# Cyber-Security Myth

## Introduction

Although the Internet has made phenomenal advances during the last few decades, it remains fragile and vulnerable to attacks large and small to this day. Users are confused as to its convoluted workings and are often unable to distinguish between a hack by an intruder and a break in the protective software.

One such recent event occurred on 2025 November 18 when Cloudflare suffered a global outage that briefly broke a huge slice of the internet[1]. This was not an isolated incident. The previous one happened only eight months prior, and there were more before that. Similarly, Amazon Web Services (AWS) has been disrupted frequently[2]. This kind of Internet outage has become almost routine and the reliability of these services designed to defend against cyber intrusions has come into question.

## The Problem

The Internet's vulnerability has been an issue for decades. Last year, the Federal Communications Commission (FCC) issued a Notice of Proposed Rule Making (NPRM)[3] that identified the Border Gateway Protocol (BGP)[4] as the target for mitigating the risk. The Internet Architecture Board (IAB), representing the Internet community, responded with a comment expressing concerns[5]. Nevertheless, the White House published a Roadmap[6] which focused on the BGP integrity as the means to enhancing Internet routing security.

In this regard, it is important to bear in mind that the BGP is required to transport packets between Autonomous Systems (ASes)[7] that are selected by the Domain Name Server (DNS)[8], based on IPv4 addresses assigned to subscribers by the Dynamic Host Control Protocol (DHCP)[9], which was created to deal with the IPv4 address shortage. This protocol stack has resulted in a complex system architecture vulnerable to attack from many angles, each requiring another patch in response.

## The Solution

A flawed system invites a never-ending series of hacks and patches. A much more robust Internet can result from a simplified and streamlined architecture that eliminates the root-cause of IPv4 address shortages, thus negating the need for any of the above-mentioned four protocols. Such is the result of a deterministic system dubbed EzIP[10].

## Technology and Architecture Evolutions

When the Internet first started, well-defined large IPv4 address blocks were allocated to the five Regional Internet Registries (RIRs). For example, Hilbert curves[11] depicting earlier day AFRINIC (Africa), APNIC (Asia-Pacific), ARIN (North America), LACNIC (Latin America and Caribbean) and RIPE (Europe, the Middle East and Central Asia) allocations were easily discernable[12].

Although each RIR assigned its allocated addresses to Internet Access Providers (IAPs) within its own region, IAPs themselves were not required to observe the same restriction. This opened up the IP address fragmentation flood gate, allowing the physical location of a subscriber be not geographically associated with the region where the assigned IP address was originally allocated to.

As IPv4 address pool began to deplete, DHCP sustained IAP operations by dynamically reusing available public IPv4 addresses. DNS was then introduced to ease the burden on subscribers due to such an environment in constant flux. Since this protocol pair appeared to satisfy the urgent needs at the time, it became the default Internet building block. (See Footnote for the ramifications of this peculiar pairing.)

Upon early-adopter institutions agreeing to release surplus IPv4 address blocks for public auctioning to lessen the IPv4 address pool exhaustion pressure, it was no longer practical to expect an IPv4 address carrying any meaningful physical location information, let alone the possibility of geolocating a subscriber. A separate branch of the industry was born to serve this need. The resolution and accuracy of its reports, however, were often questionable at the best[13].

Along the way, IAPs possessing one or more IPv4 address blocks developed their respective IP packet delivery schemes. Address blocks sharing the same transport policy grouped together to form one AS. Since the range of each AS varies and is often limited, the BGP was relied upon to forward IP packets across the AS borders. As the number of ASes grew, so did the complexity of the BGP responsible for packets traversing any appreciable distance often just locally, not to mention those destined to global addresses having to cross multiple AS borders.

Although each of these protocols are inherently distributed, their operations do require significant coordination which relies on centralized efforts, leading to the dominance by a limited few resourceful businesses, such as Content Delivery Network (CDN)[14] operators which include Cloudflare, AWS, etc. These become the core infrastructure for the Internet transport facility.

## Contradictions

There are more than a handful of Internet practices that make its principles and operations confusing:

The Internet promotes leveling the playing field. But Vatican City gets 21.4 IPv4 address allocation per capita, while over a dozen entities receiving none, with other nations getting every possibility in between[15]. (Note: Seychelles having 58.4 allocation is an oddity, as the result of businesses taking advantage of the local political environment for global opportunities.)

The End-to-end connectivity was promised by the Internet. However, its current predominant operation model, CDN impedes such goal, even within a local community.

The Internet took issue with telco monopoly and government regulation on the Public Switched Telephone Network (PSTN). Yet, the Internet is now dominated by multinational conglomerates, practically monopolizing business sectors, respectively, to the point of ignoring responsibilities and evading regulations. Isn't this kind of centralization precisely opposing the distributed Internet vision?

Also, the potential of roughly 200 global jurisdictions fragmenting the Internet to become a geopolitical Splinternet[16] is being criticized by the Internet community, while the ASes have already made the Internet an Onion-net with at least 77K layers[7]. Furthermore, since most of ASes selectively serve only parts of the world, each layer of the onion peels resembles more like a partial fish net with holes in it!

The most puzzling fact is that the Internet vigorously defends its borderless principle, while its own primary routing mechanism has evolved to be BGP, where the "B" stands for the borders around each ASes!

Overall, due to the highly involved dynamic and distributed nature of these protocols, the Internet becomes susceptible to a wide range of malicious security breaches, from daily harassment to ransomware.

Perhaps it is prudent at this juncture to mention that somehow IPv6, without taking advantage of its own huge address pool, adopted these IPv4 practices evolved through interim needs. Now, the significance of IPv6 appears to be fading away quietly[17], while there is no more mention of the IPv4 phase-off date. Since IPv6 doesn't advertise any notable advantages over IPv4, most ongoing Internet discussions no longer distinguish between the two.

**References**


1. Cloudflare Outage History (2019-2025)
   https://controld.com/blothe/biggest-cloudflare-outages/

2. A History of AWS cloud and Data Center Outages
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. Reporting on Border Gateway Protocol Risk Mitigation Progress; Secure Internet Routing
   https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. Border Gateway Protocol
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. Comments of the Internet Society, Internet Architecture Board, and Internet Corporation for Assigned Names and Numbers in the Matter of "Reporting on Border Gateway Protocol Risk Mitigation Progress"
   https://datatracker.ietf.org/doc/statement-iab-comments-of-the-internet-society-internet-architecture-board-and-internet-corporation-for-assigned-names-and-numbers-in-the-matter-of-reporting-on-border-gateway-protocol-risk-mitigation-progress/

6. Roadmap to Enhancing Internet Routing Security
   https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. Autonomous system (Internet)
   https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

8. Domain Name System
   https://en.wikipedia.org/wiki/Domain_Name_System

9. Dynamic Host Configuration Protocol
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. A Deterministic Internet
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

11. Hilbert Curve

https://en.wikipedia.org/wiki/Hilbert_curve

12. Visualizing the IPv4 Space Using Hilbert Curves
https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. Internet Geolocation
https://en.wikipedia.org/wiki/Internet_geolocation

14. Content Delivery Network
https://en.wikipedia.org/wiki/Content_delivery_network

15. List of Countries by IPv4 Address Allocation
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

16. Splinternet
https://en.wikipedia.org/wiki/Splinternet

17. Geoff Huston: The Internet's Past, Present, and Future
(TM: 1:08:18, "IPv6 – Increasingly irrelevant")
https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

**Footnote**

The DHCP and DNS are the most mind-boggling Internet technology pair that has been flying at everyone's face for all these years. That is, DHCP promises individual privacy by assigning IP addresses to subscribers dynamically as needed, only to be immediately and totally negated by DNS that presents, upon request, whatever latest IP address assigned to a party, based on merely that target's identity anyway! These make ordinary subscribers ostriches with the false belief of being protected, while keeping a lot of IT engineers gainfully employed. This is a perfect example of the Chinese proverb, “Spear vs. Shield” (矛盾).

Nevertheless, additional layers of protocols based on this scheme proceeded to build up through AS, BGP to establishing CDN that enabled the multi-national conglomerate dominance, all the way to major services such as Cloudflare and AWS that promised to provide reliable packet transport with improved security. However, the robustness of these services has been in the spotlight often. And, when Internet was breached, no one seemed willing to assume the responsibility and to look for alternatives for reducing the vulnerability. Perhaps it was difficult to assign blames, because the whole Internet was so distributed?

On the other hand, the current Internet configuration is an ideal facility for a perpetrator who can simply assume any arbitrary fictitious IP address as a valid ordinary Internet subscriber to commence the attack, then abandons it afterwards, leaving hardly any permanent records with valid identity for forensic traceability.