

# Routing security: What do operational data tell?

Andrei Robachevsky <robachevsky@isoc.org>

# **An approach to routing resiliency**

## **Talking to network operators**

- **Understanding needs, incentives**
- **Fostering good will and collective responsibility**

## **Technology agnostic**

- **Looking at everything that matters**

## **Raising awareness**

- **Understanding risks**
- **Providing factual data**

# Data is needed

**Several operators we talked to indicated the need for global operational statistics in this area**

- **Better understanding of risks**
- **Monitoring dynamics/long-term trends**

**Routing security incidents (route hijacking, other policy violations)**

- **Type, duration and causes**
- **Detection and measures**

# Type of questions

## # and type of registered incidents @NOC

- Your prefix is hijacked
- Your customer's prefix is hijacked
- Other policy violations

## Duration of incidents

## Typical causes

## Typical measures

## Captured exceptions from installed controls

# Your input is appreciated

**Network operators are not asked to provide data that is strictly company confidential;**

**All requested data is in form of statistical information and doesn't need to reveal specifics, like AS numbers, prefixes, etc.**

**Even if such information is submitted for the discretion of the Internet Society, it will be fully anonymized before sharing with anyone, and presented in collated form.**

Questions?  
Feedback?  
Interest?

[robachevsky@isoc.org](mailto:robachevsky@isoc.org)