

Best practices and model measures to combat wildlife crime linked to the Internet

Version: August 2021

Information provided by Parties

Information provided by Parties in response to [Notification 2020/31](#), highlight a diverse range of measures in place and activities undertaken, and indicate that some Parties have already made commendable progress to combat wildlife crime linked to the Internet. Parties that responded include Cambodia, Canada, China, the European Union, Malta, New Zealand and the United Kingdom of Great Britain and Northern Ireland.

The information received to date¹, highlights the following:

a) Changes made to national legislation and other domestic measures that pertain to wildlife crime linked to the Internet

- Development or strengthening of national legislation and regulations related to virtual transactions, including introducing legal obligations for internet-based sites advertising CITES listed species to clearly specify the CITES permitting requirements for potential customers or the total prohibition of items for which commercial trade is not allowed under CITES;
- Enhancing national legislation so that the regulation of online wildlife trade is as strict as that of the offline trade;
- In cases where it is not possible (or necessary) to develop or enhance national legislation, Parties reported continued attention to this issue through the inclusion of online wildlife trafficking as a priority under national/regional action plans, through the development of specific units or teams that have included efforts to combat wildlife crime linked to the Internet as part of its mandate, or by including a cyber-crime department or unit in specific working groups dealing with wildlife crime;
- Development of new and enhanced standards for Regulating Illegal Wildlife Trade Online that include regulation procedures, management of information on illegal activities, intervention, and user education among other, and;
- Developing and implementing specific national action plans for wildlife crime linked to the Internet or include the issue in existing national action plans to combat wildlife crime.

¹ This also includes relevant information received in response to Notification [No. 2017/036](#) by Australia, Canada, New Zealand, the United Kingdom of Great Britain and Northern Ireland and the United States of America. For additional details, see [Best practices and model measures to combat wildlife crime linked to the Internet, version August 2019](#).

b) Websites adhering to codes of conduct to address and prevent illegal trade in wildlife

- An [Alliance of Internet companies](#) was formed in China to address wildlife crime linked to the Internet.
- A number of Parties engage in the issue through the [Global Coalition to End Wildlife Trafficking Online](#). This Coalition brings together online technology companies to collaborate and reduce wildlife trafficking online on their platforms. The 36 companies which have joined the Coalition have adopted codes of conduct to fight wildlife trafficking on their platforms.² Additional companies joining the Coalition adopt or strengthen their codes of conduct to join.

c) Best practice models that pertain to regulation of online marketplaces and social media platforms

- Use or development of web-trolling software applications to better self-police;
- Identification and removal of postings offering illegal wildlife products for sale;
- Support efforts to engage online platforms and online technology companies and educate online consumers;
- Encourage online platforms to publicly denounce illegal wildlife trade over the Internet and to support efforts to combat wildlife crime linked to the Internet;
- Use information gathered through monitoring of online platforms to inform activities, investigations or operations and conduct investigations targeting illegal wildlife trade linked to the Internet;
- Utilisation of a form to capture information known by the specimen owner, including the specimen provenance (i.e. when, where and how the specimen came to be in the owner's possession and any knowledge about how and when the specimen entered the country);
- Signature of a Memorandum of Understanding between Government and online sales platforms to facilitate information sharing between the signatories on potential cases of illegal wildlife trade;
- Online sales platforms proactively banning or restricting sale of CITES listed species that are commonly traded illegally through such platforms;
- Online sales platforms providing a 'Law Enforcement Portal' to facilitate cooperation and requests from law enforcement agencies on specific cases detected;
- Proactively work with online platforms to facilitate the exchange of information related to wildlife crime linked to the Internet (including timely removal of advertisements, stricter measures to prevent any new illegal advertisements and increased collaboration with law enforcement);
- Increased focus by relevant national and local departments in charge of market regulation to further strengthen the monitoring of wildlife trade via the Internet, and;

² The [progress report](#) of the Coalition (March 2020), highlights that more than 3 million prohibited species listings have been removed or blocked by the Coalition companies.

- Enhance training related to wildlife crime linked to the Internet to increase capacity in combating such crimes (at least one enforcement staff from each agency should receive training).

d) Results of scientific research on the correlations between use of the Internet and the rate of wildlife crime

- Several social media platforms seem to be enhancing their rules on the trade of wildlife on their websites. This however in some cases shifts some sales to other areas or groups within the same platform;
- Relevant resources have been made available on the wildlife crime linked to the Internet webpage. See also:
 - [OPERATION WILDNET-III](#) carried out by the Wildlife Crime Control Bureau (WCCB) of India focusing on internet-based wildlife crime;
 - “Stop Wildlife Cybercrime” report³ (*confidential report for law enforcement and CITES authorities only. A public version is available [here](#)*), developed under the auspices of the [EU Wildlife Cybercrime Project: Disrupting and dismantling wildlife cybercriminals and their networks in the European Union](#), and;
 - Flora Guard project report:⁴ [Tackling the illegal trade in endangered plants in endangered plants.](#)

e) Trends in wildlife crime linked to the Internet identified, including any changes in trade routes and methods of shipment observed⁵

- Some Parties have noted a steady increase in online purchases/transactions of CITES listed species that lack the required CITES documentation.
- Key findings from recent research on wildlife crime linked to the Internet in China⁶ indicate the average monthly number of new wildlife product advertisements online has declined by 73% compared to that in 2012-2016.
- Research carried out by the CITES Team of the UK Border Force at Heathrow airport into online sales of Elephant Ivory sold via internet platforms facilitated a targeted operation that to date has resulted in approximately five hundred (500) separate seizures

³ The report focuses on online trade in reptiles and birds in the Netherlands and Belgium, with findings relevant also to other EU countries and Parties outside of Europe. This report provides information e.g. on online sellers’ modus operandi, key websites being used, techniques for online surveys, and provides insights on good “indicator species” to identify illegal wildlife trade online. Requests for additional information can be sent to the EU wildlife cybercrime project.

⁴ The project explores a novel socio-technical approach to tackling internet-facilitated illegal wildlife trade, which it is hoped will be of use to law enforcement and other stakeholders for research and investigative purposes. See generally: www.floraguard.org. Requests for additional information can be sent to the FloraGuard project.

⁵ It should be noted that some Parties have highlighted in their responses that the information provided is in some cases anecdotal and that more data would be required to confirm trends. Reports provided are current observations and efforts are ongoing to continue research and analysis on this issue.

⁶ The research was reported by China and conducted by TRAFFIC. See ‘Wildlife Cybercrime Trends in China: Online Monitoring Results 2017-2018’. Requests for information can be sent to the CITES MA of China or TRAFFIC.

(predominantly elephant ivory) leading to house searches, arrests and prosecutions. As a result of this enforcement activity there has been a significant decline in the number of seizures made each month in the country.

Information provided by International Consortium on Combating Wildlife Crime (ICCWC) partners

Information provided by [ICCWC](#) partners is summarized below:

- Investigations related to wildlife crime linked to the Internet should take place at two levels:
 1. The Strategic monitoring of online trade (and dark web where needed), which requires specialized online investigators/analysts trained to monitor patterns over longer periods of time in specific market activities (wildlife and other commodities) and through the use of analytical software. These officials are likely to be placed in cybercrime units of enforcement agencies.
 2. Tactical Online investigations, which requires the capacity to establish fake online accounts, build an online persona, understanding the key features of online marketplaces and chat apps, conducting under-cover online and offline operations, collecting crucial information leading to arrests, seizures and further intelligence development. Any wildlife investigator can develop such capacity without being a cybercrime expert.
- INTERPOL established capacity at the INTERPOL Global Complex for Innovation in Singapore for support Parties in addressing wildlife crime linked to the Internet.⁷
- INTERPOL developed the *INTERPOL Wildlife crime linked to the Internet: Practical Guidelines for Law Enforcement Practitioners*.⁸

Additional relevant activities, reports and publications:⁹

⁷ See Notification to the Parties No. 2019/042 dated 8 August 2019: <https://cites.org/sites/default/files/notif/E-Notif-2019-042.pdf>

⁸ See: https://cites.org/sites/default/files/EST/INTERPOL_Guidelines-Wildlife_Crime_Linked_to_Internet-March2020-PUBLIC.pdf

⁹ Additional best practices/model measures reported previously by ICCWC partners include: INTERPOL *Cyber Wildlife Crime Investigations course, training and mentorships programmes* in Africa and Asia. For additional information and requests for support, contact INTERPOL at environmentalcrime@interpol.int; INTERPOL is working with countries that have cyber forensics laboratories to develop a set of training modules focused on investigating wildlife cybercrime. For additional information refer to paragraph 16 of [SC70 Doc 30.3.2](#); UNODC project on *Disrupting Environmental Crime Markets* focuses on illegal trade on the Internet, illicit financial flows and threat finance with two main components. For additional information refer to paragraph 16 of [SC70 Doc 30.3.2](#); UNODC and INTERPOL have experts working to support efforts of Parties in Africa and Asia with the provision of training and targeted support by putting in place in-country experts working specifically to support the efforts of Parties to address wildlife crime linked to the Internet. For additional information refer to paragraphs 16 and 17 of [SC70 Doc 30.3.2](#); and The World Customs Organization (WCO) [Working Group on E-Commerce \(WGEC\)](#) has a Safety and Security stream which explores the topic of illicit trade over the Internet in a cross-cutting manner covering illicit trade in general. Wildlife crime is one of the risks being considered.

- INTERPOL report on “European Union's Best Practices in Fighting Wildlife Crime Linked to the Internet” (confidential for law enforcement and CITES authorities only)
- UNODC training courses on tactical online investigations for law enforcement officers (Lao PDR, September 2019; and Malaysia, February 2020).
- UNODC assessment of capabilities of Law Enforcement Agencies to investigate Cybercrime, including those involved in the investigation of wildlife crime (Uganda, May 2019)