Internet Society

Threats to the Internet Way of Networking

The Internet is an incredible resource because it was built to foster a culture of collaboration and participation for the collective good.

But the open architecture that makes it strong and successful is not invincible. Governments and businesses are increasingly making decisions that could harm the Internet's foundation, and they may not even know it.

Actions that impact any one of the Internet's critical properties could erode the foundation as a whole.

PROPERTY 1
An Accessible Infrastructure With a Common Protocol

PROPERTY 2
Open Architecture of Interoperable and Reusable Building Blocks

PROPERTY 3
Decentralized Management and a Single Distributed Routing System

PROPERTY 4
Common Global Identifiers

PROPERTY 5
A Technology Neutral, General-Purpose Network

Here are a few examples of regulatory actions that could harm the Internet:

THREAT 1

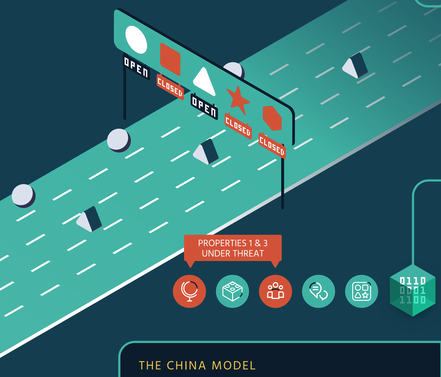
Removal of intermediary liability protection

Internet intermediaries include Internet service providers (ISPs), Internet exchange points (IXPs), content delivery networks (CDNs), domain name registries and registrars.

Intermediaries play important roles in our daily experiences online: they manage network infrastructure, provide Internet access, facilitate content delivery, help networks connect to each other, and allow users to use and deliver services over the Internet.

Just like a postal service wouldn't be held liable for the contents of people's letters or packages, intermediaries rely on laws that don't hold them responsible for the actions of users of their networks.

PROPERTIES 2, 3 & 5 UNDER THREAT



PROPERTIES 1 & 3 UNDER THREAT

THREAT 2

Centralized control over interconnection and routing

In some countries, there is a trend towards centralized decision-making and reduced autonomy of operators in defining how they manage network interconnection and routing.

RUSSIA'S SOVEREIGN INTERNET LAW

Network operators will have to provide the regulator, Roskomnadzor, with network diagrams and technical design of the communications facilities so that "technical means of countering threats" (TMCT) can be installed.

If the regulator identifies a security threat to its public communications network, it can use TMCT to change traffic routing, close or limit communication lines and channels, directly contact user, and change the configuration of communications. If Roskomnadzor declares a communications emergency, it will be able to control routing and other operator decisions.

THE CHINA MODEL

China's big three operators China Telecom, China Unicom, and China Mobile run 70% of networks and much of the backbone infrastructure of smaller networks. They run the three gateways which filter Internet traffic in and out of China. The choke-points that these three companies hold on interconnection with all networks outside of China severely limits the access of China's network providers and Internet users to the global Internet.

U.S. CLEAN NETWORK PROGRAM

The U.S. Clean Network program challenges the open architecture of the Internet at its very core. The "Clean Carrier" and "Clean Cable" programs would force vast amounts of Internet traffic to route into third countries, extending the distances data must travel, increasing the potential for surveillance and manipulation of Internet traffic, increasing the risk of Internet outages, and in general increasing costs to everyone on the Internet.

Having a government dictate how networks interconnect impacts the Internet's agility, resiliency and flexibility.

It's up to all of us to **protect** and **enhance** the **future** of the Internet.

By using the **Internet Impact Assessment** to show policymakers how laws, decisions and trends could impact the foundation of the Internet responsible for its success, we can help make sure it keeps working for **everyone.**

To learn more, please visit:
internetsociety.org/impact-assessment