**Dear Network Operators, Where Are Your MANRS?!**

***The Internet Society Announces Major Momentum in Internet Security Initiative***

***and Encourages More Network Operators to Sign up***

Washington, D.C. – October 13, 2016 – The [Internet Society](http://www.internetsociety.org/) today announced the number of participants in the organization’s [Mutually Agreed Norms for Routing Security](https://www.routingmanifesto.org/) (MANRS) initiative has more than quadrupled in its first two years, growing from 9 to 42 [network operators](https://www.routingmanifesto.org/testimonials/). Launched in November 2014 with an initial group of nine operators, the MANRS initiative, part of the [Routing Resilience Manifesto](https://www.routingmanifesto.org/), obliges participants to take action to improve the resilience and security of the routing infrastructure to keep the Internet safe for businesses and consumers alike. The network operators participating in this effort run autonomous system networks (ASNs) across 21 countries, reflecting a broad-based concern about risks to the Internet’s routing system and an increased willingness to signal technical excellence to the public and to their operator peers.

The most recent additions are SUNET and NORDUnet, two leading research and education networks in Scandinavia. Thirty-three network operators have now committed to MANRS since the initial launch with 9 members. Among the new members joining during the initiative’s second year was Internet Initiative Japan (IIJ), the first participant from Japan. “Coordination and cooperation based on our relationships of mutual trust are the key elements to run the Internet, and we have shared responsibilities to improve the Internet operations,” said Junichi Shimagami, Director and CTO of IIJ. In a follow-up action, the Japan Network Information Center (JPNIC) facilitated the [translation of the MANRS document into Japanese](https://www.routingmanifesto.org/2016/06/japanese-translation-of-manrs-document-now-available/). The MANRS initiative, which reduces networking risks and promotes best practices, is now well established in Asia, North and South America, Africa and Europe. Countries with the largest number of members include Russia (six), Netherlands (five), USA (five) and Germany (four).

“As networks have come under increased stress from corporations, governments and other actors, not all benign, the visibility of the Internet’s routing infrastructure as a critical component has become as high as that of the Domain Name System (DNS) or other core infrastructure,” said Olaf Kolkman, Chief Internet Technology Officer (CITO) at the Internet Society. “By promoting routing security and resilience, MANRS gives operators a way to demonstrate their commitment to networking excellence, helping to restore trust in the Internet to anxious peers, businesses, customers and individuals.”

In joining MANRS, participants certify that they have taken action in at least one of these four areas: filtering, anti-spoofing, coordination and global validation, with coordination not allowed as the only action. Most operators have implemented all four, including Comcast, one of the world’s largest broadband operators, which has done so across 33 ASNs. None have acted on fewer than three.

The first action, filtering, helps prevent the propagation of incorrect routing information. This technique provides assurance against “fat-finger” errors that can lead to "hijacking" traffic directed to other networks, resulting in widespread outages. Up-to-date filters also have mitigated known cases of “route leaks,” defined in the IETF’s RFC 7908 in June 2016 as “the propagation of routing announcement(s) beyond their intended scope.” The second action entails preventing traffic with spoofed source IP addresses, a practice that can help dramatically diminish the prevalence and impact of distributed denial of service (DDoS) attacks. The third action facilitates timely communication and coordination among peers, which is essential for incident mitigation and better assurance of the technical quality of relationships. The fourth is facilitating the global validation of routing information, which limits the scope of routing incidents and makes the global system more resilient.

Implementing MANRS helps improve Internet security and resilience and helps enable a sustainable business environment. MANRS provides added value for the network operator and its customers: better protection against traffic anomalies caused by misconfigurations; cleaner setups resulting in easier troubleshooting and lower time-to-resolution (TTR); improved peering conditions; and opportunities for valuable collaboration with other operators through a discussion forum and professional network. Although committing to MANRS has its costs, the scope of the actions is specifically defined to minimize costs and the risks of implementing them.

As word about MANRS has spread and the need for guidance has grown, a team of participants has convened to draft a Best Current Operational Practices (BCOP) document, walking interested parties through the steps to become MANRS-compliant. That document is expected to be presented for review by regional BCOP communities at [RIPE 73](https://ripe73.ripe.net/) in late October. Related efforts involve future training modules and self-assessment guides. Monitoring and debugging (e.g. looking-glass) tools are also under consideration. The MANRS initiative is currently testing the use of BGPStream and Spoofer to check for compliance. Once consensus on application of these tests is reached, it will publish them for transparency and potentially integrate them into the sign-up process.

Public discussions of MANRS tend to occur alongside network operator meetings, such as NANOG, RIPE, and APNIC/APRICOT. A representative from MANRS spoke yesterday, October 12, 2016, at the [Internet Society’s ION Bucharest Conference](http://www.internetsociety.org/deploy360/ion/bucharest2016/), co-located with the Romanian Network Operators’ Group. A [recently released video](https://www.youtube.com/watch?v=-QUACFOwsAU&feature=youtu.be) featuring Internet Society CITO Olaf Kolkman provides an overview of MANRS and collaborative security. Operators interested in joining MANRS can [sign up online](https://www.routingmanifesto.org/signup/).

**About the Internet Society**  
The Internet Society is the trusted independent source for Internet information and thought leadership from around the world. It is also the organizational home for the Internet Engineering Task Force (IETF). With its principled vision and substantial technological foundation, the Internet Society promotes open dialogue on Internet policy, technology, and future development among users, companies, governments, and other organizations. Working with its members and Chapters around the world, the Internet Society enables the continued evolution and growth of the Internet for everyone.  For more information, visit:  [www.internetsociety.org](http://www.internetsociety.org).

[Twitter@InternetSociety](https://twitter.com/internetsociety) | [Facebook@Internet Society](https://www.facebook.com/InternetSociety/) | [LinkedIn@Internet Society](https://www.linkedin.com/company/internet-society?trk=top_nav_home)

[YouTube@InternetSocietyVideo](https://www.youtube.com/user/InternetSocietyVideo) | [Google+@Internet Society](https://plus.google.com/+InternetSociety/about)

###

**Internet Society Contact: Media Contact:**

Allesandra de Santillana Brittney Jubert

Senior Manager Wireside Communications®

Media Relations For the Internet Society

+41-22-807-1451 +1-804-593-4167

[desantillana@isoc.org](mailto:desantillana@isoc.org) [bjubert@wireside.com](mailto:bjubert@wireside.com)

[www.internetsociety.org](http://www.internetsociety.org/) [www.wireside.com](http://www.wireside.com/)