CYBERSECURITY READINESS PODCAST SERIES

Episode 105

The Invisible Layer: Governing Routing Security as a Supply Chain Risk

with Andrei Robachevsky, Technical Director, Internet Integrity Program, Global Cyber Alliance

Host	Dr. Dave Chatterjee, Duke University
Guest	Andrei Robachevsky, Technical Director, Internet Integrity Program, Global Cyber Alliance
Referenced Report	MANRS Report, February 2026 (Global Cyber Alliance)
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 105 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Andrei Robachevsky — Technical Director of the Internet Integrity Program at the Global Cyber Alliance, founding contributor to MANRS (Mutually Agreed Norms for Routing Security), former CTO of RIPE NCC, and former Senior Director of Technology Programs at the Internet Society — to examine a cybersecurity risk that almost no enterprise security team is governing: the internet routing layer.

Opening with the June 2024 Cloudflare 1.1.1.1 BGP hijack incident — where two Brazilian network operators' routing mistakes propagated to over 300 networks across 70 countries, silently rerouting traffic for several hours without triggering a single enterprise security alert — Dr. Chatterjee frames the episode's central challenge: organizations with excellent perimeter controls, clean firewalls, and healthy identity systems can still have their user traffic redirected to unintended destinations by failures occurring on networks they have never heard of, in countries they have no operations in, governed by routing norms they have never been asked to consider.

Drawing on the February 2026 MANRS Report, Robachevsky explains that the Border Gateway Protocol (BGP) — the foundational routing system across nearly 80,000 autonomous networks — has no built-in authentication. Routing incidents occur 200 to 300 times per month, most of them invisible to enterprise security teams, manifesting as unexplained outages or performance degradation rather than identifiable threats. The implications range from SLA breaches and customer trust erosion to man-in-the-middle exposure on silently rerouted traffic.

Analyzed through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) framework, the conversation delivers a clear and actionable message: routing security is not a network engineering problem — it is a supply chain governance problem. The tools already exist. RPKI exists. MANRS exists. MANRS+ is nearly here. The gap is entirely on the governance side, and it is closeable. The organizations that will not find themselves in the next routing incident are the ones that start with a map of their connectivity supply chain and a single question to every provider: are you MANRS+ certified?

Discussion Highlights

The Opening Incident: When the Routing Layer Goes Dark

Dr. Chatterjee opens with the June 27, 2024 Cloudflare 1.1.1.1 DNS resolver outage as the defining illustration of invisible infrastructure risk. Two small Brazilian network operators made BGP routing mistakes — one mistakenly announced ownership of Cloudflare's address space; another broadcast that claim to the broader internet. Because the global routing system is built on trust, not verification, major providers including at least one Tier 1 carrier accepted those false announcements and began sending Cloudflare traffic somewhere it was never meant to go.

The IT team at a mid-sized financial services firm on that same Wednesday morning ran through their entire security checklist: firewalls clean, identity systems healthy, cloud configurations unchanged, no endpoint alerts. By every internal measure, they were secure. And yet their users could not reach their services. What none of their tools were designed to see is that the routing layer — the foundation beneath every security control they had deployed — had failed at a point they did not own, did not monitor, and had never been asked to govern.

How BGP Works — and Why It Fails

Robachevsky explains the structural vulnerability at the heart of internet routing: BGP, the Border Gateway Protocol, is essentially "routing by rumor." Networks exchange reachability information with their neighbors, who pass it on to their neighbors — without any built-in authentication to verify whether the announcements are true. A misconfigured or malicious network can announce that it owns an address block it does not own, and the information propagates.

The MANRS Observatory counts 200 to 300 routing incidents per month. Most never reach headline status — they manifest as unexplained slowdowns, intermittent outages, or performance degradation, and are often resolved before the root cause is identified. The consequence for enterprises is not only disruption: rerouted traffic opens the door to man-in-the-middle attacks, eroding the trust guarantees that TLS and other transport security measures are designed to provide.

> *"The routing system is at the foundation of the internet. And yet, because it's so foundational, it's below the radar. It's just not seen by enterprises and enterprise security. It is assumed that it simply works."*
> **— Andrei Robachevsky, Technical Director, Global Cyber Alliance**

Routing Security as Supply Chain Risk

The conceptual reframe that makes routing risk governable, Robachevsky argues, is to treat it the same way organizations treat software or ICT supply chain risk. The routing layer is not an abstract technical concern — it is the connectivity supply chain that connects every customer, partner, cloud provider, and digital asset the organization depends on.

CISOs, risk offices, and boards already have frameworks for managing supply chain dependencies. The question of who is in your routing supply chain, how they are connected, and whether they meet routing security standards is the same question organizations already ask of their software vendors and third-party processors. The governance vocabulary is already there — it just has not been applied to the layer that everything else sits on top of.

> *"If you look at the nature of the dependency on the routing system — the connectivity fabric that connects your customers, your partners, your applications, your digital assets in the cloud — you realize there are a lot of similarities to how you manage supply chain. Routing security should be managed exactly the same way."*
> **— Andrei Robachevsky**

The CPD Framework Applied to Routing Security

Dr. Chatterjee applies the Commitment–Preparedness–Discipline (CPD) framework to routing security, with Robachevsky's analysis of the Cloudflare incident illustrating each pillar across the multiple actors involved:

CPD PILLAR	APPLICATION TO ROUTING SECURITY
COMMITMENT	Routing risk must be explicitly named, entered in the risk register, and owned by a named leader. The 2024 incident illustrated both sides: Cloudflare, as victim, had committed to routing monitoring; the Brazilian ISPs and the Tier 1 carrier had not.
PREPAREDNESS	Organizations must map their full routing supply chain — not just their direct connectivity provider, but every network in the path between their users and their services. Providers must be assessed for routing security posture, and incident response plans must account for failures that originate outside the organization's perimeter.
DISCIPLINE	Routing security posture cannot be verified once at procurement and assumed to hold. Controls must be continuously monitored. Provider commitments must be verified against live behavior, not just documented intent. MANRS Observatory provides exactly this continuous audit capability.

MANRS and the Path to MANRS+

Robachevsky explains the MANRS initiative — Mutually Agreed Norms for Routing Security — which he helped found at the Internet Society in 2014. Starting with nine network operators, MANRS has grown to over 1,300 participating networks. MANRS defines a minimum baseline of routing security controls, with the emphasis on broad adoption rather than high barriers: the more networks that implement the baseline, the safer the entire internet routing fabric becomes.

For enterprises, however, the baseline is not sufficient. A new "MANRS+" program is under development to represent a higher-grade participation level designed specifically for enterprise-grade routing security requirements. MANRS+ includes more stringent controls, explicit auditing requirements for higher assurance, DDoS mitigation capability standards, and secure configuration requirements. Critically, no MANRS+ connectivity provider exists, as the program has not been rolled out yet. To fully

develop meaningful criteria that will meet the needs of both network operators and enterprises, Robachevsky calls on enterprise leaders to join the MANRS+ working group and define the standard before it is defined for them.

> *"Routing security will not improve without demand. And that demand has to come from enterprises. Define the standard rather than being the standard defined for you."*
> **— Andrei Robachevsky**

The Governance Gap: Tools Exist, Will Does Not

Both speakers close with the same observation: this is not a problem waiting for new technology. RPKI — Resource Public Key Infrastructure, the cryptographic system for verifying routing announcements — already exists. MANRS already exists. MANRS+ is nearly ready. The gap is not technical; it is governance.

Dr. Chatterjee returns to the financial services firm from the opening: they did everything right and still got hurt, because nobody had told them that the routing layer was theirs to govern. The organizations that will not be in that story the next time a BGP hijack propagates across 70 countries are the ones that treat routing as a supply chain risk, map their connectivity dependencies, and demand routing security evidence in every provider procurement conversation.

> *"The gap maps precisely onto the three pillars: Commitment — to say out loud that routing is a risk this organization owns. Preparedness — mapping the supply chain and asking the right questions. Discipline — verifying that the answers you got at procurement are still true six months later."*
> **— Dr. Dave Chatterjee**

Actionable Recommendations

Map Your Routing Supply Chain

Identify every provider in the path between your users and your services — connectivity providers, cloud interconnects, CDNs, SD-WAN underlays. You cannot govern what you have not mapped. This is the foundational step before any other routing security control becomes meaningful.

Embed Routing Security in Vendor Procurement

Add routing security requirements to your procurement framework alongside SLA, pricing, and performance criteria. Ask every connectivity provider for evidence of their routing security posture. Demand MANRS participation as a baseline requirement and MANRS+ certification as a differentiating criterion.

Give the Board a Single Meaningful Metric

Report to the board on the percentage of critical service providers that are MANRS+ certified. One number tells leadership exactly how much of the routing supply chain has been independently verified — and how much has not. This translates a deeply technical problem into a governance posture question boards can act on.

Apply Continuous Verification, Not One-Time Assessment

Routing security posture is not static. Use tools like the MANRS Observatory to continuously monitor whether providers are meeting the commitments they made at procurement. Annual reviews cannot match the pace at which routing configurations change. Discipline means verifying that the answers you received are still true today.

Recognize the Man-in-the-Middle Risk of Rerouted Traffic	Apply the CPD Lens to Routing Risk Governance
Routing incidents do not only cause outages. Silently rerouted traffic — traffic traveling via unintended paths — opens the door to interception and man-in-the-middle attacks even when TLS is in use. Organizations that assume transport encryption is sufficient without governing the routing layer beneath it are accepting risk they have not acknowledged.	Before the next provider review: establish Commitment by naming routing as a risk the organization owns; build Preparedness by mapping the full dependency graph and documenting a routing incident response plan; enforce Discipline by verifying provider posture continuously rather than assuming it holds from one procurement cycle to the next.

Time Stamps

0:00	Opening scenario — the June 2024 Cloudflare 1.1.1.1 BGP hijack and the invisible routing failure
0:49	Host framing: the financial services firm that did everything right and still got hurt
5:42	Andrei Robachevsky introduction and welcome
6:25	Guest career highlights — MANRS founding, RIPE NCC CTO, Internet Architecture Board
9:39	How BGP works and why routing incidents go undetected by enterprise security tools
12:48	Why senior leaders don’t connect rerouting to business impact — and how to change that
13:29	Routing security framed as supply chain risk — the governance vocabulary that makes it actionable
15:56	Business impacts: outages, SLA breaches, customer trust erosion, man-in-the-middle exposure
17:05	CPD framework applied to routing security — Commitment, Preparedness, Discipline
20:09	Robachevsky maps the Cloudflare incident actors to the CPD pillars
23:31	Three practical recommendations: supply chain inventory, routing controls, provider selection criteria
25:51	Host synthesizes key governance actions: map the chain, embed criteria in procurement, board metric
28:15	MANRS explained — 1,300 networks, minimum baseline, MANRS Observatory continuous audit
28:21	MANRS+ — higher-grade certification, stricter requirements, DDoS mitigation, audit assurance

30:18	The chicken-and-egg problem: enterprise demand needed to ignite MANRS+ provider certification
30:18	Closing synthesis: the gap is governance, not technology — RPKI and MANRS already exist
32:07	Guest closing remarks — call for enterprise leaders to join the MANRS+ working group
32:50	Host closing remarks and final thanks

Memorable Quotes

"What they couldn't see — what none of their tools were designed to see — is that traffic flowing between their users and their services had been silently rerouted. Not by an attacker who broke through their defenses. By a failure at a network they had never heard of, in a country they had no operations in."
— Dr. Dave Chatterjee

"The routing system is at the foundation of the internet. And yet, because it's so foundational, it is below the radar. If something bad happens on the underlying routing fabric, it often manifests as some other type of incident — an outage, a performance degradation. By the time you get to the essence of the problem, the incident might already be gone. But the damage is done."
— Andrei Robachevsky, Technical Director, Global Cyber Alliance

"If you look at routing as a supply chain risk, you as an enterprise will have a much clearer approach to how you want to address this issue — not the same way a network operator or ISP would approach it from a purely technical perspective."
— Andrei Robachevsky

"Many routing incidents cause rerouting of traffic — traffic going via an unintended path — opening the door to man-in-the-middle attacks. So they erode your trust as well. Not having visibility into your supply chain is generally not considered a good thing."
— Andrei Robachevsky

"What is the single most important thing an enterprise should do about routing security? Map your routing supply chain. Identify every provider in the path between your users and your services. Ask each one for evidence of their routing security posture. You cannot govern what you haven't mapped."
— Dr. Dave Chatterjee

"Routing security will not improve without demand. And that demand has to come from enterprises. Define the standard rather than being the standard defined for you."
— Andrei Robachevsky