TRAFFIC
REPORT

JULY 2019

COMBATING WILDLIFE CRIME LINKED TO THE INTERNET
GLOBAL TRENDS AND CHINA'S EXPERIENCES

TRAFFIC

COMBATING WILDLIFE CRIME LINKED TO THE INTERNET

Global Trends and China's Experiences

ABBREVIATIONS AND ACRONYMS

CCPCJ	Commission on Crime Prevention and Criminal Justice
CITES	Convention on International Trade in Endangered Species of Wild Fauna and Flora
CNY	China Yuan
EU	European Union
ICCWC	The International Consortium on Combating Wildlife Crime
IGCI	INTERPOL Global Complex for Innovation
INTERPOL	The International Criminal Police Organization
IRI	The Internet Research Institute
NFGA	National Forestry and Grassland Administration
NWCU	National Wildlife Crime Unit
ROCB	Regional Office for Asia-Pacific Capacity Building
SDG	Sustainable Development Goals
UNODC	United Nations Office on Drugs and Crime
UNEP-WCMC	The UN Environment World Conservation Monitoring Centre
USD	United States Dollar
USFWS	The United States Fish and Wildlife Service
WCO	World Customs Organization
WCU	Wildlife Crimes Unit

ACKNOWLEDGEMENTS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The annual total value of the global trade in illegal wildlife and wildlife products, excluding timber and fisheries, is estimated at about USD 19 billion (IATA, 2019). It is one of the biggest global criminal activities after drugs, counterfeit money and human trafficking, and is regarded as a high-income, low-risk organized crime. This has led to a growth in criminal networks engaging in wildlife crime and led to a number of rare species becoming at risk of extinction (Haken, 2011).

With the rapid development of internet technologies and e-commerce, online shopping has become increasingly popular. Yet, alongside the everyday benefits brought by evolving technology, the internet has also provided new channels for criminals to trade in illegal products, including species of wild and endangered fauna and flora. Illegal wildlife trade has become a common occurrence online, including on social media through popular platforms. As a result, combating the illegal trade in wildlife and wildlife products on the internet has become an urgent issue.

China's internet and courier industry is developing rapidly. According to the China E-Commerce Report 2017, China's e-commerce transaction value reached CNY 29.16 trillion (~USD 4.33 trillion) in 2017, and the number of online shopping users reached 533 million (China E-Commerce Report, 2017). The 2017 Express Market Regulation Report reported that in 2017 the business volume of China's courier enterprises reached 40.07 billion packages, accounting for 40% of the world's total, and ranking first in the world for four consecutive years. The Chinese government has started to combat the illegal wildlife trade through both online and logistics channels with notable success and is looking to share these experiences from public-private sector collaborations more widely.

TRAFFIC has tracked wildlife trade on the internet for many years. Since 2012, TRAFFIC's regular monitoring has consistently uncovered a large number of illegal wildlife products available on Chinese internet platforms. Based on this research, TRAFFIC is actively supporting the Chinese government and Chinese enterprises to address incidences of online availability of such products and delivering training to combat the illegal wildlife trade online.

This report discusses the policies and measures to address wildlife crime in the EU, Kenya, the US, and several key international associations; highlights the characteristics of China's wildlife cybercrime and experiences in combating such crime; and provides suggestions of strategies going forward. The main findings of the report are:

• The Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) made the link between illegal wildlife trade and the internet, placing it on the agenda for the first time in 2010 and formulating relevant CITES Decisions 17.92-17.96 in 2016. However, the problem of illegal wildlife trade, as linked to the internet, has received insufficient attention internationally. Wildlife cybercrime is not yet regarded as a crime category in its own right in international or national legislaton, and related policies and law enforcement actions are not sufficiently comprehensive or targeted.

• The EU and the US have introduced relevant policies and measures for combating illegal wildlife trade linked to the internet. Although Kenya actively promoted the issue of combating illegal wildlife trade online at the 17th Conference of the Parties to CITES in 2016, it has yet to take substantive measures domestically. Other countries have yet to report specific efforts to address illegal wildlife trade linked to the internet.

• Some leading internet companies have introduced relevant policies and taken active measures to combat illegal wildlife trade. Internet companies can play a greater role by further policing their own platforms, educating users, and adapted new technologies to combat illegal wildlife trade linked to the internet.

• Given the magnitude of its online commerce, China will need to remain at the forefront of the fight against wildlife cybercrime. The internet and logistics/courier industries are important areas for combating illegal wildlife trade online and the transport of specimens from seller to buyer. Collectively China's internet and logistics/courier companies have taken important measures to combat illegal wildlife trade linked to the internet and will need continued focus in the future.

1. BACKGROUND

With the fast growth of the internet, more and more people now communicate and trade goods through online platforms and applications. However, the convenience and relative anonymity afforded by trade via the internet has led to its use by criminals as a more covert channel for criminal activity. According to The International Criminal Police Organization (INTERPOL)'s definition of "cybercrime", wildlife cybercrimes should be considered "cyber-enabled crimes", which refers to a cluster of traditional crimes that have taken "a new turn" with the advent of the internet, including financial crime and terrorism. Wildlife crimes related to the internet mainly relate to the use of the internet as a channel illegally to buy and sell endangered wild animals and plants and their products. Since January 2012, TRAFFIC has closely monitored illegal wildlife trade trends and found clear shifts taking place from physical to online markets (Xiao & Wang, 2015; Xiao et al., 2017).

The Chinese government has a record of cracking down on illegal wildlife trade, including wildlife cybercrime. At the legislative level, the recently amended "Wild Animal Protection Law", which came into force on 1st January 2017, highlighted wildlife cybercrime with articles specifically forbidding online trading platforms to provide services for the illegal sale, purchase and utilisation of wildlife and relevant products, establishing a legal basis for combating illegal wildlife trade on the internet. This is the first time Chinese legislation specifically highlighted wildlife cybercrime.

At the law enforcement level, the General Office of the State Council published a special notification on 29th November 2016 to "Orderly terminate commercial processing and sales activities of ivory and products", which provides specific guideline for enforcement actions (General Office of the State Council, 2016). The Notification further confirms the "banning of illegal trading of ivory tusks and products on the internet as well as other trading channels", and requires law enforcement authorities at all levels to enhance market regulation, increase publicity and education, with "specific emphasis on detecting and destroying illegal processing workshops, blocking illegal trading channels in markets and on the internet". Since 31st December 2017, the Chinese government has ceased all elephant ivory processing and sales (hereafter referred to as the "ivory trade ban" (General Office of the State Council,2016).

On 22nd November 2017, three prominent Chinese internet companies – Baidu, Alibaba, and Tencent – joined another eight internet companies to launch the "Alliance on Combating Illegal Wildlife Trade Online". The Alliance commits its members to adopt policies of "zero tolerance" regarding illegal online trade of wildlife and wildlife products on their internet platforms. This includes: strictly inspecting information on illicit wildlife and wildlife products; timely removal of information pertaining to illegal wildlife products; and the monitoring of (and taking precautionary actions against) suspicious users on their platforms (TRAFFIC, 2017). On 8th March 2018, the Alliance was joined further by 10 tech giants including Google, Facebook and eBay, to form the "The Coalition to End Wildlife Trafficking Online" (hereafter referred to as "the Coalition"). At the first anniversary of the Coalition on 6th March 2019, eight new internet companies joined the Coalition, bringing the total to 32 members (TRAFFIC, 2019). The Coalition has set a bold goal of reducing wildlife trafficking online by 80% by 2020.

Thus far, China has achieved some success in its actions to combat the illegal wildlife trade online. Due to strengthened law enforcement efforts in physical markets in recent years, some traders that once relied on the physical market have increasingly shifted their "marketplace" to online trading platforms and social networks. In response, the Chinese government, as well as Chinese internet companies, are actively adapting new technologies for use to address wildlife cybercrimes, such as data aggregating tools and monitoring systems. However, with the internet trade being fast and convenient, often providing anonymity at low transaction costs, effective control of illegal online trade in wildlife and wildlife products remains a challenge. China's booming e-commerce sector, and the expansive courier logistics networks that cover the entire country that supports it, from major cities to rural villages, further exacerbates the ability to identify and intercept movements of illegal trade in wildlife and wildlife products.

Due to the transnational nature of illegal wildlife trade, efforts to combat it on the internet should not be limited to China and its cyberspace. As early as 2013, monitoring of online advertising of illegal ivory products targeted at European Union (EU) countries revealed illegal ivory advertisements and online auctions of ivory worth more than a EUR 1 million (~USD 1.12 million) in 10 EU countries (INTERPOL and IFAW, 2013). In recent years, more cases of illegal wildlife trade online have been reported around the world. These new features raise new challenges in enhancing law enforcement. Preliminary research published by INTERPOL in June 2017 also revealed that illicit wildlife trade is "infiltrating" into the Darknet (INTERPOL, 2017).

In this context, TRAFFIC analysed the status and trends of illegal wildlife trade linked to the internet and collated actions taken in China, other countries and international organisations in combating wildlife cybercrime from October 2017 to March 2019. Relevant policies and measures were reviewed, with the aim of forming a comprehensive understanding of the characteristics of wildlife cybercrime and the current situation, as well as concluding with recommendations on law enforcement for China and the world.

2. STATUS REVIEW OF THE INTERNATIONAL CRACKDOWN ON WILDLIFE CYBERCRIME

Relevant international organisations and some countries have begun to place an emphasis on wildlife crime linked to the internet and introduced policies and related measures. The current focus and measures to date include:

2.1 Inter-governmental Organizations

In November 2010, the CITES Secretariat, INTERPOL, the United Nations Office on Drugs and Crime (UNODC), the World Bank and the World Customs Organization (WCO), launched the International Consortium on Combating Wildlife Crime (ICCWC), which aims to integrate the efforts of all parties to promote international cooperation on law enforcement against wildlife and forest crimes. ICCWC members have also published a series of reports and toolkits such as the "ICCWC Indicator Framework for Combating Wildlife and Forest Crime" (ICCWC, 2016), "Wildlife and Forest Crime Analytic Toolkit" (UNODC, 2012), "World Wildlife Crime Report" (UNODC, 2016a), and "Financial Flows from Wildlife Crime " (UNODC, 2016b), among others, with the aim of providing technical support to front-line law enforcement officials in combating wildlife crime.

2.1.1 CITES Secretariat

As early as CoP15 (2010) in Doha, CITES Parties agreed to "establish, at the national level, a unit dedicated to investigating wildlife crime linked to the internet or incorporate wildlife trade issues into existing units that investigate or monitor computer or cyber-crime". During CITES CoP17 (2016) in South Africa, new decisions on wildlife cybercrime were agreed by parties, namely "Enforcement matters and illegal international trade in wildlife".

Multiple documents issued during CoP17 suggest that CITES is tackling the issue of wildlife cybercrime through the establishment of a working group composed of major internet companies, non-governmental organisations, lawyers and other relevant experts from both countries of origin and consumption. CITES recommends that all Parties provide the Secretariat with changes and updates on domestic legislation and initiatives on cybercrime, as well as any best practices on how to manage the online market and social network platforms effectively (including law enforcement agreements). The Secretariat places special emphasis on private sector engagement and recommends that the Parties seek input from the providers and owners of online markets and social media platforms.

2.1.2 INTERPOL

INTERPOL has long played an important role in combating transnational organised crime, particularly in coordinating information sharing among 192 Member States and establishing joint law enforcement mechanisms. In 2014, INTERPOL established the INTERPOL Global Complex for Innovation (IGCI) in Singapore, which is dedicated to bringing together law enforcement experts on cybercrime and key partners from the private sector for detecting and preventing digital crime.

In June 2017, the IGCI released its first report on illegal wildlife crime on the Darknet. According to the report, from December 2016 to April 2017, researchers identified 21 advertisements for rhino horn, ivory and tiger products on the Darknet. This was far less than the researchers expected given the size of the Darknet. The results closely mirror another study by the University of Kent in the United Kingdom (UK). The research team contends that unlike the trade in drugs, weapons, and pornography, there is currently less of a perceived need to keep illegal wildlife trade hidden within the Darknet (Harrison et al., 2016). Still, the penetration of illegal wildlife trade from the open internet

to the Darknet serves as a wake-up call for law enforcement authorities. It remains uncertain whether wildlife cybercrime will transfer further to the Darknet. If such activities shift to the Darknet, the difficulty of combating of wildlife crime, from an intelligence and law enforcement perspective, would likely increase.

INTERPOL also provides workshops and training sessions to law enforcement authorities in many countries, alongside its intelligence gathering and research roles. The contents of these workshops for law enforcement cover how to collect and analyse data from digital devices; identify and safely operate digital devices for investigations; facilitate the understanding of law enforcement authorities on illegal wildlife trafficking; trading on internet platforms and the Darknet; and how to improve law enforcement capacity (INTERPOL, 2017). The organisation also develops training courses to empower law enforcement officers with the necessary skills to combat the increasing trade in wildlife on internet platforms (USAID, 2018).

2.1.3 WCO

Customs officials around the world are at the forefront of the fight against the illegal transnational trade in wildlife. The WCO is the only inter-governmental organisation of Customs administrations from 182 countries. The WCO's Law Enforcement Commission conducts research on law enforcement, intelligence exchanges, and governance of wildlife trade based on international conventions. The WCO's Customs Enforcement Network (CEN) is responsible for information gathering and collection of endangered species seizures statistics reported by Customs officials in various countries. No public statement specifically on wildlife cybercrime has been issued by the WCO, as of November 2018. However, the WCO has begun to include content on combating wildlife crime linked to the internet in its capacity building curriculum. For example, in a meeting on Combatting Environmental Crimes organised by the WCO Regional Office for Asia-Pacific Capacity Building (ROCB A/P) on 20-23rd November 2018, TRAFFIC and Alibaba (the world's largest e-commerce company) were invited to give presentations on China's work on combating wildlife crime linked to the internet.

2.1.4 UNODC

The UNODC aims to help member countries combat illegal drugs, crime, and terrorism. Cybercrime and "Wildlife and Forest Crime" are both categorised as "Emerging Crimes" under the crime structure of the UNODC (UNODC, 2016). In 2015, the UNODC launched "The Cybercrime Repository" under the framework of the "Commission on Crime Prevention and Criminal Justice" (CCPCJ), which aims to assist the Member States to prevent and combat cybercrime effectively. Inquiries can be conducted into the database attached to their repository of registered cases of cybercrime and "wildlife, forest and fisheries crime" (UNODC, 2015).

Currently no specific research projects have been carried out to target cross-cutting issues between cybercrime and wildlife crime, however the UNODC has initiated some cross-disciplinary research. For example, the "Linking Organized Crime and Cybercrime" conference held in Chuncheon, South Korea, on 7-8th June 2018, listed wildlife crime as a "new or emerging type of organized crime in cyberspace" for the first time (UNODC, 2018).

2.1.5 The World Bank

The World Bank runs two separate projects, the Global Wildlife Program and the Cyber Security Program. As of writing, the two projects are still working independently. At present, there is no specific research or policy guidance targeting the emerging issue of wildlife crimes in cyberspace. While "crime" is analysed in the World Bank's flagship "World Development Report", it only lists war crimes, violent crimes, and urban crimes; no focus is given to cybercrimes or wildlife crimes.

2.2 National Governments

2.2.1 The European Union (EU)

The EU Action Plan against Wildlife Trafficking contributing the Sustainable Development Goals (SDG) of UN 2030 Agenda came into effect in 2016, with wildlife cybercrime and the importance of the private sector emphasised. This proposes that tackling wildlife cybercrime is one of the most important elements to fight against organised crime more effectively, and awareness raising is need for relevant enforcement agencies and private sectors bodie, who potentially may facilitate illegal wildlife trade. The Action Plan covers five years (2016-2020) with detailed framework and lists of policies/tools as enforcement authorities of EU Member States were required to report the progress to the EU Wildlife Trade Enforcement Group twice a year (European Commission, 2016).

According to its framework, intelligence sharing and cross-boundary cooperation are among several objectives, alongside the development of an up-to-date database and efficient dialogs. The resources for cybercrime is supposed to be used in wildlife crime in the cases linked to the internet in 2020 so that the effectiveness of tackling organized wildlife crime could be improved. However, although "increase business sector engagement" is highlighted as a specific objective (objective 1.3), the actions designed are at the awareness raising stage. Full utilisation and monitoring of online channels and online markets are not included as one of the expected results during 2020, while improvements to the current rates of detection of illegal activities and implementation of current EU rules on wildlife trade are regarded as essential.[28] Fortunately, the increased need to address wildlife cybercrime has been recognised as EU Member States implement the EU Action Plan (European Commission, 2018).

The UK government is among those which took early measures to tackle wildlife cybercrime, a move which was highlighted by the CITES Secretariat. For example, the UK government has proposed legislative changes that would make it an offence not to include the CITES permit number in the body of an advertisement for wildlife products (though to date this proposal has not been implemented) (CoP17 Doc. 29-CITES, 2016). At the institutional level, the UK government established the National Wildlife Crime Unit (NWCU), which focuses on intelligence gathering, information sharing, and assisting investigations on wildlife crime. The group is made up of 12 staff and they monitor some wildlife-related cybercrime activities where resources allow. The Metropolitan Police Service has a Wildlife Crime Unit (WCU) which also monitors wildlife-related cybercrime activities when resources allow. However, a report from the organisation World Animal Protection claims that criminals are still using eBay as "a viable trading marketplace" despite the fact that ivory products are banned from being listed on eBay (Worth, 2018), and the WCU and NWCU's resources are "far outweighed" by criminals (World Animal Protection, n.d.).

2.2.2 The United States of America (US)

In 2016, the US Agency for International Development funded the "Wildlife Crime Tech Challenge". The challenge was won by a team of environmental and data scientists from New York University for their Enforcement Gaps Interface tool. This tool can search hidden wildlife advertisements based on text, price and location using data mining and image recognition functions. With 80% accuracy, the technology could help law enforcement authorities better identify and reduce illegal wildlife trade by providing vital information from websites with wildlife advertisements to law enforcement efficiently. The researchers are also working on developing derivative Chinese language as well as to meet specific demands in California (Zhang, 2017).

The United States Fish and Wildlife Service (USFWS) is one of the major agencies in charge of combating wildlife crimes in the US It has conducted two enforcement operations, namely Operation Cyberwild in 2011 and Operation Wild Web in 2012, with satisfactory results. In recent years, neither special action nor law enforcement policies have been issued to tackle wildlife cybercrime. As of 2018, USFWS has yet to establish a special unit to target wildlife cybercrime.

2.2.3 Kenya

Kenya is one of the world's major sources of trafficked wildlife products. At CITES CoP17, Kenya actively lobbied to put illegal wildlife trade via the internet on the agenda. In May 2016, the Kenyan government stated that it is accelerating the implementation of international legislation in the hope of strengthening international cooperation in combating cybercrime (Xinhua News, 2016). A media report also quoted the Permanent Secretary-General of the Ministry of Environment and Natural Resources of Kenya, who said that the country had recognised loopholes in laws tackling cybercrime and new legislation targeting wildlife cybercrime is in preparation to enhance illegal wildlife trade law enforcement (Xinhua News, 2016). In June 2017, the country launched "The Computer and Cybercrime Bill"; however, wildlife cybercrime was not specifically listed as a crime in the bill (Article19.org, 2018).

2.3 Internet Platforms

With the development of internet technologies, people are increasingly inclined to shop online, but have equally spurred criminals to misuse internet platforms for the sale of illicit commodities – including illegal wildlife and their products – through posts, advertising and other channels online. In response, many internationally renowned e-commerce companies, social media, and other internet companies have introduced policies and measures to combat illegal wildlife trade, and actively participate in publicity activities for wildlife protection. For example, it is forbidden to sell illegal wildlife products such as ivory on some companies' platforms. Companies also identify, filter advertisements involving illegal wildlife trade, and deal with the illegal information accordingly. Global tech companies including Tencent, Alibaba, Google, eBay along with 28 other companies have also established the Coalition.

However, critics have pointed out that the crackdown on illegal wildlife trade by e-commerce, social media, and other internet companies is insufficient and illegal wildlife trade is still active. For example, researchers at the University of Kent in the UK contend that the lack of illegal wildlife products available on the Darknet is precise because internet companies have provided a legal and free platform for illegal transactions of wildlife products (Marley, 2017).

3. CHARACTERISTICS OF WILDLIFE CRIME LINKED TO THE INTERNET IN CHINA AND CHINA'S EXPERIENCES

China has been at the forefront in the fight against illegal wildlife trade linked to the internet. At the 17th Conference of the Parties to CITES in 2016(CoP17), the China CITES Management Authority along with international organisations and internet companies, co-organised a side event with the theme of "Combating Wildlife Cybercrimes". At the event, China shared the strategies and experiences of Chinese internet companies in combating illegal wildlife trade. The characteristics of China's wildlife cybercrime and the Chinese government's experience in combating such crimes, including through public-private partnerships with internet companies, provide an important reference point for current and future national and global responses, including multilateral action.

3.1 Characteristics of wildlife cybercrime in China

3.1.1 Thriving online trade and platforms foster wildlife cybercrimes

E-commerce in China continues to grow at a rapid pace. According to the latest data released by the Ministry of Commerce, online retail sales in China have changed from a quantity-driven growth to quality-driven growth in 2017, with retail sales exceeding CNY7.18 trillion (~USD1.04 trillion). The year-on-year growth reached 32.2%, more than 6 percentage points higher than the growth rate from the previous year (Ministry of Commerce People's Republic of China, 2018).

According to the latest data released by the State Post Office, in 2017, the country's courier companies together delivered a total of 40.06 billion parcels, an increase of 28% year-on-year; with business revenue accumulated to CNY495.71 billion (~USD72 billion), a year-on-year increase of 24.7%. China ranks number one globally with regard to a total volume of parcels mailed-29 parcels were mailed and/or received per person in 2017, an increase of nearly 6 parcels over the previous year.

The booming e-commerce business together with express logistics networks linking major cities with rural villages in China, provide ideal infrastructure for facilitating illegal wildlife cybercrime. According to a study from the Internet Research Institute (IRI), an increasing amount of illegal wildlife products are being sold through online channels. Based on publicly reported cases of illegal wildlife trade from January to May in 2015, 30.6% involved online links, and from January to May in 2016, the proportion increased to 46.3% (IRI, 2017).

3.1.2 Online sales and delivery have become a major pattern of wildlife cybercrime

Law enforcement to counter wildlife crime, particularly on the ground (offline), has been greatly strengthened in China. However, control and regulation of the illegal online trade remains fraught with challenges. The characteristics of online trading such as its speed, convenience, anonymity, and low cost, have made online sales and deliveries a major component of wildlife cybercrime.

As the online trade in illegal wildlife products grows, the offline trade has declined significantly. Meanwhile, law enforcement countering wildlife crimes in physical markets in China has continued to strengthen, which has constrained the operations of illegally operated stores selling wildlife and their products. Taking ivory as an example, TRAFFIC found a decline of 52% between 2014 and 2016 in the number of stores with ivory for sale in Beijing, while volumes of ivory traded dropped by 76% during the same period, indicating a significant reduction of trade over time at some physical markets (Zhao et al., 2017).

This reduction of sales seen in physical stores does not necessarily equate to a decline in wildlife crimes. To understand the illegal online trade of endangered species and their products on the internet, TRAFFIC monitors illegal advertisements for endangered species and products on 31 websites and e-commerce platforms. These are documented and published in monthly monitoring reports. Findings indicate that between 2012 and 2016, the most advertised wildlife products were ivory products, which account for more than 60% of the total. Rhino horns and associated products were the second most traded products and accounted for 20% of the total. At its peak in 2012, nearly 4,000 illegal advertisements for wildlife products were identified in a single month. Although the situation had improved by 2016, advertisements for illegal wildlife products can still be found each month (Xiao et al., 2017).

Social media has also become increasingly important in fostering illegal wildlife trade. Advertisements and posts on social media platforms not only serve to signal the availability of wildlife and wildlife products to potential buyers, they also enable sellers to connect to a wider field of interested buyers. Advertisements for illegal wildlife can be shared to potential buyers through private chats on social media and hence increase the rate of exposure. Similar patterns have been observed with physical market sellers who actively court buyers as "friends" on social media platforms, through which large numbers of posts for illegal wildlife products can be advertised. They are often sent to a select group who are carefully screened and selected by the sellers. These recipients not only show a strong interest in wildlife products but also have high purchasing power. By targeting those who are less likely to report illegal activities, sellers bear a much lower risk of being investigated.

3.1.3 Rising difficulties in online regulation due to criminals' "hide-and-seek games"

Compared with traditional wildlife crime, wildlife cybercrime is characterised by high levels of concealment, and consequently an increased difficulty in obtaining evidence of the crime.

However, criminals now rarely use descriptive words that might be associated with illegal wildlife products when advertising and negotiating trading details. Instead, the common practice is to use substitute names to describe wildlife products. For example, ivory is often called "XY", "jelly", "blood material" amongst other names, while rhino horn is called "XJ" and "Xi Jiao" amongst other names (the list of substitute names continue to grow). By doing so, criminals avoid being identified as such and having their posts deleted after detection. Furthermore, the substitute names allow criminals to avoid regulation and law enforcement by providing plausible deniability, giving them space to argue and defend themselves if detected. The continuous updating of substitute names raises further challenges for regulating websites and social media platforms.

Furthermore, the trend of using pictures instead of texts has further made detection difficult, requiring manual filtering. This greatly increases the amount of time needed to monitor online markets and platforms and lengthens the period of time that illegal posts and advertisements remain online, to the advantage of criminals. Also, a large number of advertisements for wildlife products are intentionally published during the period from 9 pm to 6 am the next day when there is weaker manual detection and posts are voluntarily deleted by criminals after a few hours. By doing so, criminals engage in a game of "hide and seek" with regulators.

3.1.4 Loose regulation of courier companies and the facilitation of illicit carriages

Two major patterns have emerged in wildlife seizure cases involving courier companies. First, the complicity of courier company staff in co-operating with criminals and enabling the delivery of illegal wildlife products, effectively waiving thorough cargo screening processes and other checks; and second, screening procedures that are not effectively implemented at the sending and receiving end by courier companies.

Once a product is shipped, tracing the transaction is equally difficult. To avoid enforcement actions, traders and buyers often provide fictional or substitute names when filing details of the sender, receiver and address, often only leaving a phone number exclusively for communication with delivery services. Some experienced criminal suspects even hire a third-party to pick up packages from courier companies. Consequently, law enforcement authorities must spend a considerable amount of time, as well as human, material, and financial resources to counter the use of courier companies to transport illegal wildlife products. This can include verifying and cross-examining chat logs, receipts, and other relevant information, which can create bottlenecks in regulatory and enforcement actions to combat wildlife crime.

3.2 China's experiences in combating illegal wildlife trade online

3.2.1 Strict supervision, strengthened law enforcement and inter-departmental collaboration

The Chinese government regards the protection of wildlife and the fight against illegal wildlife trade as an important part of reinforcing an ecological civilisation. In response to the threat of cybercrime, China has promulgated a series of laws and regulations to supervise the e-commerce business. Regarding wild animals, the Wild Animal Protection Law came into force on 1st January 2017 and highlighted wildlife cybercrime, forbidding online trading platforms from providing services for the illegal sale, purchase and utilisation of wildlife and relevant products. This law lays the legal groundwork for combating illegal wildlife trade on the internet.

Multiple laws and regulations seek to regulate the courier and logistics industry, including the "Postal Law", "Anti-Terrorism Law", and "Regulations on the Prohibition of Dispatch of Articles", which clearly stipulate the use of a "real-name registration system" and requires inspections from both the receipt and delivery end. Delivery companies are obliged to implement the inspection regulation strictly, to check on site whether the items to be delivered are on the list of prohibited articles, and to verify whether the name, nature, and quantity, amongst other elements, match the details on the mailing sheets, in order systematically to prevent prohibited articles from entering the delivery channels.

Under the leadership of the National Forestry and Grassland Administration (NFGA) and the Ministry of Public Security, the National Forest Bureau conducts enforcement actions against illegal activities that destroy forests and wildlife resources. The National Forest Police Bureau has handled many high value illegal wildlife trade cases across multiple provinces and districts and involving a large number of suspects and organised criminal gangs. In their report on such actions in 2015, they noted the emergence of internet transactions in cross-regional wildlife trafficking. As a result, there has been an increased emphasis on the use of the internet in wildlife crime. For example, in 2018 the National Forest Police Bureau launched a crackdown against wildlife crime called "Spring Thunder 2018". Measures against the illegal trade in wildlife products on internet platforms were one of the key targets.

In order to improve the long-term mechanism for co-ordinating law enforcement between departments in November 2016, the State Council of China approved the establishment of the Inter-Ministerial Joint Conference Mechanism on Combating Illegal Wildlife Trade. The mechanism consists of 22 departments, including the Central Communication Department, the Ministry of Foreign Affairs, the National Development and Reform Commission, the Ministry of Industry and Information Technology, and the Ministry of Public Security, amongst others, and was led by the NFGA.

3.2.2 Internet companies increase supervision and actively promote wildlife protection

Chinese internet companies have taken an active approach in combating illegal wildlife trade since 2012, from adopting a zero-tolerance approach in addressing illicit wildlife trade on their own platforms, to forming an alliance of companies to co-ordinate efforts in 2017. These companies work co-operatively to delete information on illegal wildlife products in a timely manner; explore and apply new technology such as machine learning to filter and delete illegal wildlife information; educate users on wildlife conservation, amongst other measures.

Chinese internet companies are also actively collecting a wide range of data to assist law enforcement authorities in combating illegal wildlife trade. From identifying users, which helps law enforcement to develop user profiles and relationships with actors, to co-operating on forensics to identify species in trade, internet companies are able to collate information and evidence of crime in ways that may be difficult for law enforcement to obtain alone. The establishment of a standard mechanism between internet companies and law enforcement agencies, and the active co-operation with the law enforcement agencies in the investigation and evidence collection process all play important roles in reducing intermediate links and improving law enforcement efficiency. Additionally, the huge influence these internet companies could apply to their users is also an important source of intelligence. For example, "Tencent for the Planet" is used to report information about illegal wildlife trade and other intelligence on the Tencent platform so that illegal advertisements leaked to the public can also be detected and transferred to law enforcement authorities.

3.2.3 Cutting the shipment of illegal wildlife products through courier channels

In reality, over half the seizures of illegal wildlife products occur at the transportation stage. Restricting opportunities for the physical transportation of illegal wildlife products has become a top priority. China's courier industry attaches great importance to the delivery and control of wildlife products. Attempts by the courier industry to diminish channels for illegal transportation of wildlife products have led to a strengthening of controls over the delivery network, including: delivery control; policy and delivery system improvements; information sharing and verification; security inspections and control in the receiving and transit links; and scientific and technological means to provide early warning and interception of shipments of illegal wildlife products.

The courier industry has adopted the "real-name system" for senders and receivers, which directly interfaces with the Ministry of Public Security's system. It can quickly and effectively verify real names from the sender's information within three seconds. The "real name system" can determine the identity of the sender and information on the person responsible for delivering the item. The courier company will prevent wildlife from being illegally sent out by collecting real names, out-of-box inspections, second-opening inspections, and security check-ups, to reduce the risk of illegal product transportation. Suspicious goods will be submitted promptly to the Ministry of Public Security for further action.

4. CONCLUSIONS

The rise of the internet, especially the popularity of social networks and e-commerce, has provided many avenues for wildlife crimes. Criminological studies have shown that the internet has generated opportunities for every step of the supply chain for illegal wildlife trafficking, such as communication, dissemination, management, organisation and contact, information technology, promotion, and advertising and inducement (Lavorgna, 2014). Although relevant international organisations and a few exemplar countries have begun to place emphasis on wildlife crime linked to the internet and introduced policies and related measures, they pale in comparison with the sheer scale of activities on the internet and its borderless nature.

Under current mainstream criminal research and law enforcement structures, cybercrime and wildlife crime are often divided into two separate units. However, INTERPOL and UNODC have begun to add wildlife crime to their research and monitoring of cybercrime, and some government departments have started to research strategies for targeting wildlife cybercrime through forums such as training workshops.

Although elements of the international community raised the issue of emerging wildlife cybercrime for nearly a decade, law enforcement authorities at transnational, national and local levels have only conducted basic research on wildlife cybercrime. Practices in China indicate collaboration is essential between law enforcement agencies and the private sector to effectively clamp down on wildlife cybercrime. Services provided by the private sector, in fields such as communications, fintech, e-commerce and logistics could be used by criminals to carry out criminal activities. The strategies highlighted to combat wildlife crime and wildlife cybercrime require the participation of the private sector together with government law enforcement authorities. Germany also advocates the importance of collaboration with the private sector in policy discussions on emerging wildlife cybercrime—in April 2015, the Federal Ministry of the Environment, the Federal Agency for Nature Conservation, and the Ministry of the Environment of the Federal State of North Rhine-Westphalia initiated discussions on how to gather policymakers and authorities with online marketplaces in order to forge a plan to tackle wildlife cybercrime.

The innovative attempts of the Chinese private sector and the governmental agencies on advertisement control, information sharing, and public education present valuable examples of inter-disciplinary collaboration. The success and lessons learnt from China could be replicated in other countries. However, best practices on preventing, monitoring, tracking, and combating wildlife cybercrime still need to be examined and scaled up internationally and domestically.

In China, bilateral collaborations have been established between several internet companies and enforcement authorities, while multi-lateral collaborations among private sector and governmental agencies still face challenges due to trust and jurisdiction issues. Similar obstacles might also be present in other countries and on transnational collaborations.

Information detection and monitoring techniques to counter wildlife cybercrime at the disposal of law enforcement authorities are not yet of a high standard, which could impact the efficiency and effectiveness of law enforcement. Although some scientists have claimed breakthroughs in technologies to trace information regarding the illegal wildlife trade on the internet, it is not clear whether such technological breakthroughs can be adopted by law enforcement. Moreover, the technology breakthroughs, i.e. innovations, have not been scaled up because of a lack of funds and interest from investors—even internet service providers have not expressed a strong interest and available funds for scaling up such technology (Marley, 2017).

5. RECOMMENDATIONS

5.1 Enhance law enforcement on legitimate online platforms

Monitoring and enforcement actions to counter wildlife cybercrime should focus on legitimate/open source online platforms since trade in illegal wildlife products on the Darknet remains at a negligible scale (Harrison et al., 2016). In addition, considering the fast-paced development of the internet, law enforcement agencies should pay close attention to new internet platforms in order to detect and crack down on illegal activities in a timely manner.

5.2 Increase investment in research and development for efficient monitoring systems

Technological tools such as machine learning can be an extremely valuable aids for law enforcement, and governments should consider investing in their development and application, even without other enabling market forces to drive development. Internet companies and platform operators should also encourage the development of such automatic screening systems to reduce the cost of manual screening and lower the legal risks in regards of wildlife cybercrime. Additionally, these systems with data aggregating mechanisms may analyse trends in illegal wildlife trade on-line. In order to enhance initiatives on combating wildlife cybercrime, all stakeholders with capacity should highlight the development of these systems.

5.3 Establish independent wildlife cybercrime law enforcement unit

To dismantle boundaries between rights of jurisdiction and improve the efficiency of information transfer, a specific law enforcement unit dedicated to wildlife cybercrime should be established. It is suggested that the unit should be built on the basis of wildlife crime, cybercrime, organised crime, and transnational crime. The combined human resources and talents developed through such an enforcement unit could help raise the level of expertise and capacity in law enforcement, while making it increasingly difficult for the criminals to operate covertly.

5.4 Improve information sharing mechanisms

Consensus has been reached on the rapidly growing trade of CITES-listed species through e-commerce. Various documents from the CITES Secretariat and the UN General Assembly have repeatedly reiterated the necessity of establishing a national-level monitoring mechanism for on-line trade in CITES-listed species, and strengthening information sharing among NGOs, the private sector (including internet companies), and governments and law enforcement authorities in various countries. The CITES Trade Database managed by The UN Environment World Conservation Monitoring Centre (UNEP-WCMC) currently gathers detailed historical trade information, which is essential for trend forecast and policy-making. However, this report-based data acquisition system is limited in its capacity to respond to rapidly changing on-line information. IGCI, established by INTERPOL in Singapore, has the potential to address monitoring and establish a database specifically for illegal wildlife trade linked to e-commerce as it gathers resources from different stakeholders to identify and analyse threats and crimes linked to the internet. As the information sharing system/databases have been established, collaborations between IGCI and UNEP-WCMC on CITES trade monitoring would be crucial to enable more rapid, data-driven responses to the illegal online trade of CITES-listed species. In order to enable such collaboration, it should be clarified to what extent the database of IGCI could be shared openly, and whether the CITES Secretariat could authorise IGCI to manage information sharing in regards of online trade of CITES-listed species.

5.5 Private sector partnership and mobilisation

The practices of Chinese internet companies and logistic companies should be scaled-up both in China and internationally. Essential practices for scaling up include:

- Establishing company policies on self-governance and capacity building in regards to illegal wildlife trade;
- Enhancing investments by individual companies on programme/software and equipment for screening and inspection;
- Improving legal awareness and basic species identification skills of employees, such as trainings delivered to company representatives in various workshops that should be disseminated within their companies. It is suggested that the private sector should organise their own capacity building sessions against illegal wildlife trade rather than passively waiting for annual trainings organised by third parties with limited available seats.

For internet companies specifically, the Coalition should be further expanded—more companies outside of China should be brought into the Coalition. A global approach with representatives from all regions, e.g. Africa/LAC, might be a feasible point to move forward. Besides, co-operation among companies and enforcement authorities at different levels should be strengthened. This will require some clear mechanisms for information sharing and mutual assistance to be established by the Coalition members.

For the courier and logistics industry, in addition to the suggestions above, the companies should recognise and emphasise their legal responsibility to assist enforcement actions at both policy and practice levels. The frontline personnel should be able to identify contraband and report suspicious items to their supervisor, and the company should transfer the information to enforcement authorities in a timely manner while securing the evidence simultaneously. Logistics companies and their employees should actively co-operate with investigations from governmental authorities including the postal service, public security, and industry and commerce. Moreover, for Chinese logistics companies, the real-name mailing and receiving policy initiated by the Ministry of Transport of the People's Republic of China should be fulfilled. The companies should publicise the policy to their customers and implement it through identification checks. Courier industry associations and companies from other countries could also look to current Chinese industry practices and assess their applicability in the local context, especially on policies concerning inspection and real-name mailing and receiving. Local governments and legislative institutions should facilitate the establishment and implementation of such policies in order to combat wildlife cybercrime domestically and reduce gaps in joint enforcement actions.

REFERENCES

Article19.org. (2018). Kenya: computer and cybercrimes bill 2017. Retrieved from https://www.article19.org/wp-content/uploads/2018/04/Kenya-analysis-April-2018.pdf

CoP17 Doc. 29-CITES. (2016). Combating wildlife cybercrime. Washington, D.C.: Federal Wildlife Permit Office, U.S. Fish and Wildlife Service, U.S. Dept. of the Interior. Retrieved from: https://cites.org/sites/default/files/eng/cop/17/WorkingDocs/E-CoP17-29.pdf

Conf. 11.3. (Rev. CoP15)-CITES. (2010). Compliance and enforcement. Retrieved from: https://www.cites.org/sites/default/files/eng/res/all/11/E11-03R15.pdf

Department of Commerce and Information Technology. (2017). China e-commerce report 2017, Ministry of Commerce China. (in Chinese). Retrieved from: https://www.sohu.com/a/233871778_353595

European Commission. (2016). EU action plan against wildlife trafficking. Retrieved from: http://ec.europa.eu/environment/cites/pdf/WAP_EN_WEB.PDF

European Commission. (2018). Progress report on the implementation of the EU action plan against wildlife trafficking. Retrieved from https://www.europeansources.info/record/progress-report-on-the-implementation-of-the-eu-action-plan-against-wildlife-trafficking/

General Office of the State Council. (2016). No.103—notice of the general office of the state council on orderly stopping the commercial processing and sale of ivory and ivory products. Retrieved from: http://lawinfochina.com/display.aspx?id=b61d5ae616d85834bdfb&lib=law

Haken, J. (2011). Transnational crime in the developing world. Retrieved from: https://gfintegrity.org/report/briefing-paper-transnational-crime/

Harrison, J. R., Roberts, D. L., & Hernandez-Castro, J. (2016). Assessing the extent and nature of wildlife trade on the dark web. Conservation Biology, 30 (4), 900-904. doi:10.1111/cobi.12707

IATA. (2019). Illegal trade in wildlife fact sheet. Retrieved from: https://www.iata.org/pressroom/facts_figures/fact_sheets/Documents/fact-sheet-wildlife.pdf

ICCWC. (2016). ICCWC indicator framework for combating wildlife and forest crime—assessment guidelines. Retrieved from: https://cites.org/sites/default/files/eng/prog/iccwc/ICCWC-Ind-FW-ASSESSMENT-GUIDELINES-FINAL.pdf

Internet Research Institute (IRI). (2017). Trend of illegal wildlife trade online in China. (in Chinese). Retrieved from: http://www.iricn.com/news/reports/295.html

INTERPOL. (2017). INTERPOL launches first digital forensics training course for wildlife investigations. Retrieved from: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2017/INTERPOL-launches-first-digital-forensics-training-course-for-wildlife-investigations

INTERPOL. (2017). Research identifies illegal wildlife trade on the darknet. Retrieved from: https://www.interpol.int/en/News-and-Events/News/2017/Research-identifies-illegal-wildlife-trade-on-the-Darknet

INTERPOL and IFAW. (2013). An investigation into the ivory trade over the internet within the European Union. Retrieved from: https://www.interpol.int/en/content/download/5181/file/Project Web – An investigation...

Lavorgna, A. (2014). Wildlife trafficking in the Internet age. Retrieved from https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-014-0005-2

Marley, J. E. (2017). eBay is outselling the dark web in illegal wildlife trade. Retrieved from: https://www.alternet.org/2017/11/ebay-outselling-dark-web-illegal-wildlife-trade/

Ministry of Commerce People's Republic of China. (2018). Regular press conference from Ministry of Commerce, China. (in Chinese). Retrieved from http://www.mofcom.gov.cn/xwfbh/20180125.shtml

TRAFFIC. (2017). Chinese internet giants launch alliance to combat wildlife cybercrime. (Press release). Retrieved from: https://www.traffic.org/news/chinese-internet-giants-launch-alliance-to-combat-wildlife-cybercrime/

TRAFFIC. (2019). Global internet giants gather to protect wildlife with technology. (Press release). Retrieved from: https://www.traffic.org/news/global-internet-giants-gather-to-protect-wildlife-with-technology/

UNODC. (2012). Wildlife and forest crime analytic toolkit. Retrieved from: https://www.unodc.org/documents/Wildlife/Toolkit_e.pdf

UNODC. (2015). The cybercrime repository. Retrieved from: https://sherloc.unodc.org/cld/v3/sherloc/index.jspx?tmpl=cybrepo

UNODC. (2016a). World wildlife crime report trafficking in protected species. Retrieved from: https://www.unodc.org/documents/data-and-analysis/wildlife/World_Wildlife_Crime_Report_2016_final.pdf

UNODC. (2016b). Financial flows from wildlife crime. Retrieved from: https://www.unodc.org/documents/Wildlife/Financial_Flow_Wildlife_Crime.pdf

UNODC. (2018). Call for papers: linking organized crime and cybercrime. Retrieved from: http://www.unodc.org/dohadeclaration/en/news/2018/01/call-for-papers_-linking-organized-crime-and-cybercrime.html

UNODC. (2019). United nations office on drugs and crime. Retrieved from: http://www.unodc.org/unodc/en/organized-crime/intro/emerging-crimes.html

USAID. (2018). How does developing enforcement capacity reduce wildlife crime? Increasing program effectiveness by understanding common assumptions.Retrieved from: https://webcache.googleusercontent.com/search?q=cache:v7Hhi5LpNM8J:https://rmportal.net/combating-wildlife-trafficking/documents/how-does-developing-enforcement-capacity-reduce-wildlife-crime-1/at_download/file%3Fsubsite%3Dcombating-wildlife-trafficking+&cd=6&hl=en&ct=clnk

World Animal Protection. (n.d.). Wildlife crime in the uk. Retrieved from: https://www.worldanimalprotection.org.uk/sites/default/files/uk_files/documents/wildlife_crime_in_the_uk_report.pdf

Worth, D. (2018). Illegal ivory dealers starting to use similar code words to hide online sales. University of Kent. Retrieved from: https://www.kent.ac.uk/news/environment/19318/illegal-ivory-dealers-starting-to-use-similar-code-words-to-hide-online-sales

Xiao, Y., Guan, J., & Xu, L. (2017). Annual report of the online monitoring on wildlife cybercrime in China in 2016. Retrieved from: https://www.traffic.org/site/assets/files/2108/briefing-online_wildlife_trade-2016.pdf

Xiao, Y., & Wang, J. (2015). Moving targets: Tracking online sales of illegal wildlife proucts in China. TRAFFIC. Retrieved from: https://www.traffic.org/site/assets/files/2536/moving_targets_china-monitoring-report.pdf

Xinhua News. (2016). Kenya mulls law to combat wildlife cyber-crime by end of year. (Press release). Retrieved from: https://www.arabstoday.net/en/187/kenya-mulls-law-to-combat-290816233531

Xinhua News. (2016). Kenya to domesticate international cybercrime law. (Press release). Retrieved from: http://www.chinafrica.cn/The_Latest_Headlines/201605/t20160518_800057078.html

Zhang, C. (2017). Cyber-stalking wildlife traders. Retrieved from: https://scienceline.org/2017/06/cyber-stalking-wildlife-traders/

Zhao, Y., Xu, L., Xiao, Y., Guan, J., & Lau, W. (2017). Revisiting china's ivory markets in 2017. Retrieved from: http://www.wwfchina.org/content/press/publication/2017/Briefing-Revisiting%20Chinas%20Ivory%20Markets%20in%202017(4).pdf

TRAFFIC
the wildlife trade monitoring network

TRAFFIC, the wildlife trade monitoring network, is a leading non-governmental organization working globally on trade in wild animals and plants in the context of both biodiversity conservation and sustainable development.

For further informationg contact:
TRAFFIC
Global Office
David Attenborough Building
Pembroke Street
Cambridge CB2 3QZ
UK
Telephone: (44) (0) 1223 277427
Fax: (44) (0) 1223 277237
E-mail: traffic@traffic.org
Website: www.traffic.org

The Rufford
Foundation
www.rufford.org