Middlebury Institute *of*
International Studies at Monterey
Center on Terrorism, Extremism, and Counterterrorism

Ghost Markets of the Darknet

Assessing the Feasibility of Military-Grade Arms Acquisition in West Africa

By Ekaterina Grishakova and Satyajit Lall

Center on Terrorism, Extremism, and Counterterrorism

CTEC is a research center that applies advanced analytical approaches to deepen academic, tech, and policymakers' understanding of challenging emergent extremism threats. Founded in 2018 and based at the Middlebury Institute of International Studies, CTEC researchers mentor the next generation via internship and Fellowship opportunities for students in the Middlebury Institute's Nonproliferation and Terrorism Studies degree program. CTEC is a mixed-methods research center, meaning that our experts and students use analytic tradecraft, data science, and linguistics to closely examine extremist patterns and trends. CTEC is poised to remain at the forefront of terrorist threat mitigation as center experts work with legislators, law enforcement entities, and intelligence agencies to build safeguards against emerging risks associated with anti-government extremist actors.

About the Authors

Ekaterina Grishakova is a master's degree candidate in nonproliferation and terrorism studies at the Middlebury Institute of International Studies in Monterey (MIIS) specializing in emerging threats and challenges to international security with a focus on terrorism, extremism, counterterrorism, and Arabic as her language of study. She is currently pursuing an MA thesis on the expansion of the Islamic State of Khorasan beyond the Central Asian region.

Ekaterina is also a graduate research assistant at the Center on Terrorism, Extremism and Counterterrorism at the Middlebury Institute, working on projects concerning illicit financial flows, including terrorism and proliferation financing, and the influence of artificial intelligence on violent non-state actor activity.

Satyajit Lall is a master's candidate in Threat Intelligence at the Middlebury Institute of International Studies, specializing in terrorism financing, illicit financial networks, and cybersecurity. His work examines the convergence of emerging technologies and transnational threat ecosystems, with a particular focus on cryptocurrency-enabled financial crime and extremist financing architectures.

He currently serves as a Graduate Research Assistant at the Center on Terrorism, Extremism and Counterterrorism, contributing to research on extremism, conflict transformation, climate-linked conflict, and evolving global threat vectors. He is also a Research and Intelligence Intern at the Center for New Age Warfare Studies, New Delhi, where he produces OSINT-driven analysis on terrorism and security dynamics in South Asia.

Lall is the author of 1971: Strategy, Campaign, Valor, a comprehensive military-geopolitical-technical history of the Bangladesh Liberation War.

Acknowledgements

Professor Jason M. Blazakis
Professor Karen Nershi
Fawad Hussain (MIIS Graduate, Fall 2025)
Middlebury Institute of International Studies

Abstract

If Amazon can deliver a bicycle made in Italy to someone's doorstep in Peru in less than two weeks, can a militant non-state organization order an RPG from a dark web marketplace and receive it in their area of operations before being demolished by a counterterrorism campaign?

This paper attempts to answer this question and others that stem from it, assessing the possibility of a hypothetical splinter faction from the West African insurgent group Jama'at Nusrat al-Islam wal-Muslimin (JNIM) acquiring an RPG or weapon of the same class relying on dark web-based marketplaces. More specifically, the paper investigates the logistical details such as possible means of delivery – internally or internationally across continents; available payment methods; and the issue of trusting online black-market weapons listings. Finally, the study evaluates what it would mean if such procurement were repeatable at scale. In doing so, it looks into the extent to which dark web-enabled access to heavier weapons could complement or disrupt existing illicit arms networks, arriving at the conclusion that the dark web based weapons markets are a force multiplier in the already existing illicit market of firearms rather than full-fledged replacement.

"Amateurs talk about tactics, but professionals study logistics".
- General Robert H. Barrow, Commandant of the Marine Corps

Introduction

Studies concerned with the role of the dark web in the illicit firearms market have been rather scarce, especially when compared to research on offline arms trafficking trends. As the significance of digital technology use among non-state actors continues to grow, understanding the threat posed by dark web marketplaces to regional and international security is increasingly relevant. Relevant research carried out by the RAND Corporation, the International Crisis Group, the Australian Institute of Criminology, SIPRI, and the UNODC examines general aspects of the online market for illicit arms. However, it does not distinguish between risks posed by criminal and insurgent actors or between the types of weapons available.

The purpose of this report is to assess the ability of a newly formed insurgent group to purchase small arms and light weapons relying on dark web-based marketplaces. To assess this risk, the case study of a hypothetical insurgent group in West Africa acquiring an RPG-7 will be tested through examining the availability of the desired weapon system on dark web-based marketplaces, the possibility of finding it in the necessary region, and information regarding logistical matters visible on the websites analyzed, together with the militant landscape in the selected region.

1. **Role of dark-web markets in illicit arms trade**

The online arms trafficking market is significantly less developed than the physical black market for weapons, and neither is it as diverse as the dark web markets for narcotics and malware; however, it has proved to be a force multiplier, enabling the movement of weapons on the black market already and increasing the possibility of diversion of legally owned firearms. In particular, dark web marketplaces allow suppliers to connect directly with potential customers while guaranteeing greater anonymity.

On the dark web, firearms can be found on domains hosted by the TOR browser –those ending with .onion– and are located on single vendor shops where individual vendors sell a variety of illicit goods, as well as on cryptomarkets, platforms appearing and acting as a regular online retail store, offering customers around the world, a wide range of categories of products. With large-scale platforms like the *Silk Road, Alpha Bay, and Hydra Market* getting shut down in 2013, 2017, and 2021, respectively, smaller-scale, often more subject-specific marketplaces began emerging on the dark web. According to Broadhurst et al. from the Australian Institute of Criminology, *The Armory, Black Market Guns, Black Market, Darkseid, Euro Guns, Luckp-47, UK Guns and Ammo, Firearms72, DeepWeb Guns Store, Guns & Ganja Private Club,* and Danaucolt Ghost Gun, are online markets focused on sales of firearms and

explosives.[1] Platforms like *Abacus Market, RussianMarket,* and *TorZon Market*, which are active to date, on the other hand, remain diverse in the goods and services they sell, and among other categories, are known to offer firearms.

Regardless of their scope, however, cryptomarkets share a notable characteristic: they guarantee anonymity for both the seller and the buyer. Although both sellers and buyers on dark web marketplaces may have 'ratings' formed in the marketplace community forums, these ratings are connected to their online identities rather than to any personal information. Cryptomarket platforms rely on the encryption associated with their dark web location and take user anonymity more seriously, using advanced message encryption on their sites, notifying users where to conduct further communication, and sharing methods for avoiding detection when paying for illicit items.[2] Information leaks, although they happen, are most likely to occur in direct communication between the seller and buyer outside the marketplace, as a result of fraud and scams on the marketplace, or when third parties hack the platform.

Multiple challenges are posed by purchasing firearms on dark web-based marketplaces. For example, despite establishing a connection between suppliers and customers, payments are most often made outside the marketplace itself, using cryptocurrency, commonly Bitcoin and Monero, as they provide for the most anonymity[3], the shipping also takes place outside of the platform. Physical delivery is the hardest aspect of purchasing weapons of the dark web. The movement of a firearm — let along a larger weapon system — is logistically difficult with transactions requiring either the buyer to collect the weapon in person or the seller to deliver it directly. Therefore, both parties must be in the same country or leverage existing illicit arms trade routes and porous borders for the weapon to reach its destination.

Another challenge is that accessing dark web marketplaces can be difficult in itself, given the nature of dark web browsers, which make it impossible to search for a website because links to them are not indexed the same way as on the clear web. Therefore, potential consumers must either access the links from clear or deep-net websites or receive information directly from another individual. And while there are multiple ways to find a dark web marketplace, identifying a trustworthy seller is the most challenging, given the lack of regulation on dark web platforms, which poses a primary risk to the security of customers and suppliers.

Using the dark web for acquiring weapons is inefficient for large terrorist groups. Logistical constraints make recurring large-scale purchase of firearms or explosives from a single supplier nearly impossible. This way, concerns with the illicit arms sales taking place on the dark web have been associated with

---

[1] Roderic Broadhurst et al., "Trends & Issues in CrimeandwhenCriminal location Justice," March 2021, https://www.aic.gov.au/sites/default/files/2021-03/ti622_illicit_firearms_and_other_weapons_on_darknet_markets.pdf.
[2] Giacomo Persi Paoli et al., "Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web," Rand.org (RAND Corporation, July 19, 2017), https://www.rand.org/pubs/research_reports/RR2091.html. P. 20
[3] Ibid

lone-wolf terrorists.[4] And while lone actor terrorism continues to be a visible trend, the presence of more advanced weapons systems on dark web marketplaces allows for single or smaller-scale purchases that would satisfy the needs of smaller violent extremist organizations or individual cells within advanced networks.

Therefore, while the dark web-based illicit arms market forms yet another avenue for violent non-state actors to obtain weapons, it continues to pose numerous security and logistics-related challenges, which in some situations outweigh the benefits. In contrast, for others, especially when an actor lacks a connection to existing networks of illicit arms flows, it still seems favorable.

2. Terrorist groups' use of the dark web

Violent extremist actors have been exploiting cyberspace to their advantage for over two decades already, for purposes of communication, basing propaganda and recruitment campaigns on websites they run and social media, as well as relying on cryptocurrency for raising and moving funds. However, as counterterrorism operations on the dark net have intensified in the mid-2010s, terrorist groups shifted their activity into dark web platforms,[5] which provided a greater degree of anonymity, making extremist content harder for authorities to track.

Besides the aforementioned activities, which were carried from the clear net to more obscured layers of the internet, the dark web is also used by terrorist groups and lone-wolf actors alike for purchasing explosives and firearms.[6] For example, the German Federal Police investigations confirmed that the perpetrator of the 2016 Munich shooting, a lone-wolf terrorist aiming to carry out one attack, purchased the weapon from a single-vendor store on the dark web.[7] Along with this, there is evidence suggesting that the 2015 terrorist attacks in Paris also used a similar scheme a year earlier. There, the Islamic State-linked group used a platform on the dark web to purchase assault rifles from a seller likely residing in Germany, earlier suspected of being involved in illicit arms trafficking by local authorities. And although the exact extent to which the dark web was used in procuring the weapons has not been made certain for the Paris attacks, both cases demonstrated that violent non-state actors have the possibility of facilitating firearms purchases through using dark web platforms. Therefore, the emergence of a similar pattern can

---

[4] Gabriel Weimann, "Terrorist Migration to the Dark Web," *Perspectives on Terrorism* 10, no. 3 (2016), https://www.jstor.org/stable/26297596.
[5] Beatrice Berton, "The Dark Side of the Web: ISIL's One-Stop Shop?" (EU Institute for Security Studies, 2015), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf.
[6] Gabriel Weimann, "Terrorist Migration to the Dark Web," *Perspectives on Terrorism* 10, no. 3 (2016), https://www.jstor.org/stable/26297596.
[7] Giacomo Persi Paoli et al., "Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web," Rand.org (RAND Corporation, July 19, 2017), https://www.rand.org/pubs/research_reports/RR2091.html. P. 25

be extrapolated onto other regions with the presence of violent non-state actors interested in purchasing weapons and those willing to sell them.

3. Militant landscape in West Africa

Illicit weapon acquisition in West Africa operates amid well-established illicit networks which include cross-border smuggling routes from North Africa, inherited from the Libyan state collapse, diversions from national stockpiles and battlefield capture from under-resourced security forces. This way, any assessment of possibilities of online procurement of weapons must happen amid the context of regional illicit trade patterns, as dark web-based trade will have to compete against existing robust 'offline' networks.

West Africa remains one of the most unstable regions in the world, being faced with a multitude of socio-political and economic challenges — such as poverty, unemployment, a young and growing population – – around 60% of the population in Sahel states is under the age of 25[8] — ethnic and religious rivalries, high crime rates and the fragility of political regimes along with internal and interstate conflicts. Robust illicit arms flows are another characteristic that contributes to regional instability. These challenges create conditions for the emergence and growing influence of armed extremist groups, making terrorism and extremism among the main threats to regional security.

According to the Global Terrorism Index (GTI), the Sahel has remained one of the regions most vulnerable to the threat of terrorism over the past six years: five of the ten countries most affected by terrorism in the past year — Burkina Faso, Mali, Niger, Nigeria, and Cameroon— are located in the Sahel.[9] In 2024, countries in the Sahel accounted for 19% of all terrorist attacks worldwide, resulting in 51% of deaths linked to acts of terrorism.[10]

Salafist-jihadist groups in the region pose the greatest threat. Existing terrorist and insurgent groups in West Africa are divided between Al-Qaeda, the AQIM and its affiliates together forming Jama'at Nusrat al-Islam wal-Muslimin (JNIM) on one hand, and branches of the Islamic State — IS West Africa province, IS in the Greater Sahara on the other.[11] Given that group activities span large territories, factions often break off, resulting in a complex network of formal affiliations and loose alliances. Rivalry between Islamic State affiliates and Al-Qaeda linked groups surfaced around 2020 after the 'Sahelian Anomaly' —

[8] United Nations Economic Commission for Africa, SAHEL 2043: Towards a resilient, inclusive and prosperous Sahel region https://repository.uneca.org/entities/publication/4fb4237c-9f44-4ba0-8ca9-0a609522d0fd
[9] Global Terrorism Index 2025-World https://reliefweb.int/report/world/global-terrorism-index-2025
[10] Ibid
[11] Heni Nsaibia and Caleb Weiss, "The End of the Sahaweakenedffiliationelian Anomaly: How the Global Conflict between the Islamic State and Al-Qa`ida Finally Came to West Afaffiliationaffiliationrica," Combating Terrorism Center at West Point, July 31, 2020, https://ctc.westpoint.edu/the-end-of-the-sahelian-anomaly-how-the-global-conflict-between-the-islamic-state-and-al-qaida-finally-came-to-west-africa/.

nearly five years of coexistence between JNIM and ISGS that defied the global al-Qaeda/Islamic State rivalry — ended resulting in open conflict between the two groups.[12]

Regardless of their affiliation, however, groups of either side of the IS - Al-Qaeda rivalry share similar goals: establishing 'shadow governments' and gaining territorial control with the further goal of forming a Shariah law-controlled state in the Sahel region. This way, most violent non-state actors in the Sahel operate as insurgencies, making security forces and state institutions, rather than the civilian population, their primary targets.

Against the backdrop of US-led strikes against violent non-state actors in West Africa throughout 2025 and 2026, both Al-Qaeda and Islamic State-linked groups have suffered losses. However, they were not significantly weakened. Sustained counterterrorism pressure resulted in further decentralization of both the JNIM and ISGS, accelerating their fragmentation and geographic spread. JNIM *katibas* — particularly Katibat Macina — expanded southward from central Mali into the tri-border regions adjacent to Benin, Togo and Côte d'Ivoire, shifting the operational center of gravity of Sahelian jihadism away from its historical base in the North[13].

4. Methodology: finding an RPG on the dark web

This study uses a mixed-methods research approach to assess the feasibility of a hypothetical insurgent group in West Africa, like the JNIM, obtaining an RPG-7 (Russian: Ручной Противотанковый Гранатомет *"Ruchnoy Protivotankoviy Granatomyot"*) via dark web marketplaces. The research design is based on the triangulation of three distinct streams of evidence: direct observation of marketplace listings on the dark web, systematic engagement with existing empirical datasets on illicit arms availability online, and a review of field-based weapons tracing data that documents how small arms and light weapons, including the RPG-7, are transferred (illegally) to non-state actors across the Sahel region.

The first component involved the systematic sampling of active darknet marketplaces accessible via TOR Marketplace identification usually adheres to the methodology outlined by Broadhurst et al. in their 2021 Australian Institute of Criminology study, which surveyed twenty darknet markets, eight omnibus and twelve niche, over a 5 and a half month data collection window.[14] The research team conducted targeted keyword searches across TOR accessible platforms, typing terms such as "RPG-7," "rocket launcher,"

---

[12]Ibid

[13]International Crisis Group, *Understanding JNIM's Expansion Beyond the Sahel*, Report No. 321/Africa (Brussels: International Crisis Group, February 20, 2026), https://www.crisisgroup.org/rpt/africa/sahel-west-africa/321-le-jnim-et-le-dilemme-de-lexpansion-au-dela-du-sahel; "New Frontlines: Jihadist Expansion is Reshaping the Benin, Niger, and Nigeria Borderlands," ACLED, March 27, 2025, https://acleddata.com/report/new-frontlines-jihadist-expansion-reshaping-benin-niger-and-nigeria-borderlands.

[14] Roderic Broadhurst, Jack Foye, Chuxuan Jiang, and Matthew Ball, "Illicit Firearms and Other Weapons on Darknet Markets," *Trends & Issues in Crime and Criminal Justice*, no. 622 (Canberra: Australian Institute of Criminology, March 2021), 5–6, https://www.aic.gov.au/sites/default/files/2021-03/ti622_illicit_firearms_and_other_weapons_on_darknet_markets.pdf.

"anti-tank," "grenade launcher," and other common informal designation for various variants of the weapon (e.g., RPG-7V, Type 69), since RPGs have been formally been manufactured under different designations, depending upon the country and arms dealer involved. At least one active listing for an RPG-7 was identified on a Tor-hosted marketplace during the period of observation, with the listing advertising the weapon alongside cryptocurrency-denominated pricing and detailed vendor-specified shipping parameters.[15] This listing was documented, though no purchase was actually attempted, in keeping with the ethical constraints observed within existing practice.[16]

The second draws upon the extant empirical literature that attempts to quantify both the scale and characteristics of dark web arms markets. Central to this is the RAND Europe study by Persi Paoli et al., which examined at least twelve cryptomarkets and estimated the global value of the dark web arms trade at approximately $80,000 per month (in 2017), with firearms accounting for nearly ninety percent of total revenue.[17] This finding is supplemented by the Broadhurst et al. dataset cataloging approximately 2,124 weapons across twenty markets,[18] the observational study by Copeland, Wallin, and Holt of six dark web vendor sites over six months,[19] and the crawler-based analysis conducted by Leonidou et al. across ten Tor-hosted marketplaces.[20] Altogether, these studies forged a near-composite understanding of the depth of various darknet markets, the variants of weapons available, general trends in vendor conduct, and transactional reliability. However, the latter remains an outlier in terms of consistency.

The selection of the RPG-7 as the primary focal case warrants a quick justification. This "cold war era" system remains among the most widely proliferated light weapons globally, with production spanning the Soviet Union and its successor states, China (under the Type 69 designation), Pakistan, and six other countries[21] Its operational profile, defined by low unit cost, limited training requirements (as compared to smart weapons), portability (as compared to other anti-armor weapons, and effectiveness against both armored vehicles and built-up positions, renders it especially attractive to insurgent and terrorist groups

---

[15] Tor-hosted marketplace listing, product tag: RPG-7, accessed [September 13, 2025], http://pxbzggitxizmnd5rttrzttg7n6dzcns52aykn2z2xbs3tjku4r4rt3ad.onion/index10e8.html?product_tag=rpg-7. Note: .onion addresses are accessible only via the Tor browser and are subject to frequent changes in availability.
[16] Broadhurst et al., "Illicit Firearms," 6; Giacomo Peroli, Judith Aldridge, Nathan Ryan, and Richard Warnes, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, CA: RAND Corporation, RR-2091, 2017), 23–24, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf.
[17] Persi Paoli et al., *Behind the Curtain*, 42–47
[18] Broadhurst et al., "Illicit Firearms," 7–12.
[19] Christopher Copeland, Mikaela Wallin, and Thomas J. Holt, "Assessing the Practices and Products of Darkweb Firearm Vendors," *Deviant Behavior* 41, no. 8 (2020): 94available9–968, https://doi.org/10.1080/01639625.2019.1596465.
[20] Pantelitsa Leonidou, Nikos Salamanos, Arist—eidis Farao, Maria Aspri, and Michael Sirivianos, "A Qualitative Analysis of Illicit Arms Trafficking on Darknet Marketplaces," in *The 18th International Conference on Availability, Reliability and Security (ARES 2023)* (New York: 2023), https://doi.org/10.1145/3600160.3605087.
[21] Ryszard Woźniak, "Possibility of Protection of Helicopters Against Projectiles Launched from RPG-7," *Biuletyn Wojskowej Akademii Technicznej* 55, no. 4 (2006), http://www.witu.mil.pl/www/biuletyn/zeszyty/2006/0097p15.pdf.

actively engaged in asymmetric warfare against state forces.[22] There is extensive literature and publications, including those by agencies such as the FBI that have created datasets for weapons ranging from handguns to even light machine guns, but not RPGs. Therefore, this paper aims to address the noticeable gap in these pre-established datasets.

While darknet-related weapon sales make for popular headlines, they certainly don't constitute the most popular and practical ways of acquiring firearms illegally. Which brings us to the third component of this study: a comparison with decades-old, established 'offline' trafficking networks, examining how non-state armed groups across the Sahel typically acquire RPG-7 systems and comparable light weapons, thereby presenting the rationale for why a group might divert from the usual to begin with. This part of the analysis draws primarily on pre-existing field-based weapons tracing conducted by Conflict Armament Research across eight countries in North and West Africa, which documents serial-number-level evidence linking Libyan stockpiles (post Gaddafi regime), Sudanese arsenals (pre civil war), and supply chains extending to armed groups operating in Mali, Niger and the greater Sahel region.[23] In addition to this, the Small Arms Survey's HSBA tracing project details the approximate origins, alleged custody chains, and regional circulation patterns of weapons (including the RPG family) in Sudan and South Sudan, throwing light on some of the pathways through which such systems enter and diffuse across West-African conflict environments.[24] The UNODC's TOCTA Sahel firearms assessment, grounded in official data from various countries, law enforcement agencies, and fieldwork across Burkina Faso, Chad, Mali, Mauritania, and Niger, provides the most accurate mapping of present-day trafficking routes, source states, and the marrow of state stockpile diversion as the primary supply mechanism for armed groups in the region.[25] These offline and pre-existent dynamics serve as the very basic benchmark against which the viability, cost structure, and risk profile of dark web procurement are evaluated.

A few initial limitations need to be addressed. Firstly, no transactions were conducted on darknet marketplaces by the authors themselves; the analysis therefore relies mainly on listing data, vendor self-representations, and available reputation indicators, such as discussions about the vendor on various darknet forums. A substantial proportion of dark web arms listings are widely accepted as fraudulent, some of which constitute potential law enforcement honeypots, or involve vendors who accept payment

---

[22] Savannah de Tessières, *At the Crossroads of Sahelian Conflicts: Insecurity, Terrorism, and Arms Trafficking in Niger* (Geneva: Small Arms Survey, January 2018), 41–58, https://www.smallarmssurvey.org/sites/defaulin the first placet/files/resources/SAS-SANA-Report-Niger.pdf.
[23] Conflict Armament Research, *Investigating Cross-Border Weapon Transfers in the Sahel* (London: Conflict Armament Research, November 2016), https://www.conflictarm.com/reports/investigating-cross-border-weapon-transfers-in-the-sahel/.
[24] Jonah Leff and Emile LeBrun, *Following the Thread: Arms and Ammunition Tracing in Sudan and South Sudan*, HSBA Working Paper 32 (Geneva: Small Arms Survey, May 2014), https://www.smallarmssurvey.org/sites/default/files/resources/HSBA-WP32-Arms-Tracing.pdf.
[25] UNODC, *Firearms Trafficking in the Sahel*, Transnational Organized Crime Threat Assessment — Sahel (Vienna: UNODC, 2022), hself-representationsttps://www.unodc.org/documentsmainly /data-and-analysis/tocta_sahel/TOCTA_Sahel_firearms_2023.pdf.

without delivering goods.[26] Second, the inherently ephemeral nature of darknet markets, subject to seizure, exit scams, and voluntary or involuntary closure, limits the ability to reproduce the observed marketplace environment in an academic document accurately.

Third, the scope of the study is confined to the RPG-7 system, and its findings should not be uncritically extended to other categories of weaponry, such as smart weapons, which play a similar role. Finally, the analysis of the West African militant landscape and JNIM-affiliated splinter dynamics is grounded in open-source intelligence, institutional reporting, and published field research, operating in the theoretical world without direct access to actual terrorist groups.

5. Case Study presentation: How will a group in the Sahel do this?

The Hypothetical Actor:

The International Crisis Group's February 2026 report substantiates the emergence of precisely the kind of factional fragmentation seen around the world within many insurgent groups, that underpins the hypothetical actor considered here: the JNIM, extends its operational footprint into coastal West Africa with lower-tier fighters increasingly pushing southward into Benin, Togo, and Côte d'Ivoire against the strategic preferences of senior leadership, with ACLED data indicating that attacks in northern Benin rose from 22 in 2021 to 176 in 2024.[27] A small splinter faction emerging from this expansion corridor, breaking away from a parent *katiba* over would likely retain access to basic small arms via inherited stocks, yet lack the entrenched trafficking relationships built over decades of conflict, to access higher-order military capabilities through known offline supply chains.[28] It is precisely this lack of structure, faced by splinter groups and further compounded by exclusion from durable procurement networks, that renders the lucrative idea of dark web acquisition an attractive counteroffer worth investing in.

---

[26] Persi Paoli et al., *Behind the Curtain*, 47; Broadhurst et al., "Illicit Firearms," 6. RAND notes that scamming "occurs across all product categories on dark web markets, and perhaps more frequently for vendors of firearms.
[27] International Crisis Group, *Understanding JNIM's Expansion Beyond the Sahel*, Report No. 321/Africa (Brussels: International Crisis Group, February 20, 2026), https://www.crisisgroup.org/rpt/africa/sahel-west-africa/321-le-jnim-et-le-dilemme-de-lexpansion-au-dela-du-sahel; "New Frontlines: Jihadist Expansion is Reshaping the Benin, Niger, and Nigeria Borderlands," ACLED, March 27, 2025, https://acleddata.com/report/new-frontlines-jihadist-expansion-reshaping-benin-niger-and-nigeria-borderlands.
[28] Conflict Armament Research, *Investigating Cross-Border Weapon Transfers in the Sahel* (London: Conflict Armament Research, November 2016), https://www.conflictarm.com/reports/investigating-cross-border-weapon-transfers-in-the-sahel/; Savannah de Tessières, *At the Crossroads of Sahelian Conflicts: Insecurity, Terrorism, and Arms Trafficking in Niger* (Geneva: Small Arms Survey, January 2018), 41–58, https://www.smallarmssurvey.org/sites/default/files/resources/SAS-SANA-Report-Niger.pdf.

Discovery: Can the Group Locate RPG-7 Listings?

Statistical sampling undertaken for this study confirms that RPG-7 listings do appear quite regularly across Tor-accessible darknet marketplaces.[29] However, the broader structural composition of these markets diverges significantly from the 'illegal firearm'-dominant ecosystem. Broadhurst et al. demonstrate that pistols constitute 84 percent of all firearms listings across twenty darknet markets, with rifles accounting for 10 percent and submachine guns 6 percent, while light weapons and ordnance appear only marginally and inconsistently.[30] The RAND Europe study similarly emphasizes that although darknet markets may sometimes facilitate the redistribution of already illicitly circulating weapons, listings for systems such as RPG's are rare, with no common buyer chain connecting them and disappointingly likely to constitute fraudulent offerings.[31]

Therefore, the key concerns that would befall a potential customer start with navigating an unstable information environment, one that requires reexamining the legitimacy of a seller repeatedly with a less-than-ideal quality of sources for verification, a high probability of deception, and the usual agency-trap.[32] These risks can be applied to any darknet-related purchase but get amplified further in the case of RPGs.

Copeland, Wallin, and Holt find that even within conventional firearms markets, pre-purchase verification is effectively non-existent, with buyers relying almost exclusively on vendor self-reporting and reputation systems that are themselves susceptible to manipulation.[33] Extending this logic, Leonidou et al. document that concealment and shipping practices on darknet markets are optimized for small, modular weapons, including pistols hidden within power tools and rifles embedded in household appliances — yet provide no evidence of comparable methods applicable to crew-served or anti-armor systems.[34]

---

[29] Tor-hosted marketplace listing, product tag: RPG-7, accessed [April 9, 2026], http://pxbzggitxizmnd5rttrzttg7n6dzcns52aykn2z2xbs3tjku4r4rt3ad.onion/index10e8.html?product_tag=rpg-7.
[30] Roderic Broadhurst, Jack Foye, Chuxuan Jiang, and Matthew Ball, "Illicit Firearms and Other Weapons on Darknet Markets," *Trends & Issues in Crime and Criminal Justice*, no. 622 (Canberra: Australian Institute of Criminology, March 2021), 7, https://www.aic.gov.au/sites/default/files/2021-03/ti622_illicit_firearms_and_other_weapons_on_darknet_markets.pdanti-armorpotentialf
[31] Giacomo Persi Paoli, Judith Aldridge, Nathan Ryan, and Richard Warnes, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, CA: RAND Corporation, RR-2091, 2017), 47, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf.
[32] The *agency trap refers to the problem where owners of smaller businesses become exhausted by their agency relying entirely on them being involved in day-to-day operations to grow further.*
[33] Broadhurst et al., "Illicit Firearms," 6; Persi Paoli et al., *Behind the Curtain*, 47.
[34] Christopher Copeland, Mikaela Wallin, and Thomas J. Holt, "Assessing the Practices and Products of Darkweb Firearm Vendors," *Deviant Behavior* 41, no. 8 (2020): 955–960, https://doi.org/10.1080/01639625.2019.1596465

Payment: Cryptocurrency Acquisition in West Africa

Dark web transactions are overwhelmingly denominated in cryptocurrency, with Bitcoin informally demanding attention equal to the U.S. Dollar online.[35] That said, a splinter faction operating between Benin and Burkina Faso may not have the electronic infrastructure to horde 'piles of crypto' for buying guns. This is contrasted by Nigeria's emergence as a global leader in cryptocurrency adoption in its economy, alongside the expansion of mobile money systems across West Africa, providing even the remotest areas with functional on-ramps, transforming local liquidity into digital assets.[36]

However, the Financial Action Task Force identifies that fourteen of twenty-five grey-listed jurisdictions are located in Africa, further reflecting structural weaknesses in CFT regimes and local banking systems that simultaneously voluntarily or facilitate illicit flows while limiting much-needed formal financial sophistication.[37]

While the dominant financing modalities in the Sahel remain cash-imperious systems, hawala networks, and remnants of the barter system, the UN Counter-Terrorism Committee Executive Directorate observes that terrorist organizations are increasingly experimenting with cryptocurrency.[38] Accordingly, while conversion of extortion proceeds or illicit commodity revenues into Bitcoin via peer-to-peer exchanges is technically feasible, it introduces exposure to blockchain analytics firms such as TRM Labs and Chainalysis, as well as enforcement agencies including FinCEN and OFAC, adding yet another layer of threats for a prospective user of these services.[39]

Logistics and Delivery: The Critical Bottleneck

An RPG-7 launcher measures approximately 950 mm in length and weighs 6.3 kg unloaded, while its PG-7VL warhead (most popular example on the dark web) adds a further 2.6 kg and needs to be transported separately.[40] This gives us the first and arguably most important constraint of successfully transferring the RPG from buyer to seller: it's a big weapon and doesn't exactly disassemble like a LEGO set.

---

[35] Pantelitsa Leonidou, Nikos Salamanos, Aristeidis Farao, Maria Aspri, and Michael Sirivianos, "A Qualitative Analysis of Illicit Arms Trafficking on Darknet Marketplaces," in *The 18th International Conference on Availability, Reliability and Security (ARES 2023)* (New York, ACM, 2023), Table 4, https://doi.org/10.1145/3600160.3605087
[36] Persi Paoli et al., *Behind the Curtain*, 42.
[37] "African Governments Should Rethink Their Approach to Combating Money Laundering and Terrorist Financing," Atlantic Council, May 30, 2025, https://www.atlanticcouncil.org/blogs/africasource/african-governments-should-rethink-their-approach-to-combating-money-laundering-and-terrorist-financing/.
[38] Ibid.
[39] UNOCT/UNCCT, *Countering the Misuse of Virtual Assets and Virtual Asset Service Providers for Terrorism Financing Purposes* (New York: United Nations, 2024), https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/uncct_cft_va_report_2024_en.pdf.
[40] FATF, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* (Paris: FATF, 2020), https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html.

This observation is consistent with other empirical findings on darknet transfers and logistics.[41] RAND Europe has explicitly identified that darknet marketplaces don't amplify or increase the number of 'under the table' supply chains but remain dependent on pre-established networks. This constraint, by itself, has prevented the dark web from expanding at the rate at which many initial studies predicted.[42]

Leonidou et al. have further documented that the usual 'stick a rifle in bag of rice' strategies that have successfully transported AK-47s from Pakistan to East Africa can't be applied to the RPG in particular, specifically because Soviet factories never intended for the weapon to be broken down and disguised as power tools, appliances, or automotive components, or other modular items capable of passing as legitimate commercial goods.[43]

The logistical challenge intensifies further amid existing regulations of the region. West African postal and customs systems, while uneven and at times underregulated, bring up additional difficulties absent in the European and North American case studies. States in the Sahel are dependent on limited coastal transit hubs — Abidjan, Dakar, Cotonou, and Lomé among others– through which international shipments pass before being distributed inland.[44] These nodes, already subject to advanced screening targeting narcotics, arms, and fuel trafficking, result in customs and security agencies prioritizing anomalous or oversized parcels for inspection for these reasons.[45]

Together with this, the structural assessment can be reinforced by records provided by law enforcement. The J-CODE undercover operation. This operation took place as a series of international FBI-led campaigns launched in 2018 with the aim of combating illicit substance trafficking on the dark web, specifically targeting fentanyl and opioid sales, but ended up expanding its scope to include other items sold on the dark web as well. The J-CODE operation resulted in the seizure of over 100 firearms, including one grenade launcher, narcotics, along with $23.6 million in cash and cryptocurrency. This case, therefore, illustrates the continued centrality of postal and courier systems as enforcement chokepoints, placing them among the key challenges for dark net-only purchases.[46] However, this case reflects a domestic U.S. distribution environment with mature logistics infrastructure rather than transnational movement into conflict zones. Legislative initiatives such as the 2025 Dark Web

[41] Ryszard Woźniak, "Possibility of Protection of Helicopters Against Projectiles Launched from RPG-7," *Biuletyn Wojskowej Akademii Technicznej* 55, no. 4 (2006), http://www.witu.mil.pl/www/biuletyn/zeszyty/2006/0097p15.pdf.
[42] How Drugs Are Sold on the Dark Web," LegtScript, December 7, 2023, https://www.legitscript.com/high-risk-and-problematic-products/how-drugs-are-sold-on-the-dark-web/.
[43] Persi Paoli et al., *Behind the Curtain*, viiilayers of friction.
[44] Leonidou et al., "Qualitative Analysis," Table 4.
[45] Ibid.
[46] "Tackling Cybercriminals Trafficking Illegal Goods from Dark Web," SL Cyber, December 2, 2025, https://slcyber.io/overcoming-the-challenges-of-cybercriminals-trafficking-illegal-goods-from-the-dark-web/

Interdiction Act also acknowledge existing blind spots and vulnerabilities in shipping systems, though their doctrine and tactics revolve around narcotics, not military-grade weapons.[47]

6. Comparative Assessment: Dark Web versus Offline Procurement

A structured comparison across the five analytical dimensions mentioned before yields a consistent hierarchy of feasibility.

Particularly, in terms of **accessibility**, the dark web offers a degree of advantage, requiring only basic digital access and the ability to use cryptocurrency. Offline trafficking networks, in contrast, depend on embedded relationships, networks based on trust, and reputational capital. For this reason, barriers for newly formed splinter factions that are excluded from their core organizations' supply chains are particularly acute.

Regarding the **cost**, available data remains inconclusive. Pricing observed on darknet markets for military-grade weapons is highly unreliable and often reflects speculative or fraudulent listings rather than actual transaction values.[48] Field evidence from Conflict Armament Research suggests AK-pattern rifles in the Sahel typically cost between $1,200 and $1,400, with RPG-class weapon systems having higher — though still accessible— prices for violent non-state organizations.[49]

On the other hand, the usual offline channels remain significantly more reliable. Darknet arms markets are often subject to scams, exit fraud, or infiltration by law enforcement. These challenges lead to a higher probability of failure, especially when purchasing rare items like rocket launchers. Nevertheless, the tried and tested 'in-person' ways of obtaining firearms, such as smuggling, state diversion, or battlefield capture, tend to usually ensure a higher statistic of successful delivery.

Offline channels are appreciated for their logistical advantages over online methods. Evidence-based tracing data from Conflict Armament Research and the Small Arms Survey demonstrate that RPG-7 systems circulate primarily through overland convoy networks, diversion from state stockpiles, and battlefield capture across conflict-ridden Libya, Sudan, Mali, and Niger.[50] These systems depend on territorial access, physical mobility, and an established arms trafficking infrastructure, which are

---

[47] "Corridors of the Alliance of Sahel States: Logistical Vulnerabilities, Security Constraints, and Adaptation Dynamics," Policy Center for the New South, December 2025, https://www.policycenter.ma/publications/corridors-alliance-sahel-states-logistical-vulnerabilities-security-constraints-andresults in.law-enforcemenIn terms oft

[48] UNODC, "Sahel Programme," https://www.unodc.org/westandcentralafrica/en/sahel.html; UNODC, *Firearms Trafficking in the Sahel*, Transnational Organized Crime Threat Assessment — Sahel (Vienna: UNODC, 2022), https://www.unodc.org/documents/data-and-analysis/tocta_,sahel/TOCTA_Sahel_firearms_2023.pdf.

[49] U.S. Immigration and Customs Enforcement, "ICE HSI New York Operation Leads to Arrests of 3 Dozen Darknet Vendors Selling Illicit Goods, Weapons, Drugs Seized and More Than $23.6 Million," press release, https://www.ice.gov/news/releases/ice-hsi-new-york-operation-leads-arrests-3-dozen-darknet-vendors-selling-illicit.

[50] Dark Web Interdiction Act of 2025, S. 1975, 119th Congress (2025–2026), https://www.congress.gov/bill/119th-congress/senate-bill/1975/text.

impossible for darknet procurement architectures. The interdiction of a six-vehicle arms convoy in northern Niger in 2014, transporting multiple tons of military materiel, illustrates both the scale and infrastructural sophistication of offline arms logistics in the region.[51] Along with this, the Small Arms Survey's HSBA project documents RPG-7 circulation through transfers from state to non-state actors and battlefield looting campaigns in Sudan and South Sudan, reinforcing the centrality of physical networks over digital marketplaces.[52]

Summing up the comparison, it can be concluded that darknet procurement offers superficial accessibility advantages for a newly formed splinter faction excluded from already established supply chains, while its structural limitations — particularly in logistics and delivery — render it an impractical mechanism for acquiring RPG-7 systems. Offline trafficking networks remain not only more reliable but fundamentally more congruent with the physical, operational, and logistical characteristics of military-grade weapons circulation in the Sahelian environment.[53]

7. **Policy Implications and Risk Assessment:**

Despite redistributing access to existing illicit stocks through a digital interface, the darknet does not create a new supply line. The dark web thus exists as an effective supplementary channel but cannot be considered a reliable replacement for offline networks.[54] Europol's IOCTA 2024 has led to marketplace instability, exit scams, and repeated takedowns, fragmenting the dark web landscape, making it more difficult to control. This process has heightened the threat to recent groups that have not yet become part of established trafficking networks, and 'lone wolf' operating outside organized militant groups.[55]

Policymakers should keep an eye on this channel but not prioritize it over the much larger offline trafficking issue. The main strategies for combating illegal weapons continue to be traditional measures such as stockpile management, marking and tracing, and international cooperation availability.[56]

---

[51] Persi Paoli et al., *Behind the Curtain*, 37–41; Broadhurst et al., "Illicit Firearms," 10–12.
[52] "Tracing Illicit Weapons in the Sahel," Inkstick Media, June 24, 2024, https://inkstickmedia.com/tracing-illicit-weapons-in-the-sahAssessmentthat el/.
[53] Jonah Leff and Emile LeBrun, *Following the Thread: Arms and Ammunition Tracing in Sudan and South Sudan*, HSBA Working Paper 32 (Geneva: Small Arms Survey, May 2014), https://www.smallarmssurvey.org/sites/default/files/resources/HSBA-WP32-Arms-Tracing.pdf.
[54] Giacomo Persi Paoli et al., *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (RAND Corporation, RR-2091, 2017), viii.
[55] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2024* (The Hague: Europol, July 2024), https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf.
[56] Persi Paoli et al., *Behind the Curtain*, viii; UNODC, *Firearms Trafficking in the Sahel*, TOCTA Sahel (Vienna: UNODC, 2022); SIPRI, *Supporting Small Arms and Light Weapons Controls Through Development Assistance* (Stockholm: SIPRI, 2021), https://www.sipri.org/sites/default/files/2021-0systems through which these purchases must pass. Improving parcel inspection at West African ports—such as Abidjan, Cotonou, Dakar, and Lomé—could simultaneously target dark web procurement and traditional smuggling. Additionally, ECOWAS border security, already stretched thin after the January 2025 AES withdrawal, needs urgent support and reinforcement.2/2102_salw_assistance_in_ssa.pdf.

Logistics remains the critical 'digital thorn in the side' of any prospective darknet marketplace. The most effective intervention point is therefore not the digital marketplace, but the postal and customs infrastructure through which purchases must pass. If the weapon doesn't have a visa, it's getting apprehended, despite what the buyer may have planned. Increasing funding towards parcel inspection and export control institutions and agencies at the West African ports of Abidjan, Cotonou, Dakar, and Lomé would simultaneously address dark-web procurement and usual conventional smuggling.[57] To supplement this, the Economic Community of West African States (ECOWAS) border interdiction capabilities, which are already strained by the January 2025 withdrawal of the Alliance of Sahel States (AES),[58] need urgent reinforcement and financial assistance.[59]

The cryptocurrency plus darknet procurement equation highlights a significant detection and information-sharing/cooperation gap among international actors. Most international agreements such as the UN Firearms Protocol, the Arms Trade Treaty, and ECOWAS conventions were originally designed to combat offline trafficking.[60] However, counter-terrorism financing frameworks have only begun to address the increasing indulgence of cryptocurrencies by non-state actors, particularly in Africa.[61] Bridging this gap begins with stronger institutional cooperation between African and International agencies working towards the same goal, including sharing intelligence among cybercrime units, counter-terrorism divisions, and arms control agencies. Additionally, monitoring ongoing cryptocurrency activity on West African on-ramps should be incorporated into ECOWAS and GIABA counter-terrorism financing strategies.[62]

Conclusion

Despite illicit arms trade online not being as advanced as its physical '*offline*' counterpart, and posing multiple security risks and logistical problems for both consumers and suppliers, it has allowed virtually any actor with the right access to technology and funds to connect with suppliers without relying on third parties — criminal organizations or other violent extremist groups — securing a higher degree of anonymity and leaving less traces of the purchase, at the same time being able to assess the available options of the product, its location and supplier.

---

[57] "Illicit Firearms Markets Accessible Through the Dark Web," in *Illicit Firearms Markets and Organized Crime* (Oxford: Oxford University Press, 2024).
[58] Burkina Faso, Mali and Niger who ended their membership in ECOWAS
[59] International Crisis Group, *Understanding JNIM's Expansion Beyond the Sahel*, Report No. 321/Africa (February 2026).
[60] UNODC Global Firearms Programme, policy analysis annex to RAND *Behind the Curtain*, 2017.
[61] FATF, *Comprehensive Update on Terrorist Financing Risks* (Paris: FATF, July 2025); "African Governments Should Rethink Their Approach to Combating Money Laundering and Terrorist Financing," Atlantic Council, May 2025.
[62] Méryl Demuynck, Tanya Mehra, and Reinier Bergema, *Cashing in on Guns*, ICCT Synthesis Report (The Hague: ICCT, September 2020).

As can be seen from the examined case of a hypothetical newly formed insurgent group in West Africa, although the dark offers some advantage for finding the necessary weapon system and serves as a starting point for communication between a potential supplier and customer, the payment, actual acquisition and transportation of the weapon would have to be determined on a one-on-one basis with the seller, reflecting in essence, the practices used when carrying out a purchase of a firearm in person. This finding, therefore, makes the dark web a force multiplier rather than a replacement for already existing illicit arms flows.

Works Cited:

ACLED. "Conflict Watchlist 2025: Sahel and Coastal West Africa." December 2024. https://acleddata.com/conflict-watchlist-2025/sahel-and-coastal-west-africa/.

ACLED. "New Frontlines: Jihadist Expansion is Reshaping the Benin, Niger, and Nigeria Borderlands." March 27, 2025. https://acleddata.com/report/new-frontlines-jihadist-expansion-reshaping-benin-niger-and-nigeria-borderlands.

Al Jazeera. "Munich Attack: David Sonboly 'Planned Attack for Year.'" July 24, 2016. https://www.aljazeera.com/news/2016/7/24/munich-attack-david-sonboly-planned-attack-for-year.

Armament Research Services (ARES). "Operation RUGER." September 30, 2017. https://armamentresearch.com/tag/2016-munich-shooting/.

Atlantic Council. "African Governments Should Rethink Their Approach to Combating Money Laundering and Terrorist Financing." May 30, 2025. https://www.atlanticcouncil.org/blogs/africasource/african-governments-should-rethink-their-approach-to-combating-money-laundering-and-terrorist-financing/.

Berton, Beatrice. "The Dark Side of the Web: ISIL's One-Stop Shop?" EU Institute for Security Studies, 2015. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf.

Broadhurst, Roderic, Jack Foye, Chuxuan Jiang, and Matthew Ball. "Illicit Firearms and Other Weapons on Darknet Markets." *Trends & Issues in Crime and Criminal Justice*, no. 622. Canberra: Australian Institute of Criminology, March 2021. https://www.aic.gov.au/sites/default/files/2021-03/ti622_illicit_firearms_and_other_weapons_on_darknet_markets.pdf.

Campbell, John. "Weapons in the Sahel." Council on Foreign Relations Blog, November 22, 2016. https://www.cfr.org/blog/weapons-sahel.

Center for Preventive Action. "Violent Extremism in the Sahel." Global Conflict Tracker. Council on Foreign Relations, February 18, 2026. https://www.cfr.org/global-conflict-tracker/conflict/violent-extremism-sahel.

Church Law Center. "Federal Dark Web Arrests Surge Under Operation Dark HunTor." December 26, 2025. https://www.church.law/new-dark-net-arrests-and-prosecutions-in-federal-court/.

CNN. "Munich Gunman Planned Attack for a Year, Officials Say." July 24, 2016. https://www.cnn.com/2016/07/24/europe/germany-munich-shooting/index.html.

Conflict Armament Research. *Frontline Perspective: Weapons Seized from Salafi Jihadist Groups in the Central Sahel, 2015–2023*. London: Conflict Armament Research, 2024. https://www.conflictarm.com/publications/.

Conflict Armament Research. *Investigating Cross-Border Weapon Transfers in the Sahel*. London: Conflict Armament Research, November 2016. https://www.conflictarm.com/reports/investigating-cross-border-weapon-transfers-in-the-sahel/.

Copeland, Christopher, Mikaela Wallin, and Thomas J. Holt. "Assessing the Practices and Products of Darkweb Firearm Vendors." *Deviant Behavior* 41, no. 8 (2020): 949–968. https://doi.org/10.1080/01639625.2019.1596465.

Dark Web Interdiction Act of 2025. S. 1975, 119th Congress (2025–2026). https://www.congress.gov/bill/119th-congress/senate-bill/1975/text.

Demuynck, Méryl, Tanya Mehra, and Reinier Bergema. *Cashing in on Guns: Identifying the Nexus between Small Arms, Light Weapons and Terrorist Financing*. ICCT Synthesis Report. The Hague: International Centre for Counter-Terrorism, September 2020. https://icct.nl/sites/default/files/import/publication/SALW-Report.pdf.

De Tessières, Savannah. *At the Crossroads of Sahelian Conflicts: Insecurity, Terrorism, and Arms Trafficking in Niger*. Geneva: Small Arms Survey, January 2018. https://www.smallarmssurvey.org/sites/default/files/resources/SAS-SANA-Report-Niger.pdf.

Europol. *European Union Terrorism Situation and Trend Report (TE-SAT) 2024*. The Hague: Europol, 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf.

Europol. *European Union Terrorism Situation and Trend Report (TE-SAT) 2025*. The Hague: Europol, 2025. https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat.

Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. The Hague: Europol, July 2024. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202024%20-%20EN_0.pdf.

FATF. *Comprehensive Update on Terrorist Financing Risks*. Paris: FATF, July 2025. https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html.

FATF. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. Paris: FATF, 2020. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html.

Federal Bureau of Investigation. "Operation DisrupTor: JCODE Shuts Down Darknet Drug Vendors." FBI News Stories, September 22, 2020. https://www.fbi.gov/news/stories/operation-disruptor-jcode-shuts-down-darknet-drug-vendor-092220.

HSToday. "JNIM's Expansion in the Sahel and Coastal West Africa." March 2026. https://www.hstoday.us/subject-matter-areas/counterterrorism/jnims-expansion-in-the-sahel-and-coastal-west-africa/.

"Illicit Firearms Markets Accessible Through the Dark Web." In *Illicit Firearms Markets and Organized Crime: Global, Regional, and Local Perspectives*. Oxford: Oxford University Press, 2024.

Inkstick Media. "Tracing Illicit Weapons in the Sahel." June 24, 2024. https://inkstickmedia.com/tracing-illicit-weapons-in-the-sahel/.

Institute for Economics and Peace. *Global Terrorism Index 2025*. Sydney: Institute for Economics and Peace, 2025. https://reliefweb.int/report/world/global-terrorism-index-2025.

International Crisis Group. *Understanding JNIM's Expansion Beyond the Sahel*. Report No. 321/Africa. Brussels: International Crisis Group, February 20, 2026. https://www.crisisgroup.org/rpt/africa/sahel-west-africa/321-le-jnim-et-le-dilemme-de-lexpansion-au-dela-du-sahel.

Leff, Jonah, and Emile LeBrun. *Following the Thread: Arms and Ammunition Tracing in Sudan and South Sudan*. HSBA Working Paper 32. Geneva: Small Arms Survey, May 2014. https://www.smallarmssurvey.org/sites/default/files/resources/HSBA-WP32-Arms-Tracing.pdf.

LegitScript. "How Drugs Are Sold on the Dark Web." December 7, 2023. https://www.legitscript.com/high-risk-and-problematic-products/how-drugs-are-sold-on-the-dark-web/.

Leonidou, Pantelitsa, Nikos Salamanos, Aristeidis Farao, Maria Aspri, and Michael Sirivianos. "A Qualitative Analysis of Illicit Arms Trafficking on Darknet Marketplaces." In *The 18th International Conference on Availability, Reliability and Security (ARES 2023)*. New York: ACM, 2023. https://doi.org/10.1145/3600160.3605087.

Marsh, Nicholas. "Brothers Came Back with Weapons: The Effects of Arms Proliferation from Libya." *PRISM* 6, no. 4. Washington, DC: NDU Press. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_6-4/6-Marsh.pdf.

Nsaibia, Heni, and Caleb Weiss. "The End of the Sahelian Anomaly: How the Global Conflict between the Islamic State and Al-Qa'ida Finally Came to West Africa." *CTC Sentinel* 13, no. 7. Combating Terrorism Center at West Point, July 31, 2020. https://ctc.westpoint.edu/the-end-of-the-sahelian-anomaly-how-the-global-conflict-between-the-islamic-state-and-al-qaida-finally-came-to-west-africa/.

Persi Paoli, Giacomo, Judith Aldridge, Nathan Ryan, and Richard Warnes. *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web*. Santa Monica, CA: RAND

Corporation, RR-2091, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf.

Policy Center for the New South. "Corridors of the Alliance of Sahel States: Logistical Vulnerabilities, Security Constraints, and Adaptation Dynamics." December 2025. https://www.policycenter.ma/publications/corridors-alliance-sahel-states-logistical-vulnerabilities-security-constraints-and.

Schroeder, Matt. "Beyond the Dark Web: Arms Trafficking in the Digital Age." Small Arms Survey, February 16, 2018. https://www.smallarmssurvey.org/resource/beyond-dark-web-arms-trafficking-digital-a.

Security Affairs. "After Mass Shooting in Germany, It Is Dark Web Paranoia." July 28, 2016. https://securityaffairs.com/49774/deep-web/germany-dark-web-paranoia.html.

SIPRI. *Supporting Small Arms and Light Weapons Controls Through Development Assistance*. Stockholm: SIPRI, 2021. https://www.sipri.org/sites/default/files/2021-02/2102_salw_assistance_in_ssa.pdf.

SL Cyber. "Tackling Cybercriminals Trafficking Illegal Goods from Dark Web." December 2, 2025. https://slcyber.io/overcoming-the-challenges-of-cybercriminals-trafficking-illegal-goods-from-the-dark-web/.

Small Arms Survey. *The West Africa–Sahel Connection: Mapping Cross-Border Arms Trafficking*. Briefing Paper. Geneva: Small Arms Survey, December 2019. https://www.smallarmssurvey.org/sites/default/files/resources/SAS-BP-West-Africa-Sahel-Connection.pdf.

The Register. "German Police Nick Alleged Admin of Dark Web Gun Sales Site." February 11, 2018. https://www.theregister.com/2017/06/12/german_police_arrest_dark_web_site_admin/.

United Nations Economic Commission for Africa. *SAHEL 2043: Towards a Resilient, Inclusive and Prosperous Sahel Region*. Addis Ababa: UNECA. https://repository.uneca.org/entities/publication/4fb4237c-9f44-4ba0-8ca9-0a609522d0fd.

UNOCT/UNCCT. *Countering the Misuse of Virtual Assets and Virtual Asset Service Providers for Terrorism Financing Purposes*. New York: United Nations, 2024. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/uncct_cft_va_report_2024_en.pdf.

UNODC. *Firearms Trafficking in the Sahel*. Transnational Organized Crime Threat Assessment — Sahel. Vienna: UNODC, 2022. https://www.unodc.org/documents/data-and-analysis/tocta_sahel/TOCTA_Sahel_firearms_2023.pdf.

UNODC. "Sahel Programme." https://www.unodc.org/westandcentralafrica/en/sahel.html.

UNODC Global Firearms Programme. "UNODC Analyses the Policy Implications of Illicit Firearms Trafficking on the Dark Web." July 19, 2017. https://www.unodc.org/unodc/en/firearms-protocol/news/unodc-analyses-the-policy-implications-of-illicit-firearms-trafficking-on-the-dark-web.html.

U.S. Department of Justice. "First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More Than 35 Defendants." Press release, 2019. https://www.justice.gov/archives/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35.

U.S. Department of Justice. "International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in Over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and Over $6.5 Million." Press release, September 22, 2020. https://www.justice.gov/opa/pr/law-enforcement-seize-record-amounts-illegal-drugs-firearms-and-drug-trafficking-proceeds.

U.S. Immigration and Customs Enforcement. "ICE HSI New York Operation Leads to Arrests of 3 Dozen Darknet Vendors Selling Illicit Goods, Weapons, Drugs Seized and More Than $23.6 Million." https://www.ice.gov/news/releases/ice-hsi-new-york-operation-leads-arrests-3-dozen-darknet-vendors-selling-illicit.

UN Security Council. *Letter Dated 27 January 2020 from the Panel of Experts on Yemen Addressed to the President of the Security Council*. S/2020/70. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2020_70.pdf.

Varisco, Andrea Edoardo, Pieter D. Wezeman, and Alexandra Kuimova. *Illicit Small Arms and Light Weapons in Sub-Saharan Africa*. Stockholm: Stockholm International Peace Research Institute, 2022. https://www.sipri.org/sites/default/files/2022-12/salw_ssa_2.pdf.

Weimann, Gabriel. "Terrorist Migration to the Dark Web." *Perspectives on Terrorism* 10, no. 3 (2016). https://www.jstor.org/stable/26297596.

Woźniak, Ryszard. "Possibility of Protection of Helicopters Against Projectiles Launched from RPG-7." *Biuletyn Wojskowej Akademii Technicznej* 55, no. 4 (2006). http://www.witu.mil.pl/www/biuletyn/zeszyty/2006/0097p15.pdf.