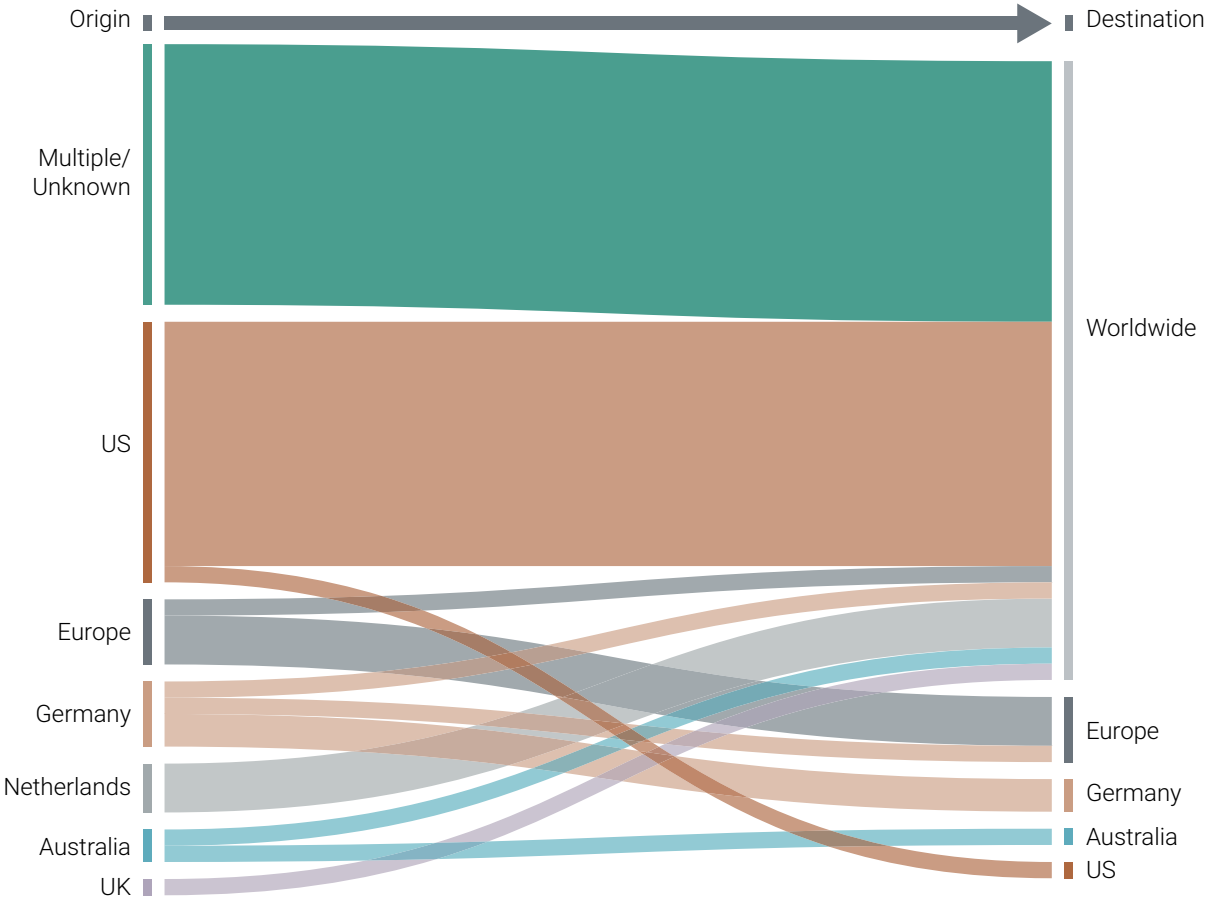
> The packaging and stealth of firearms, explosives and weapons must be sophisticated in order to disguise the consignment from customs and postal service screening.

5.4.1. Packaging and stealth

The packaging and stealth of firearms, explosives and weapons must be sophisticated in order to disguise the consignment from customs and postal service screening. Only a small portion of listings (n=69 – 12 per cent of the listings excluding the digital products) 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 [11])
- Stealth and concealment were reassured by suppliers (15).

Figure 5.3 Shipping routes used for firearms listings generating sales (n=46)



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.[125] 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

125 The subreddit rules for r/DarkNetMarkets instruct users to not 'post stealth details'.

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.[126] 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 the likelihood of the package being seized by authorities.[127] 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 may that *per se* are not illegal could be a way around controls.[128]

5.4.2. Delivery and shipping options

It was uncommon (n=69 – 12 per cent of the listings excluding the digital products) to specify delivery and shipping instructions in the listing description. As discussed in section 4.5, on many cryptomarkets, there are fields to allow the vendor to specify the country they are shipping from and where they intend to ship to. Further, vendors can post more detailed delivery options on their vendor profile. Vendors often refer prospective buyers to these sources of information, or contact them via secure email or messaging apps. In addition to those discussed in the previous section, there are some reoccurring features in delivery and shipping:

- Several vendors stated they usually ship items 2–3 times per week (14)
- In some cases, shipping discounts are offered for bulk buys (2)
- Tracking numbers and specific courier services are suggested by vendors (8).

5.4.3. Refund and reship policy

Similarly to online market places on the clear web (e.g. eBay, Gumtree and AbeBooks), vendors on cryptomarkets can specify their own terms and policies for issuing refunds and reshipping items. These policies are commonly found on a vendor's profile page, to which prospective buyers are encouraged to refer (3 listings). The most important information is often reiterated on individual listings (n=40; 5 per cent). Below are the common themes emerging from the listing information about vendors' refund and reshipping policies:

- A small number of vendors offered a three-day cooling-off period, where the firearm could be inspected and returned if the buyer wished. Only the cost of the gun, not the costs associated with shipping and posting, would be reimbursed by the vendor (2).
- Some vendors offered free samples of ammunition, where buyers would have to cover only the postage costs (8).
- Buyers were asked to consider paying a

126 Freeman (2016).

127 Freeman (2016).

128 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.

> In terms of number of monthly transactions, evidence suggests that the firearms shipping from the United States are the most commonly purchased.

premium to track consignments, to insure against lost packages and for the right for a reimbursement or reshipment of goods (5).

- Very infrequently, vendors advertised a 100 per cent guarantee to refund or reship a package, should the buyer not receive the parcel or be unhappy with the item received (4).
- Slightly more often, vendors were clear that no refund or reship would be given for seized or lost firearms (6).
- One vendor did extend the offer to resolve a hypothetical 'lost in the post' case if proof could be produced (1).

Refund and reshipping policies are specified and implemented by individual vendors. All buyers must take vendors at their word. Most listings urge buyers to contact the vendor using secure messaging services (n=123; 15 per cent).

Discussion

Table 5.1 suggests that the large majority (almost 60 per cent) of the firearms listings are associated with the United States as '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 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 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 (i) most the firearms shipping from the United States are pistols/handguns, with a lower unit price compared to heavier firearms; and/or that (ii) the market price for the same firearm type in the United States is significantly cheaper than elsewhere.

The dominant position of the United States in this ranking is not entirely surprising given the legal status of firearms in the country. There are, on average, 89 registered civilian firearms for every 100 residents in the United States, a total of about 270,000,000, without counting the unregistered weapons circulating on the black market; at both the aggregate and the per capita level, the United States ranks first in the world for firearms in civilian possession.[129]

While it is not possible to establish a causal link between (legal) civilian ownership and

129 Karp (2011).

> Europe is a much more active recipient market than the United States, generating revenue about five times higher.

scale of illegal trade, it is reasonable to believe that such high quantities pose significant arms control challenges. For example, the ATF reported that, in the calendar year 2012 alone, the National Crime Information Center received reports reflecting 190,342 lost and stolen firearms nationwide, about 9 per cent of which (about 16,600) were the result of thefts/losses from Federal Firearms Licensees (FFLs).[130,131] In calendar year 2016, the number of lost and stolen firearms from FFLs increased to 18,394, about half of which were reported as stolen and half as lost.132 These weapons are likely to fuel the illicit market in the United States, potentially including trade via the dark web.

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 intra-continentally rather than inter-continentally.[133]

130 US ATF (2012).

131 There are over 137,000 FFLs in the United States, divided into 11 different types: Type 01-Dealer (56,754); Type 02-Pawnbroker (8,076); Type 03-Collector (57,345); Type 06-Manufacturer of Ammunition (2,481); Type 07-Manufacturer of Firearms (11,083); Type 08-Importer (1,105); Type 09-Dealer of Destructive Devices (71); Type 10-Manufacturer of Destructive Devices (332); Type 11-Importer of Destructive Devices (217). US ATF (2017a).

132 US ATF (2017b).

133 Kruithof et al. (2016)

6 Overarching implications

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

6.1. Impact on the illicit firearms market

6.1.1. 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 globalised 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 5). 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 3 and 4 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.[134]

The emergence of the dark web has the potential to take the concept of the globalised arms trade to a different, potentially disruptive, level.

The 2016 European Union (EU) Drug Markets Report argues that the global reach of the internet, and the dark web in particular, makes it a 'relevant facilitator' of illicit trafficking.[135] On the other hand, while in theory the nature of dark web arms trafficking is global, it requires an information and communications technology (ICT) infrastructure that enables connectivity. Thus, it is reasonable to believe that countries or regions where internet accessibility is not available or is limited are less likely to be exposed to this type of phenomenon. In fact, the International Telecommunication Union (ITU) reported that by the end of 2016 about 53 per cent of the world's population did not have internet access.[136] In the same report, the ITU

134 RAND Europe–UNODC seminar, Vienna, 23 May 2017.

135 EMCDDA & Europol (2013, 119).

136 ITU (2016, 2).

highlights that the so-called 'digital divide' (i.e. the separation between the online and offline population) varies significantly at the regional level, as illustrated in Table 6.1.

Table 6.1 Estimated percentage of offline population by region

Region	% of offline population
Africa	75%
Americas	35%
Arab States	58%
Asia and the Pacific	58%
Commonwealth of Independent States	33%
Europe	21%

Source: Adapted from ITU (2016, 2)

While the number of observations of available shipping routes obtained through this study (see Chapter 5) might not be sufficient to determine the statistical correlation between dark web firearms trafficking routes and internet accessibility or usage, the figures presented in Table 6.1 are compatible with the findings of our analysis of shipping routes that identified the United States and Europe as key regions.

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 how 'bulk orders' exist, but are limited to a smaller number of weapons (usually between two and six), which are in any case shipped in multiple packages to minimise the risk of detection. As mentioned by experts consulted as part of this study, until now, dark web arms traffickers have dealt in parcels, not containers.[137]

This factor, in combination with the dependence on certain infrastructure and services, implies that, as mentioned by one law enforcement representative, the dark web is unlikely to become the method of choice to provide weapons which 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.[138] 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.[139]

137 RAND Europe expert workshop, 20–21 March 2017 (representative of law enforcement agency).

138 RAND Europe expert workshop, 20–21 March 2017 (representative of law enforcement agency).

139 RAND Europe expert workshop, 20–21 March 2017 (representatives [3] of law enforcement agency).

Box 6.1 Cryptomarkets and Business-to-Consumer e-commerce

Outside of the scope of this study, but worth noting as a possible area for further research, are the possible connections between developments associated with the growing demand and use of Business-to-Consumer (B2C) e-commerce and the use of the dark web to conduct illicit transactions (either on cryptomarkets or on other platforms). In very basic terms, dark web-based illegal trade is a form of illicit B2C e-commerce and the two phenomena share several key features, such as globalised markets, user-friendly payment systems, shipping and handling of products, language barriers and logistics challenges. Therefore, as e-commerce continues to grow, it is reasonable to believe that some of the developments and increased sophistication introduced to support and facilitate the use and viability of B2C e-commerce may act as enablers of illicit trade on the dark web. Analysing the data gathered in discussion with law enforcement and policy makers, the project team believes that two of the most relevant areas to monitor would be the evolution of cryptocurrencies and the developments of the shipping industry aimed at improving efficiency by reducing time and costs (e.g. through automation).[140] In a recent report by the Ecommerce Foundation, the CEO of a major international mail, shipping and distribution organisation stated that, in relation to recent logistical developments to meet the increasing demand, there is '…a growing demand for added transportation to handle the rising number of shipments entering countries from abroad'.[141] More to the point of dark web-enabled trafficking, 'new solutions for final-mile delivery have also become popular as a way of ensuring that the last mile delivery is handled as efficiently as possible'.[142] Some of these improved, faster and reliable support services in favour of a highly satisfactory 'customer experience' may be at odds with law enforcement efforts to identify and disrupt dark web-enabled illegal trafficking in firearms or other products.

6.1.2. 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.[143] 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',[144] suggest that small arms are the dominant product range available over the dark web.

140 Lacefield (2016).

141 Michael Hastings, CEO at Asendia USA in Ecommerce Foundation (2016, 12).

142 Michael Hastings, CEO at Asendia USA in Ecommerce Foundation (2016, 12).

143 'Small arms' are, broadly speaking, weapons designed for individual use. They include, inter alia, revolvers and self-loading pistols, rifles and carbines, sub-machine 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 missiles systems, and mortars of a calibre of less than 100 mm. UNGA (2005).

144 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.

Example of package deal including a rifle, a revolver and related ammunition offered on a cryptomarket

This causes several control issues as many types of small arms are legally available for purchase in many countries, making the identification of those shipped illegally less immediate. 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 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 as the proliferation of guidelines and 3D models, in combination with the increased quality of commercially available 3D printers, may result in more untraceable weapons, as users will become increasingly able to manufacture fully functioning weapons or, most likely, parts and components that could be used to replace, on an already existing firearm, the original ones bearing identification markings (see section 3.2.3).

> The proliferation of guidelines and 3D models, in combination with the increased quality of commercially available 3D printers, may result in more untraceable weapons.

Finally, as previously mentioned, the results presented in Chapters 3 and 4 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 which are subject to a different, less strict, regulation.[145] 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.

6.2. Impact on market actors

6.2.1. 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.[146]

> 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.

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. As described in Chapter 2, the dark web is not necessarily difficult to access and several guides and tutorials are available on the clear web. A basic user would require, or obtain by consulting the mentioned guidelines, a basic level of understanding of anonymity software and encryption techniques to conceal one's identity. On the other hand, users particularly interested in enhancing their anonymity would benefit from a certain familiarity with technical terminology, networking techniques and testing of security settings to ensure 'digital fingerprints' are not left during dark web sessions. In addition, while some vendors accept other forms of payments (see Box 4.2), conducting business on cryptomarkets may require knowing how to purchase cryptocurrencies from exchanges, 'tumbling or mixing' Bitcoins to reduce the posting of personally identifying metadata on public ledgers.[147]

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

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

147 Bitcoin tumbling, also referred to as Bitcoin mixing or Bitcoin laundering, is the process of using a third-party service to break the connection between a Bitcoin address sending coins and the address(s) they are sent to. Since the Bitcoin blockchain is a public ledger that records every transaction, mixing coins is critical for anyone who wants to obscure exactly where they send and store their Bitcoin, or from where they receive it (Darknet Markets, 2015).

This may suggest, as a reasoned conjecture, that internet literacy may, to some extent, shape the distribution of potential dark web users who may decide to engage in illicit trading on cryptomarkets. While this may be true at the individual level (i.e. internet literacy may indeed be a barrier for a portion of a population), given the limited scale of dark web-enabled firearms trade (see Chapters 3 and 4), the degree of internet literacy at the macro or national level is not, *per se*, an indication of the likelihood that cryptomarkets could become a vehicle for illicit arms trafficking in a given country. Considering the potential impact of just a small number of vendor accounts, a country with a higher rate of internet literacy would not necessarily be more exposed to the threat of dark web-enabled arms trade than another country with a lower rate of internet literacy.

In very simple terms, anyone possessing the IT skills described above, or the basic skills required to search and consult online resources and tutorials, and interested in buying a firearm illegally 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 kind of individuals to connect to an international network of vendors, extrapolated from the B2C principle of e-commerce, deeply changes the way individuals can procure firearms. The case of the disturbed teenager Liam Lyburd presented in section 1.1 illustrates the complexity of this issue: individuals who might not otherwise be able to access the street-level firearms black market can now procure firearms through the dark web.

> Anyone possessing the basic skills required to search and consult online resources and tutorials, and interested in buying a firearm illegally can connect to a cryptomarket and within minutes have access to tens of different vendors offering their products.

6.2.2. The perceived anonymity of cryptomarkets may attract specific types of individuals

Another implication at the individual level is the profile of people who might engage in this type of arms trafficking. As described in section 1.1 and further documented in Appendix C, there are reports of terrorist cells and organised criminal groups, as well as lone-wolf terrorists or individual criminals, using the dark web 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.[148] This can include vulnerable or fixated individuals affected by mental conditions (e.g. Liam Lyburd), minors and other categories of individuals who would not necessarily be willing or able to purchase a weapon or ammunition on the streets.

As discussed in Chapter 2, 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,

148 RAND Europe interview with law enforcement representatives (3).

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.

> 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.

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 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.

6.2.3. 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). Based on an analysis conducted by Kruithof et al. these key actors are:[149]

- 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 finalised through the marketplace.
- Developers are commissioned to carry out web design (and maintenance); and,
- 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. A more detailed discussion of this issue is provided in Section C of the annex to this report.

6.3. Law enforcement and policy implications

6.3.1. 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.[150] While these strategies were analysed in relation to drugs trade, their general principles and associated challenges can be adapted and transposed to the context of arms trafficking. Table 6.2 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.

149 Kruithof et al. (2016, 104).

150 Kruithof et al. (2016).

Table 6.2 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.
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-anonymise 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 market places.	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:

- 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 policy makers and law enforcement agencies.[151] 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.[152]

- 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,[153] 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).[154] In addition, cooperation between law enforcement agencies and public or private postal/courier service providers is key to ensure 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 implies that such public–private interfaces often cross several jurisdictions, with 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, if necessary, 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.[155]

6.3.2. 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 6.2 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.[156] For example, the United Kingdom has committed in the 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'.[157] The creation of the unit is to enable the analysis of multiple data sources,

151 RAND Europe interview with policy representative.

152 RAND Europe expert workshop, 20–21 March 2017.

153 RAND Europe expert workshop, 20–21 March 2017.

154 Kruithof et al. (2016).

155 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.

156 RAND Europe expert workshop, 20–21 March 2017 (Representatives from law enforcement and policy-making community).

157 HM Government (2016).

> Policy makers may also achieve impact through different types of interventions beyond the realm of law enforcement operations.

coordinate with multiple agencies and deal with issues at scale. This type of commitment is critical to mobilise the necessary resources and ensure that law enforcement agencies receive the required 'top-cover' for conducting their operations.

Secondly, the previous sections highlighted the challenge that law enforcement agencies face with respect to legal restrictions. Therefore, policy makers 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 the respecting of civil rights and democratic principles.

Finally, at the national level, policy makers may also achieve impact through different types of interventions beyond the realm of law enforcement operations. Similarly to what the literature suggests with respect to drugs,[158] 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 US National Institute of Justice, which encompasses a combination of different programmes tailored to local communities,[159] or initiatives promoted by organisations like the American Psychological Association focusing on prevention (e.g. spotting warning signs in youth) and education.[160] This 'soft' measure may be considered as complementary to law enforcement operations, and would be more forward-looking and designed taking into account the new generation of digital natives.[161]

6.3.3. However, the international policy community will also need to take action and take account of this new phenomenon

The proliferation of and trafficking in small arms have been acknowledged as a global security threat for a few decades, with the first official milestone set by the UN 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.[162] 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 UN in the new Sustainable Development Goals (SDGs), which in Target 16.4 state: 'By 2030, significantly reduce illicit arms flows'.[163]

The 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

158 See for example, Christin (2013).

159 For more information see National Institute of Justice (2017).

160 For more information see American Psychological Association (n.d.).

161 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.' (Oxford Dictionaries, n.d.).

162 UN (2001).

163 SDG 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'. UNGA (2015).

and preventing arms proliferation and misuse, reducing and preventing armed violence, reducing economic and social cost of small 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, reliable licensing and authorisations processes including background checks.

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 standardised.
- **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 harmonised 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.[164]

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.

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. In this regard, the Global Firearms Programme of the UNODC prepared an analysis of three international legal instruments based on the results of this study with a view to identify how or to what extent the already existing international legal framework provides an adequate and effective response to dark web arms trafficking. This analysis, provided as an annex to this report, reviews three legally binding instruments at international level that are of particular relevance to this study:

164 King (2015).

- 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 (ATT).

These three instruments have been reviewed by the UNODC to identify those provisions that may support policy makers and law enforcement agencies in their efforts to tackle dark web-enabled arms trafficking. Some high-level conclusions from this analysis are included below, while further details are provided in the document attached to this report.

Based on its analysis of the international legal framework, the UNODC identified the following high-level policy considerations:

- 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 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 Party to it.[165] There are also several States that have not yet adhered to the ATT. Further efforts towards universalisation 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 the foreseen preventive and security as well as enforcement measures.

165 For a full list of States Parties to the Firearms Protocol, see UNGA (2001).

7 Conclusions

As described in Chapter 1, the overarching goal of this study is to provide law enforcement, policy and decision makers with an 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.

The project team built this evidence base based on three main pillars: 1) size and scope (e.g. what is available on the market and in what quantities); 2) value (e.g. what are the dark web market prices of the products offered and how much is the dark web arms trade worth); 3) 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).

This chapter summarises the main points emerging from the study related to these three pillars and their implications, mapping them to the study objectives described in Section 1.2.

General objectives

Objective 1: to understand the modus operandi of buying and selling firearms and related products on the dark web.

- 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. 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.

  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 specialised 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 finalised, the products purchased are normally shipped by post using special shipping techniques to minimise the risk of detection. In the context of firearms, these techniques often involve disassembling the weapon and shipping different parts in multiple packages.

Objective 2: to consider the viability of dark web markets for firearms selling, and more specifically, the extent to which these sellers may engage in scamming by taking payment for products they do not deliver, or may not possess.

- There is contrasting evidence in relation to the prevalence of scamming in the context of firearms trade on cryptomarkets. While the general the perception among users is that vendors selling firearms are mostly scammers or law enforcement agencies, a number of recent cases suggest that real vendors also operate on cryptomarkets. The data available does not allow to determine in a rigorous way the extent to which scamming occurs.
- Analysing the metrics most commonly used by researchers to assess the probability of scamming, feedback ratings and life-span of listings, does not provide solid enough evidence to determine with confidence that listings for firearms and related products are mostly scams. For example, compared to drugs, the mean feedback for firearms is only marginally lower; in contrast, the mean feedback for ammunition is higher than the mean feedback for drugs. Looking at the life-span of listings, while it is true that firearms have the lowest life-span, in absolute terms the figures are comparable in scale and the difference in life-span may be due to the different nature of the products being sold.
- In conclusion, given the potential impact on security of even one weapon being sold through the dark web, the allegedly higher possibility of scamming should not be used as reason to dismiss or minimise the relevance of the issue. From a risk assessment perspective, as well as for policy making and operational planning purposes, it is recommended that, in absence of other sources of information, each listing and vendor are considered real while accepting that a portion of them may be scammers or law enforcement agencies.

Market analysis

Objective 3: to estimate the 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').

> 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.

- 60 vendor accounts were identified for which firearms listings were held across all accessed markets. Using PGP 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 sub-machine guns. The majority of firearms offered for sale are live weapons, with the exception of the sub-machine guns, where replicas are the majority. The condition of the firearm, new or used, does not appear as 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 permit the scale of dark web arms trafficking to be determined 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 firearms than what is normally accessible on the streets (despite the latter being, to a certain extent, country-specific).

Objective 4: to estimate the 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 United States appears as the dominating source country in terms of both number of listings and number of monthly transactions.

the region of $80,000. The majority of both transactions and 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 both other products sold on cryptomarkets (e.g. Kruithof et al. [2016] estimated that drugs listings generated a total of monthly revenue of $14.2m) 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 as no robust estimates of the latter exist.
- Concerning the volume of monthly transactions, in 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 policy makers and law enforcement agencies.

Objective 5: to identify 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.

Implications

On the basis of the findings outlined above, and acknowledging both the limitations of our methodology and the potentially disruptive role played by scamming, it is possible to summarise the main implications and considerations as follows:

Objective 6: to identify the potential impact of dark web enabled arms trafficking on the overall arms 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 anonymising 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, removes also the majority of 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 organisations.

Objective 7: to identify the potential implications of dark web enabled arms trafficking for law enforcement agencies and policy makers, at both the national and international level, including implications for existing international legal instruments designed to tackle the issue of illegal arms trade and transnational organised crime.

- Law enforcement agencies are facing a series of operational challenges related to the main intervention strategies which exist to combat this problem. 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 policy-making community, both at the national and international level.
- At the national level, policy makers should ensure that the threat posed by illegal arms trafficking on the dark web is recognised and adequate resources are mobilised to ensure that law enforcement agencies are staffed, trained and equipped to respond effectively. In addition, policy makers 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 existing international instruments designed to tackle the general issue of arms trafficking. These instruments provide a range of control measures to limit the diversion of legally owned firearms to the black market and to trace illegal firearms back to the last known legal owner, providing an investigative lead into the point of diversion.

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.

- 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 which may require updating or further development.
- Based on the analysis of the international legal framework conducted by UNODC (attached to this report), it appears that key international legal instruments such as the Organised Crime Convention, the Firearms Protocol and the ATT 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 (e.g. the US) are not yet State Parties to the instruments identified, limit the extent to which tools and measures provided by such instruments can be used in practice.

Final remarks

This study has demonstrated that significant value can be obtained by using empirical analysis methodologies to investigate dark

web-enabled arms trafficking. Taking into account the caveats and limitations described throughout the report, this study represents the first systematic, evidence-based assessment of the trafficking in firearms (including their parts, components, accessories and ammunition) and explosives. However, based on the observations above, further research is necessary to further develop the understanding of the market characteristics (e.g. 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, more continuous monitoring activity should be undertaken. 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.

References

AgoraMarket. 2015. 'Agora to Pause Operations.' Reddit.com/r/AgMarketplace, 25 August. As of 27 June 2017: https://www.reddit.com/r/AgMarketplace/comments/3idznd/agora_to_pause_operations/

Aldridge, J., & R. Askew. 2016. *When Drug Dealers Can Advertise: How Drug Cryptomarkets Enable Drug Dealers to Advertise*. Presented to the International Society for the Study of Drug Dependence.

———. 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

———. 2015. 'A Response to Dolliver's "Evaluating Drug Trafficking on the Tor Network: Silk Road 2, The Sequel".' *International Journal of Drug Policy* 26(11): 1,124–25.

———. 2016a. '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.

———. 2016b. Hidden Wholesale: How Drug Cryptomarkets May Transform Traditional 'Offline' Drug Markets. *International Journal of Drug Policy* 35: 7–15.

Alwakeel, R. 2015. 'Jailed: IT Boss Who Posed as Revenge-seeking Woman to Buy Gun on Dark Web.' *Evening Standard*, 26 November. As of 27 June 2017: https://www.standard.co.uk/news/crime/jailed-it-boss-who-posed-as-revengeseeking-woman-to-buy-gun-on-dark-web-a3124306.html

American Psychological Association. n.d. 'Gun Violence and Prevention.' Apa.org. As of 27 June 2017: http://www.apa.org/topics/violence/gun-violence-prevention.aspx

Anderson, L. 2016. 'Marcinelle: Policeman Arrested in Possession of Weapons Planning Double Assassination.' *The Brussels Times*, 28 September. As of 27 June 2017: http://www.brusselstimes.com/belgium/6556/marcinelle-policeman-arrested-in-possession-of-weapons-planning-double-assassination

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

Barlow, E. 2013. '"Executive Outcomes" and the Dark Net.' Eebenbarlowsmilitaryandsecurityblog.blogspot, 23 November. As of 27 June 2017: http://eebenbarlowsmilitaryandsecurityblog.blogspot.com/2013/11/executive-outcomes-and-dark-net.html

Barratt, M. J. 2012. 'Silk Road: eBay for Drugs.' *Addiction* 107(3): 683–83.

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.

BBC (British Broadcasting Company) News. 2015. 'Liam Lyburd: People Will Die… Newcastle College Plot Was Real.' BBC.com, 30 June. As of 27 June 2017: http://www.bbc.co.uk/news/uk-england-33676472

———. 2016. 'Munich Shooting: David Sonboly "Planned Attack for Year".' BBC.com, 24 July. As of 19 May 2017: http://www.bbc.com/news/world-europe-36878436

———. 2017. 'Boy, 14, Tried to Buy Sub-machine Gun on the Dark Web, Court Hears.' BBC.com, 8 April. As of 27 June 2017: http://www.bbc.com/news/uk-northern-ireland-39538330

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

Bevan, J., 2009. 'Revealing Provenance: Weapons Tracing During and After Conflict.' In *Small Arms Survey 2009: Shadows of War,* 106–33. As of 27 June 2017: http://www.smallarmssurvey.org/fileadmin/docs/A-Yearbook/2009/en/Small-Arms-Survey-2009-Chapter-03-EN.pdf

Biddle, S. 2012. 'The Secret Online Weapons Store That'll Sell Anyone Anything.' Gizmodo.com, 19 June. As of 27 June 2017: http://gizmodo.com/5927379/the-secret-online-weapons-store-thatll-sell-anyone-anything

Biermann, K. & K. Polke-Majewski. 2017. 'Rechter Waffenshop ist Offline.' Zeit.de, 2 February. As of 27 June 2017: http://www.zeit.de/gesellschaft/zeitgeschehen/2017-02/migrantenschreck-illegale-waffen-website-offline

Bilton, N. 2013. 'Disruptions: A Digital Underworld Cloaked in Anonymity.' NYTimes.com, 17 November. As of 27 June 2017: https://bits.blogs.nytimes.com/2013/11/17/disruptions-a-digital-underworld-cloaked-in-anonymity/?_r=2

BitcoinTalk. 2012. 'The Armory - Weapon Marketplace.' BitcoinTalk.org, 5 August. As of 27 June 2017: https://bitcointalk.org/index.php?topic=66587.msg1079466#msg1079466

Boggan, S. 2013. 'It's Not Just Child Porn: Fake Passports, Guns, Cocaine, Even Hitmen for Hire are a Few Clicks Away on the Internet.' DailyMail.co.uk, 22 November. As of 27 June 2017: http://www.dailymail.co.uk/news/article-2512136/Its-just-child-porn-Fake-passports-guns-cocaine-hitmen-hire-clicks-away-internet.html

Branwen, G. 2012. 'Tor DNM-related Arrests.' Gwern.net, last modified 15 June 2017. Date accessed: 10 June 2017. As of 27 June 2017: https://www.gwern.net/DNM%20arrests

———. 2013. 'Darknet Market Mortality Risks.' Gwern.net, last modified 7 April 2017. Date accessed: 201 June 2017: As of 27 June 2017: https://www.gwern.net/DNM%20survival

———. 2015a. '[PSA/Article] Hyannis Man Charged With Bitcoin Purchase of Firearm and Silencer on "Darknet".' Reddit.com/r/DarkNetMarkets, 3 April. As of 27 June 2017: https://www.reddit.com/r/DarkNetMarkets/comments/31afi7/psaarticle_hyannis_man_charged_with_bitcoin/cq3ejul/

———. 2015b. '17 Arrests Due to Flipped Agora Seller "weaponsguy".' Reddit.com/r/DarkNetMarkets, 14 May. As of 27 June 2017: https://www.reddit.com/r/DarkNetMarkets/comments/35ytiw/17_arrests_due_to_flipped_agora_seller_weaponsguy/

Buxton, J., & T. Bingham 2015. The Rise and Challenge of Dark Net Drug Markets. *Policy analysis.* As of 27 June: http://www.drugsandalcohol.ie/23274/1/Darknet%20Markets.pdf

C3LT1C. 2015. 'Agora: A True Survivor in a Brave New World.' Deepdotweb.com, 24 September. As of 27 June 2017: https://www.deepdotweb.com/2015/09/24/agora-a-true-survivor-in-a-brave-new-world/

Callimachi, R., M. Eddy, & A. Jacobs. 2016. 'Gunman in Munich Kills 9, Then Himself, the Police Say.' NYTimes.com, 22 July. As of 27 June 2016: https://www.nytimes.com/2016/07/23/world/europe/munich-mall.html?_r=0

Chen, A. 2011. 'The Underground Website Where You Can Buy Any Drug Imaginable.' Gawker.com, 1 June. As of 1 May 2015: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

———. 2012. 'Now You Can Buy Guns on the Online Underground Marketplace.' Gawker.com, 27 January. As of 27 June 2017: http://gawker.com/5879924/now-you-can-buy-guns-on-the-online-underground-marketplace

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.

Cox, J. 2015. 'Scams and Undercover Cops Are Denting the Dark Web Gun Trade.' Motherboard.vice, 26 November. As of 27 June: https://motherboard.vice.com/en_us/article/scams-and-undercover-cops-are-denting-the-dark-web-gun-trade

———. 2016a. 'Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds.' Motherboard.vice, 24 February. As of 27 June 2017: https://motherboard.vice.com/en_us/article/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds

———. 2016b. 'Staying in the Shadows: The Use of Bitcoin and Encryption in Cryptomarkets.' In *Internet and Drug Markets, EMCDDA Insights*, edited by EMCDDA, 41–47. Luxembourg: Publications Office of the European Union.

Darknet Markets. 2015. 'A Simple Guide to Safely and Effectively Tumbling (Mixing) Bitcoins.' Darknetmarkets.org. As of 27 June 2017: https://darknetmarkets.org/a-simple-guide-to-safely-and-effectively-mixing-bitcoins/

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., & L. Giommoni. 2016. 'Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous.' *Crime, Law and Social Change*, 67: 1–21.

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.

Deepdotweb. 2014a. 'Swiss Man Arrested for Running a Known Scam Site.' DeepDotWeb.com, 19 November. As of 27 June 2017: https://www.deepdotweb.com/2014/11/19/swiss-man-arrested-for-running-a-known-scam-site/

———. 2014b. 'Breaking: Sheep Marketplace Owner Arrested.' DeepDotWeb.com, 27 March. As of 27 June 2017: https://www.deepdotweb.com/2015/03/27/breaking-sheep-marketplace-owner-arrested/

———. 2014c. 'BlackBank market now offering multisig escrow.' DeepDotWeb.com, 16 February. As of 27 June 2017: https:/www.deepdotweb.com/2014/02/16/blackbank-market-now-offering-multisig-escrow/

———. 2015a. '17 Arrests in International "Dark Web" Firearm Sting.' DeepDotWeb.com, 14 May. As of 27 June 2017: https://www.deepdotweb.com/2015/05/14/four-australians-charged-in-international-dark-web-firearm-sting/

———. 2015b. 'Agora Market to Stop Listing Lethal Weapons.' DeepDotWeb.com, 7 July. As of 27 June 2017: https://www.deepdotweb.com/2015/07/07/agora-market-to-stop-listing-lethal-weapons/

———. 2017a. 'Dark Net Markets Comparison Chart.' DeepDotWeb.com. As of 27 June 2017: https://www.deepdotweb.com/dark-net-market-comparison-chart/

———. 2017b. 'Rules for Market and Vendor Shops Listing.' DeepDotWeb.com. As of 27 June 2017: https://www.deepdotweb.com/rules-for-market-vendor-shops-listing/

———. 2017c. 'The Armory.' DeepDotWeb.com. As of 27 June 2017: https://www.deepdotweb.com/marketplace-directory/listing/the-armory-1/

———. 2017d. 'Updated: List of Dark Net Markets (Tor & I2P).' DeepDotWeb.com, last modified 1 May 2017.Date accessed: 19 September 2016. As of 27 June 2017: https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/

Dolliver, D. S. 2015. 'Evaluating Drug Trafficking on the Tor Network: Silk Road 2, The Sequel.' *International Journal of Drug Policy* 26(11): 1,113–23.

Ecommerce Foundation. 2016. *Global B2C E-commerce Report 2016*. As of 27 June 2017: https://www.ecommercewiki.org/wikis/www.ecommercewiki.org/images/5/56/Global_B2C_Ecommerce_Report_2016.pdf

EMCDDA (European Monitoring Centre for Drugs and Drug Addiction). 2015 'The Internet and Drug Markets. Summary of Results from an EMCDDA Trendspotter Study.' As of 27 June 2016: http://www.emcdda.europa.eu/system/files/publications/928/Internet%20and%20drug%20markets%20study.pdf

EMCDDA (European Monitoring Centre for Drugs and Drug Addiction) &. 2013. *EU Drug Markets Report: A Strategic Analysis*. As of 27 June 2017: http://www.emcdda.europa.eu/publications/joint-publications/drug-markets

Europol. 2015. 'The Internet Organised Crime Threat Assessment (IOACTA).' As of 27 June 2017: https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015

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-smuggling-weapons-into-britain/

Gayle, D. 2015. 'Newcastle Teenager Liam Lyburd Found Guilty of Planning College Massacre.' *The Guardian*, 30 July. As of 27 June 2017: https://www.theguardian.com/uk-news/2015/jul/30/newcastle-teenager-liam-lyburd-found-guilty-of-planning-college-massacre

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

Goodin, D. 2015. 'New Attack on Tor Can Deanonymize Hidden Services with Surprising Accuracy.' ArsTechnica.com, 31 July. As of 27 June 2017: https://arstechnica.com/security/2015/07/new-attack-on-tor-can-deanonymize-hidden-services-with-surprising-accuracy/

Gorman, R. 2015. 'Man Jailed for Attempting to Buy Hand Gun in Case of Terrorist Attack.' NottinghamPost.com, 11 December. As of 27 June 2017: http://www.nottinghampost.com/man-jailed-attempting-buy-hand-gun-case-terrorist/story-28347495-detail/story.html

Grams. 2017. Market Comparison. Grams.onion. As of 27 June 2017: http://grams7enufi7jmdl.onion/markets

Greenberg, A. 2013. 'Silk Road Competitor Shuts Down and Another Plans to Go Offline After Claimed $6 Million Theft.' Forbes.com, 1 December. As of 27 June 2017: https://www.forbes.com/sites/andygreenberg/2013/12/01/silk-road-competitor-shuts-down-and-another-plans-to-go-offline-after-6-million-theft/#450cb1347e08

———. 2014a. 'Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains.' Wired.com, 11 July. As of 27 June 2017: https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/

———. 2014b. 'Not Just Silk Road 2: Feds Seize Two Other Drug Markets and Counting.' Wired.com, 18 November. As of 27 June 2017: https://www.wired.com/2014/11/dark-web-seizures/

———. 2015. 'The Dark Web's Top Drug Market, Evolution, Just Vanished.' Wired.com, 18 March. As of 27 June 2017: https://www.wired.com/2015/03/evolution-disappeared-bitcoin-scam-dark-web/

Greenwald, G. 2013. 'NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users.' TheGuardian.com, 4 October. As of 6 June 2017: https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption

Guadamuz, A. & C. Marsden. 2015. 'Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies.' *First Monday* 20 (12). As of 27 June 2016: http://firstmonday.org/ojs/index.php/fm/article/view/6198/5163

GunBroker.com. 2017. 'Beretta 92 FS.' GunBroker.com. As of 27 June 2017: http://www.gunbroker.com/Beretta-92FS%2FBrowse.aspx?Keywords=Beretta+92+FS&BuyNowOnly=1&Sort=4&Tab=2

HM (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

Huggler, J. 2015. 'Man Arrested in Germany on Suspicion of Illegal Arms Dealing in Terror Crackdown.' Telegraph.co.uk, 27 November. As of 27 June 2017: http://www.telegraph.co.uk/news/worldnews/europe/germany/12020249/Paris-attackers-bought-weapons-from-arms-dealer-in-Germany.html

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

IrishNews. 2016. 'PSNI Officer Facing "Dark Net" Gun Charges is Alleged Involved in Drug Dealing, Court Told.' IrishNews.com, 26 October. As of 27 June 2017: http://www.irishnews.com/news/2016/10/27/news/psni-officer-facing-dark-net-gun-charges-is-alleged-involved-in-drug-dealing-court-told-757109

ISACS (International Small Arms Control Standard) 2016. *Glossary of terms, definitions and abbreviations. 01.20. 22 April. As of 27 June 2017: http://smallarmsstandards.org/isacs/0120-en.pdf*

ITU. 2016. *ICT Facts and Figure 2016*. As of 27 June 2017: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

ITV. 2016. 'Man Jailed for Trying to Buy Weapons and Ammunition on Dark Web.' ITV Report, 15 January. As of 27 June 2017: http://www.itv.com/news/granada/2016-01-15/man-jailed-for-trying-to-buy-weapons-and-ammunition-on-dark-web/

Karp, A. 2011. *Estimating Civilian Owned Firearms*. Small Arms Survey Armed Actors Research Notes, Number 9, September. As of 27 June 2017: http://www.smallarmssurvey.org/about-us/highlights/highlight-research-note-9-estimating-civilian-owned-firearms.html

King, B. 2015. *From Replica to Real – An Introduction to Firearms Conversion*s. 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

Kujawa, A. 2014. 'Bitcoin Theft in the Underground'. Malwarebytes Labs. 14 February. As of 27 June 2017: https://blog.malwarebytes.com/cybercrime/2014/02/bitcoin-theft-in-the-underground/

Lacefield, S. 2016. 'Drones in the Supply Chain: More than Just Last-mile Delivery.' *Supply Chain Quarterly*, Quarter 3. As of 27 June 2017: http://www.supplychainquarterly.com/news/20160912-drones-in-the-supply-chain-more-than-just-last-mile-delivery-/

Lewman, A. 2016. 'Tor and Links with Cryptomarkets.' In *Internet and Drug Markets, EMCDDA Insights*, edited by EMCDDA, 33–40. Luxembourg: Publications Office of the European Union.

Losensky, A. 2016. 'Berliner Darknet-Dealer muss vier Jahre ins Gefängnis.' ['Berlin's Darknet dealer has to go to prison for four years.'] BZ-berlin.de, 12 September. As of 27 June 2017: http://www.bz-berlin.de/tatort/menschen-vor-gericht/berliner-darknet-dealer-muss-vier-jahre-ins-gefaengnis

Martin, J. 2014. *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*. Palgrave Macmillan.

Matthews, S. 2014. 'Q&A With A Deep Web Arms Dealer.' Vocativ.com, 24 February. As of 27 June 2017: http://www.vocativ.com/tech/bitcoin/q-deep-web-arms-dealer/

Morselli, C., D. Décary-Hétu, M. Paquet-Clouston, & J. Aldridge. 2017. 'Conflict Management in Illicit Drug Cryptomarkets.' *International Criminal Justice Review*) [No issue or volume]: 1-18. As of 27 June 2017: http://journals.sagepub.com/doi/10.1177/1057567717709498

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

Mullen, P. E., D. V. James, J. R. Meloy, M. T. Pathé, F. R. Farnham, L. Preston, B. Darnley, & J. Berman. 2009. The Fixated and the Pursuit of Public Figures. *The Journal of Forensic Psychiatry & Psychology* 20(1): 33–47.

Munksgaard, R., & J. Demant. 2016. Mixing Politics and Crime – The Prevalence and Decline of Political Discourse on the Cryptomarket.' *International Journal of Drug Policy* 35: 77–83.

Munksgaard, R., J. Demant, & G. Branwen. 2016. 'A Replication and Methodological Critique of the Study "Evaluating Drug Trafficking on the Tor Network".' *International Journal of Drug Policy* 35: 92–96.

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

Nichol, S. 2015. 'Liam Lyburd: How a disturbed loner used the dark web to buy a Glock pistol.' Chroniclelive.co.uk, 30 July. As of 27 June 2017: http://www.chroniclelive.co.uk/news/north-east-news/liam-lyburd-how-disturbed-loner-9760812

NSWGreat. 2015. '[Complaint/Warning] Evolution Admins Exit Scamming.' Reddit.com/r/DarkNetMarkets, 18 March. As of 27 June 2017: https://www.reddit.com/r/DarkNetMarkets/comments/2zeuxo/complaintwarning_evolution_admins_exit_scamming/

Oxford Dictionaries, n.d. Definition of digital native. Accessed on 10 May 2017. As of 27 June 2017: https://en.oxforddictionaries.com/definition/digital_native

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

Petry, M. 2016. 'Waffenkaufer gesteht tat ein.' ['The rifleman admits act.'] Donaukurier.de, 20 November. As of 27 June 2017: http://www.donaukurier.de/lokales/schrobenhausen/Schrobenhausen-DKmobil-wochennl442016-Waffenkaeufer-gesteht-Tat-ein;art603,3285610

Reddit. 2014. 'Never Trust a Pirate.' /r/SilkRoad. As of 27 June 2017: https://en.reddit.com/r/SilkRoad/comments/1pfzga/never_trust_a_pirate/

———. 2015. 'Deep Dark Web Weapons Stores SCAMS and likely SCAMS – Be Warned!' /r/onions. As of 27 June 2017: https://www.reddit.com/r/onions/comments/2dmvnp/deep_dark_web_weapons_stores_scams_and_likely/

Rothwell, J., J. Huggler, & L. Finnigan. 2016. 'Ali Sonboly: Everything We Know About the Munich Gunman.' Telegraph.co.uk, 24 July. As of 27 June 2017: http://www.telegraph.co.uk/news/2016/07/23/munich-shooting-everything-we-know-about-the-shopping-centre-gun/

Segal, D. 2014. 'Eagle Scout. Idealist. Drug Trafficker?' NYTimes.com, 18 January. As of 27 June 2017: https://www.nytimes.com/2014/01/19/business/eagle-scout-idealist-drug-trafficker.html?_r=0

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

Smith, G. 2013. 'How Bitcoin Sales of Guns Could Undermine New Rules.' HuffingtonPost.com, 15 April, last modified 19 May. As of 27 June 2017: http://www.huffingtonpost.com/2013/04/15/bitcoin-guns_n_3070828.html

Solms-Laubach, F. 2015. 'Mord-Waffen kamen aus Deutschland!' ['Murder weapons came from Germany!'] Bild.de, 27 November. As of 27 June 2017 (in German): http://www.bild.de/politik/ausland/waffen/aus-pariser-terror-nacht-stammen-aus-deutschland-43565470,var=a,view=conversionToLogin.bild.html

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

The Local/DPA. 2017. '"Migrant shock", a Far-right Website Selling Illegal Guns, Taken Down.' TheLocal.de, 2 February. As of 27 June 2017: https://www.thelocal.de/20170202/migrant-shock-far-right-website-selling-illegal-guns-taken-down

The Wave. 2015. 'Swansea Man had Lethal Weapons.' TheWave.co.uk, 31 October. As of 27 June 2017: http://www.thewave.co.uk/news/local/swansea-man-had-arsenal-of-lethal-weapons/

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.

UN (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

UNGA (United Nations General Assembly). 2000. United Nations Convention against Transnational Organized Crime. Adopted 15 November. A/RES/55/25 of 15 November. As of 27 June 2017: https://www.unodc.org/pdf/crime/a_res_55/res5525e.pdf

———. 2001. *Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, Supplementing the United Nations Convention against Transnational Organized Crime (UN Firearms Protocol)*. Adopted 31 May. A/RES/55/255 of 8 June. As of 27 June 2017: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12-c&chapter=18&clang=_en

———. 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

———. 2007. *Report of the Group of Governmental Experts established pursuant to General Assembly resolution 60/81 to consider further steps to enhance international cooperation in preventing, combating and eradicating illicit brokering in small arms and light weapons*. A/62/163. 30 August. As of 27 June 2017: https://digitallibrary.un.org/record/605508/files/A_62_163-EN.pdf

———. 2008. *Report of the Group of Governmental Experts to examine the feasibility, scope and draft parameters for a comprehensive, legally binding instrument establishing common international standards for the import, export and transfer of conventional arms.* A/63/334. 26 August. As of 27 June 2017: https://digitallibrary.un.org/record/637337/files/A_63_334-EN.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

UNODC (United Nations Office on Drugs and Crime). 2004. *Legislative Guide for the United Nations Convention against Transnational Organized Crime and the Protocols thereto.* V.04-50413. As of June 2017: https://www.unodc.org/unodc/en/treaties/CTOC/legislative-guide.html

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/

US ATF (Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives). 2012. *2012 Summary: Firearms Reported Lost and Stolen*. As of 27 May 2017: https://www.atf.gov/file/11851/download

———. 2017a 'Fact Sheet – Facts and Figures for Fiscal Year 2016.' Atf.gov. As of 27 June 2017: https://www.atf.gov/resource-center/fact-sheet/fact-sheet-facts-and-figures-fiscal-year-2016

———. 2017b. *FFL Thefts/Losses United States*. April. As of 27 June 2017: https://www.atf.gov/news/pr/atf-releases-2016-summary-firearms-reported-lost-and-stolen-ffls

US DOJ (United States Department of Justice). 2014. 'More than 400 .Onion Addresses, Including Dozens of 'Dark Market' Sites, Targeted as Part of Global Enforcement Action on Tor Network' Office of Public Affairs, 7 November. As of 27 June 2017: https://www.justice.gov/opa/pr/more-400-onion-addresses-including-dozens-dark-market-sites-targeted-part-global-enforcement

———. 2015a. 'Montgomery Man Convicted for Illegal Gun Sales on Darknet Sites.' Atf.gov/, 24 June. As of 27 June 2017: https://www.atf.gov/news/pr/montgomery-man-convicted-illegal-gun-sales-darknet-sites

———. 2015b. 'Hyannis Man Charged with Bitcoin Purchase of Firearm and Silencer on "Darknet".' Justice.gov, 2 April. As of 27 June 2017: https://www.justice.gov/usao-ma/pr/hyannis-man-charged-bitcoin-purchase-firearm-and-silencer-darknet

———. 2016. 'Kansas Man Pleads Guilty to Exporting Firearms to Overseas Purchasers.' Atf.gov, 6 June. As of 27 June 2017: https://www.atf.gov/news/pr/kansas-man-pleads-guilty-exporting-firearms-overseas-purchasers

———. 2017a. 'Gun Traffickers Arrested for Allegedly Using the Dark Net to Export Guns Across the World.' Justice.gov, 31 May. As of 27 June 2017: https://www.justice.gov/usao-ndga/pr/gun-traffickers-arrested-allegedly-using-dark-web-export-guns-across-world

———. 2017b. 'Kansas Man Sentenced to 52 Months for Exporting Firearms to Overseas Purchasers Using Hidden Marketplace Website.' Justice.gov, 30 January. As of 27 June 2017: https://www.justice.gov/opa/pr/kansas-man-sentenced-52-months-exporting-firearms-overseas-purchasers-using-hidden

Vajgert, G. 1996. 'Identification of Mail Packages Used in Drug Smuggling.' *The FBI Law Enforcement Bulletin*, 1 February. As of 27 June 2017: https://www.thefreelibrary.com/Profiling%20postal%20packages.-a018447923

Van Buskirk, J., A. Roxburgh, S. Naicker, & L. Burns. 2015. Response to Dolliver – Evaluating Drug Trafficking on the Tor Network. *International Journal of Drug Policy* 26(11): 1,113–23.

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

Van Slobbe, J. 2016. 'The Drug Trade on the Deep Web: A Law Enforcement Perspective.' In *Internet and Drug Markets, EMCDDA Insights*, edited by EMCDDA, 77–83. Luxembourg: Publications Office of the European Union.

Vitáris, B. 2015. 'Allegedly: German DNM Vendor Sold the Weapons Used at Paris Terror Attacks.' DeepDotWeb.com, 2 December. As of 27 June 2017: https://www.deepdotweb.com/2015/12/02/german-dnm-vendor-sold-weapons-to-paris-terror-attacks/

———. 2016a. 'Do People Really Buy Weapons from Dark Web Markets?' DeepDotWeb.com, 12 January. As of 27 June 2017: https://www.deepdotweb.com/2016/01/12/do-people-really-buy-weapons-from-dark-web-markets/

———. 2016b. ‘Belgian Sentenced to Community Service for Ordering Weapons of War.’ DeepDotWeb.com, 1 November. As of 27 June 2017: https://www.deepdotweb.com/2016/11/01/belgian-sentenced-community-service-ordering-weapons-war/

Woolf, N. 2015. ‘Bitcoin “Exit Scam”: Deep-Web Market Operators Disappear With $12m.’ TheGuardian.com, 18 March. As of 27 June 2017: http://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars

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/

Annex – Overview of international legal instruments and their applicability to illicit firearms trafficking on the dark web

Prepared by the Global Firearms Programme of the United Nations Office for Drugs and Crime*

The contents of this article do not necessarily reflect the views or policies of the UNODC, nor do they imply any endorsement.

*Authored by Simonetta Grassi, Head of the Global Firearms Programme, and Mareike Buettner, Associate Expert

International responses to illicit trafficking in firearms, their parts and components and ammunition on the dark web

As stakeholders examine how perpetrators of recent armed attacks such as in Munich and Paris can access used firearms with a seemingly low risk of being caught, the present research shows that illicit arms trafficking on the dark web constitutes a reality that increasingly attracts public attention. For some time now, the international community, law enforcement agencies, weapons and cybercrime experts and other stakeholders have been discussing approaches to tackle the phenomenon of illicit trafficking on the dark web.

In this connection, one fundamental question is what are the means and tools available to criminal justice systems to effectively prevent and combat this new phenomenon, and hence, **how, or to what extent, the already existing international legal framework provides an adequate and effective response to trafficking in firearms, their parts and components and ammunition on the dark web**. A closer look at the most relevant instruments and their applicability can shed some light on this question.

a. Overview of the international legal framework

There are three legally binding instruments at international level that are of particular relevance to the case: the United Nations Convention against Transnational Organized Crime (the **Organized Crime Convention**), its supplementary Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition (the **Firearms Protocol**), and the Arms Trade

Treaty (the **ATT**).[166] The first targets transnational organised crime and aims at promoting cooperation to prevent and combat it more effectively, while the other two specifically aim to prevent, combat and eradicate the illicit trafficking in weapons, including firearms, as well as their parts and components and ammunition.

Adopted by unanimity in the United Nations General Assembly in November 2000, the Organized Crime Convention constitutes the main legal instrument at international level to provide specific measures to prevent and combat transnational organised crime. While the Convention also requires States to establish certain criminal offences, this chapter focuses on provisions relating to law enforcement and international police and judicial cooperation. As of 1 June 2017, there are 187 Parties to the Convention.[167]

The Firearms Protocol is one of three supplementing Protocols to the Organized Crime Convention, and was adopted in May 2001. It presented the first legally binding instrument on firearms at global level. The declared statement of purpose of this legally binding instrument is to 'promote, facilitate and strengthen cooperation among States Parties in order to prevent, combat and eradicate the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition' (article 2). It provides measures relating to the entire lifecycle of firearms, their parts and components and ammunition, including their manufacture, transfer, control and safety as well as disposal. As a criminal justice instrument, the Firearms Protocol further sets a focus on criminalisation, information exchange and international cooperation, including tracing. As of 1 June 2017, there are 114 Parties to the Firearms Protocol.[168]

Lastly, the ATT, adopted by the United Nations General Assembly in April 2013, aims to, among other things, establish the highest possible common international standards for regulating or improving the regulation of the international trade in conventional arms. Its provisions mainly address the establishment of an international weapons transfer control regime as well as addressing diversion, reporting, international cooperation, etc. As of 1 June 2017, 92 States have ratified or acceded to the ATT.

b. Applicability of the Organized Crime Convention, the Firearms Protocol and the ATT

Beyond their statement of purpose, in order to discuss the effectiveness of the introduced international legal frameworks to address arms trafficking on the dark web, attention must be brought to their concrete applicability.

The Organized Crime Convention generally applies to the prevention, investigation and prosecution of offences established in accordance with the Convention and its supplementing Protocols, where the offence is **transnational in nature** and **involves an organised criminal group** (article 3). While this seems to be a limitation, especially in cases where the perpetrator does not seem to be linked to a criminal group, it should be noted that when States invoke the Convention to request mutual legal assistance, which constitutes an important tool of international cooperation in criminal matters to facilitate the generation

166 While the 2001 Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects constitutes another crucial step in advancing the fight against the illicit proliferation of weapons, it is not taken into account in this chapter due to its non-legally binding nature.

167 In fact, there are only 11 UN member states that are not Party to the Organized Crime Convention.

168 For a complete list of States Parties to Firearms Protocol, see UNGA (2001).

of admissible evidence in the jurisdiction of the prosecuting State, it is sufficient for the requesting State to have reasonable grounds to suspect that the offence is transnational in nature and that it involves an organised criminal group (article 18 paragraph 1). This sets a lower evidentiary standard intended to facilitate assistance requests for the purpose of determining whether elements of transnationality and organised crime are present and whether international cooperation may be necessary and may be sought under the Organized Crime Convention for subsequent investigative measures, prosecution or extradition.[169] The provisions of the Convention apply mutatis mutandis to the Firearms Protocol (article 1 paragraph 2 of the Firearms Protocol).[170]

The scope of application of the supplementing Firearms Protocol, on the other hand, relates to preventing and combating the **illicit manufacturing of** and **trafficking in firearms, their parts and components and ammunition** (article 4). The research identified all of these items as being offered and transferred through the dark web. Digital products, such as manuals or instructions for the manufacturing or modification of arms and explosives as well as digital files for 3D printing firearms, which was the second-largest category of items identified as being transferred, seem to fall outside the scope of the transfer control regime set up by the Firearms Protocol and the other instruments.[171]

The general requirements that the Firearms Protocol sets for **export, import and transit control systems**, including the establishment of export and import licensing or authorisation systems, relate exclusively to international transfers of firearms, their parts and components and ammunition (article 10). On the other hand, the implicit requirements for **manufacturers**, to have a valid licence or authorisation from the competent authority of the State where the manufacture or assembly of the governed items takes place, and to apply the marking requirements established by the Protocol for firearms, are valid also for items purchased or produced at local level (article 3 d).

The Firearms Protocol further commits States Parties to establish certain **criminal offences**, such as the illicit manufacturing of and the illicit trafficking in firearms, their parts and components and ammunition, as well as the attempt to commit these offences and several modalities of aiding and abetting (article 5 paragraph 1 a, b, 2). The Protocol defines illicit trafficking to comprise different variations of transfer of the regulated items (such as import, export, sale and acquisition) '*from or across the territory of one State Party to that of another if any of the State Parties concerned does not authorize it or if the firearms are not marked*' in accordance with the measures set out in the Protocol. The Protocol applies similar applicability criteria as its parent Convention when it comes to law enforcement and international cooperation measures, stating that those measures should apply to the investigation

169 UNODC (2004, 221).

170 The term 'mutatis mutandi' should be interpreted to mean 'with the necessary modifications' or 'with such modifications as the circumstances require'; see UNODC (2004, 472).

171 The 2008 Report of the Group of Governmental Experts to examine the feasibility, scope and draft parameters for a comprehensive, legally binding instrument establishing common international standards for the import, export and transfer of conventional arms (UNGA, 2008) noted that the types of weapon systems, equipment and their components being manufactured in cooperation, under joint ventures and licensing was increasing and that most arms producing States were increasingly relying on technology transfers and upgrades from external sources, rather than from their own indigenous production. In this context, while e-books and manuals with instructions for the manufacture or modification of firearms, their parts and components and ammunition as well as 3D printing files could potentially be counted, these are not covered by the ATT.

and prosecution of this offence where it is **transnational in nature** and **involves an organised criminal group** (article 1 paragraph 2, 4 of the Firearms Protocol). It should however be noted that at national level, the offence shall be established in the domestic law of each State Party *independently* of the involvement of an organised criminal group (article 34 paragraph 2 of the Convention).

The offence of illicit manufacturing of firearms, their parts and components and ammunition (article 5 paragraph 1 a) can also be of some utility in our specific context. The definition of illicit manufacturing provides for diverse variations of the offence, which applies to the manufacturing or assembly of those items, when (a) illicitly trafficked parts and components are used; (b) the activity is done without a licence or authorisation from the competent authority where the activity takes place; or (c) where the so-manufactured or -assembled firearms are not marked in accordance with the marking requirements of article 8 of the Protocol. There is a high risk of buyers, subsequent to the transfer of the purchased items, committing the offence in the specific context referred to in this research. This can for example be the case when buyers manufacture weapons based on a purchased e-book providing instructions for the manufacture of firearms or using digital files for 3D printing firearms without holding a licence to do so or without marking the manufactured firearm as required. It can also be the case when buyers reassemble the firearms that were previously purchased on the dark web and disassembled by the vendor with a view to disguising the consignment from customs and postal service screenings (see section 5.4.1).

The above shows that the relevant provisions on transfer controls, law enforcement, international cooperation and the offences of the Firearms Protocol seem to be mainly applicable to international cases of illicit trafficking in firearms, their parts and components and ammunition on the dark web. There might however be a need to further explore the extent to which the requirement of a cross-border element is met purely by the fact that dark web traffic is routed across multiple IP addresses in different countries and through multiple international relays.

Lastly, the ATT and its transfer control regime apply to different modalities of international transfers of several categories of conventional arms, including, among others, firearms, their parts and components and ammunition. The scope of the Treaty is clearly geared towards addressing the international dimension of the trade. The export criteria to assess the risks of diversion and illicit trafficking apply prior to the actual transfer and pre-suppose the observance of an established regulatory and control mechanism, which – as described above – would be completely circumvented by the purchases via the dark web. However, what appears clear is that cases of illicit domestic trafficking of these items through the dark web would not be covered by this instrument.

b1. Involvement of an organised criminal group

In order to invoke the cooperation provisions under the Organized Crime Convention and the Firearms Protocol, States must therefore prove or at least have the suspicion that the offence involves an organised criminal group and is of transnational nature.

The Convention defines an organised criminal group as a '*structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention [or the Protocols thereto], in order to obtain, directly or indirectly, a financial or other material benefit*' (article 2 a). The research presents some useful indications as to when the involvement of such a group is likely. Hints of a possible

involvement of more than three persons in the illicit transfers arise at different levels: as vendors often seem to advertise firearms as a package deal with ammunition or parts and components, this may suggest that the vendor can procure requested items through a channel or network of contacts (see discussion after section 3.2.1). This possible conclusion could also be supported by the fact that the total of 339 firearms-related listings were assigned to only 60 vendor accounts (see section 4.3.1). While the research explains that many vendors might entertain several listings for the same item, there is also a possibility that the comparatively small number of vendors can rely on a larger arsenal of firearms, parts and components and ammunition that are not their personal items but procured through a network of people. Moreover, the mere possibility to verify how many and what listings an individual vendor maintains can provide useful insights into the vendor's portfolio. A vendor offering firearms as well as drugs and other items that are illicitly procured over the dark web, might be a member of a structured group that traffics firearms and other items for a material benefit. As discussions and research on the topic continue, further attention should also be brought to the question of the extent to which an individual vendor, who only relies on selling personal items, can efficiently maintain a good reputation on the dark web, which, as the research explains, is fundamental for attracting buyers.

Lastly, there might be a need to further analyse the extent to which the definitions provided by the Organized Crime Convention for the 'structured'[172] and the 'organized criminal' group can be applied in the context of the changing criminal environment in the virtual world, where anonymous vendors and buyers can transact across a seemingly unlimited geographical reach without knowing each other. In this connection, it might be worthwhile to note that according to the interpretative notes for the official records of the negotiation of the Organized Crime Convention and the Protocols thereto (A/55/383/Add.1, par.4), the term 'structured group' is meant to be used in a broad sense, so as to include both groups with a hierarchical or other elaborate structure and non-hierarchical groups, where the members are not formally specified. This concept is therefore meant to involve all instances of crimes that involve any element of organised perpetration.[173] In practical terms, this would suggest that in our specific context, not only is there no need to have a clear definition of the roles and functions of each group member, but the members themselves do not even need to know each other in person in order to form a structured group.

The other distinctive qualifier of an 'organised criminal group', namely the aim to 'obtain, directly or indirectly, a financial or other material benefit' seems to be largely fulfilled in our specific cases, as it relates to crimes with tangible and non-monetary objectives and aims to exclude conspiracies with purely non-material objectives, such as ideological goals, for example.[174]

b2. Transnational nature of the offence

As outlined above, the offence of 'illicit trafficking' in firearms, their parts and components and ammunition as set out in the Firearms

172 According to the Convention, a 'structured group' shall mean a group 'that is not randomly formed for the immediate commission of an offence and does not need to have formally defined roles for its members, continuity of its membership or a developed structure' (UNGA 2000, article 2c).

173 UNODC (2004, 14).

174 UNODC (2004, 23).

Protocol requires the physical, cross-border transfer of items from or across one State Party to another State Party.

The list of available shipping locations used by firearms vendors (Box 5.1 in section 5.2) shows that vendors are generally willing to transfer items from mainly North American and European countries to all parts of the globe, including explicitly, among others, Africa, Asia, North and South America and Europe. The research further indicates that only 9 per cent of the total identified confirmed transactions were of domestic nature (see discussion in section 5.1). Taking into account the scope of the research and the introduced caveats, this result still seems to provide a basis for law enforcement agencies to conduct investigations with reasonable grounds to suspect that the transfer of intercepted items was in fact of a transnational nature.

Although not explicitly required under the Protocol, it might be a good practice for States to consider establishing a separate offence that criminalises domestic illicit transfers of firearms, their parts and components and ammunition, including on the dark web, i.e. that does not set the cross-border transfer requirement. Several States already have similar provisions in place that complement the mandatory international trafficking offence of the Protocol. If States were to categorise such conduct as 'serious crime',[175] the provisions of the Organized Crime Convention would be applicable under the condition that an organised criminal group is involved and the offence is of transnational nature (article 3 paragraph 1 of the Convention). Regardless of the specific cross-border element introduced by the Firearms Protocol in the offence of 'illicit trafficking', the Convention considers an offence to be of transnational nature if: '*(a) It is committed in more than one State; (b) It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State; (c) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or (d) It is committed in one State but has substantial effects in another State*' (article 3 paragraph 2).

c. Measures that contribute to tackling illicit trafficking through the dark web

From a regulatory perspective, the transfer control system and the requirement to obtain export and import authorisations as set up by the introduced legal framework (article 10 of the Firearms Protocol, articles 5 to 8 of the ATT) seem to be completely circumvented by parties to illicit firearms transactions on the dark web who benefit from the personal and geographical anonymity features that the trade on the dark web bring.

Beyond this, the international legal framework provides additional legal and operational measures that the different stakeholders and actors of the law enforcement system can undertake as part of a comprehensive and integrated strategy to prevent, combat and eradicate the illicit trafficking in firearms, their parts and components and ammunition, especially on the dark web.

c1. Legal perspective

From a legal perspective, there is first of all a need to examine how to strengthen control over marketplace administrators. The research explains that administrators of cryptomarkets perform essential functions in transactions by providing a platform that

175 According to the Convention, a 'serious crime' shall mean 'conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty' (UNGA 2000, article 2b).

allows the display of business opportunities, facilitates the establishment of contact between the involved parties and builds confidence between vendors and buyers by offering payment escrow services and setting up feedback features (section 2.2).

Given this important role that marketplace administrators play in creating business opportunities and enabling their materialisation, an in-depth analysis of whether existing **brokering** regulations as provided by the Firearms Protocol and the ATT would be applicable, is required. While none of the introduced international instruments contains a definition of brokers, a 2007 Report of a UN Governmental Group of Experts defines them as '*a person or entity acting as an intermediary that brings together relevant parties and arranges or facilitates a potential transaction of small arms and light weapons in return for some form of benefit, whether financial or otherwise*'.[176] The Expert Group report further specifies that brokering activities can include, among others, serving as a finder of business opportunities to one or more parties; putting relevant parties in contact; assisting parties in proposing, arranging or facilitating agreements or possible contracts between them; assisting parties in obtaining the necessary documentation; and assisting parties in arranging the necessary payments. This definition and examples have also been integrated in the International Small Arms Control Standards (ISACS), which are a set of voluntary standards developed by the UN and other partners to provide a clear, practical and comprehensive guidance to practitioners and policy makers on fundamental aspects of small arms and light weapons control.[177]

While many countries do not have an arms brokering control system in place, it should be noted that the Firearms Protocol requests State Parties to consider establishing such a system (article 15). Moreover, this provision was recently reinforced by the ATT, which made it mandatory for States Parties to regulate brokering activities taking place under their jurisdiction (article 10). The establishment of a comprehensive arms brokering control system, including the establishment of illicit brokering as a criminal offence, might therefore constitute an important preventive measure and a precondition for an effective criminal justice response to illicit brokering activities conducted on the dark web and elsewhere.

A second fundamental legal question relates to the **competent authority** of law enforcement agencies and **jurisdiction** of courts of States that intend to operationally fight against illicit arms trafficking on the dark web.

The Organized Crime Convention does not stipulate within which geographical scope law enforcement agencies have the authority to investigate offences. While this depends on the national legislation of the concerned countries, it is generally assumed that law enforcement agencies are authorised to conduct investigations within the geographical scope of their own territory.

As regards the question of jurisdiction, the Convention provides that States Parties *must* establish jurisdiction over all offences established by the Convention and any Protocols to which the State in question is a party committed within the territory of the State, including its marine vessels and aircraft (article 15 of the Convention, article 1 paragraph 2 of the Firearms Protocol). States are also required to establish jurisdiction in cases where they cannot extradite a person on grounds of nationality. Furthermore, States are encouraged to

176 UNGA (2007).

177 ISACS (2016).

establish the optional jurisdiction in all other circumstances, when the nationals of a State are either victims or offenders, or when the offence is committed outside the territory, but with a view to the commission of a serious crime within its territory, or with a view to laundering the illicit proceeds deriving from these offences within its territory.

While the offence of illicit trafficking in firearms, their parts and components and ammunition is generally committed in the respective countries where the offenders ship and receive the items (i.e. the exporting and importing States), investigations might also have to take place in third countries. These may include, among others, the country where the accused offenders reside in cases where items are shipped from or to a third country, or, even though difficult to determine, the country where the server on which the cryptomarket operates is located.

Challenges relating to the authority of law enforcement agencies can also be resolved on the basis of the Organized Crime Convention through bilateral and multilateral agreements as well as international police cooperation mechanisms that can help to practically broaden this scope of authorised intervention.

c2. Operational perspective

The introduced international legal framework provides for several operational measures that law enforcement agencies and other authorised stakeholders can employ to support the fight against illicit firearms trafficking on the dark web, where the act is transnational in nature and involves an organised criminal group. The following constitutes an overview of the most relevant measures.

- Information exchange – The exchange of information, including on organised criminal groups involved in firearms trafficking, means of concealment, modus operandi, and scientific and technological information that enhances a State's abilities to counter illicit firearms trafficking, is regulated in all three instruments (article 12 of the Firearms Protocol, article 28 of the Organized Crime Convention, article 15 of the ATT). Those provisions reflect the underlying conviction that knowledge and information exchange can positively contribute to advancing the fight against illicit firearms trafficking. Such information exchange must be encouraged and facilitated at all levels, including through spontaneous exchanges of information on criminal matters between competent authorities, without prior requests (article 18 paragraph 4 of the Organized Crime Convention).
- Border control and transborder cooperation – In order to increase the effectiveness of import, export and transit controls, the Firearms Protocol requires States Parties to conduct border controls as well as police and customs transborder cooperation (article 11 b). The Organized Crime Convention reinforces transborder cooperation by encouraging States Parties to conclude bilateral and multilateral agreements that facilitate the establishment of joint investigative bodies (article 19) and to allow direct cooperation between their law enforcement agencies (article 27 paragraph 2). Both provisions provide frameworks to facilitate and enhance effective coordination among law enforcement agencies, such as through the exchange of personnel and other experts, the posting of liaison officers or other means of direct cooperation. Moreover, speedy and reliable information exchange is considered a cornerstone of effective law enforcement cooperation and the Convention requires States Parties to establish channels of communication in order to facilitate the secure and rapid exchange of information

concerning all aspects of the offences covered by the Convention and its Protocols (article 27 paragraph 1).

- International judicial cooperation – Two of the key measures provided by the Organized Crime Convention, namely mutual legal assistance (article 16) and extradition (article 18), relate to international cooperation among judicial organs. These measures help to ensure that admissible evidence and the accused offender are present in the territory of the State that has assumed jurisdiction. As outlined above, a State Party can request mutual legal assistance if it has reasonable grounds to suspect that the investigated offence is transnational in nature, including that victims, witnesses, proceeds, instrumentalities or evidence of the offence are located in the requested State Party and that the offence involves an organised criminal group (article 18 paragraph 1). The underlying philosophy of the Organized Crime Convention is to promote effective cooperation in criminal matters at all levels and by all means, providing the tools and measures necessary to overcome the often formal, legalistic and procedural obstacles that may hamper effective cooperation, and suggesting forms and ways to expedite and simplify, where possible, the means and methods of cooperation among States.
- Special investigative techniques – The Convention further foresees special investigative techniques such as controlled deliveries, electronic and other forms of surveillance, undercover operations and other measures that the investigating State Party deems appropriate and that are permitted by the basic criminal procedure principles of its domestic legal system (article 20). These techniques are especially useful in dealing with sophisticated organised criminal groups because of the dangers and difficulties inherent in gaining access to their operations and gathering information and evidence for use in domestic prosecutions, as well as providing mutual legal assistance to other States Parties.[178] In many cases, less intrusive methods will simply not prove effective, or cannot be carried out without unacceptable risks to those involved. Traditionally, the inclusion of these special investigative techniques often almost exclusively applied to drugs trafficking cases, also because their use was first encouraged through the international drug control regime; but increasingly, their use and application has expanded also to other criminal offences. A renewed understanding of these techniques and their applicability to different forms of crimes and different criminological environments, such as the dark web, is required to find the best way to operationalise and apply these tools to the new context.
- Cooperation with law enforcement authorities – The investigation of sophisticated transnational criminal groups and the process of enforcing the law against them can be greatly assisted by the cooperation of members and other participants in the criminal group.[179] The Organized Crime Convention therefore requests States Parties to take appropriate measures to encourage persons who participated in organised criminal groups to cooperate with the law enforcement agencies by supplying insights and useful information as well as factual and concrete help that

178 UNODC (2004, 183).

179 UNODC (2004, 165)

may contribute to depriving those groups of their resources (article 26). This type of incentives was developed for criminal situations in which the level of integration of the members of a criminal group is highly compact and not penetrable by outsiders, so that only the support of insights from members of the group can help. The more unknown the environment to the outside world, the more important will it be for criminal justice systems to provide for incentives, rewards or 'golden bridges' that can encourage this type of cooperation. This would apply particularly to the situation under review.

- Preventive and security measures – As rightly highlighted in the previous chapter (section 6.3.2), for criminals to traffic firearms, their parts and components and ammunition through the dark web, those items must be available and accessible to the vendor. The most important measures to reduce illicit availability of these items are foreseen in the introduced international legal framework. Those include stockpile management – including the marking and record-keeping of firearms (articles 7, 8 and 11 a of the Firearms Protocol); establishment and promotion of best practices and policies aimed at preventing transnational organised crime (article 31 paragraph 1 of the Convention); seizing, confiscating and disposing of firearms, their parts and components and ammunition that have been illicitly manufactured or trafficked (article 6 of the Firearms Protocol); deactivation of firearms that are no longer intended to be operational (article 9 of the Firearms Protocol); and the establishment of a comprehensive and secure transfer and brokering control regime (articles 10, 15 of the Firearms Protocol, article 5 and following of the ATT).

The above shows that all introduced instruments provide operational measures that can greatly contribute to addressing illicit trafficking in firearms, their parts and components and ammunition on the dark web. Based on these measures, States should develop comprehensive approaches to tackle the phenomenon. This requires, however, that stakeholders adapt their approaches and investigative techniques from the 'real' to the 'virtual' world and the changing criminal environment. These approaches should pay particular attention to the modus operandi used in web transactions, such as parcel deliveries of the procured items and the use of cryptocurrencies as payment modality. They should further focus on those occasions when criminals need to leave their anonymity behind. The latter cases include in direct communications between vendors and buyers, when shipping or receiving parcel deliveries, when cryptomarket administrators request listing of their marketplace on a web page indexed on the clear web, or when the shipment is actually taking place after the completion of the transaction on the dark web.

d. Policy-level conclusions

The above allows us to draw the following policy-level conclusions:

- The introduced legal instruments 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 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 Party to it.[180] There are also several States that have not yet adhered to the ATT. Further efforts towards universalisation 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 and components and ammunition, stakeholders can reduce the risk of those items entering the illicit market. Stakeholders should therefore double their efforts to fully transpose and implement the international legal framework at the domestic level, in an efficient and comprehensive manner, including the foreseen preventive and security as well as enforcement measures.

180 For a full list of State Parties to the Firearms Protocol, see UNGA (2001).

Appendix A – Glossary[181]

Term	Explanation/definition
Administrator	The administrator sits 'at the top of the cryptomarket hierarchy' and within this role has 'full access to the cryptomarket' (Martin 2014, 18). The administrator has an executive and managing role on the marketplace, is responsible for the policies on the marketplace and 'fulfils the role of treasurer with regard to cryptocurrency' (Van Slobbe 2016, 79).
Ammunition	The complete round or its components, including cartridge cases, primers, propellant powder, bullets or projectiles, used in a firearm. (UNGA, 2001)
Buyer	Customers on cryptomarkets who buy goods on vendors' seller pages, can provide feedback on these purchases and may be involved in discussions on forums.
Bitcoin	The best-known and most popular cryptocurrency or virtual currency, used on cryptomarkets to make purchases. On Silk Road, only Bitcoin was supported as a payment currency. Bitcoins are not issued by any government, bank or organisation, and can be purchased in person or through online exchanges such as CoinBase.
Cryptocurrency	'A peer-to-peer, client-based, completely distributed currency that does not depend on centralised issuing bodies (a 'sovereign') to operate. The value is created by users, and the operation is distributed using an open-source client that can be installed on any computer or mobile device' (Guadamuz & Marsden 2015) As a virtual asset, in contrast to traditional printed units of fiat money, cryptocurrency cannot be completely destroyed or lost and new units are impossible to create.
Crypto-exchangers	Cryptocurrencies can be purchased through online exchanges such as CoinBase.
Clear web (or clear net or surface web)	The open part of the internet that is indexed by search engines.

181 Adapted from Kruithof et al. (2016).

Term	Explanation/definition
Cryptomarket	Online marketplace on the hidden part of the web that has been intentionally hidden and is inaccessible through standard web browsers. It sells illegal drugs and other goods and services and customers can search and compare products and prices across multiple vendors (EMCDDA 2015).
Customer feedback	When making a purchase, customers are strongly encouraged to leave feedback. This feedback is posted underneath each listing and usually includes a date, a message (e.g. 'Great product, fast delivery, would repeat business') and a score. Customer feedback as a proxy for transactions will always result in an extent of underestimation of actual transactions (Aldridge & Décary-Hétu 2014; 2016b; Christin 2013; Soska & Christin 2015).
Deactivated (gun)	Genuine firearm which has been rendered inoperable (i.e. incapable of expelling a projectile) (King 2015).
Dark net (or dark web or hidden web)	The hidden part of the internet that is not indexed by search engines (Aldridge & Décary-Hétu 2014; Martin 2014).
Encryption	The process of encoding a message or information and making it unreadable by using an algorithm.
Exit scam	Scam whereby the site's administrators suddenly take the market offline and steal users' money kept in their escrow accounts (Woolf 2015).
Finalise early (FE)	A circumvent escrow that ensures direct payment without funds first being held in escrow as a backup measure in times of high concerns over exit scams or law enforcement seizure, reducing the risk that vendors and buyers lose the funds held in escrow.
Escrow	An arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorised third party may gain access to those keys. Payment is only released to the vendor when the buyer has finalised the sale by indicating that the product has been delivered.
Firearm	Any portable barrelled weapon that expels, is designed to expel or may be readily converted to expel a shot, bullet or projectile by the action of an explosive, excluding antique firearms or their replicas. Antique firearms and their replicas shall be defined in accordance with domestic law. In no case, however, shall antique firearms include firearms manufactured after 1899 (UNGA 2001).
Illicit manufacturing	Manufacturing or assembly of firearms, their parts and components or ammunition: (i) from parts and components illicitly trafficked; (ii) without a licence or authorisation from a competent authority of the State Party where the manufacture or assembly takes place; or (iii) without marking the firearms at the time of manufacture in accordance with article 8 of the UN Firearms Protocol. (UNGA 2001)

Term	Explanation/definition
Illicit trafficking	Import, export, acquisition, sale, delivery, movement or transfer of firearms, their parts and components and ammunition from or across the territory of one State Party to that of another State Party if any one of the States Parties concerned does not authorise it (UNGA 2001).
Marketplace	In the context of this study we refer to online marketplaces, which bring together multiple sellers in one location.
Moderator	Moderators 'are ranked below administrators in the cryptomarket hierarchy and assist with lower-level site maintenance and customer support' (Martin 2014, 18). As such, the moderator has less access to the infrastructure of the marketplace and user information than the administrator (Martin 2014; Van Slobbe 2016). Moderators could sometimes receive a salary from the administrators (Martin 2014).
Multisignature escrow	A cryptographic tool that allows buyers to put bitcoins in an escrow account that requires sign-off from two out of three parties – the buyer, the seller and the website itself – to retrieve the funds. (Mounteney et al. 2016).
Operation Onymous	Operation Onymous was an internationally coordinated police operation led by the FBI in the United States and involving authorities in 21 countries (Europol 2015). On 5 November 2014, the FBI, together with the US Drug Enforcement Administration, Homeland Security Investigations and European law enforcement agencies acting through Europol and Eurojust, shut down multiple marketplaces including Silk Road 2.0.
Parts and components	Any element or replacement element specifically designed for a firearm and essential to its operation, including a barrel, frame or receiver, slide or cylinder, bolt or breech block, and any device designed or adapted to diminish the sound caused by firing a firearm (UNGA 2001).
PGP Key	Pretty Good Privacy is a data encryption that provides end-to-end cryptographic privacy and authentication that vendors use to encrypt their communications, whereby each individual has a unique PGP key (Cox 2016b).
Reddit	Reddit is a website for online content covering a broad range of topics where registered members can enter and share content.
Replica (gun)	A device that is not a real firearm, but that was designed to look exactly or almost exactly like a real firearm. Replica firearms include blank-firing/ alarm firearms, air guns or even toy guns (King 2015).
Silk Road	The first large anonymous online cryptomarket located on the dark net. It was founded in 2011 and was shut down by the FBI in 2013 (Aldridge & Décary-Hétu 2014; Martin 2014). Several weeks after the taking down of Silk Road, Silk Road 2.0 was launched, which is why the former is also referred to as Silk Road 1.0 or SR1.

Term	Explanation/definition
Stealth listings	Vendors can create listings that are not available for public view, referred to as 'stealth' listings. Vendors send links to these listings privately, but transactions are still processed via the marketplace with escrow facilities remaining available to protect buyers (Aldridge & Décary-Hétu 2014).
Tor	Anonymising software that uses encryption to make it difficult for anyone to trace IP addresses (i.e. codes assigned to each computer on the internet) (Barratt 2012, 683).
Tracing	Systematic tracking of firearms and, where possible, their parts and components and ammunition from manufacturer to purchaser for the purpose of assisting the competent authorities of States Parties in detecting, investigating and analysing illicit manufacturing and illicit trafficking (UNGA 2001).
Vendor	A vendor sells his or her (illegal) goods to customers through his or her own seller page (Martin 2014).
Vendor shops	A cryptomarket that is run by one vendor, which allows vendors to deal directly with their customers avoiding the risks associated with third-party escrow or the need to pay a commission to the cryptomarket administrators.
Web crawler	Software that methodologically archives websites and extracts information from them. To do so, it starts at a fixed web page (usually the homepage), downloads that page and parses it for hyperlinks to other pages hosted on the same website. It then follows each hyperlink, adding new hyperlinks it discovers to its list of pages to visit until no new pages are found.
Web scraper	A computer software technique to extract information from downloaded web pages identified by a web crawler.

Appendix B – A brief history of firearms on the dark web

The emergence of firearms on the dark web

The sale of firearms on the dark web has been a contentious topic among buyers, vendors and market administrators – let alone law enforcement agencies and the broader public – since the emergence of early cryptomarkets. The Silk Road (SR1) rose to notoriety in June 2011 after an article posted on the technology blog *Gawker* uncovered the workings of the cryptomarket,[182] which drew others to label it as an 'Amazon or eBay' for drugs.[183] At the time, SR1's anonymous administrator (known by the moniker Dread Pirate Roberts [DPR]) limited the terms of service and banned 'anything who's [sic] purpose is to harm or defraud, such as stolen credit cards, assassinations, and weapons of mass destruction.'[184] Despite the illegal activities they facilitate, most dark web markets still have a code of conduct.

Seven months later, *Gawker* covered the reversal of SR1's terms of service and policy on listing weapons, whereby an 'entire subcategory for firearms has sprung up.'[185] The sale of weapons on SR1 caused controversy among users, most of whom were primarily concerned with the sale of narcotics, and took to message boards and forums to express their views. Selling weapons on cryptomarkets has the obvious benefit of financial gain for the site administrators, who take a commission on sales. Arguably, banning the sale of weapons should reduce attention from law enforcement agencies; it should also reduce the likelihood of vendors scamming buyers over high-value weapons and align with the principle of reducing third-party harm. By January 2012 SR1 had a meagre total of 13 firearms listings, which included handguns, semi-automatic rifles, ammunition and a silencer.[186]

'The Armory': The first cryptomarket for weapons

By early 2012, the weapons section of SR1 had been spun off onto a separate cryptomarket called 'The Armory'.187 Promising the timely delivery of weapons to anywhere around the

182 Chen (2011).
183 Barratt (2012).
184 Chen (2011).
185 Chen (2012).
186 Chen (2012).
187 Biddle (2012).

world, The Armory utilised a standard cryptomarket design: access was permitted to anyone worldwide using the Tor network, in combination with Bitcoins,[188] plus escrow services were provided by the market to protect buyers from vendor fraud. A Gizmodo journalist posing as a buyer wanting to equip a 'private army and overthrow a 3rd world government' was able to source an arms trafficker willing to sell him military-grade equipment, including 'artillery, MANPADS [Man-portable air-defence systems], ordnance, APCs [Armoured Personnel Carriers], Helos [helicopters]…'[189] The journalist pondered 'the huge and necessary question' about the authenticity of vendors:

> '…*Are these people real?* Is [it] just an elaborate scam…? …Are these 'dealers' just putting together a federal sting operation? Sure, maybe – but there's plenty of reason to believe this is just as terrifyingly real as it looks.'

The Armory, like all cryptomarkets, was susceptible to scammers looking to defraud buyers.[190] The high average price of weapons when compared to individual quantities of drugs seemed to make them a more lucrative product segment to scam. The vendor 'Arms Depot' reportedly took up half of the listings on the cryptomarket and directed traffic to his own vendor shop with reduced prices, where the transaction was finalised using the 40/60[191] method.[192] Arms Depot used their technical knowledge and delaying tactics to successfully scam users on the cryptomarket.[193] Approximately six months after opening, in July 2012 The Armory closed. In a note posted on the cryptomarket, subsequently re-blogged on the clear web, DPR explained the server costs were too high in proportion to the volume of sales, and 'it just wasn't getting used enough', without mentioning the prevalence of scamming.[194] All vendors were instructed to finalise their sales and 'withdraw your coins before the end of the countdown'. To avoid resentment from vendors who might have lost money when paying a 'vendor bond' to open their account, DPR suggested they 'contact us on the armory [sic] and we'll get you a refund'. Without hesitation, DPR silenced any speculation that SR1 would allow the sale of guns: 'The answer there is most definitely NO.'[195]

Following the policy reversals of early cryptomarket admins, the sale of weapons online in 2013 was headed into a phase characterised by mistrust, sophisticated scams and fraud, as shown below. The single-vendor site and weapons dealer 'Executive Outcomes' (EO) drew press coverage in the media, which may have boosted traffic and sales numbers.[196] By November 2013, EO was believed to be a scam site since it attracted critical reviews on the clear web and condemnation by the founder of the private military company established

188 Bitcoins are not untraceable by design, yet obfuscation techniques of Bitcoin 'tumbling' are commonly used in attempts to anonymise payments on the public ledger.

189 Biddle (2012).

190 Cox (2015).

191 A typical payment method is to require payment of 40 per cent up front, while the remaining 60 per cent is paid on receipt of the goods.

192 'Darknetsolutions' in Reddit (2015).

193 'Darknetsolutions' in Reddit (2015).

194 The following quotes are excerpts from DPR in BitcoinTalk (2012).

195 BitcoinTalk (2012).

196 Smith (2013); Boggan (2013).

in 1989, trading under the same name.[197] As part of Operation Onymous in November 2014, where raids were carried out on over 400 dark web .onion addresses, the Federal Bureau of Investigation (FBI) confirmed in a press release that EO's servers had been seized.[198]

In another sophisticated scam, a non-SR1-affiliated version of The Armory opened in July 2013, riding on the reputation and notoriety of the original version that closed 12 months prior.[199] The site has since attracted negative comments and allegations of scamming on the clear web.[200] In an interview with a *Vocativ* journalist in February 2014, the site admin(s) answered a range of questions and gave a rare insight into the operation of a single-vendor weapons site:

- Allegedly, a staff of eight manned the store on 50-hour weeks, with an undisclosed number working in acquisitions and transportation.
- Sales were estimated to range from $7,000 to $30,000, mostly though private contacts with a transaction history. Private security forces were considered to be the largest clients.
- The dark web accounted for only 10 per cent of sales, and most buyers were from the Middle East.
- The best-selling handgun was allegedly the Glock 17, while the Soviet AK47 was most popular for 'unique sales' and the Colt M4 for bulk orders; the most popular shotgun was the Remington Super Shorty.
- Sales per month were approximately 30–70, which moved to a low of 10–40 after a market downturn due to 'scared' customers and scams operating on other markets.[201]

The move of disclosing the operational details of a dark web single-vendor store was unprecedented. The initial effect of the interview might have reassured potential buyers, and gave a façade of legitimacy. The effect, however, might not have lasted long, given the overwhelming evidence on the clear net, both on subreddits and dark web market lists, of the fraudulent activity on the market.[202]

The end of the road…

The arrest of Dread Pirate Roberts, real name Ross William Ulbricht, and subsequent takedown of SR1 in October 2013[203] temporarily disrupted the ecosystem of online black markets, according to criminologists and social scientists Décary-Hétu and Giommoni.[204] Users flocked to other cryptomarkets after the SR1 'displacement' event. 'Black Market Reloaded' (BMR) was the largest and experienced a twofold increase in the number of dealers in a six-week period. A smaller market, 'Sheep', experienced a fourfold increase in vendors at the same time.[205]

197 Barlow (2013).
198 US DOJ (2014).
199 Matthews (2014).
200 Deepdotweb (2017c).
201 Matthews (2014).
202 Deepdotweb (2017c).
203 Segal (2014).
204 Décary-Hétu & Giommoni (2016).
205 Décary-Hétu & Giommoni (2016).

By December 2013 Sheep reportedly experienced a 'theft' of 5,400 Bitcoins (~$40m), forcing the cryptomarket to shut down.[206] It would be revealed later the market administrator absconded millions in cryptocurrency in an exit scam.[207] Around the same time, the admin of 'Project Black Flag' closed the site and absconded with the funds, saying they 'panicked' after the mounting stress and pressure.[208] The well-stocked weapons category of BMR[209] was the next cryptomarket to shut under the mounting pressure on their hidden servers after SR1's departure.[210]

In October 2014, a large-scale international law enforcement operation targeted dark web markets, called Operation Onymous.[211] All told, Europol along with the FBI and the Department of Homeland Security (DHS) announced the operation led to 17 arrests in as many countries, taking offline over 400 .onion dark web pages, including three cryptomarkets and seven single-vendor sites.[212] During the operation, the single-vendor shop administrator of 'Black Market' was arrested. The Swiss man arrested claimed the site was only a scam and never shipped any products.[213]

Soska and Christin, in their comprehensive study of the longitudinal evolution of the cryptomarket ecosystem, come to a similar conclusion to Décary-Hétu and Giommoni when they show how cryptomarkets are resilient to both scams and law enforcement takedowns.[214]

Suspicion, shills and scams

The cryptomarket environment continued to shift and change in 2015 in response to alleged exit scams, honeypot vendor accounts, market closures and the displacement of vendors and buyers. In March 2015, the largest online drug cryptomarket to take the place of SR1, 'Evolution', vanished off the dark web.[215] On the subreddit /r/DarkNetMarkets the self-proclaimed 'public relations' officer of Evolution, NSWGreat, notified the darknet community of the alleged exit scam by the administrators, Verto and Kimble:

> 'Confronted Kimble and Verto about it, they confirmed it and they're doing it right now.
>
> EDIT: Servers have gone down, including back up server for staff. I'm sorry for everyone's loses, I'm gutted and speechless. I feel so betrayed.
>
> EDIT2: Yes this is real, no this isn't maintenance. No I can't help anyone. Evolution

206 Greenberg (2013).

207 Deepdotweb (2014b).

208 MettaDPR in Reddit (2014).

209 Bilton (2013).

210 Greenberg (2013).

211 The target of Operation Onymous was allegedly the admin of 'Silk Road 2', who had established the site months after the close of SR1. 'Cloud 9' and 'Hydra' were also taken offline as a result of the multiagency law enforcement operation. (Greenberg 2014a)

212 Greenberg (2014a; 2014b).

213 Deepdotweb (2014a).

214 Soska & Christin (2015).

215 Greenberg (2015).

> can officially be put on the Wall of Shame.'[216]

A month later in April 2015, a widely reputable vendor, 'weaponsguy', on the then-largest cryptomarket, 'Agora', was outed – with a high degree of confidence by independent researcher Gwern Branwen – as a law enforcement honeypot vendor account.[217] The irregular feedback dates of weaponsguy, who claimed to be on holidays, were similar to a precedent set by past flipped vendors (apparently 'Dark_Mart' on Evolution followed the same pattern).[218] The activity on the flipped vendor account might have led to the arrest of a Justin Moreira from Hyannis, Massachusetts, who attempted to purchase a firearm and silencer on the dark web.[219] The supposed case of law enforcement agencies flipping cryptomarket buyers cast a long shadow over the trustworthiness of even the longest-serving vendors with strong track records of verified sales.[220]

A May 2015 press release published by the Australian Federal Police (AFP) details the international law enforcement operation leading to the arrest of 17 individuals across Australia, the United Kingdom, Europe and North America in connection to activities on the dark web.[221] Branwen was quick to post an in-depth review of the open-source evidence, plus the latest operational details in the AFP press release, to show the vendor account weaponsguy's was likely used by 'three letter' law enforcement agencies to catch prospective weapons buyers.[222]

In July 2015, the cryptomarket Agora banned the sale of lethal weapons. It published a comprehensive post outlining the reasons behind banning weapons on the marketplace. The note makes specific mention of 'honeypot listings by agencies', since it was known weaponsguy operated on Agora and there was growing speculation that Justin Moreira had a buyer's account on the same market under the moniker 'jd497'[223]:

> ––BEGIN PGP SIGNED MESSAGE––
>
> Hash: SHA512
>
> Starting from July 15th 2015 Agora will no longer list lethal weapons.
>
> Following our mission we wish such objects would be available for purchase, but the current reality of it is that the format of a market like ours does not constitute a good way to do it. Shipping weapons is hard, they are expensive and stimulate both scamming by dishonest vendors and honeypot listings by agencies looking to find buyers who might wish to obtain such weapons illegally from us. This has been reflected for a long time in both the volume and the success rates of our listings in the weapons section.
>
> At this point continuing to list weapons would do more harm than good for our users.
>
> [Signed using Agora's PGP signature]

---

216 NSWGreat (2015).
217 Branwen (2015a).
218 Branwen (2015a).
219 US DOJ (2015b).
220 Deepdotweb (2015b).
221 Deepdotweb (2015a).
222 Branwen (2015b).
223 Branwen (2015a).

One short month later in August 2015, Agora's administrators halted the operation of the cryptomarket.[224] Due to growing concerns over deanonymising server locations[225] and discovering 'suspicious activity' around their servers, they instructed all vendors and buyers to withdraw their money from their accounts and to finalise their operations because the servers were being taken offline. Assurances were given that all market data would be intact and available upon return, including all user history and profile data. Allowing users to access their funds – in a rare move against the precedent set by markets exit scamming – drew praise from the darknet community.[226]

224 AgoraMarket (2015).

225 Goodin (2015).

226 C3LT1C (2015).

Appendix C – Who is using the dark web to procure firearms?

This appendix expands on the examples provided in Chapter 1, examining in greater detail a number of recent cases in the context of terrorism and extremism, serious and organised crime, and vulnerable and fixated individuals. The cases below relate to both vendors and buyers of weapons. Not all the cases documented below are instances of 'successful' transactions over the dark web. Rather, some detail police sting operations, controlled deliveries and scams. While the introduction highlighted the most serious and significant incidences of firearm trafficking over the dark web, this appendix demonstrates the potential breadth of the threat by documenting a wide range of cases in the three actor classes.

Note:

No full review of court files and records associated with the cases below was conducted as part of this study; therefore, the information presented in this appendix is primarily based on how it has been reported by open-source outlets including the media and governmental/organisational agency press releases. While the project team attempted to identify official sources when these were available in English, the accuracy of the information provided below cannot be confirmed. Such information is provided only as a tool to document the breadth of cases reportedly linked with dark web arms trafficking.

Terrorism and extremism

Section 1.1 mentioned how dark web arms trafficking has been associated with the November 2015 terrorist attacks in Paris. However, as well as terrorism motivated by Islamist religious extremism, there have also been examples of firearms being obtained online for other ideological or political extremism. For example, between the second half of 2016 and early 2017, the 'Migrantenschrek' (literally 'Migrant Fright') clear web website, believed to be linked to right-wing extremists in Switzerland, was reportedly selling firearms.[227] According to German media outlet Zeit Online, more than 300 weapons were ordered, only 42 of which

227 The Local/DPA (2017).

could be recovered.[228] Most of the purchases were of Schreckschuss revolvers, but other weapons were also obtained. Although the Swiss authorities and police were aware of the gun sales from the site, they lacked the appropriate legislation, limiting their response; however, following a series of house searches of those who had purchased weapons from the site, it is believed that its owner became intimidated and took the site down of their own volition in early 2017.[229]

In November 2016 it was reported by the media that a 37-year-old man from Herent, Belgium, who had watched film material about the conflict in Syria and was worried about the threat posed to his family by 'asylum seekers', decided to 'protect his family' by obtaining firearms.[230] According to Deepdotweb's Benjamin Vitáris, reporting on court documents, he subsequently ordered a package of weapons from a US vendor on the dark web, which included a Kalashnikov assault rifle, a Glock automatic pistol, a silencer and ammunition.[231] Belgian police were alerted, possibly by the national border authorities, seizing the package and arresting the man when it arrived at his home address.[232]

In a similar recent example from the United Kingdom, Harry Woodward, a 21-year-old from Newark, reportedly attempted to purchase a Glock handgun and 100 rounds of ammunition from the dark web in order to 'defend himself from a terrorist incident'.[233] The National Crime Agency (NCA), after receiving intelligence from a US agency monitoring the communication between Woodward and a dark web vendor, intervened before the handgun and ammunition were delivered. Woodward has since received a 21-month sentence, and he could have been jailed for up to seven years if the weapon had come into his possession.[234]

Crime

A number of individual criminals have allegedly been involved in the procurement of weapons and firearms over the dark web, as the following instances show. In November 2016 a 35-year-old Belgian police officer from the Charleroi Security and Intelligence Group was arrested. According to *The Brussels Times*, the police officer had already successfully received a number of firearms packages containing various weapons and explosives from dark web vendors and was allegedly planning two murders of his ex-girlfriend's partners; his house was searched upon arrest and police found numerous other weapons.[235] The previous month in September 2016, the German Federal Police (BKA) arrested a 24-year-old man from Neuburg-Schrobenhausen after he attempted to buy weapons and ammunition on the dark web.[236] Upon searching his home address, a cannabis-growing operation was discovered and it was believed he was involved in supplying drugs. Likewise, on 5 September 2016, the Police Service of Northern Ireland

228 Biermann (2017).
229 Biermann (2017).
230 Vitáris (2016b).
231 Vitáris (2016b).
232 Vitáris (2016b).
233 Gorman (2015).
234 Gorman (2015).
235 Anderson (2016).
236 Petry (2016).

(PSNI) arrested one of its own officers after he used the dark web to order a handgun, a silencer and ammunition.[237] A search of his vehicle recovered a quantity of cocaine and further enquiries revealed he was involved in drug dealing.

As well as using the dark web to obtain firearms, individuals have also been arrested and convicted for their role as vendors. A November 2015 press release by the US DOJ reported the arrest of a firearms vendor who was using the dark web to sell and ship weapons internationally.[238] The man from Montgomery, Alabama had allegedly already sold 'at least 32 firearms to people all over the world', including in Australia and Sweden. Allegedly he attempted to conceal his identity and hide the contents through placing false return address labels on the packages, using various aliases, falsely declaring the contents and placing the firearms so they appeared to be computer hard drives. The Montgomery man was eventually tracked down from fingerprints on one of the handguns he had sold, and was convicted and imprisoned.[239]

Likewise, a 41-year-old man suspected of selling firearms on the dark web was arrested in Berlin during November 2016. According to a German online media site, investigations of online firearms sales in the area had led police to seize a parcel containing a weapon he had sent to a customer.[240] A technical probe (i.e. a bug) was placed in his vehicle and he was recorded talking about the sale of ammunition and firearms. Upon his arrest it was believed that he had sold ten weapons and undetermined quantity of ammunition in the previous six months and he was convicted and sentenced to four years in prison for illegal arms trafficking.[241]

A final example of a convicted firearms vendor – known by the pseudonyms 'Brad Jones' and 'Gunrunner' on BMR – shipped a variety of weapons to international purchasers, including in England, Scotland, Ireland and Australia.[242] The firearms shipped included a Glock, a Beretta, Highpoint and Walther semi-automatic pistols, revolvers, Uzi submachine guns, magazines and hundreds of rounds of ammunition. To reduce the risk of being traced, the vendor allegedly removed the weapons' serial numbers. He was tracked down and arrested after a successful interagency policing taskforce identified him.[243]

Vulnerable and fixated individuals

A man was arrested in Wales in March 2015, when a search of his home address uncovered an array of weaponry. In particular, he had a pipe gun and 9 mm ammunition he had reportedly obtained through the Agora market on the dark web. As reported in the local news, the police in Wales were apparently contacted by the Metropolitan Police, who had been monitoring the dark web marketplace.[244] Although he claimed that he had an apocalyptic view of the world and had bought the weapons for survival purposes, he had

237 IrishNews (2016).
238 US DOJ (2015a).
239 US DOJ (2015a).
240 Losensky (2016).
241 Losensky (2016).
242 US DOJ (2017b).
243 US DOJ (2016).
244 The Wave (2015).

previous convictions for attacking a woman with a hammer and a knife.[245]

Further examples include Montgomery Byrne, a 31-year-old self-employed plasterer from Bury, UK, who had built up an arsenal of weaponry. He attempted to add a Glock pistol and 300 rounds of 9 mm ammunition from US vendors on the dark web and expressed his interest in obtaining a Kalashnikov AK47 assault rifle in the future; however, the vendors were allegedly undercover officers in the US DHS, who promptly informed the UK NCA.[246]

In a similar 'sting' operation in the United Kingdom, Darren Hillyer posed as a woman wanting revenge on an ex-lover to obtain a Ruger LC 9 semi-automatic pistol and 50 rounds of 9 mm ammunition through the dark web. According to the *Evening Standard*, Hillyer tried to have the weapon delivered to his workplace in London, only for the NCA to intercept the parcel and replace it with a plastic replica, hidden inside a radio, which they could track.[247] Enquiries led back to the original buyer and when questioned by the police he initially claimed his attempted purchase was to help him apply for a role in the NCA, before eventually admitting the offence.[248] Colleagues at the central London insolvency firm where Hillyer headed an IT operation have reportedly described him as a 'fantasist' and 'Walter Mitty-type character'.[249]

Finally, and showing that age is no barrier when attempting to obtain weapons through the dark web, PSNI officers recently became aware of a 14-year-old teenager attempting to obtain a sub-machine gun and 100 rounds of ammunition. Apparently, this was to threaten and intimidate a 'third party'. As reported by the BBC, the police stated the boy met with an operative from whom he attempted to buy ammunition for £150, in the belief he could purchase the gun at a later stage. The boy was then detained by police. Appearing before Ballymena Magistrates' Court, the boy provided a pre-prepared statement naming a 'Jamaican man', who allegedly asked him to collect blank ammunition and a deactivated gun.[250] The court found no evidence of the relationship with the Jamaican man and the judge released the boy on bail of £500 with conditions that he stays at home overnight and does not possess a mobile phone or any other internet-enabled device.

The cases described above illustrate the wide spectrum of groups and individuals that have been engaged with the dark web to procure weapons and ammunition. It is interesting to note that the accessibility of cryptomarkets makes access to illegally traded firearms relatively easy also for individuals who do not necessarily have a terrorist or criminal background.

245 The Wave (2015).
246 ITV (2016).
247 Alwakeel (2015).
248 Alwakeel (2015).
249 Alwakeel (2015).
250 BBC News (2017).

Appendix D - Firearms make breakdown

	Product	Pistol	Sub-machine gun (and full-auto pistols)	Rifle	Total
Make	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

Product	Pistol	Sub-machine gun (and full-auto pistols)	Rifle	Total
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
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

	Product	Pistol	Sub-machine gun (and full-auto pistols)	Rifle	Total
	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**

Appendix E – Expert workshop agenda

Date: 20–21 March 2017

Location: London, UK

Participants breakdown by affiliation:

- Project team: 3
- Other academic experts: 2
- National government: 1
- National law enforcement agency: 8
- National law enforcement agency (non-EU): 1
- Regional law enforcement agency: 2
- International organisation: 2

Agenda:

Day 1	Day 2
• Welcome and roundtable introduction • Background and project aims • Briefing on the dynamics of cryptomarkets and methodology • Presentation of quantitative findings • Roundtable discussion • Summary of the day and closing remarks	• Presentation of qualitative findings • Roundtable discussion • Tea/coffee • (Continued) roundtable discussion • Presentation of next steps • Summary of the day and closing remarks

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 2016 Munich shooting linking the weapons used by the attackers to vendors on dark web marketplaces. Some media reports have also linked the November 2015 Paris terrorist attacks to these platforms.

Despite a perceived high level of concern in European communities following the attacks, 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. While the role of the dark web has been investigated in recent years by the academic community in relation to illicit drugs trade, little has been done to generate a rigorous evidence base documenting the size, scale and scope of dark web-enabled arms trafficking.

This report aims to fill this gap in knowledge by deploying a mixed-method approach based on primary data extracted from dark web marketplaces, document review and expert consultation. The findings of this study provide a first empirically documented understanding of the phenomenon and offer an initial insight into possible implications, as well as relevant considerations for policy and decision makers.