MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

EXECUTIVE SUMMARY

INTERNET SECURITY WITHOUT LAW:
How Service Providers Create Order Online

Eli Dourado, Research Fellow

Computer viruses can cause costly damage, including spam e-mail distribution, theft from user bank accounts, and attacks that temporarily shut down websites. Detecting and deterring these malicious programs, however, is also costly. The strong informal institutions among Internet service providers (ISPs) that dominate the enforcement of network security norms are more efficient in limiting damage from malicious computer code (malware) than a formal legal regime that would hold ISPs indirectly liable for such damage would be. Even though these informal relationships lack the enforcement power of legal remedies, they encourage ISPs to cooperate in formulating and implementing a swift response to attacks and to innovate to keep pace with changes in the nature of the threat. A greater reliance on the adversarial litigation process will reduce the three critical features of effective response to cyber threats: flexibility, speed, and extensive cooperation.

Below is a brief overview. To read the study in its entirety and learn more about its authors, please see "Internet Security without Law."

HOW ISPs ENFORCE SECURITY NORMS

The Internet consists of about 41,000 autonomous systems of varying size, connected by either commercial arrangements, where one autonomous system pays another for carrying traffic (transit agreements), or arrangements without pricing (peering agreements). Termination of agreements to carry traffic, or "depeering," is an extremely effective sanction in policing malware because the vast majority of these are informal "handshake" agreements that can be terminated promptly if one party is dissatisfied with the other's security practices or responsiveness to complaints.

- Of the more than 142,000 agreements that represent 86 percent of the world's Internet carriers, 99.5 percent are "handshake" agreements.
- Service providers who are willing to tolerate cybercriminals can usually charge higher prices but are subject to the sanction of depeering.
- When two major ISPs were presented evidence that a customer was hosting cybercriminals, they severed their agreement swiftly, and global spam levels fell about two-thirds almost instantaneously, and retail fraud plummeted from nearly $250,000 daily to almost zero.
- Even though they are immune from legal liability, ISPs have systems in place to notify their users about malware infections, even though these systems raise costs, suggesting that there is significant enforcement of security norms.

INFORMAL ENFORCEMENT VERSUS FORMAL LAW

While informal enforcement does not create perfect security—which would be cost prohibitive—it likely outperforms a formal legal regime that would hold ISPs liable for damages from a malware attack.

- Informal, at-will arrangements give network operators greater flexibility in determining the appropriate level of care and allow them to respond swiftly in a fast-changing environment than the slower speed of adaption of court-determined standards, which could obsolete very soon. As malware has moved from hosting to a centralized command system to one based on a peer-to-peer design, network operators have adapted quickly, shifting from depeering the host ISP to notifying infected customers.
- Under the informal system, security concerns are addressed promptly. Failure to do so results in equally prompt punishment, such as depeering. This is both faster and less costly than a trial.
- The informal system relies heavily on cooperation between ISPs to be effective. Replacing this cooperative model with the adversarial litigation process would reduce incentives to share information and reduce the security of the Internet.
- The informal system succeeds in securing cooperation globally, whereas securing similar international cooperation across formal legal systems, with all their differences, would be far more difficult.
- Moving to a formal liability system would leave larger ISPs subject to greater exposure and less willing to link to smaller ISPs, and it would undercut the extensive peering that is at the heart of the Internet.
- The informal system eliminates the need to record data streams for use in litigation, with all its attendant costs and privacy concerns.

For as dynamic and innovative an environment as the Internet, robust informal institutions are likely to outperform formal legal institutions, which should therefore be viewed as an arbiter of last resort.

CONTACT

Taylor Barkley, tbarkley@mercatus.gmu.edu, 703-993-8205
Mercatus Center, 3301 Fairfax Drive, 4th Floor, Arlington, VA 22201

ABOUT THE MERCATUS CENTER

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, Mercatus advances knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University's Arlington campus.

www.mercatus.org