

Internet's architectural flaws feed cyber-threats, say researchers

March 12 2013

In his State of the Union address this month, President Obama named hackers and "cyber-attacks" as amongst the greatest economic and national security threats to the United States. The President has a point; earlier this week, a report by the security firm Mandiant linked a unit of China's People's Liberation Army to hundreds of cyberattacks on Western corporations, while the *The New York Times*, *Wall Street Journal*, and *Washington Post* all recently announced they had been targeted as well.

The President's response was to issue an executive order calling for greater sharing of information between the private and public sectors on cyberattacks and threats, but [civil liberties](#) have raised questions about government invasions of privacy. How can we build a hacker-proof Internet without compromising basic freedoms?

A new report by the New England Complex Systems Institute (NECSI) lays the problem, and the solution, at the door of the Internet itself. "The current design of the Internet is inherently insecure," said Yaneer Bar-Yam, president of NECSI and a co-author of the study. Any node can be attacked from any other node, requiring the entire network to be hardened against all possible attacks—an unrealistic goal, Bar-Yam said.

"Making every computer on the Internet—including every tablet, PC, server, and smartphone—impervious to attacks is impossible," he added. An effective response requires reconstructing the architecture of the Internet itself. The report proposes substantial changes to the routers in

charge of switching [data packets](#) between [network nodes](#).

"Collective security-preventing attacks would require that the routers of the Internet themselves would need to have protocols that allow refusal of transmission based upon content or extrinsic information such as point of origin," according to the study.

The authors' discussion of Internet security is placed with the larger context of all network structures. The study compares [Internet attacks](#) to biological threats and systems, in which the same fundamental principles of network structures used in communication, transportation and defense mechanisms also apply.

"The human body bases its main line of defense in its primary transportation system—the blood stream—and in its skin and membranes," says Bar-Yam. "The immune system would collapse if it only acted within individual cells. Likewise, consider what American might look like if every home and office was required to be a fortress in the absence of the police and military patrolling neighborhoods and defending national borders."

The study, "Principles of Security: Human, Cyber and Biological," was performed at the request of a long-term planning military group, the Strategic Studies Group, which reports to the Chief of Naval Operations, the head of the Navy. The report is being released for the first time to the public this week.

More information: www.necsi.edu/research/military/cyber/

Provided by New England Complex Systems Institute

Citation: Internet's architectural flaws feed cyber-threats, say researchers (2013, March 12)
retrieved 27 April 2024 from

<https://phys.org/news/2013-03-internet-architectural-flaws-cyber-threats.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.