THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

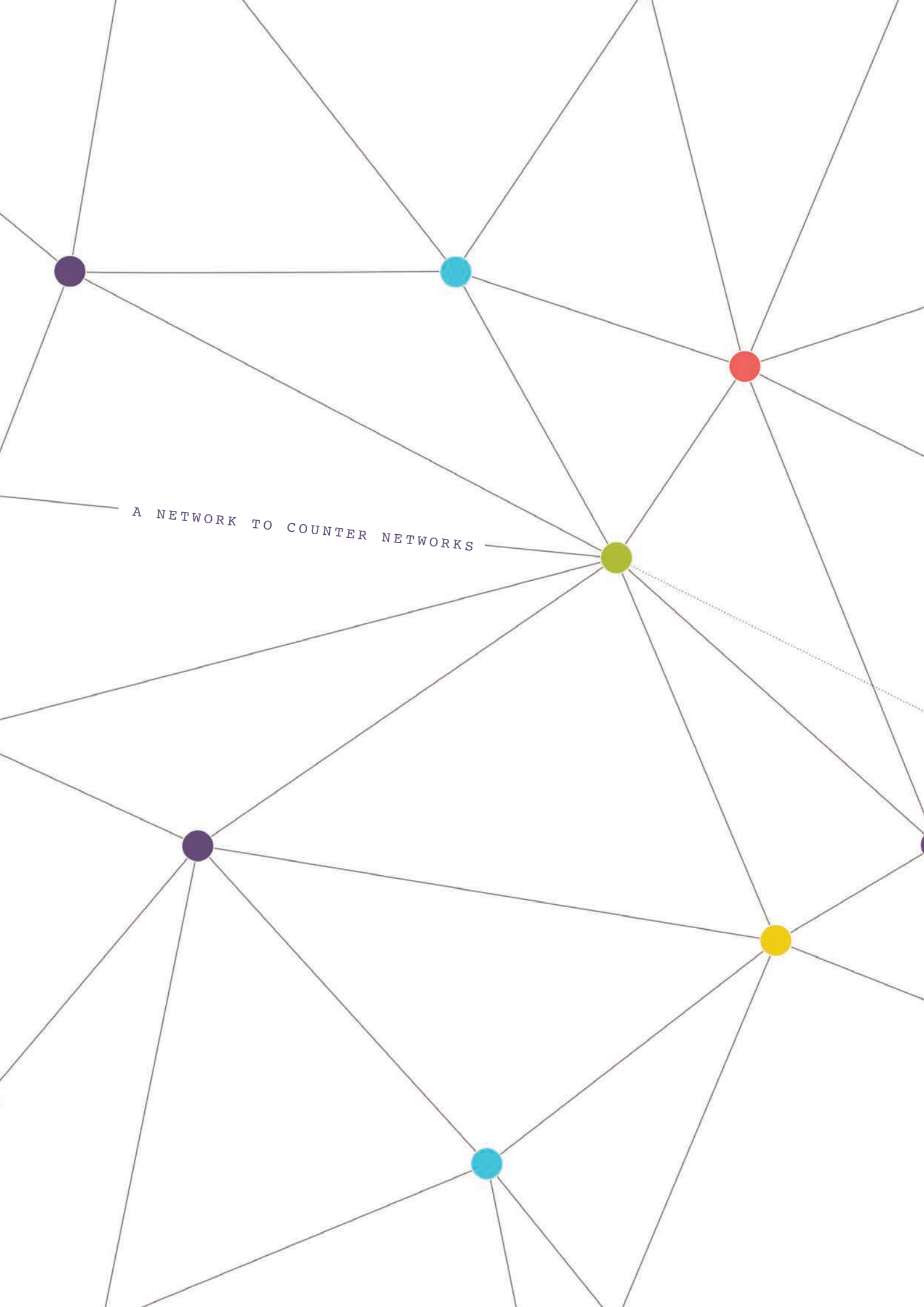
DIGITAL DANGERS

ILLICIT
WILDLIFE MARKETS AND THE DARK WEB

A SCENARIO OF THE CHANGING DYNAMICS

FELIPE THOMAZ

November 2018


A NETWORK TO COUNTER NETWORKS

ILLICIT
WILDLIFE MARKETS AND THE DARK WEB

A SCENARIO OF THE CHANGING DYNAMICS

FELIPE THOMAZ

November 2018

The Global Initiative Against Transnational Organized Crime
WMO Building, 2nd Floor
7bis, Avenue de la Paix
CH-1211 Geneva 1
Switzerland

www.GlobalInitiative.net

Summary

This brief gives an overview of the online illicit wildlife trade (IWT), and analyzes the current state of this market, and speculates on its likely developments. Although there is currently very little IWT activity on the dark web, we expect this to change as enforcement steps up, and this brief explores how that process might evolve. The online market for illicit wildlife trade appears to be disaggregated and characterized by 'blurred channels', yet, at the same time, it is relatively 'out in the open', which points either to a lack of enforcement or challenges that stymie effective enforcement. However, as and when enforcement activities are stepped up, it is probable that the IWT will respond by moving along a specific pathway. This trajectory would first see a move to centralized dark-web markets, then to specialist, and smaller, dark-web 'shops'. These market shifts would be followed by 'markets by invitation' and then distributed, peer-to-peer marketplaces. Under this scenario of a changing market, each step would be accompanied by a decline in market size caused by a decrease in potential consumers (and vendors), but this market loss would be counteracted by an increase in marketing efficiencies and organization on the part of the vendors.

Key findings

- One of the key features of online IWT is its complexity and disaggregation: there is no 'one stop shop' for animal products (as there has been for other contraband that is marketed online). This has a number of impacts on consumer behaviour, both encouraging and discouraging purchase.
- If any effective enforcement pressure is brought to bear on the online IWT, the degree of market consolidation will change as markets evolve, as will the level of vendor organization.
- Each step made by vendors in the attempt to safeguard these illicit markets will benefit those who manage to continue operating, but the overall size of the potential market will diminish. This is because, up to a certain point, the greater privacy that vendors will achieve will lead to markets reaching fewer customers.
- Current enforcement strategies favour shutting down or shifting platforms, but such tactics will serve only to displace the networks, rather than terminate them.
- Successful interventions should target the underlying consumer psychology of these markets and the social processes that allow them to flourish.

Introduction and background

This aim of this brief is to examine the market for illicit wildlife goods traded in the black markets of the dark web. But, it is important first to clarify terminology and assign boundaries to the discussion given the current state of IWT, the dark web and the black markets residing there.

The web can be subdivided into three levels: the surface web, the deep web and the dark web. The surface web comprises pages that can be indexed by search engines, such as Google, Bing and Yahoo, by following links from one page to another. The deep web is the collection of pages that cannot be indexed, common examples being personal financial accounts, and other confidential online information. Access to this kind of information requires password authentication, and therefore cannot (and should not) be indexed by search engines.

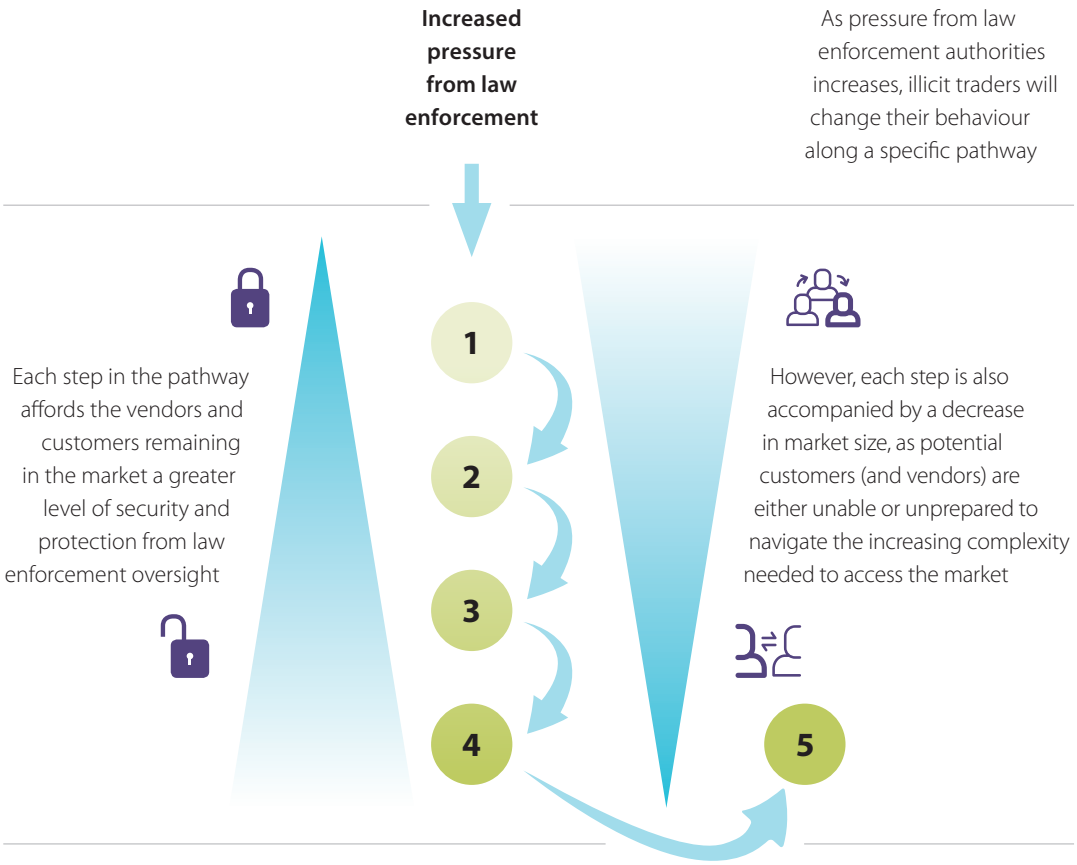
Finally, the dark web is a collection of pages that are intentionally hidden and rendered inaccessible, except where one has access through the use of specialized software. This process of concealment does not necessarily per se

imply illegal activity or ill-intent, but simply the desire for privacy. However, among these unconnected, hidden pages we also find dark net markets (DNMs). These are pages that serve as platforms where vendors and buyers come together to conduct transactions involving a wide range of illicit goods (e.g. drugs, weapons, stolen data). The process of finding these markets is unlikely to happen unintentionally in the course of everyday web browsing because to access DNMs, one requires a special browser (known as 'the onion router', or TOR), as well as specific knowledge of the market's exact web address. (For example, the now closed market AlphaBay was last accessible using the following URL: http://pwoah7foa6au2pul.onion, which would not work on a normal web browser, nor would it be discoverable using everyday search engines. That information would have to come by other means, such as a community of like-minded individuals involved in the specific trade.)

Which brings us to one initial limitation concerning analysis of the role of DNMs for the illegal wildlife trade. At the time of writing, in terms of the IWT, there is essentially no transactional volume of any sort taking place in the dark web. Looking through a history of product listings appearing in now closed black markets, their related community forums, as well as their operational counterparts today, the presence of wildlife material is only briefly mentioned. These are usually forum posts where an individual claims to have items available (e.g. pangolin or ivory), and asks if any community members are interested. Of those responding, the interest seems to mostly concern arbitrage opportunities (i.e. purchase for resale). That is not to say that illicit wildlife trade is not taking place on the web: it simply means it takes place in (mostly) plain view on the surface web (i.e. through trading websites and open listings), and in the deep web (through private messages and private trading groups). With this in mind, this brief will initially concentrate on the characteristics of the surface- and deep-web environments, followed by the conditions that may, speculatively, force illicit wildlife markets 'underground' into the dark web, and the dynamics that may then emerge in that market environment (see Figure 1). The relevance of this brief is about encouraging preparedness for an eventual transition of IWT to the dark web in a response to greater pressure and enforcement on the surface web, and developing a pre-emptive strategy, so that this eventual market is not allowed to properly form and flourish unnoticed.

Secondly, it is important to recognize that this discussion of the web marketplaces for IWT needs to be generic in nature, and therefore risks losing granularity. This is a speculative analysis of the likely scenarios that will emerge if the IWT markets shift to the dark web. It does not attempt to assess the implications for different species. The combination of, first, the nature and characteristics of associated tradeable wildlife goods (e.g. whole animals, pelts, bones, extracts), secondly, the supply chain and its international footprint, and, thirdly, the target market, gives rise to a multitude of discrete, individual markets. This brief, on the other hand, concentrates on the aggregate, global character of what generally applies to all such smaller markets that form part of the whole, but caution must be exercised when breaking down the analysis in terms of the implications for specific species, and national or local contexts.

Figure 1: The trajectory to the dark net



1. Current online IWT: the market in wildlife products currently takes place mostly in plain view, on the surface web (trading websites, open listings) and the deep web (private messages and trading groups). The trade is disaggregated and the distinctions between small-scale and wholesale suppliers are blurred.

2. Centralized dark web markets: in response to increased pressure, traders first move away from the easily observable surface web and into centralized DNMs. This increases market cohesion and allows customers to search more easily. However, many customers and vendors will not commit to the more complex technology required to access these forums.

3. Specialized smaller dark web shops: increased law-enforcement pressure, the costs of administering DNMs, competition between DNMs and erosion of trust all contribute to the breakdown of the market into smaller storefronts. This affords vendors greater privacy, as all communications become encrypted one-on-one conversations, but the costs of searching for customers is increased.

4. Markets by invitation: the next step is for marketplaces to form that allow access only to those invited to participate. This is an effective safeguard against police infiltration, yet the cost is a loss of market membership, as some are unable or unwilling to prove themselves worthy of entry.

5. Distributed peer-to-peer marketplaces: this stage is hypothetical and dependent on technology currently being tested. These marketplaces would use blockchain technology and smart contracts to create a distributed marketplace that does not rely on any single individual to continue operating. All communications within the marketplace could be encrypted through the same technology. If proved successful, this form of marketplace could replace many of the activities in stages 1 to 4.

Methods

The information that forms the basis of this brief has been derived from the author's research on digital illicit markets as well as his collaborations with international law-enforcement agencies, military operations and American district attorney offices, which aim to understand and disrupt a variety of illicit trade operations taking place on the web.

The data was gathered through a systematic scraping of the dark web, and processed for topic discovery and natural language processing using machine learning and other artificial-intelligence-assisted approaches (e.g. IBM Watson Natural Language Understanding). Relational data, such as consumer–vendor networks, were processed using social-network topology analysis and similar approaches.

Current environment of the online illicit wildlife trade

Illicit trade networks rely on other networks

One core defining characteristic of illicit markets is that its participants, whether they are market organizers, vendors or customers, must be able to manage and mitigate uncertainty and risk. Although the same holds true for legal markets and their legitimate participants, illicit marketplaces are additionally burdened by the lack of institutions to assist with conflict resolution or to redress grievances. Put simply, a vendor or buyer of an illicit product cannot make a claim to the police if robbed or turn to legal support when contracts are not upheld; nor can he refer grievances to business bureaus that regulate trade. These limitations heighten the risk of doing business in an illegal trading environment, and add to the uncertainty around partner selection and potential outcomes.

The issue becomes increasingly complicated in the dark web, where users can, and do, use a multitude of pseudonyms that are loosely tied to platforms, and which can be co-opted or stolen by third parties. The identity of the underlying user cannot be easily validated outside of the use of encryption signatures, and even those have been known to be compromisable (the Dutch police once intercepted such identifiers and proceeded to collect information on partners of known drug vendors by communicating with trusted digital signatures[1]). In short, the true identity of your potential business or transaction partner is essentially always in question.

One approach to resolving this underlying issue of uncertainty and risk is to rely on other, non-criminal networks to access information and coordinate activities. The classic example is that of drug dealers who may use extended-family relationships to choose business partners, thus gaining information and security through a family network to help safeguard their criminal operations. One should also consider the fact that consumers of illicit goods do not know intuitively how to enter the market or how to operate in it securely. All of these are learnt and socialized behaviours, which rely for information on outside, surface-level networks.

Within the IWT markets more specifically, a number of surface-web networks exist for the appreciation, study and then collection of various animals. These social networks are designed to attract those segments of the market that might be interested in whole animals. And there are similar networks focused on the procurement of, and general practices concerning, various illicit animal-based products that are consumed for their supposed health benefits (e.g. tiger-bone wine or pangolin scales). These kinds of networks serve the same function: to educate potential consumers about various approaches to acquisition and to ultimately connect potential consumers to vendors. One can frequently identify situations where an online group member makes a general enquiry, for example: 'I would love to have one of those', which may be followed by a reply, such as, 'I've sent you a private message'. At this

point in the dialogue, the potential vendor shifts the conversation from the surface web to the privacy of the deep web, away from direct observation, to organize details of the transaction.

These social networks are platform-agnostic. It would be easy to point to Facebook, for example, and highlight the number of animal-based groups active there, serving as this external network function. But that would underestimate the scale of the issue: such connections are possible, and they exist, across the entirety of the surface web, wherever people are able to interact and congregate online. This serves to illustrate that it is important to understand and distinguish between enabling technologies and platforms, and the social processes taking place there. Successful interventions in the area of IWT are likely to focus on the latter – the social processes and the underlying consumer psychology – rather than platform control and regulation, as that would serve only to displace the location of the network, rather than stop it functioning.

Successful interventions in the area of IWT are likely to focus on social processes and consumer psychology rather than platform control.

There are numerous examples of such failed interventions in the illegal drugs markets. In the illicit online drugs market, it has been shown that attempts to ban surface-level communities may have resulted in a shift in the platforms that are used, but not in loss of market coordination. Ongoing research documented a 10 000-strong community of consumers of illegal drugs regrouping on another platform in the space of a few days, with no directly observable loss of market efficiency. There is no a priori reason why this should be any different in the case of illicit wildlife consumers and their communities.

Variation in scale of transactions and market disaggregation

Observing the IWT on the surface web reveals a notable range in transaction quantities and types, from single animals exchanged among small collector networks (e.g. Asian Arowana fish in the US, where their import is illegal, or various reptile groups) to substantial supply-chain arrangements that service a buyer–seller relationship (e.g. a guaranteed supply of 100 lion pelts a month).

This points to a 'disorganized' supply chain and one defined by the blurring of different channels (i.e. retailers and wholesalers becoming increasingly identical). Ideally, in a standard business process, organization of the supply chain would allow for a controlled flow of goods from sourcing and production, through intermediaries, such as retailers, until the product reaches the demand side. In that kind of environment, the consumer would be presented with only appropriate options (e.g. not being offered a tanker of milk when he is interested in only a litre). However, the channel blurring seen in the online IWT is characterized by a lack of clear divisions between the various intermediaries and purchasing stages along the supply chain. Hence, a consumer seeking just a small quantity of pangolin products, for example, might well arrive at an online 'wholesaler' offering the same in units of 40 kilograms.

At least two significant and opposite effects may arise from this blurring. The first is a deterrent effect caused by an increase in the cost and time burden associated with the consumer search. The search process incurs a cost to the consumer, in terms of the time and effort expended to identify relevant information. Blurred channels and inappropriate product offerings have the effect of increasing the cost of the search, as potential consumers encounter a large amount information that is not relevant to their needs during the process. This increased cost and burden of information acquisition may act as a deterrent to potential consumers of illicit wildlife products.

However, the converse may also apply: the visibility of the multiple sources and channels that make illegal wildlife products available on the internet could have the opposite effect. For example, wholesale stockists of illicit wildlife products provide potential consumers with a source of reference information in terms of prices and quantities. Although the hypothetical consumer may not purchase in wholesale quantities, this nevertheless provides him

with a price benchmark that may inform smaller-scale purchases once price and quantity ratios can be ascertained (e.g. one bottle of tiger bone wine, as opposed to an order for several crates).

Furthermore, the extra time and effort expended on the search process, as a consequence of this channel blurring and supply-chain 'confusion', may have an effect on the consumer's cognitive purchasing motivation. In theory, the heightened search 'cost' and effort may have the effect of consumers assigning greater value to items, and hence lead to an increased likelihood of their making transactions.

Altogether, the variability in the way illicit wildlife goods are offered and traded online points to a disaggregated market. Put simply, there is no 'one-stop shop' for illicit wildlife goods and related services. And, although it may seem unlikely that one would emerge, this is precisely what might be expected if there were to be an increase in the level of enforcement and penalties associated with this type of crime. And this has been the case with other categories of illicit goods traded in DNMs, such as drugs (e.g. cocaine, heroin, LSD and MDMA) and weapons, which can be sourced under the 'same roof'. Such dark-net online markets have come into existence because they simultaneously reduce consumer risk and uncertainty, while reducing search costs. Again, there is no a priori reason why the online IWT should behave any differently from these other illicit markets if a scenario were to emerge where enforcement pushes it from the surface web towards the dark net.

The nature of black markets and apparent lack of enforcement

There are a number of studies in conservation that apply standard economic theory to the IWT, seeking to explain the elasticity of demand, pricing effects and supply effects on hunters and poachers. And although it is beyond the scope of this report to refute this significant body of literature, it is worth pointing out that the validity of such studies is compromised by certain limitations. For one, it is worth noting that, based on the author's own research,[2] black markets are fundamentally very different from their legal counterparts. By analyzing the social-network structure of black markets, and the patterns of connectivity between members, it is evident that their organization does not mimic traditional social-network theory and its implications. This has a knock-on effect in terms of expectations for market function, profitability, the flow of information, risk exposure, privacy concerns and demand. And while there is still much work to be done to explicitly test the extent of these differences, it is clear that black-market environments are very much unalike, and drawing conclusions from the application of older theory on their function should be done with the utmost of caution.

One noticeable difference between licit and black markets can be detected in the impact of changes in CITES[3] appendix listings on how the markets react. Whereas, hitherto, legal market channels cease operations, and licit consumers who are informed about changes in CITES listings tend to disengage from trading, black markets – perhaps obviously – continue their operations unhindered by changes in CITES listings. And perhaps most telling is the fact that, counterintuitively, when species are listed in Appendix I (indicating that commercial trade in wild-caught specimens is illegal), it does not have the effect of changing their price on the black market.

When we consider this lack of response in black-market behaviour to changes in the normative severity of CITES listings, as well as the fact that IWT remains plainly visible on the surface web (even though online activity may tend to become more submerged, shifting to private modes of communication when it comes to closing deals), it is hard to conclude that the enforcement of regulations has had any substantial impact on the structure or operation of the illegal wildlife trade. It appears that the perception of risk related to the illicit wildlife market is therefore fairly low, and possibly diminished by the confusion created by legal definitions and norms (farmed as opposed to wild lions being just one example[4]).

It is hard to conclude that the enforcement of regulations has had any substantial impact on the structure or operation of the illegal wildlife trade.

The dark web: A future scenario for online IWT

How, then, might these black markets foreseeably change if the degree of enforcement were to become more severe? Would the risk associated with online illicit trading of wildlife become heightened? We analyze some scenarios next.

Stage 1: The move to the dark web and aggregation

The first stage following an increase in enforcement, which would impose a growing degree of risk to IWT market organizers, vendors and consumers, is likely to be a response that sees market activities move away from readily observable online environments to concealed parts of the internet. This shift is likely to mirror the change observed in the illicit online drugs trade, where offerings moved from surface-level discussion groups to the secrecy of the dark web.[5]

This shift is also accompanied by an aggregation of separate offerings into greater cohesive markets, such as the DNMs for illicit drugs discussed above. It is possible that specific markets for wildlife will emerge that amalgamate species and related goods into perhaps one or several dedicated markets. It is more likely, however, that, at least initially, they will be absorbed into existing DNMs (e.g. those for drugs and weapons). However, co-locating IWT markets with those for illicit drugs and weapons might be unsustainable in the long term for those consumers in the market for wildlife who self-justify their purchases in the name of tradition or view them as culturally relevant. Hence, segmentation would occur as a result of pressure for DNMs specifically for wildlife. Those in the drug markets also engage in personal 'justifications' for their habits, both socializing and diminishing the burden they feel as a result of consuming and commercializing illicit drugs. It is likely, however, that wildlife consumers would perceive themselves as quite different from this market segment, necessitating a dedicated market environment for their community in the dark web.

The aggregation of groups into dedicated markets would be accompanied by a marked increase in cohesion (where separate micro-communities become one) and efficiency of exchange, which, in turn, is likely to have a number of significant effects. Initially, this single community structure facilitates communication, and the exchange of ideas, norms and 'best practices'. Not only does this increase the normalization of the practices associated with IWT, but also the learning rate of new and novel ways to bypass legal barriers and methods to avoid enforcement, or at least mitigate the risks thereof. These shifts in the market environment would lead to reduced search costs for consumers, and may point to an increase in the range of categories that are purchased as a result of their being co-located in the market. For example, it is feasible that collectors of one type of exotic fish might extend their purchasing patterns to different species.

However, a noticeable counterforce to this market efficiency would come from the increased complexity of safely navigating and operating in the dark web. There are a number of technologies that need to be understood and mastered to make effective use of a DNM (e.g. TOR browser, private encryption keys and cryptocurrencies). Many potential consumers will simply either be unable to follow the community to the dark web, or they will find the technical effort and cost off-putting and will therefore choose to disengage from the market.

Many potential consumers will simply either be unable to follow the community to the dark web, or they will find the technical effort and cost off-putting.

The DNMs and dark-web communities will continue to rely on surface-level networks, as described previously. No consumer knows inherently how to access, engage with or operate in a DNM. These skills have to be acquired, hence surface-web IWT communities will remain as a point of entry, recruitment and education, and provide an environment where those who choose not to transition

to the dark web can still interact with peers. This way, they would remain part of the overarching problem, although their transaction volume would be zero.

Therefore, this foreseeable shift to the dark web would be marked by a significant increase in market organization, and improved efficiency and access for those participating, but the overall number of participants would decrease given the technical complexity and costs involved in navigating the new terrain.

Stage 2: The market splinters

The nature of DNM operations (including the vendor fee structure and escrow deposits) – combined with the level of skills needed by participants (mentioned above) and mounting pressure from law enforcement – will eventually lead to a situation where the operation of these aggregate DNMs becomes sub-optimal, if not unfeasible. This will be brought about by the need for competition between DNMs and an erosion of trust between vendors, consumers and market organizers, leading to a splintering of the market into a larger number of independent, specialized 'storefronts' operating and competing in the dark web.

One advantage for participants trading in this market is that they will be afforded an increased degree of privacy in their activities. It will become much more difficult to observe activity and trace transactions, as most online communication will begin to take the form of encrypted one-to-one discussions. However, this benefit also comes at a cost: it will be harder for buyers to discover new products and find online storefronts. Consumer searches will therefore become more costly, and operating in the market more technically challenging.

Again, this shift in the market structure makes it increasingly difficult to enforce regulations, as connecting individuals to specific transactions and behaviours becomes more difficult. At the same time, the number of consumers willing to participate will diminish, given the higher costs associated with maintaining multiple accounts, pseudonyms, and varied digital wallets to interact with separate markets. Therefore, the benefits to the remaining active members of the community are offset by the decline in the number of willing participants.

Stage 3: Community by invitation

The next step taken by DNM participants in their efforts to evade encroachment of law enforcement would be the formation of sub-communities and marketplaces that restrict access to those who are explicitly invited to participate. The logic behind this shift is that law-enforcement agents are likely to fail the vetting process or would be unable to show themselves to be legitimate DNM participants (as an example, current hacker forums require demonstrations of skill by providing data dumps from breached services, or own-coded software to be distributed freely to community members).

This level of restriction to the markets will make it even more difficult to observe and catalogue consumer behaviour and the nature and scope of transactions, or to connect specific individuals to illicit transactions. Some of the current observable invitation-only markets in other domains even deploy their own dedicated cryptocurrencies, as opposed to trading in Bitcoin, which is more universally tracked, thus creating an additional barrier between these communities and outside parties.

The increasing degree of market privacy is accompanied by a further decline in potential participants.

As with the previous stage, the increasing degree of market privacy is accompanied by a further decline in potential participants. There will be a subset of consumers who are either unwilling or unable to go through the process of proving themselves worthy of an invitation. Again, the improvement in safeguards for the remaining participants comes at the expense of a declining overall market.

Stage 4: Distributed markets

The last stage is dependent on new technology currently being tested, which, if successful, might not necessarily become the final form of DNMs, but rather a dominant aspect that replaces the three previously described formats. Distributed marketplaces rely on blockchain technology and newly adapted smart contract approaches to create markets that no longer rely on single, central hosting and control by few individuals. Instead, these markets exist as distributed copies that are coordinated across all participants in the marketplace, so that the elimination of any individual (e.g. following arrest by the authorities) does not affect the continued operation of the market as a whole. This approach would also have a baked-in ability to encrypt all consumer-to-consumer and consumer-to-vendor communications by leveraging the same technology-enabling transactions.

A number of such marketplaces can be seen today. OpenBazaar[6] is one example of a legal deployment of such a marketplace concept. However, no current DNM version has been widely adopted – although one should bear in mind that legal distributed markets, like Open Bazaar, could just as easily be co-opted to sell illicit goods, as their decentralized and uncontrolled nature makes it difficult to censure their content.

If distributed marketplaces were to be adopted for illicit markets, such as IWT, they would attract a larger number of potential trading participants because of the lower costs associated with mastering the required technologies, as they are arguably relatively simple and automated. And although they are more visible to law-enforcement agencies, the encrypted communications will make enforcement of regulations complicated. The distributed nature of the market will also make its complete shutdown incredibly difficult, if not impossible.

Conclusion

When one looks at the current IWT environment and the likely future trajectory this illicit market will take under increased pressure from law enforcement, a few things become clear: each step in the criminals' attempts to safeguard their markets will lead to certain benefits for those who operate in them, but, as the markets get forced into the dark net, it will come at the cost of an overall diminishing market. As IWT enters the dark web, the market sheds consumers along the way as a result of dwindling interest and the need for greater technological aptitude to keep pace with the changing market. Additionally, regardless of the approach taken to safeguard their trade, illegal markets always rely on outside networks for support. They also exhibit classic consumer behaviours and processes (like the search concept). It is these that might provide more fertile ground for intervention strategies than structural changes (e.g. disallowing certain platforms), as the latter might have the effect of merely shifting where illicit transactions take place, as opposed to achieving a meaningful reduction in harmful behaviour.

Greater enforcement will drive consumers to the dark web, just as it has with other illicit goods and activities. This shift will lead to both greater organization around consumers and better outcomes for criminals, who might realize greater operational efficiencies, international coordination, demand and profits. It is to be expected that this coordination and profitability will result in a greater prioritization of wildlife trade in the portfolio of criminal organizations. However, by understanding, firstly, the interaction between surface- and dark-web communities, secondly, consumer behaviour and the nature of information searches, and, thirdly, the loss of market potential within each stage of market obfuscation, regulators and enforcement agencies should be able to mitigate these gains and create conditions where the IWT market becomes less functional.

Further reading

DW Challender, SR Harrop and DC MacMillan, Understanding markets to conserve trade-threatened species in CITES, *Biological Conservation*, 187, 2015, 249–259.

ALS Hansen et al, Digital surveillance: A novel approach to monitoring the illegal wildlife trade, PLOS ONE, 7, 12, 2012, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0051156.

S Heinrich et al, Where did all the pangolins go? International CITES trade in pangolin species, *Global Ecology and Conservation*, 8, 2016, 241–253.

NG Patel et al, Quantitative methods of identifying the key nodes in the illegal wildlife trade network, *Proceedings of the National Academy of Sciences*, 112, 26, 2015, 7948–7953.

GE Rosen and KF Smith, Summarizing the evidence on the international trade in illegal wildlife, *EcoHealth*, 7, 1, 2010, 24–32.

Mara E Zimmerman, The black market for wildlife: Combating transnational organized crime in the illegal wildlife trade, *Vanderbilt Journal of Transnational Law*, 36, 2003, 1657–1690.

Acknowledgements

The author would like to thank the Government of Norway for funding this report. Digital Dangers forms part of a partnership project between INTERPOL and the Global Initiative Against Transnational Organized Crime, in cooperation with the UN Office on Drugs and Crime.

About the author

Felipe Thomaz is Associate Professor of Marketing, Saïd Business School, University of Oxford.

Notes

1 Read more on Operation Bayonet at https://www.wired.com/story/hansa-dutch-police-sting-operation/.

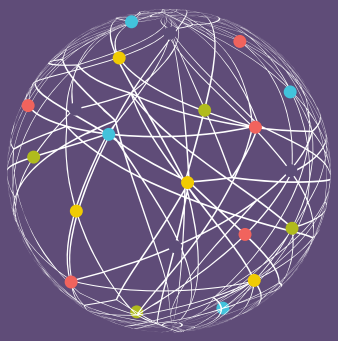
2 Study currently under peer review. For a copy, see https://www.sbs.ox.ac.uk/about-us/people/felipe-thomaz.

3 Convention on International Trade in Endangered Species of Wild Fauna and Flora; see https://www.cites.org/eng/disc/what.php.

4 Lions are legally farmed in South Africa. Therefore, claims of legality and sources of products online can be confusing and misleading for consumers. Assumptions of legality can also easily be made by potential buyers.

5 For example, one of the oldest digital drug markets (The Farmer's Market) moved from email-based marketing to the dark web; see https://en.wikipedia.org/wiki/The_Farmer's_Market.

6 OpenBazaar is a peer-to-peer and open-source application where users set up stores and transact over unrestricted goods using cryptocurrency (e.g. Bitcoin, Etherium). For more information, see https://openbazaar.org/.



THE GLOBAL INITIATIVE
AGAINST TRANSNATIONAL
ORGANIZED CRIME

www.globalinitiative.net

A NETWORK TO COUNTER NETWORKS