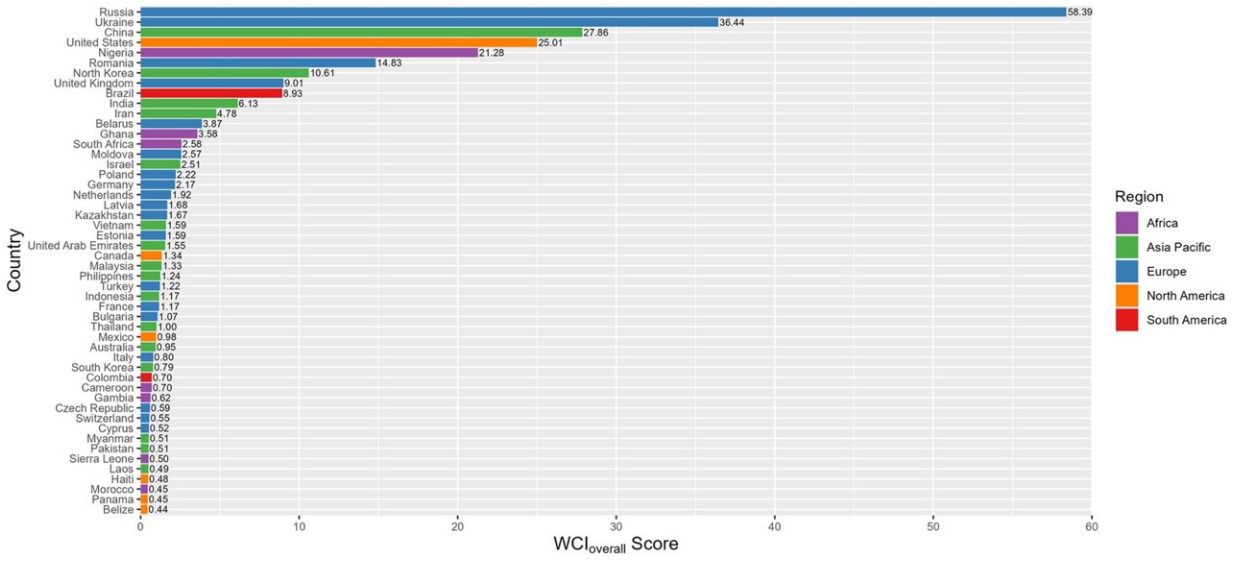
Most cybercriminal threats are concentrated in just a few countries, new index shows

April 10 2024



Top 50 countries by WCI overall score. Credit: Bruce et al., 2024, PLOS ONE, CC-BY 4.0 (creativecommons.org/licenses/by/4.0/)

A newly developed World Cybercrime Index shows that most cybercriminal threats are concentrated in several countries, with different countries associated with distinct cybercrime types. Miranda Bruce (University of Oxford/University of New South Wales), Jonathan Lusthaus (University of Oxford), Ridhi Kashyap (University of Oxford), Nigel Phair (Monash University), and Federico Varese (Sciences Po) present these findings in the open-access journal *PLOS ONE*.

Worldwide, cybercrimes are estimated to cost hundreds of millions to perhaps trillions. However, locating where offenders tend to operate poses challenges because they often use strategies to mask their locations, and legal documents capture a limited number of cases that may not be globally representative.

To help clarify, the authors surveyed leading cybercrime experts on the geographical distribution of cybercriminal threats. They developed and refined the survey through expert focus groups and pilot surveys before distributing it widely in 2021.

A total of 92 top cybercrime experts from around the world completed the survey, in which they named the countries they believed to be the biggest hubs for five cybercrime categories—technical products or services, attacks and extortion, data or identity theft, scams, and cashing out or money laundering.

The researchers used the survey results to construct the novel World Cybercrime Index, enabling comparison between countries. It suggests that cybercriminal threats are primarily concentrated in a small number of countries, with China, Russia, Ukraine, the US, Romania, and Nigeria ranking in the top 10 for each of the five categories. However, 97 countries were named by at least one expert as being a hub for a particular category.

Different countries were associated more often with distinct categories. For instance, cybercrimes related to technical products or services were the top category in China, data or identity theft in the US, and attacks and extortion in Iran.

The World Cybercrime Index could aid future cybercrime research, and it could help target preventive efforts tailored to specific hubs. However, the authors also note the need to address their study's limitations, such as

by including a larger, more globally representative pool of experts, reducing variation in participants' interpretations of survey questions, and addressing the sometimes blurred lines between profit-driven cybercrime and state-protected actions.

The authors add, "Profit-driven cybercrime, often seen as a fluid and global type of organized crime, actually has a strong local dimension. The World Cybercrime Index shows that 97 countries are significant cybercrime hubs, but most cybercrime is produced in just six of them."

More information: Mapping the global geography of cybercrime with the World Cybercrime Index, *PLoS ONE* (2024). DOI: 10.1371/journal.pone.0297312

Provided by Public Library of Science