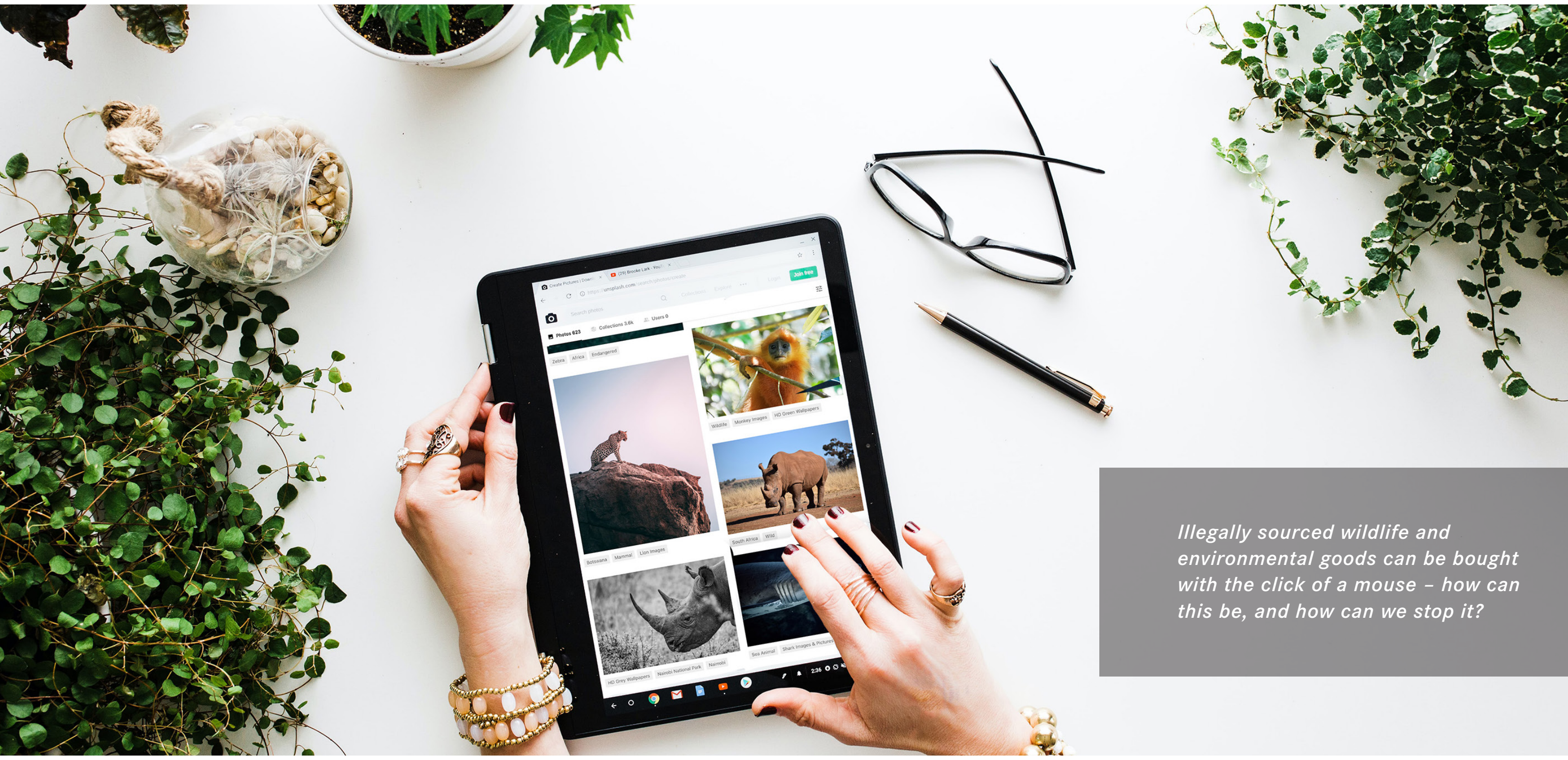

Illegally sourced wildlife and environmental goods can be bought with the click of a mouse – how can this be, and how can we stop it?

Photo by Brooke Lark on Unsplash

Online marketplaces and sale of environmental products

Why is it still easy to buy illegal wildlife online?

Among the many activities that have shifted more online due to the pandemic is illegal wildlife trade.

This is hardly surprising. Illicit trade tends to go along with trends in legitimate trade, and various studies already point to growth in online retail sales of all types of consumer goods.

It is concerning, though. This is not only because the internet makes it easy to buy and sell endangered products across borders and to evade domestic legislation. It is also because of the internet's role in socialisation and norm formation. Seeing endangered species being auctioned openly on Facebook while you catch up with friends or browse news makes this crime seem normal and acceptable.

This is not new, just a worrying acceleration. The online sale of wildlife products and other environmental goods, live and dead, was already rampant across social media, classified ads sites, B2B wholesaler websites and catalogue sites. Why isn't being detected and taken down, and the criminals caught?

How policy priorities and regulations (would) support enforcement efforts

One barrier to effective action against the online sale of environmental goods is under-resourcing of law enforcement. With stretched funds, it is hard for police to raise illegal wildlife trade up their priority lists. This is particularly acute in many developing countries that are the sources of these illegal goods.

The problem of low prioritisation is changing in some areas, for example in the decision to include environmental crime as one of the 10 EMPACT priorities, Europol's priority crime areas, under the 2018-2021 EU policy cycle.

A second challenge is weak regulation of the cyber sphere. There is some excellent work underway through voluntary initiatives and partnerships with tech companies such as the Coalition to End Wildlife Trafficking Online. But the limitations of voluntary action by NGOs and the private sector are highlighted by the persistent and continued sale of endangered wildlife online.

For example, many platforms including Facebook have imposed clear bans on all trade in live animals and seem to be getting better at deleting content that is reported by NGOs and citizen activists. But it is hard to analyse these results without transparent data on the posts deleted and their content, which is not available.

Plus, one can still easily find people auctioning live wild animals and whole pieces of ivory or rhino horn openly to their followers. In some cases, social media adverts feature illegal wildlife, i.e. the social media firms are not only facilitating but also directly profiting off IWT.

Tech companies would need to invest significantly in tools to more effectively stop both the trade and related socialisation, as well as to systematically store and provide usable information on illegal wildlife sales to law enforcement. The fragmentation of the social media and online sales platforms by language adds to the complication.

Without clear regulation that applies to all relevant online platforms internationally, it is hard to imagine any single company making that type of investment. (Though we would like to be proven wrong!)

Drilling down from the tip of the iceberg

In truth, we are only just scratching the surface of the illegal sale in environmental goods, even of products that are bought and sold openly on the public web.

Data on the scale and scope on online sales of illegal wildlife trade are still dangerously patchy. By combining techniques for machine learning and social media analysis, GITOC research reveals that the largest markets for some products may be totally off the radars even of conservation and law enforcement specialists. Adverts appear on a multitude of platforms, often attached to personal phone numbers and in clear violation of the platform’s policies.

Europol’s work on wildlife and other environmental crimes supports this finding – that a lot of illegal activity hides in plain sight on the open web. In European priority areas (reptiles, glass eels and birds) a major issue is the intermingling of legal and illegal supply chains, which make it easy to “launder” illegal species into legal markets and trade them openly online.

Though the international law enforcement response is at an early stage, secure communication channels and partnerships like the EU Wildlife Cybercrime Project and EnviCrimeNet are starting to bear fruit. There are also valuable efforts to build capacity for cyber investigations among law enforcement and to include cyber and financial investigation specialists in environmental crime teams, an approach strongly advocated by the Basel Institute.

Shining a light into the dark web

The data gets even patchier as you enter the dark web. A 2018 GITOC report on Illicit Wildlife Markets and the Dark Web predicted that online sales of wildlife products would rise on the dark web, where the perpetrators are more professional and probably linked to other criminal activities like illegal drugs and arms sales.

Although the dark web helps to protect the buyer and seller’s anonymity to some extent, the tide is turning. Law enforcement operations to seize and close down dark web markets now often involve the authorities continuing to run the site for a short period. This is providing valuable intelligence on sellers, buyers and operational methods – intelligence which will increase as it is shared and compared across jurisdictions and sectors.

Following the (virtual) money

Cryptocurrencies are mostly used for illegal transactions on the dark web, again in an attempt to conceal the identities of the buyer and seller.

Unfortunately for criminals, cryptocurrencies are not as anonymous as many people think. In many cases, blockchain analysis makes it possible to trace transactions, deanonymise them and even geolocate them. The international response to emerging financial crime threats relating to cryptocurrencies is also strengthening fast, as indicated by the latest annual Global Conference on Criminal Finances and Cryptocurrencies co-organised by Europol, INTERPOL and the Basel Institute on Governance.

Regulations are helping to shine light here. If criminals want to cash out their illegal funds, they have to do this through cryptocurrency exchanges, which now fall under the scope of the Financial Action Task Force standards on anti-money laundering and are therefore obliged to monitor transactions and conduct customer due diligence.

The implication? We could do a lot to improve detection of illegal wildlife trade online by combining two sets of red flags that are currently kept separately.

- Red flags that trigger regular suspicious transaction reports (STRs) by financial institutions including cryptocurrency exchanges.

- Red flags on environmental or wildlife crimes such as the customer's background, location, profession and activity patterns, many of which are identified by initiatives such as the United for Wildlife Taskforces.

If good communication channels exist between financial institutions and law enforcement, this could help detect suspicious transactions and money laundering activities by environmental criminals that result in investigations on the ground.

Importantly, even small pieces of information about a single seizure, transaction or customer have triggered large cases in the past. Europol and INTERPOL play a key role in ensuring this information is channelled to the relevant authorities in compliance with legal frameworks and in a form that can be actioned. Financial institutions and other companies wishing to share information can reach out to the EU Wildlife Cybercrime Project or the National Units of Europol or INTERPOL.

Building specialist skills and special relationships

Building capacity for cryptocurrency analysis among law enforcement is a clear urgency. Another low-hanging fruit is capacity for forensic analysis of digital devices seized in wildlife crime investigations, which often contain a wealth of data on transactions, operations and platforms. A third is building and maintaining the channels and relationships that are necessary for effective information exchange.

Although these all hit against the barriers of unequal resources and competing priorities in different countries, specialists in cybercrime, cryptocurrencies and (virtual) financial investigation have a clear place in the fight against illegal online sales of environmental goods. Their role will only grow as both legal and illegal trade continue to intermingle and shift online.

Event details

The fifth event in the Corrupting the Environment webinar series explored the latest trends in the online sale of environmental goods, including live animals and wildlife products.

Moderated by **Juhani Grossmann,** Team Leader - Green Corruption programme, Basel Institute on Governance, the event featured the following expert panel: **José Antonio Alfaro Moreno,** Team Leader, European Serious and Organised Crime Centre (ESOCC), Europol; **Simone Haysom,** Senior Analyst, Global Initiative Against Transnational Organized Crime; and **Federico Paesano,** Senior Financial Investigation Specialist, Basel Institute on Governance.

The OECD’s participation in the Corrupting the Environment webinar series was supported by the European Union through the Instrument contributing to Stability and Peace (IcSP).

The Basel Institute’s Green Corruption programme is supported by:

LIECHTENSTEIN

UKaid from the British people

PMI impact

Targeting Natural Resource Corruption

USAID FROM THE AMERICAN PEOPLE

WWF

CMI U4 ANTI-CORRUPTION RESOURCE CENTRE

TraCCC

TRAFFIC the wildlife trade monitoring network