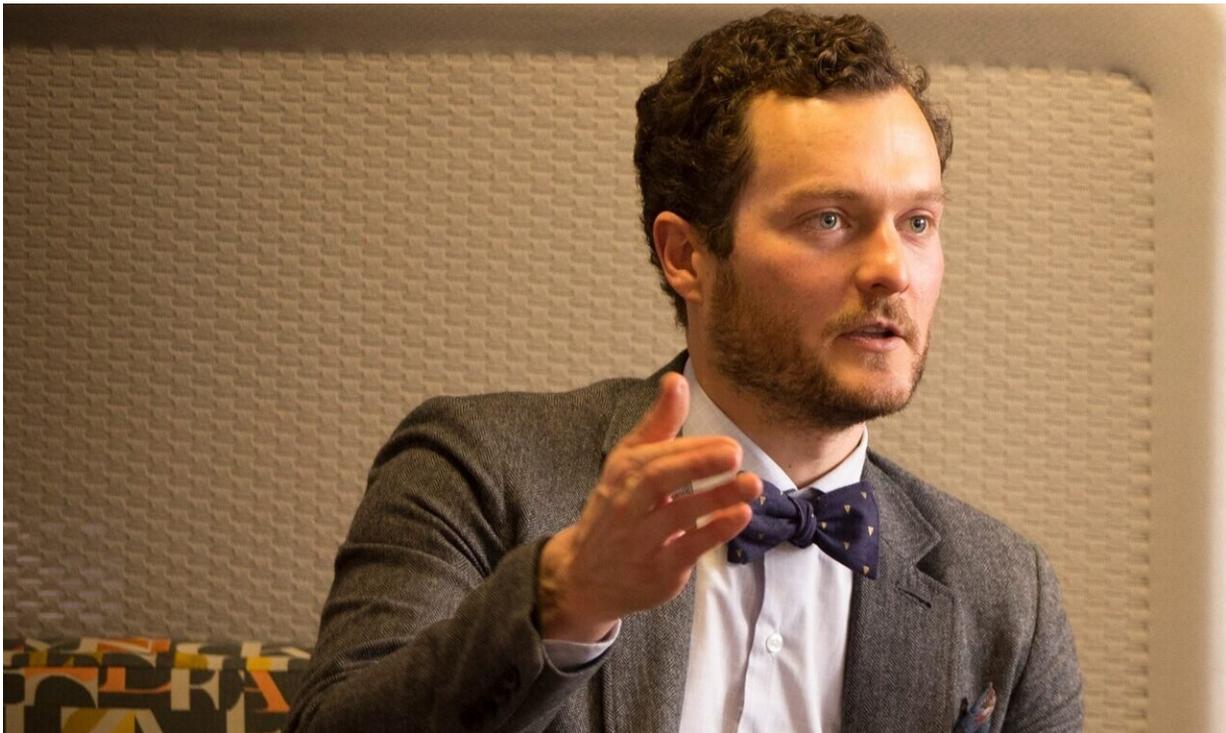


Malicious dark web activity unevenly prevalent in free nations, researchers find

November 30 2020



Eric Jardine, an assistant professor in the Department of Political Science, is an expert in the fields of cybersecurity and the dark web. Photo by Jason Jones for Virginia Tech, taken before the coronavirus pandemic. Credit: Virginia Tech

Even in nations with strict online censorship laws, citizens can still bypass firewalls and access hidden information.

The Onion Router provides [internet users](#) with the largest anonymity network in the world. Widely known as Tor, the system helps users circumvent censors while protecting their personal data.

But not without consequence.

From trafficking illicit drugs and sharing malware to distributing child abuse content, the [dark web](#) can shield [illegal activity](#) from detection.

Virginia Tech Assistant Professor Eric Jardine and two colleagues explored user activity within the Tor network in a new study published in the *Proceedings of the National Academy of Sciences*.

"The Potential Harms of the Tor Anonymity Network Cluster Disproportionately in Free Countries" provides an estimation of the global spread of harm and benefits from the Tor system.

The researchers found that potentially harmful use within the Tor system is not uniformly spread around the world.

"Potentially harmful use clusters disproportionately in liberal democratic regimes, which already have significant rights protections, and incidentally, host most of the Tor anonymity network infrastructure," said Jardine.

Jardine coauthored the study with Andrew Lindner, an associate professor at Skidmore College, and Gareth Owenson, a consultant with Cyber Espion Ltd in the United Kingdom.

While other studies have focused on Tor network traffic, the researchers' article is the first to provide a viable net estimate focused on how users of Tor utilize the network.

By studying new data collected from Tor entry nodes, the researchers found only 6.7 percent of users globally likely employ Tor for malicious purposes on an average day.

"We found that most Tor users head toward regular web content that could likely be considered benign," said Jardine, a faculty member in the Department of Political Science. "So even though the Tor anonymity network can be used for some highly malicious purposes, most people on an average day seem to use it more as a hyper-private version of Chrome or Firefox."

The proportion of users employing Tor for nefarious purposes clustered unevenly, however, with a higher prevalence in liberal democratic countries than in countries lacking freedom, the researchers found.

Among the many implications for research and policy, "the results suggest that anonymity-granting technologies, such as Tor, present a clear public policy challenge and include clear political context and geographical components," the authors wrote.

"Leaving the Tor network up and free from law enforcement investigation is likely to lead to direct and indirect harms that result from the system being used by those engaged in child exploitation, drug exchange, and the sale of firearms," the researchers noted.

Yet "simply working to shut down Tor would cause harm to dissidents and human rights activists," the authors wrote, "particularly, our results suggest, in more repressive, less politically free regimes where technological protections are often needed the most."

The Tor Project manages the code behind the Tor network and is an incorporated not-for-profit entity in the United States. The majority of the infrastructure of the Tor network is clustered disproportionately in

free nations.

The researchers suggested their findings could refuel the debate over shutting down the dark net.

Jardine, an expert in cybersecurity and the dark web, said the idea for the project arose after he designed a framework based on the observed relationship between Tor [network](#) usage and the political conditions within individual nations.

"This framework suggests political need drives the use of Tor in repressive regimes," Jardine said. "It also suggests that the opportunity to use Tor to mask bad activity is the primary incentive for use in liberal democracies. The derivative prediction of this model would be that harms and benefits should cluster unevenly around the world. But initially, I did not have a way to test this prediction."

Partnering with Lindner and Owenson provided Jardine with the opportunity to test his predictions.

Jardine plays an active role in Virginia Tech's Tech for Humanity initiative, serving as deputy director of dark web initiatives for the recently launched Tech4Humanity Lab.

"The Tech4Humanity Lab, as a part of the wider Tech for Humanity Initiative, is all about leveraging the potential of technology to improve the human condition," said Jardine. "This study is a first step toward understanding how many people are likely using an anonymity-granting tool. Understanding the pattern of technological use is a prerequisite to understanding how to leverage it for the good."

More information: Eric Jardine et al., "The potential harms of the Tor anonymity network cluster disproportionately in free countries," *PNAS*

(2020). www.pnas.org/cgi/doi/10.1073/pnas.2011893117

Provided by Virginia Tech

Citation: Malicious dark web activity unevenly prevalent in free nations, researchers find (2020, November 30) retrieved 19 April 2024 from <https://techxplore.com/news/2020-11-malicious-dark-web-unevenly-prevalent.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.