How can policymakers improve global routing security?

Information for ICT and telecoms policymakers

Today, the Internet plays an essential role in the majority of societies around the world. From banking to education, health to logistics, just about every sector relies on Internet-based applications and services to function.

Our increased dependence on digital technologies brings with it growing concerns around Internet security. While there are many dimensions to Internet security, securing the key building blocks of the Internet's infrastructure is critical.

The Internet's routing system enables data to flow from one point to another. Ensuring that this data flows correctly, and to its intended recipient, is the foundation of Internet security.

Thousands of Internet routing incidents occur every year, leading to economic and social harm by:

- making key services unreachable;
- disrupting e-commerce;
- allowing malicious actors to spy on users and with it, the potential to compromise systems.

While existing security measures can help address many of these routing incidents, the solutions they provide are often limited. The interconnected nature of networks means that many solutions only work when other networks make the same improvements. **We need collective action to make a real change.**

In support of the larger Internet security agenda, we encourage policymakers to work with network and infrastructure operators, critical infrastructure protection agencies and standards bodies, among others, to improve global routing security while also preserving vital aspects of the system that have allowed the Internet to be open and universal.

What is MANRS?

Mutually Agreed Norms for Routing Security (MANRS) is a set of best practices based on existing norms. These practices support network operators to improve the security of the global Internet routing system.

MANRS defines four simple but concrete actions for network operators to implement to greatly improve Internet security and reliability. These include:

1. **Filtering** – defining a clear routing policy and implementing a system to ensure that announcements to adjacent networks are correct.
2. **Anti-spoofing** – enabling source address validation (SAV) and implementing anti-spoofing to prevent packets with incorrect source IP addresses from entering and leaving the network.

3. **Coordination** – maintaining globally accessible up-to-date contact information to assist with incident response.
4. **Global validation** – publishing data that enables other stakeholders to validate routing information on a global scale.

The first two, filtering and IP source validation, address the root causes of common routing incidents. The second two, coordination and global validation, help limit the impact of incidents and decrease the likelihood of future incidents.

MANRS actions define outcomes rather than specific methods. This allows implementation to change with technology and helps establish MANRS actions as best practice.

Alongside routing incidents, MANRS seeks to address ecosystem challenges in the global routing system.

MANRS improves economic incentives for routing security by allowing network operators to demonstrate their commitment to:

- Security – securing core Internet infrastructure for greater global Internet security.
- Customers – to ensure the services they provide adhere to routing security best practices.
- Competitors – to ensure routing security incidents don't have a cascading effect on other network operators.
- Policymakers – to ensure a robust and resilient national Internet infrastructure in support of the larger Internet security agenda.

An independent study by 451 Research[1], commissioned by the Internet Society, found that traffic routing, hijacking, and interception were the leading security concern for enterprises. Distributed denial of service (DDoS) attacks and address spoofing came in second.

94% of enterprises said that, in a competitive situation, they'd be willing to pay more for a vendor who was an MANRS member.

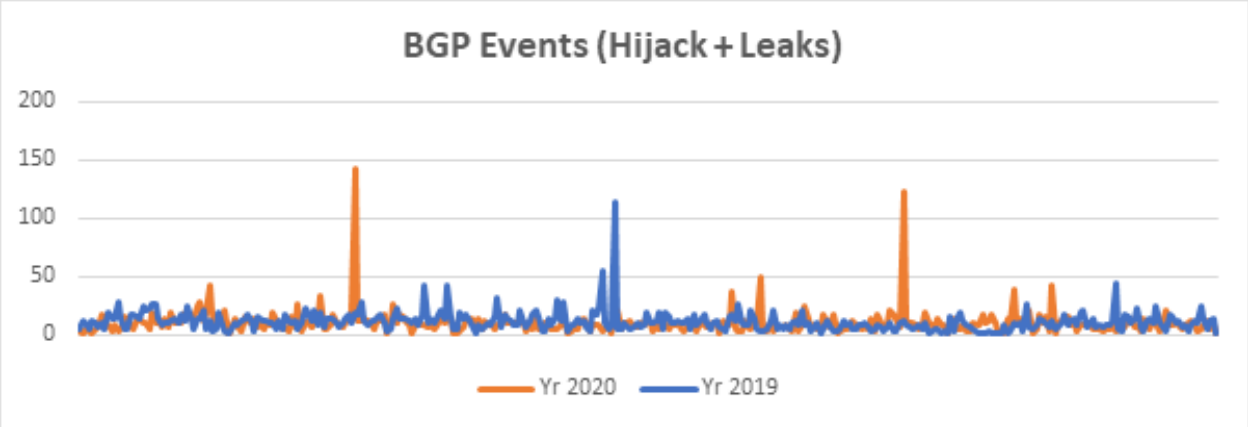
This highlights the importance of MANRS implementation as an indicator of a network operator's sound security practices.

As a policymaker, you can use this to encourage the adoption of MANRS among network providers while improving awareness regarding routing security for users, including enterprises.

[1] MANRS project study report: https://www.manrs.org/wp-content/uploads/2017/10/MANRS-451-Study-Report.pdf

Why does MANRS matter for Internet security?

In 2020, there were a total of 3,873 major network incidents that involved border gateway protocol (BGP) related attacks. Of these, 64% were hijacks and the rest were route leaks.



In 2019, there were 4,232 major network incidents that involved BGP, of which:

- 3.8% of all networks were affected by a routing incident
- 2% of all networks were responsible for the 4,232 routing security incidents.

These incidents can:

- create a serious strain on infrastructure
- result in dropped traffic
- allow for unauthorized inspection of traffic
- be used to perform Denial of Service (DoS) attacks.

In July 2020, there were two significant routing incidents in the global BGP routing system[2], impacting more than 1,500 networks worldwide. This highlighted the need for network operators to implement good routing security practices. These incidents impacted major North American network providers including TWC, Rogers and Charter, among others[3].

The only effective way to address routing security threats is through global collective action, as no one organization or group can do it alone.

Governments and policymakers can play a key role in facilitating such collective action.

2. Big route leak shows need for routing security https://www.manrs.org/2020/07/big-route-leak-shows-need-for-routing-security/

3 .Another border gateway protocol Incident Impacts TWC, Rogers, Charter and others https://www.manrs.org/2020/07/another-bgp-incident-impacts-twc-rogers-charter-and-others/

What role can you play, as a policymaker?

1. **Avoid regulatory barriers:** help improve market incentives for better routing security by avoiding any regulatory barriers and facilitating cooperation and collaboration.

2. **Encourage good practices:** encourage and facilitate initiatives in a way that preserves the strengths of the global routing system, including its overall resilience, ease of use, flexibility and scalability.

3. **Promote common guidelines:** you are uniquely placed to promote common guidelines for network operators, help facilitate industry best practices for routing security, and promote their implementation.

4. **Grant incentives:** where feasible, enable the process through incentives like grants and tax rebates.

5. **Eliminate legal barriers:** help identify and eliminate legal barriers on information sharing and responses to routing incidents. Network and infrastructure operators and security researchers may worry that disclosing routing security incidents or threats could place them in legal jeopardy. Providing safeguards for them can help allay such concerns.

6. **Lead by example:** as governments typically run large networks of their own, they can lead by example by improving Internet infrastructure reliability and security using MANRS best practices.

Given the significant impact of routing incidents on critical networks, we need to give high priority to protecting and improving our network infrastructure. However, research shows a general lack of understanding of the fact that simple steps can dramatically reduce such incidents.

Some measures outlined above aren't entirely new, and some organizations may already be working to integrate such measures in the near future. To ensure a healthier and more robust network infrastructure, we must prioritize the measures highlighted in this document, and back their implementation with adequate resources.

- Find out more about MANRS: manrs.org
- Read about the Internet Society's work: internetsociety.org