Public Report

wada

Performance-Enhancing Drug Trafficking on the Dark Web

Intelligence and Investigations Department — Confidential Information Unit

In collaboration with WADA Science Department and Prof. David Décary-Hétu, School of Criminology, Université de Montréal

Table of Contents

Note: To ensure operational confidentiality, only a selection of key activities and conclusions are presented within this report.

1 Overview

In November of 2020, a team of specialists (the **Project Team**) comprised of WADA's Confidential Information Unit, WADA's Science Department and Prof. David Décary-Hétu launched a project (**Project**) to examine performance-enhancing drug (PED) trafficking within the dark web.

The Project objectives were fourfold:

Firstly, to better understand the nature of PED trafficking on the dark web and whether it represents an important source of PEDs for elite and amateur athletes.

Secondly, to assess the type and quality of PEDs being trafficked on the dark web.

Thirdly, to determine whether the dark web is a source of novel substances capable of evading detection methods.

Lastly, to map the criminal script for dark web PED trafficking to better understand how to counter this activity.

The Project targeted the following English and French speaking platforms (**Target Group**):

- → Large dark web marketplaces (cryptomarkets);
- → Small independent single vendor dark web marketplaces;
- → Dark web discussion forums; and
- → Cloud-based instant messaging services.

2 Project Methodology

The Project undertook a multidisciplinary approach with data monitoring performed by Prof. David Décary-Hétu and his research team, testing and analysis conducted by WADA's Science Department, and intelligence collection under the supervision of WADA's Confidential Information Unit.

This approach is unique in-so-far as it combined a **data driven** open-source intelligence (OSINT) approach with advanced **scientific testing** and active **human intelligence collection** (HUMINT). Each one of these techniques explored a different aspect of the dark web landscape.

The strength of this Project is that these three approaches complemented one another, presenting the most holistic understanding of PED trafficking within the dark web published to date. This Project draws from hundreds of hours of direct online contact with PED traffickers.

Although the Project Team engaged in numerous online interactions with dark web vendors, organizing face-to-face interactions fell outside the scope of this Project. All relevant intelligence has been passed to appropriate national anti-doping and law enforcement organizations for further follow up.

Note: English and French dark web platforms comprised the Target Group. As the dominant language for global dark web trade, targeting English platforms provided the broadest possible data set. Nonetheless, it is possible some regional trade may be underrepresented within the data.

3 Three Phases – Operational Research

The Project comprised three phases:

3.1 Phase 1 – Dark Web Monitoring

The Project Team monitored the sales activity of target dark web platforms during a 10-month period.

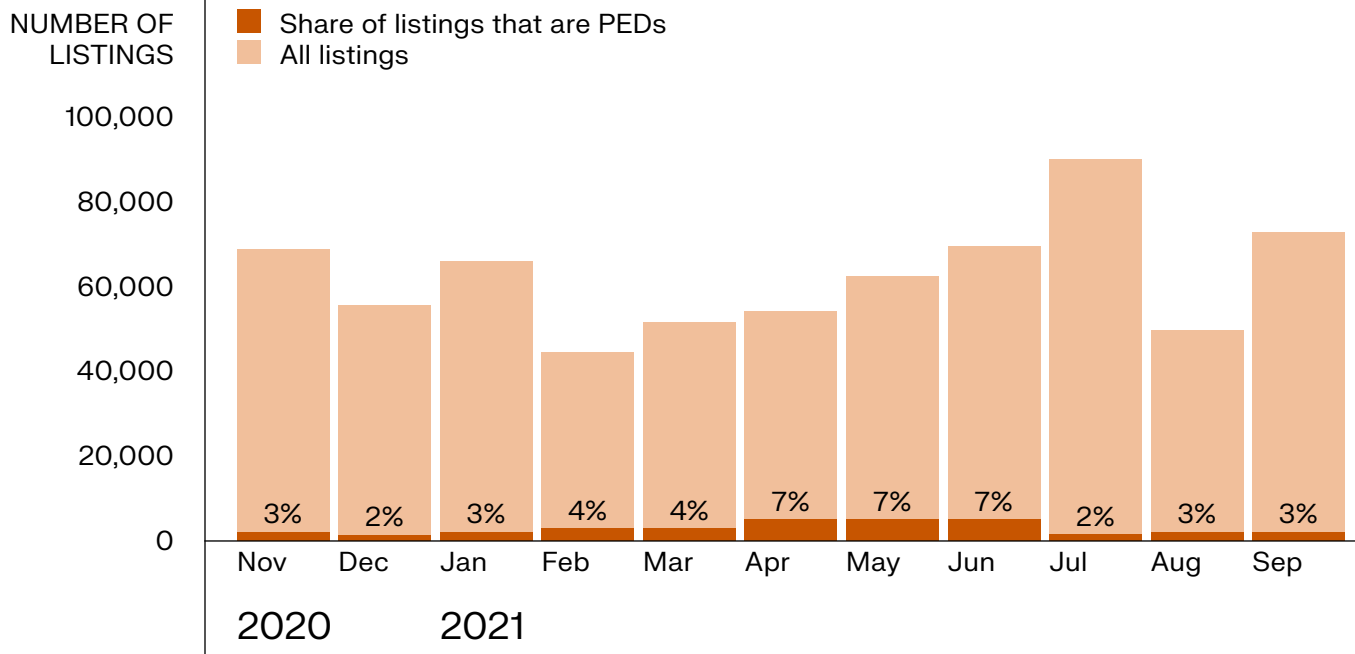
Between December 2020 and September 2021, the Project Team identified 17 large dark web marketplaces and nine small independent single vendor dark web marketplaces. Using the DATACRYPTO software tool[1], the Project Team collected snapshots of dark web platforms once a month.

Highlights:

→ PED trafficking appears to be a marginal activity, both in absolute numbers and relative to the overall clear web and dark web underground economy (see figure 1).

[1] DATACRPTO software has previously been used to collect data for several academic papers and government reports and has a proven track record in studying cryptomarkets. Ref. Kruithof et al., 2016, Martin et al., 2018 & Demant et al., 2018: 262. The Project Team extracted key data for each listing, including the title, description, region shipping from, region shipping to, price, and name of seller.

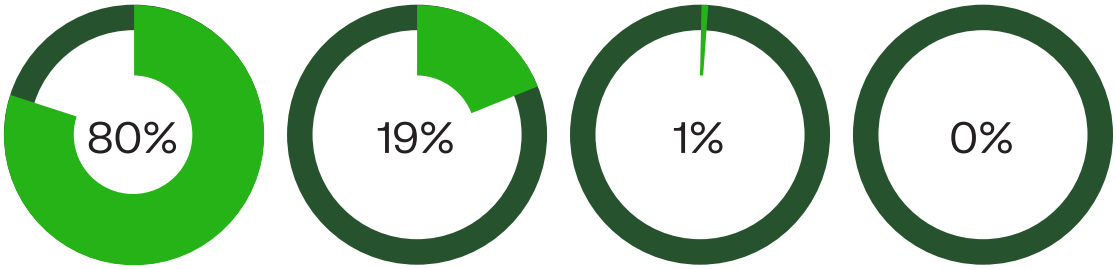
Figure 1: Monthly dark web listings as a percentage of total dark web listings (Target Group)[2]



→ Dark web PED trafficking favors small scale rather than bulk purchasing. The average price of a dark web PED listing stands at USD 135, with only 36 advertisements found over a 10-month period with a price indicative of wholesale (over USD 1,000).

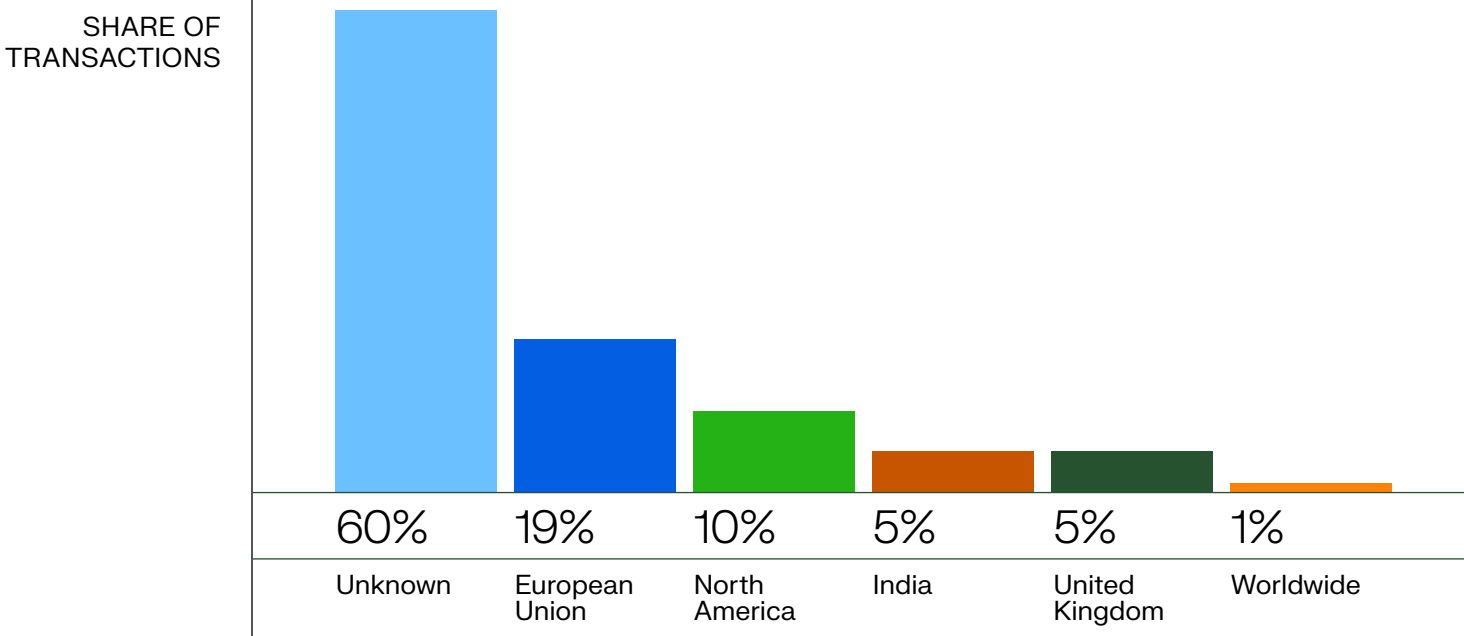
[2] Figure 1 demonstrates the relatively small percentage of dark web PED listings as a percentage of the total volume of dark web listings, which include such items as conventional narcotics, weapons, and stolen credit cards among others. The Target Group includes dark web marketplaces and independent single vendor dark web marketplaces with over 1,000 listings that have been in activity for at least a month.

Figure 2: Average price per dark web PED listing (Target Group)



→ While many end-user transactions on the dark web remain untraceable, Project data indicates the vendors on dark web marketplaces operate in many cases from Europe and the United States.

Figure 3: Origin of PEDs advertised on the dark web



3.2 Phase 2 – Purchase and Analysis of Substances

The Project Team purchased and analyzed a wide range of PEDs from select dark web vendors.

The Project Team sought to identify, purchase and analyze a selection of key PEDs trafficked within the dark web. Using cryptocurrencies, the Project Team purchased products from e-commerce platforms as well as directly from underground laboratories and illicit pharmaceutical companies. These purchases included well-known PED categories, such as selective androgen receptor modulators (SARMs), growth hormones, myostatin inhibitors, androgenic-anabolic steroids among others (See Figures 4 and 5 below). In addition, the Project Team discovered and analyzed two novel performance enhancing substances previously unknown to WADA.

Figure 4: PED sample purchased from the dark web

Figure 5: PED sample purchased from the dark web

Figure 6: Substance Analysis

+ more than advertised
- less than advertised
= as advertised

DECLARED CONTENT	DECLARED USAGE	ANALYTICAL CONTENT	ANALYTICAL USAGE
GHRP-6	5 mg/vial	GHRP-6	+
S-23	0.5 mg/ml	S-23	+
Clenbuterol, Yohimbine	40 mg/mL Clenbuterol, 5.4 mg/mL Yohimbine	Clenbuterol, Yohimbine	+
CJC-1295 no DAC	2 mg/vial	CJC-1295	+
S-23	50 mg/mL	S-23	+
YK-11	20 mg/mL	Y-11	+
SR9009	20 mg/ml	SR9009	=
EPO	3000 IU/vial	EPO	=
rEPO	2000 iu/0.2 mL	rEPO	=
rEPO	3000 iu/0.3 mL	rEPO	=
rEPO	3000 iu/vial	rEPO	=
GHRP-6	10 mg/vial	GHRP-6	-
GHRP-6	10 mg/vial	GHRP-6	-
MK-677	25 mg/ capsule	MK-677	-
RAD-140	10 mg/vial	RAD-140	-
LGD-4033	10 mg/capsule	LGD-4033	-
hCG	5000 iu	hCG	-
YK-11	20 mg/ml	YK-11	-
LGD-4033	20 mg/ml	LGD-4033	-
Tesamorelin	2 mg/vial	Tesamorelin	-
PEG-MGF	2 mg /vial	PEG-MGF	-
GHRP-6 (expected)		Glycine-GHRP-6	
BCP-157		BCP-157	
Ligandrol	25 mg /capsule	MK-677	Wrong PED
Ipamorelin	10 mg	GHRP-2	Wrong PED
GHRP-6, CJC-1295	5 mg/vial, 5 mg/vial	GHRP-2	Wrong PED
ACE-083 or BPC-157 or RAD 140 Testolone		Glycine-Ipamorelin	Wrong PED
CJC-1295	5 mg/vial	GHRP-6	Wrong PED
ACE-031	1 mg	Glycine-GHRP-6	Wrong PED
ACE-083 or BPC-157 or RAD 140 Testolone		AOD-9604	Wrong PED
BPC-157	5 mg/vial	Unknown peptide	Wrong PED
ACE-083 or BPC-157 or RAD 140 Testolone			

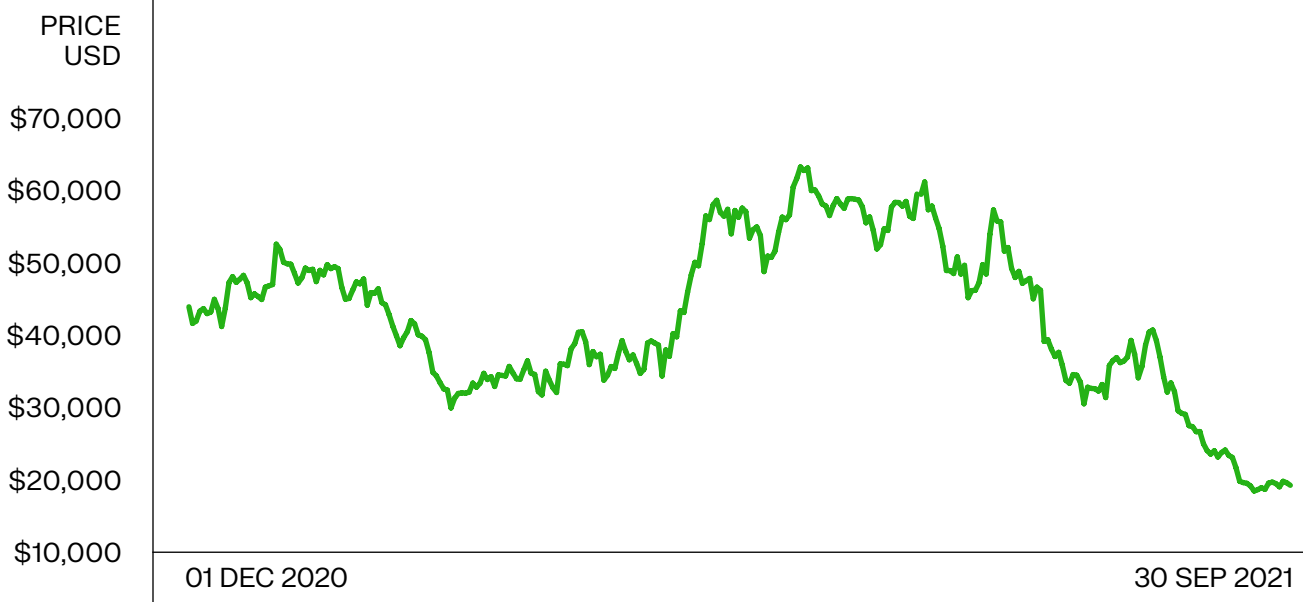
Note: Actual dosage which is categorized as same is considered within 10% of the dosage claimed by the producer.

The names of the producers were removed to protect investigative techniques and methods.

Highlights:

→ The Project Team experienced several significant challenges when purchasing PEDs on the dark web, such as purchasing cryptocurrencies using funds held in Canadian financial institution accounts, rapidly fluctuating cryptocurrency exchange rates, shipping delays, and overall vendor reliability issues. This made for a very poor user experience.

Figure 7: Evolution of bitcoin to USD exchange rate (2020-2021)



→ 26% of purchased samples were inaccurately labeled (Figure 8) while about 48% of all analyzed samples contained concentrations which were less than advertised (Figure 9).

Figure 8: Proportion of trafficked PEDs accurately labeled

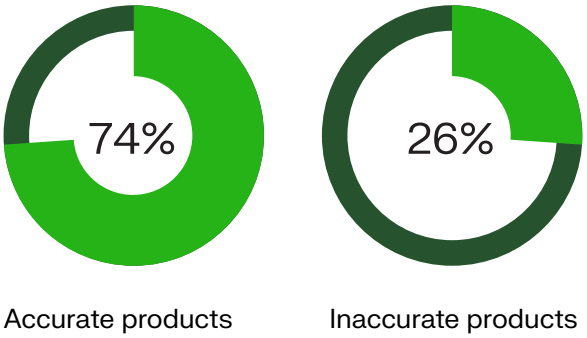
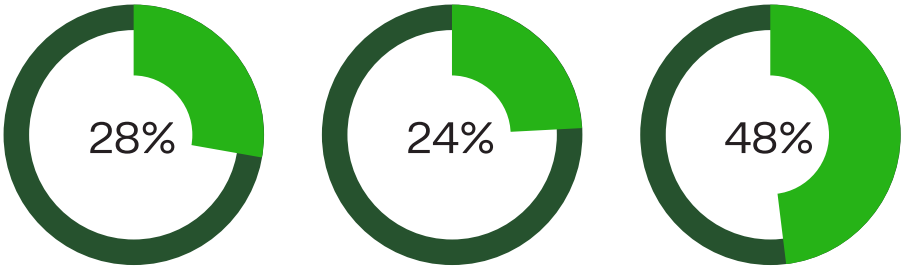


Figure 9: Statistics on the accuracy of PED dark web advertisements



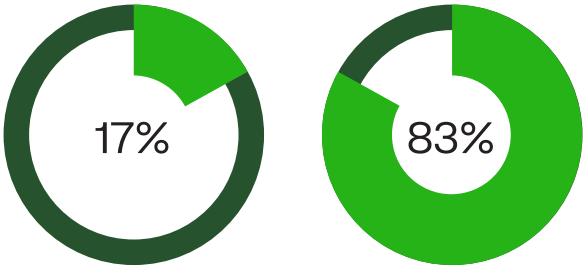
Concentration more than advertised

Concentration as advertised

Concentration less than advertised

→ Of note, some vendors from both legitimate and illicit pharmaceutical companies did provide the Project Team with both accurately labeled products and accurate concentrations.

Figure 10: Overall statistics on the accuracy of PED dark web advertisements



Product and concentration received as advertised

Product and/or concentration received not as advertised

3.3 Phase 3 – Collection of Human Intelligence (HUMINT)

The Project Team gathered human intelligence on dark web criminal networks manufacturing and trafficking PEDs.

PEDs appear to be produced in bulk in Asian countries, and then shipped to Europe, North America and Australia to be refined and sold to end-users. Local distributors use online advertisements on all available platforms to maximize visibility and compete for market share.

Many vendors are willing to engage in conversations about their activities, especially if they believe this will lead to a sale. Vendors use cloud-based instant messaging services such as Telegram and Wickr to communicate. These encrypted channels are preferred over public forums and the clear web.

Highlights:

- → The Project uncovered some examples of genuine pharmaceutical products being trafficked on the dark web, though the bulk of products come from illicit pharmaceutical laboratories and homebrewers.
- → Though many vendors compete for dark web sales, only a very small proportion of vendors account for the majority of actual sales.
- → Retail sales dominate the dark web marketplace, while bulk sales are insignificant by comparison.
- → Vendors use publicity to attract customers and offer seasonal discounts.
- → Vendors use a wide range of techniques to mask the true nature of their shipments, including hiding them within beauty and hair care products.
- → The majority of home brewers source their raw products in Asia and sell to customers in Western industrialized countries
- → Most customers appear to be bodybuilders and amateur athletes rather than professional athletes participating in international competitions.[3]

[3] The Project did collect unverified information from two dark web PED dealers who claimed to traffic PEDs to athletes from two Olympic sports. The Project Team was unable to obtain additional details on the customers nor on the level they competed in.

Figure 11: PED Criminal Script

1

Manufacturing of PEDs

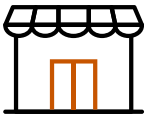
a. Legitimate international pharmaceutical companies
b. Regional pharmaceutical companies
c. Underground unlicensed laboratories/illicit pharmaceutical companies
d. Home brewers

2

Distribution channels of PEDs

a. Cryptomarkets
b. Single private shops
c. Direct dealing on discussion forums

3



Retail / Wholesale PEDs

Vast majority of listings advertise retail-sized quantities (less than USD 1,000) rather than wholesale, though wholesale is possible through the dark web

4

Advertisement of PEDs

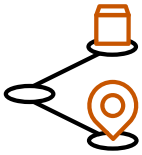
a. Sales (ex. Black Friday Sale, New Opening Sale)
b. Publicity on discussion forums
c. Publicity on the clear web
d. Publicity on social networking sites like Facebook and YouTube

5

Shipments of PEDs are disguised as packages containing

a. Telephone covers
b. Beauty products
c. Supplements

6



Routes of PEDs

a. Raw products often originate from Asia
b. Distribution to end-users in Asia and Western industrialized countries
c. Lack of end-user monitoring sign of inadequate regulation and export controls

7

End-users of PEDs

a. Cursory intelligence suggests a small number of competitive athletes source PEDs from the dark web
b. Majority of end-users appear to be amateur bodybuilders who are unlikely to undergo doping controls

4 Key Conclusions

Objective 1: Better understand the nature of the PED trafficking on the dark web and whether it represents an important source of PEDs for elite and amateur athletes.

4.1 Nature of PED Trafficking

→ While dark web marketplaces offer hundreds if not thousands of PED advertisements, these represent only a very small fraction of all dark web marketplace listings. Cursory observations point to a vast clear web PED marketplace which dwarfs its much smaller dark web equivalent.

→ Purchasing PEDs on the dark web include a significant set of challenges – fraud, cryptocurrency fluctuations, delivery delays etc. Purchasing PEDs on the dark web is often a troublesome and risky proposition.

→ All dark web platforms offer some means of anonymous communication between supplier and buyer; however, the dark web does not appear to host a "community" of PED users who exchange PED expertise and information. Most public and group communications are hosted on clear web forums which openly exchange advice on PED use.

→ The popularity of clear web forums when compared with their anonymous dark web equivalents suggests that participants have little fear of law enforcement. This feeling of security likely reflects a lack of harmonization in monitoring and enforcement among law enforcement.

→ The scarcity of dark web group chats suggests that if high-level professional and amateur athletes are using the dark web marketplaces to source PEDs, they are likely communicating through private channels, such as encrypted messaging apps and face-to-face meetings.

4.2 Dark Web PED Clientele

→ Actors who were willing to discuss their clientele noted they primarily included amateur bodybuilders and gym-types. Given the significant supply challenges identified within this report, it is unsurprising that amateur body builders rather than elite athletes are the intended customer base. Doped elite athletes would require a dependable delivery service to maintain an effective doping cycle and avoid detection.

→ Nonetheless, the Project Team did identify a select group of dark web suppliers who specifically referenced elite athletes as clientele and a supposed ability to evade anti-doping detection.

Objective 2: To assess the type and quality of PEDs being trafficked on the dark web.

4.3 **Laboratory Analysis**

→ Laboratory analysis strongly suggests that purchasing PEDs through the dark web is a risky proposition. Cursory testing data suggests products are often mislabeled or contain significant discrepancies in terms of their concentration.

Objective 3: Determine whether the dark web is a source of novel substances capable of evading detection methods.

4.4 **Novel Substances**

→ The Project Team found scarce mention of new substances or techniques to evade doping screenings. In this respect, most dark web suppliers appear to traffic the same well-known PEDs available on the clear web. The Project Team did discover two novel substances previously unknown to WADA. This discovery appears to be the exception to the rule.

4.5 **Detection Evasion**

→ An initial analysis of PEDs sourced on the dark web did not reveal any gaps in anti-doping testing mechanisms although further analysis is recommended.

Objective 4: Map the criminal script for dark web PED trafficking to better understand how to counter this activity.

4.6 **Targeting Dark Web PED Vendors**

→ All Project Team communications with vendors who claimed the ability to advise customers on circumventing anti-doping analysis occurred within private messaging apps. This reinforces that anti-doping organizations and law enforcement agencies should prioritize first-hand contact with vendors rather than passive collection via open-source intelligence.

→ Phase 3 conclusions suggest that there are commonalities among the supply and shipping methods used by dark web PED traffickers. As such, law enforcement could presumably disrupt this activity by targeting specific areas within the supply and distribution chain.

→ The criminal script approach makes it possible for law enforcement agents to identify bottlenecks and more vulnerable actors and stages. In this case, it appears that raw powder sourcing and laboratory production are somewhat concentrated, thus making them vulnerable to disruption efforts by law enforcement.

- Surprisingly, SARMs, which are quasi-legal products and are easily sourced in multiple jurisdictions, are actively being trafficked on the dark web. It is possible that dark web vendors who traffic SARMs are also involved in other criminal activities and, as such, are immunizing their legal activities from criminal ones by conducting all of their activities under the anonymous umbrella of the dark web.
- Although significantly smaller in scope than the clear web, PED trafficking on the dark web appears to operate unchecked. The dark web affords actors the advantage of anonymity, which combined with weak regulations and a lack of enforcement, allows dark web PED suppliers the freedom to operate with relative impunity. At present, it appears that the principal reason the dark web represents a relatively small marketplace is the convenience and lack of enforcement within the clear web.

5 Recommendations

These recommendations are intended for anti-doping organizations, anti-doping researchers, and applicable public authorities and law enforcement organizations.

→ **Targeted engagement with dark web PED vendors and manufacturers**
Targeted engagement of PED vendors centered around large-scale purchases may make it possible to forge stronger ties with dark web actors and collect higher value human intelligence.

→ **Clear Web Project**
This Project could be replicated on the clear web. Employ a similar project methodology targeting select clear web actors, compare results, and recommend comprehensive counter measures targeting both marketplaces.

→ **Target Anti-Doping Evasion**
This Project documented public forum messages discussing the circumvention of doping controls. Use a direct approach to collect additional information from these online actors to identify new substances and evasion techniques for the purpose of bolstering detection methods.

→ **Broadcast research findings**
This Project highlights what does and does not work when interacting with dark web vendors and PED manufacturers. This information could be of significant value in helping law enforcement and Anti-Doping Organizations develop effective strategies for generating information and evidence. Disseminate intelligence and research findings to relevant stakeholders.

→ **Adopting a multi-disciplinary approach**
No single source of intelligence provides the necessary knowledge to fully understand PED trafficking on the dark web. Open source and human intelligence, combined with the purchase and analysis of PEDs, provide a holistic view of this illicit trafficking. Each complements the other and adds depth to overall findings. Whenever possible, a multi-disciplinary approach should be adopted by anti-doping researchers.

6 End Notes

This key summary report draws from an extensive 70-page internal report documenting the entirety of WADA's year-long examination of PED trafficking on the dark web.

As part of this Project, WADA's Confidential Information Unit has prepared eight intelligence packages, which have been distributed to key law enforcement and anti-doping stakeholders for review and investigation. WADA's Confidential Information Unit is following up with recipients.

A comprehensive Project presentation for anti-doping intelligence and investigation partners is envisioned during the latter half of 2022.

Disruptions of Dark Web Activities

The dark web is constantly under attack, which can impact upon both the size and scope of its activities.

There are three main vectors for dark web interruptions:

1. **Police intervention.** Law enforcement agencies routinely target the dark web, and, in fact, our analysis suggests that globally over 140 operations were launched in the last five years alone. These operations are aimed at taking down platforms and arresting their administrators and participants. While most operations are limited in scope, some target the largest marketplaces and lead to dozens of arrests.

2. **Internal fraud.** Platform administrators control all the transactions of their participants. When platforms grow to a certain level, the temptation to steal from the participants also increases. In the case of the Sheep Marketplace, for example, the administrators of the platform are believed to have stolen tens of millions of dollars from participants.[4]

3. **External attacks.** Administrators earn a commission on every transaction they facilitate and are constantly competing for market share on the dark web. They have been known to attack other markets to steal user information, discredit competitors, or simply steal funds held in escrow. Administrators also enlist hackers to attack other markets.

When viewed together, these attack vectors explain some of the ebb and flow observed in the number of listings. They also explain why some platforms were unavailable during some months of the data collection period.

[4] Robertson, A 2013, 'Online black market members hunt down $100 million in bitcoins, blame site owners for theft', The Verge, 2 December, https://www.theverge.com/2013/12/2/5167670/sheep-marketplace-bitcoin-heist-nets-at-least-5-million-owners-blamed

wada

media@wada-ama.org
CIU@wada-ama.org