The Internet Protocol Journal

December 2025 Volume 28, Number 3

A Quarterly Technical Publication for Internet and Intranet Professionals

In This Issue

You can download IPJ back issues and find subscription information at:
www.protocoljournal.org

ISSN 1944-1134

From The Editor

Security continues to be a major concern for both Internet users and technology developers. *Standards Development Organizations* (SDOs) such as the *Internet Engineering Task Force* (IETF) have approached security by developing new—or enhancing old—protocols. Examples include *Resource Public Key Infrastructure* (RPKI) for routing and *Domain Name System Security Extensions* (DNSSEC) for the DNS. But protecting and securing the collection of networks that comprises the Global Internet requires a comprehensive analysis of attack traffic patterns as well as a coordinated approach by network operators. Leslie Daigle of *The Global Cyber Alliance* (GCA) provides some examples of measurements from so-called "honeypot" networks and offers suggestions for ways to improve the response to cyber attacks.

The term "Internet Governance" emerged sometime in the mid-1990s to describe numerous existing and emerging administrative efforts to manage Internet resources such as IP addresses and top-level domain names. According to Wikipedia, Internet Governance is "...the effort by governments, the private sector, civil society, and technical actors to develop and apply shared principles, norms, rules, and decision-making procedures that shape the evolution and use of the Internet." The term "multistakeholder" is used to refer to the various parties involved in these activities. Like Internet Governance itself, multistakeholderism is subject to some debate. In this issue we bring you two opinion pieces on this topic. First, Geoff Huston provides some history and background and then asks if multistakeholderism has ended. Avri Doria responds with a counter-opinion and provides an overview of current efforts and future directions for multistakeholder approaches.

All 95 previous issues of this journal are available on our website. You will find two ZIP archives; one will expand to a folder with each individual issue, and the other will expand into a single PDF file with more than 3,600 pages. Our website also contains index files for each volume as well as a cumulative index file of all issues to date. Check out **protocoljournal.org** for more details.

—Ole J. Jacobsen, Editor and Publisher
ole@protocoljournal.org

Securing a Borderless Internet:

Observations from Global Attack Data and the Case for Collaborative Defense

by Leslie Daigle, Global Cyber Alliance

The Internet's continued expansion into every sector of society has elevated its importance and correspondingly heightened the impact of its vulnerabilities. As critical services move online, the Internet's loosely coupled, globally distributed architecture faces increasing pressure from malicious activity that exploits both technical weaknesses and operational inconsistencies between networks.

This article outlines several ongoing attack campaigns observed at global scale and the important consequences of this seemingly "innocuous" low-bandwidth traffic, and provides objective evidence in recent data collected from the *Global Cyber Alliance* (GCA)[0] honey farm. Discussion includes why traditional defensive measures such as geographic blocking are inadequate, and how collaborative approaches, including *Mutually Agreed Norms for Routing Security* (MANRS)[1,7], can be a model for improving resilience across the Internet's shared infrastructure.

The Internet's Security Challenge: A Structural Overview

The Internet is amazing, powerful, chaotic. And *absolutely impossible to secure alone*. Traditional approaches to security focus on curtailing reach and imposing restrictions. Whether applied at the national level through regulation, or at the organizational level by administrative blocking, those approaches fail to provide real security improvements, and they generally lead to inconsistent (non-interoperable) behavior.

A better target is "Internet integrity"—ensuring both security and accessibility across a resilient infrastructure.

Unlike closed, centrally administered systems, the Internet is an interconnection of independently operated networks. These entities cooperate voluntarily through shared protocols, routing policies, and operational conventions. The strength of this model lies in its openness, but its distributed nature also complicates coordinated security measures. The global mesh that gives us connectivity everywhere also creates a complex attack surface. Resources can be registered in one country, hosted in another, used in a third, and abused in a fourth.

Three characteristics are particularly relevant:

- *Jurisdictional Diversity*: The administrative domains responsible for registering IP resources, hosting infrastructure, and operating networks often reside in different countries. Attackers routinely exploit these jurisdictional discontinuities.
- *Operational Heterogeneity*: Network operators vary widely in maturity, staffing, automation, and security posture. This situation creates uneven defenses, producing opportunities for attackers to move laterally or launch global campaigns by abusing weaker networks.

- *Inherent Reachability*: The Internet's default is connectivity. With few exceptions, networks are reachable by any other network. This reachability is essential for global interoperability, but it provides attackers with immediate, worldwide access to potential targets.

Together, these factors make it impossible for any single operator to "secure the Internet" in isolation, or even secure their own resources. No network can ensure its own routing security, for example—networks must rely on their neighbor networks. Effective defense depends on consistent practices adopted collectively.

Insights from a Global Honey Farm

To better understand the operational realities of contemporary threats, the GCA maintains a network of roughly 200 honeypot sensors distributed across multiple regions. These systems present no advertised services; their purpose is solely to observe unsolicited traffic[2].

Despite their passive configuration, the sensors receive a continuous stream of probing attempts—ongoing, simultaneous interactions between networks spanning every continent. The volume and global distribution of this traffic demonstrate that unwanted scanning and exploitation attempts reach essentially all IPv4 addresses, regardless of geography or network size.

In discussing this "unwanted traffic" with network infrastructure operators, it is often dismissed as inconsequential, neither consuming undue bandwidth nor impacting their customers. In fact, analysis of this data reveals not only the scale of background noise on the Internet but also the presence of distinct, well-coordinated attack campaigns that have massive impact on real-life commercial and regional interests.

Here are four examples of campaigns that have had significant global impact, as seen from GCA's vantage points:

APT36

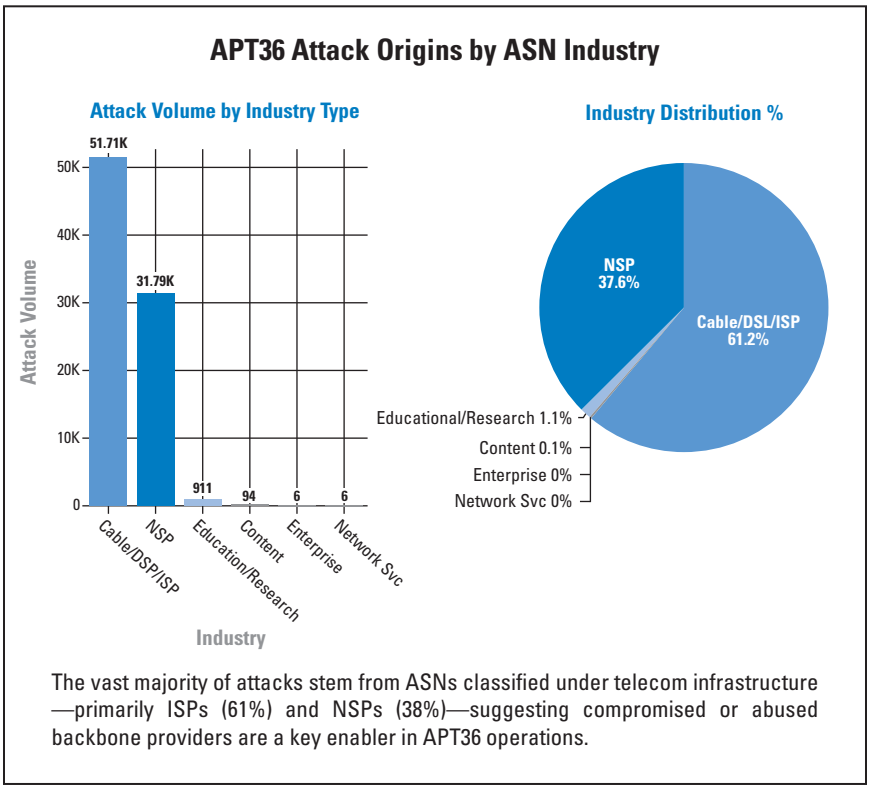
APT36 (*Transparent Tribe*) provides a clear example of how advanced persistent threat groups increasingly exploit legitimate telecommunications infrastructure to conduct operations in plain sight. Long associated with geopolitical espionage, the group is believed to be aligned with Pakistani state interests, and it typically targets Indian government and military entities through phishing, credential harvesting, and targeted malware delivery. While its activity has been observed for more than a decade, operations surged in 2025—first identified in external reporting and then independently confirmed through data from GCA's *Automated IoT Defence Ecosystem* (AIDE) platform.

AIDE supports multiple protocols, including *Secure Shell* (SSH), *Telnet*, *File Transfer Protocol* (FTP), *Hypertext Transfer Protocol* (HTTP), *Hypertext Transfer Protocol Secure* (HTTPS), and the *Simple Mail Transfer Protocol* (SMTP). Between April and August 2025, AIDE recorded 116,374 incidents on Indian sensors alone, originating from 75 *Autonomous System Numbers* (ASNs) based in Pakistan.

The breadth of this activity demonstrates that APT36 operations are neither localized nor opportunistic; instead, they rely on widely distributed *Internet Service Provider* (ISP) infrastructure to obfuscate origin, increase resiliency, and sustain long-running campaigns. Traffic attributed to the group appears globally across sensors, reflecting an architecture deliberately built to avoid geographical confinement.

AIDE data shows how APT36 leverages these networks to deploy multi-architecture malware, route attacks through legitimate providers, and take advantage of gaps in routing hygiene. This combination allows the group to operate at Internet scale while blending malicious traffic into ordinary global flows. See Figure 1.

Figure 1: APT36 Attack Origins by ASN Industry (Industry classifications sourced from PeeringDB)



The vast majority of attacks stem from ASNs classified under telecom infrastructure —primarily ISPs (61%) and NSPs (38%)—suggesting compromised or abused backbone providers are a key enabler in APT36 operations.

The implications extend well beyond technical routing anomalies: abuses of telecom and backbone infrastructure undermine trust in critical networks, create economic disruption, and contribute to rising geopolitical tension. What happens inside ISP and backbone networks ultimately affects hospitals, schools, businesses, and governments that depend on stable, secure connectivity. Strengthening routing security and addressing systemic weaknesses is therefore more than an operational best practice—it is essential for national security, regional stability, and the reliable functioning of the Internet as a whole. See [3] for more details about this campaign.

Red Tail

Cryptocurrency mining malware is often treated as background noise—malicious but largely inconsequential beyond wasted compute cycles. The *RedTail* campaign challenges that assumption. Financially motivated and attributed to infrastructure associated with the Lazarus Group, RedTail represents a sustained, multi-month crypto-mining operation that exhibits the persistence and sophistication more commonly associated with state-aligned activity than routine cybercrime.

Between February and August 2025, GCA's AIDE honeypot network recorded recurring RedTail activity, including pronounced surges in late April and again in July. Much of this traffic originated from legitimate ISPs, cloud-hosting platforms, and other network service providers, illustrating how abused or compromised infrastructure can be repurposed to deliver attacks at scale.

AIDE data shows that RedTail operators exploited known vulnerabilities, deployed custom binaries across multiple architectures, and maintained their infrastructure for months at a time. When attacker nodes are ranked by longevity rather than raw event volume, a consistent operational discipline emerges: some nodes remained active for nearly the entire 26-week observation period, others for 20–24 weeks, and even the shortest-lived persisted for more than 8 weeks. Maintaining infrastructure for this duration requires resource investment, coordination, and an ability to operate across multiple networks without rapid takedown—traits that align with state-sponsored operations.

The campaign also reflects known Lazarus Group tradecraft. Recent operations—including the $1.46 billion Ethereum theft from *Bybit* and the earlier *AppleJeus* malware distribution campaign—demonstrate the group's capacity for financially motivated attacks executed with speed, scale, and cross-platform capability. RedTail's deployment of multi-architecture malware and its dependence on private mining pools for monetization mirror these patterns, reinforcing the assessment that the campaign sits well above typical crypto-mining activity in sophistication and strategic intent.

Although AIDE captures attacks in controlled environments, the concentration of RedTail activity targeting sensors in India, Australia, and Singapore—nearly 40 percent of its global footprint—suggests that real-world networks in major financial and technology hubs would face similar exposure. The phased lifecycle of the campaign, spanning reconnaissance through escalation and sustained exploitation, underscores the fact that crypto mining at this level is not merely an operational nuisance. It is a strategic risk: long-running, resource-intensive campaigns that leverage legitimate network infrastructure can degrade provider networks, impose economic costs, and contribute to broader geopolitical and financial instability. See [4] for more detail.

Kimsuky

Kimsuky represents another example of how state-aligned actors exploit global infrastructure to support persistent, policy-focused espionage. Widely assessed in open-source reporting, including analyses by the *Cybersecurity and Infrastructure Security Agency* (CISA) and The MITRE Corporation, to be associated with North Korean intelligence collection, the group is known for targeting diplomats, researchers, policy institutes, and think tanks in South Korea, Japan, and the United States. These organizations often lack high-assurance security postures, making them attractive targets for actors seeking strategic or policy-relevant information.

Kimsuky's operations commonly involve social engineering, spear phishing, reconnaissance activity, credential theft, and the deployment of custom malware families such as *BabyShark* and *AppleSeed*. Although some threat intelligence providers characterize the group as state-directed, this attribution stems from external assessments rather than any conclusions drawn from our own data. What can be confirmed is the pattern of behavior: a sustained interest in research institutions and policy environments, combined with a resourceful approach to global infrastructure use.

AIDE data illustrates this infrastructure strategy clearly. While some traffic originates from Asia-Pacific economies consistent with the group's primary targets, the highest volumes are associated with offshore hosting, with Panama-based services leading, followed by infrastructure in the United States, United Kingdom, and Germany. This strategy reflects a deliberate preference for leveraging non-APAC providers to obscure operational footprints and complicate attribution. This approach is aligned with external reporting on Kimsuky's 2024 "forceCopy" campaign, which relied heavily on offshore *Virtual Private Server* (VPS) nodes to evade takedowns.

The resulting geographic distribution underscores a broader trend: threat actors increasingly route operations through diverse, globally distributed infrastructure to bypass regional controls and extend campaign longevity. In Kimsuky's case, this approach enables sustained espionage activity against organizations whose missions intersect with national policy and international security, yet whose defensive resources are often limited. For more information, see [5].

Dark Pink

The *Dark Pink* campaign illustrates how modern cyber espionage operations rely on globally distributed infrastructure to sustain persistent targeting of governmental and military systems. Public reporting since 2022—beginning with Group-IB's initial analysis—has used the "Dark Pink" label to describe activity aimed at government, defense, and education organizations across Southeast Asia, including Cambodia, Indonesia, Malaysia, the Philippines, and Vietnam.

External researchers have characterized the group's behavior as consistent with long-term strategic access operations. CrowdStrike has further linked Dark Pink to an earlier activity cluster known as *Ocean Buffalo*, which it associates with Vietnam-originated domestic surveillance that later expanded internationally. These associations, however, reflect external assessments rather than conclusions derived from GCA's own data.

AIDE observations align with the narrative of an evolving campaign that continues to broaden its operational footprint. While Dark Pink's historical focus lies in Asia Pacific, AIDE data shows that much of the infrastructure used to stage activity now resides outside the region. Of all sessions attributed to the campaign, 47 percent originated from European networks, followed by 33 percent from Asia Pacific and 19 percent from the United States. This distribution suggests that even if the operators of the campaign began by targeting organizations within Asia Pacific, they have increasingly shifted to European and North American hosting to obscure the origins of their operations, improve reach, and complicate defensive analysis.

Operationally, Dark Pink exhibits a wave-like pattern: periods of low activity punctuated by concentrated bursts of probing and exploitation attempts, particularly against military and governmental systems in Indonesia, the Philippines, and Malaysia. The reliance on staging infrastructure across Europe and North America reinforces the broader trend seen across multiple campaigns: attackers use globally dispersed hosting and service providers to mask activity, evade localized defensive measures, and sustain long-duration operations aimed at high-value targets. For more details, see [6].

Why Geographic Blocking Fails

Whether the full scope of the nature of attack campaigns is understood or not, anyone connecting to the Internet today must engage in some level of defensive posture toward attack traffic.

In response to increased malicious activity, some organizations apply coarse filtering, such as blocking entire regions or countries. Honey farm observations suggest that such approaches offer limited security benefits for several reasons:

- *Attack traffic is globally distributed*: Even region-specific campaigns employ infrastructure across multiple continents. Blocking by geography frequently misses the actual sources.
- *Legitimate infrastructure is commonly abused*: A significant proportion of unwanted traffic originates from compromised hosts within well-established ISPs and cloud providers. Blocking these networks would be operationally unacceptable.
- *Blocking introduces negative externalities*: Users accessing services from abroad may be inadvertently denied access, despite legitimate need. Furthermore, over-blocking can encourage brittle application behavior and complicate troubleshooting.

- *Outbound traffic may be the real problem*: Networks can inadvertently source attacks if customer equipment becomes compromised, thereby harming the reputation of the network and, in some cases, the valuation of its IPv4 address space.

Geographic controls do not address the fundamental problem: inconsistent operational practices across networks.

The Hidden Cost: The Reputation of Your Network

Attack traffic doesn't just consume bandwidth or CPU cycles. It degrades the reputation of the networks it comes from. IPv4 space that becomes associated with malicious behavior loses value. Connectivity providers may quietly de-prefer your IP address ranges. Security vendors may red-flag your AS.

Collaborative Security: A Path Forward

Given the structural characteristics of the Internet, meaningful improvements in security require coordinated operational norms. The MANRS initiative provides a useful model[1,7].

MANRS defines a baseline of routing-security actions, such as filtering incorrect announcements, validating route origins, and coordinating incident reporting. Crucially, these norms were developed in consultation with operators rather than imposed externally. Data from the *MANRS Observatory* shows:

- Steady growth in participating networks,
- Increasing deployment of *Route Origin Authorizations* (ROAs), and
- A decline in observed routing incidents and misconfigurations.

These trends demonstrate that collaboratively defined practices can measurably improve global routing hygiene.

The success of MANRS suggests a broader lesson: operational security challenges are best addressed by communities of practice within the network operator ecosystem. When operators adopt common standards and coordinate responses, they reduce the attack surface not only for themselves but also for the entire Internet.

Conclusion

The Internet is not a monolith. It is a collective artifact shaped by millions of networks, thousands of operators, and countless decisions made every day. Its vulnerabilities are shared. Its strengths are shared. And its future depends entirely on whether collaboration remains its guiding principle.

The Internet's openness and global reach—qualities central to its success—also expose it to sustained, globally distributed malicious activity. Data from GCA's honey farm illustrates the breadth of these threats and the degree to which attackers exploit legitimate infrastructure across many regions.

Traditional defensive strategies such as geographic blocking are insufficient and may introduce new risks. Instead, improving the security of the Internet requires coordinated action among network operators. Initiatives like MANRS demonstrate that voluntary, consensus-driven norms can lead to measurable improvements.

Security cannot be achieved through panic or isolation. It must come from coordinated action, shared norms, and a willingness to confront uncomfortable truths about the role our own networks play.

As the Internet continues to evolve, its security will depend on sustained collaboration among the networks that collectively operate it. No single organization can secure the Internet, but together, operators can significantly reduce the scale and impact of malicious activity across the global ecosystem.

References

[0] The Global Cyber Alliance: **https://globalcyberalliance.org/**

[1] Andrei Robachevsky, "Improving Routing Security," *The Internet Protocol Journal*, Volume 22, No. 2, July 2019.

[2] AIDE: **https://gcaaide.org**

[3] APT 36: **https://globalcyberalliance.org/aide-data-apt36/**

[4] Red Tail: **https://globalcyberalliance.org/aide-data-redtail**

[5] Kimsuky: **https://globalcyberalliance.org/aide-data-kimsuky/**

[6] Dark Pink: **https://globalcyberalliance.org/aide-data-darkpink/**

[7] Mutually Agreed Norms for Routing Security (MANRS): **https://manrs.org/**

LESLIE DAIGLE is the Chief Technical Officer & Internet Integrity Program Director of the Global Cyber Alliance. She is responsible for the technology strategy that advances GCA's development and deployment of global solutions. She also leads the Internet Integrity Program, which focuses on working with Internet infrastructure operators to improve the security of the Internet as a whole. Leslie was previously the Internet Society's first Chief Internet Technology Officer, when she helped to (re)create the global dialog on important technical issues, calling stakeholders to action by providing achievable targets and facilitating their own collaboration across (corporate) organizational boundaries. Leslie is co-founder and co-host of the *TechSequences* podcast, which explores the many facets of Internet technology, along with its intended (and sometimes unintended) consequences. E-mail: **ldaigle@globalcyberalliance.org**

Opinion: The End of Multistakeholderism?

by Geoff Huston, APNIC

When the Internet outgrew its academic and research roots and gained some prominence and momentum in the broader telecommunications environment, its proponents found themselves to be opposed to many of the established practices of the international telecommunications arrangements—and even opposed to the principles that lie behind these arrangements. For many years, governments were being lectured that the Internet was *special*, and to apply the same mechanisms of national telecommunications and trade regulations to the Internet might not wreck the entire Internet, but they would surely isolate the nation that was attempting to apply these measures.

Within this broad category was the notion that conventional means of conducting trade in services were not applicable to the Internet. While an early mantra of "The Internet must be free!" quickly foundered when it encountered pragmatic realities of trying to pay the bills, the next mantra of "Don't tax the Internet!" gathered significant momentum. What was meant here was an admonition to governments not to attempt to unduly constrain the flow of data with taxes and related imposts, as such actions applied carelessly would likely imperil the future value of the Internet. This situation offered a unique opportunity to take the role of public communications away from the sclerotic and bloated telephone monopolies and apply some of the vibrant innovative energy that was driving the computer industry into the communications realm.

WSIS

But while the Internet might have had some claim to exceptionalism in the 1990s, such a characterisation was unsustainable in the longer term. It was clear by the time of the millennium that the previous regime of national telephone operators and the treaties that governed the international aspects of this global service had been sidelined. The Internet was sweeping all before it, and each time it engaged with another sector it appeared to emerge from the encounter as a clear victor. The Internet might still be exceptional, but by the year 2000 people recognised that it was not always exceptional in a good way. In 2003 and 2005, the *United Nations* (UN) hosted the two-part *World Summit on the Information Society* (WSIS)[1] to try to help nations accept these changes, and ideally to ensure that all economies would benefit from this revolution in computing and communications.

This WSIS summit was in the context of the emergence of the so-called "Information Society" and a recognition of a widening *Digital Divide*, where richer nations were in an obvious position to exploit the possibilities that became apparent with the combination of abundant computation and communications services—and thereby amass further wealth—while poorer nations yet again found themselves on the other side of the divide.

Far from being a tool to help equalise the inequities in our world by allowing all to access information, education, and open global markets for their services, the Internet appeared to be yet another tool to further entrench this divide between rich and poor.

The United States was a focal point in these discussions. At the time the Internet was still strongly associated with the United States, and the US had spent much of the previous decade both promoting its benefits and profiting from the revenue flowing into US companies that were early adopters of Internet-based services. This promotion of the Internet and the free flow of information was certainly not without elements of self-interest on the part of the US, as it appeared that the interests of the newly emerging corporate behemoths of the Internet and the geo-political and geo-economic aspirations of the US appeared to have much in common.

However, it's often difficult to tackle the larger picture in these large-scale international forums, so it was no surprise to see attention turn to the individual elements that were contained within this picture. One of these elements that became a topic of discussion in its own right was the status of the body that oversaw the protocol parameters of the Internet—including the names and IP addresses that are used as part of the central core of the Internet. This oversight, implemented by the *Internet Assigned Numbers Authority* (IANA)[2], was originally part of the activities that the US *Defence Advanced Research Project Agency* (DARPA) funded. After a few more changes within the US Government agency landscape, responsibility for this function was shifted to a self-funded model operated by a private sector entity, the *Internet Corporation for Assigned Names and Numbers* (ICANN)[3], with some level of US engagement remaining in place. This setup was variously portrayed as a control or as a safeguarding measure. Irrespective of the nature of the motivation, the result was that the *National Telecommunications and Information Administration* (NTIA)[4], part of the US Department of Commerce, oversaw a contract between the US government and ICANN regarding the operation of the IANA function.

Perceptions matter, and the lingering perception here was that the Internet was still essentially under the control of a single sovereign state, the United States.

This unique US role was always going to be a problem for other nations. The international telephone and postal networks were governed by international treaty instruments that had been in place for more than a century. To have a single nation state positioned at the apex of this Internet structure was—to say the least—controversial. Naturally this topic was a major one in 2003 at the first WSIS gathering. The UN Secretary General at the time, Kofi Annan, convened a *Working Group on Internet Governance* (WGIG)[5], a grand title that either conflated this topic to an even greater level of prominence or appropriately stated its central importance to the entire set of concerns with the structure of the Internet at the time.

Again, opinions vary here. No clear consensus came out of this WGIG activity, and the 2005 WSIS gathering could not reach any form of agreement on this matter either.

Internet Governance Forums

During the WSIS process the US apparently refused to consider any changes to its pivotal role in the management of the protocol parameters of the Internet. The WSIS summit eventually agreed on a compromise approach that deferred any determination on this matter and instead decided to convene a series of meetings to discuss the underlying policy principles relating to Internet Governance. We saw the inauguration of a series of *Internet Governance Forum* (IGF)[6] meetings. These forums were intended to be non-decisional forums for all stakeholders to debate the issues. Originally intended to be convened for a period of five years, culminating in the fifth IGF meeting in Vilnius, Lithuania, in 2010, it has continued with a further five-year extension of its mandate, and then a ten-year extension, culminating with the recent IGF meeting in Norway at the end of June 2025.

Even within its limited objectives of being a forum for little other than discussions, the IGF found it challenging to claim universal success in achieving its mission. The IGF did not manage to address the underlying tensions relating to the pivotal position of the US in the Internet. In 2011 we saw the *IBSA* proposal (called IBSA because it came from a summit convened by India, Brazil, and South Africa) for a UN committee in Internet Related Policy. In 2013, as a reaction to the US surveillance stories being publicly aired on *WikiLeaks*, numerous Internet organisations, including ICANN, the *Regional Internet Registries* (RIRs)[7], and the *Internet Engineering Task Force* (IETF)[8], released the "Montevideo Statement," calling on the US to step back from its central role. The US surveillance disclosures also appeared to be a major factor in Brazil's sponsorship of the 2014 *NetMundial*[9] initiatives, which also appeared to have the support of ICANN. Once more the call was for the cessation of US control over the protocol parameter function of the Internet. At much the same time Edward Snowden released a set of materials that documented how US agencies were undertaking widespread surveillance by using the Internet.

These WikiLeaks and Snowden disclosures weakened US resolve, and in October 2016 the previously unthinkable happened: The US Government signed away its functional role and passed control of the protocol parameter function to an independent ICANN.

If the IGF was the forum to discuss the public policy issues related to the privileged position of the US Government with respect to the Internet, then the principal rationale for the IGF also finished in October 2016. In theory, at any rate, the US no longer claimed the ability to place its finger on the scale with respect to the carriage of these matters.

On the other hand, this definition of the role and scope of the IGF is perhaps far too narrow. The IGF process has managed to gather a more sophisticated shared understanding of the layers within the Internet and the ways in which these various components both share common objectives and create tensions when competing to achieve similar objectives. The elements of carriage networks, consumer devices, servers and service delivery networks, applications, and application behaviours all operate in a semi-autonomous manner. The previous model of the locus of control of an entire service environment sitting within the telephone company within each nation state was not repeated with the Internet. The Internet has exposed each of the various component service activities as discrete activities, and instead of orchestrating these components within the framework of the procurement processes of the larger service entity, a variety of new markets have been exposed. Technology standards, fibre and mobile services, and computers in all forms from handsets to servers, applications, service providers, and content publishers all operate semi-autonomously, and the orchestration of their actions is through markets and market interactions. The Internet is not operated by a single service delivery company, nor is it a defined destination; it is a series of inter-twined markets. The implication for governance processes was profound, and the IGF has managed to both expose these changes and steer a constructive path of commentary and dialogue on these changes as they have happened.

Internet Governance Today

I'd like to nominate three major themes of national and international interest in today's Internet that have some relevance to the topic of Internet Governance.

The first is the issues that can still be summarised as the *Digital Divide*. The haves and have nots still exist across the full spectrum of our world. The digital divide is as big as it ever was, and there is no visible movement in directions that might ameliorate the societal impacts of these changes. If anything, the scope of this divide has further broadened. In absolute terms it may be that more individuals have some form of Internet access than was thought could possibly be achieved even 10 years ago. But today that's still only half of the world's population, and the other four billion people remain isolated from the mainstream. The divide also operates across other dimensions, including the cost of access; the quality and speed of access; the accessibility of information; and the extent to which goods, services, and information are accessible using a local language. They all form both subtle aspects and not-so-subtle aspects of digital exclusion.

But when we talk of a digital divide, we can broaden our view and look at the position of the world's most valuable digital enterprises, namely Apple, Microsoft, Nvidia, Amazon, Alphabet, and Meta, which have a market capitalisation of some 12 trillion USD (just before the recent Trump-induced stock meltdown).

The aggregate position of these six enterprises is so substantial and so powerful that everybody else—individuals, corporations, and most governments—find themselves on the impotent side of this digital divide.

The second theme is also not new, but it has dramatically increased in importance in the past two decades. Its components have various labels, including Cyber Security, Malware, Abuse, Spam, and Viruses. It can be summarised in the observation that today's Internet is a toxic place that provides haven not only for various criminal and fraudulent activities but also for darker actions encompassing the current set of concerns relating to terrorism and cyber-offensive tactics from state-based actors. The uncomfortable observation is that technology-based countermeasures may be failing us, and the fabric of our society seems to be very vulnerable to concerted hostile cyberattacks. We've adopted strong encryption in many parts of the environment as a means of protecting users against various forms of organised surveillance, but in so doing we've turned off the lighting that would otherwise expose various acts of malfeasance to our law enforcement bodies. We have had to make some tough decisions about balancing personal privacy and open attribution. But this lack of clear attribution and greater ability to embed communications behind strong encryption means that various forms of policing the digital world have become expensive, frustrating, and ultimately very selective in their application. Some also have observed that these digital megaliths have made vast profits from their dominant position, while at the same time they have managed to transfer the costs of large-scale deployment of poor-quality software and tools back on the public sector.

The third theme lies within the changes occurring within the Internet itself. In recent years we've seen the proliferation of *Content Distribution Networks* (CDNs)[10, 11] that attempt to position all of the data and services that any user might request as close as possible to the user. It used to be the role of the network to bring the user to the content portal, but now we are seeing content shifting itself ever closer to the user. In and of itself that's a relatively significant change to the Internet. The public carriage component of the Internet is shrinking and being replaced by private feeder networks that service these rapidly expanding CDNs. The bigger question concerns the residual need for global names and addresses in this CDN-centric environment. The Internet is no longer a telecommunications network that carries user traffic across a common network. Today's Internet is a content distribution network that is very similar to a television broadcast network where the transmission component is limited to the last-mile access network. The essential difference here is that on the Internet each user can define their own program.

One possible response to these concerns is the perception that these situations are instances of collective failure of the Internet Governance framework. Allowing the private sector unfettered control of the public communications space has produced very mixed results.

Yes, the obsessive concern with catering precisely to what users want has produced a remarkably efficient and capable supply chain that can bring the economies of massive scale to market of a single unit, and it is a modern-day marvel. But at the same time the private sector is largely uninterested in the general health and welfare of the larger environment, and the Internet appears to be the victim of such collective neglect.

The public sector's forbearance with the cavalier attitude that various Internet players show may be reaching a breaking point. The EU initiative with *General Data Protection Regulation* (GDPR)[12] is a clear signal that the honeymoon with technology is over, and various national regimes clearly want to see a more responsible and responsive attitude to public concerns from these players. Doubtless we will continue to see fines being set at levels intended to be eye-watering for even the largest of players. While this measure has the unintended side effect of eliminating the smaller players from the market and potentially stifling competition, a major public sector goal is to bring some sense of broader social responsibility back to the major players. This regulatory stance will no doubt continue in both the EU and in many other regimes.

But is this increased national engagement a failure of the Internet Governance framework or a failure of a more conventional role of public sector regulation of a market? Private corporate entities have a primary duty to their shareholders, and they do not necessarily have the same over-arching obligation to the public good. If self-interest and public interest coincide, then that is a wonderful coincidence of fortune, but when they differ, corporate self-interest necessarily wins. It is naive to expect the private sector to heed any messages of constraint and prudence unless it has the authority of regulatory impost with some form of punitive enforcement measure.

If governments are feeling emboldened to enact regulatory measures for an industry that until now has enjoyed some level of immunity from conventional social responsibilities, then how do these same governments feel about the actors that look after the elements of Internet infrastructure?

Rebuilding National Barriers

The recent erratic moves by the US President to initiate a trade war on a global scale will have far-reaching implications far beyond stock markets and will inevitably include the digital world and what we refer to as Internet Governance. The US moves on the unilateral imposition of tariffs can be interpreted as a vote of no confidence in global trade and open markets—and a resurgence of a theme of strategic national self-reliance in all areas of economic activity, including the digital realm.

The question, of course, is how will others react?

Recently I saw a notice from a DNS hosting provider that relates to hosting Russian domain names:

> "We are contacting you about a recent communication from the Russian Federal Service for Supervision in Communications and Information Technologies and Mass Media (Roskomnadzor).
>
> This message relates to the potential future restrictions on foreign hosting providers and the need for domain administrators who use foreign DNS infrastructure to transition to Russian hosting providers listed in the official register."

Many national regimes are visibly concerned about the large amounts of their digital infrastructure that foreign enterprises are operating, and by "foreign" it is more often than not simply "US."

Today's deregulated digital communications environment is held together by commercial contracts. The extent to which such arrangements can be torn asunder by seemingly erratic US presidential edicts no doubt causes many to lose sleep! In a bad-case scenario, can these US entities be coopted to hold a country's digital infrastructure hostage as part of the "art" of a national trade deal? In the extreme worst-case scenario, can these entities be forced to operate in an overtly hostile and disruptive manner in terms of services provided to foreign entities? What happens in a modern national digital economy when its infrastructure underpinnings are deliberately sabotaged by such entities acting under duress from some form of executive order?

The order in which we operate the Internet today is held apart from the conventional treaty body for communications, the *International Telecommunication Union* (ITU)[13]. The reason is that President Clinton in the late 1990s led a coalition of friendly economies, notably Australia, Canada, Japan, and the EU, to support the move to recognise a private institution to perform the allocation and administration functions for Internet infrastructure elements (notably names and addresses) based on what we came to call "multistakeholderism." The US recognition of this form of industry self-regulatory governance was more like an insubstantial veneer for many years, as the US administration (in the guise of the *National Telecommunications and Information Administration* (NTIA) within the Department of Commerce) performed an oversight role of the root zone of the DNS in the background. However, as we've already noted, the US administration withdrew from this oversight role around a decade ago and has largely disengaged, being unwilling to continue to pay the diplomatic price of being the backstop in holding this coalition together in the face of large-scale devaluation of US international diplomatic capital by the WikiLeaks and Snowden incidents.

You could argue that by 2020 the job was done in any case. The "value" of the Internet was tightly held by a small elite of truly massive US enterprises, and any role of the US administration to support these enterprises in the international realm was no longer necessary. Other countries have been willing to go along with these arrangements for a variety of reasons—one is the ill-defined promise of digital prosperity and that other national communities could benefit from this shift to digital infrastructure.

But the distribution of wealth and social power in this "new" world is vastly different from the old industrial world. Having valuable digital enterprises domiciled in a nation does not translate to widespread economic prosperity. The digital enterprise does not rely on large workforces, and the immense concentration of wealth often results in inventive efforts to avoid conventional forms of corporate taxation by the state. The problem is that the distribution of this digital wealth is very uneven, and while a small clique of individuals may live in an extreme level of opulence, large proportions of domestic populations are disenfranchised and marginalised.

Not unsurprisingly, we are now seeing a response to this situation, in the form of a wave of populism gaining social power in many national communities: not just in the US, but in Germany, France, Hungary, the UK, and other western economies. Such populism is based in part on restoring an old-world order that "protects" national economies and eschews many forms of globalism.

At the moment this situation is being expressed in various ways in a visible shift to national compartmentalism, not only in limiting the cross-border flow of physical goods through the imposition of punitive tariffs, but also in the efforts to contain digital assets and infrastructure roles to national entities domiciled within national boundaries.

Obviously, this situation does not look good for the Internet. It is increasingly likely that we will return to an order where international dealings are strictly defined by using a myriad of regulations overseen by treaty-based organisations. It's extremely challenging to espouse the benefits of an open multistakeholder global communications environment when the dream has been so basely corrupted by the exploitative excesses of the small clique of digital megaliths.

The year 2025 is particularly challenging when WSIS+20 is reopening the basic debate about the merits of multistakeholderism. "National Internet Sovereignty" is a powerful meme these days, and multilateralism, as compared to multistakeholderism, has a seductive appearance of addressing demands for greater levels of national autonomy, particularly in communities where populism is a dominant social force. This debate is taking part in an environment when the change in the stance of the US administration has effectively scrapped all the old order.

It is unclear as to how (or even whether) the US will continue to expend efforts to support multistakeholderism, and the erratic record of the US on the recent topic of tariffs lends further credence to the stance that the US is no longer a widely trusted and stable advocate of the benefits of multistakeholderism in the international realm.

In mid-2024 we saw efforts by other national entities, *.au Domain Administration* (auDA) for **.au**, *Canadian Internet Registration Authority* (CIRA) for **.ca**, *InternetNZ* for **.nz**, and *Nominet* for **.uk** to create a coalition to speak up for multistakeholderism: A *Technical Community Coalition for Multistakeholderism* (TCCM)[14] is evidence of others attempting to fill this clear gap. Notable is the absence of the US.

I wish this group well, but it is extremely challenging to make the case that today's international climate is in their favour. Given the significant problems in cyber vulnerabilities, the entrenched position of US megalithic digital corporates, and the extremely erratic position of the US administration at present, the case that the ideals of the Internet that were espoused in WSIS some 20 years ago, and the promises of multistakeholderism in the development of digital economies where everyone benefits are still realistic prospects today is extremely hard to make. It's far easier to observe that we gave it a try and Alphabet, Microsoft, Amazon, and Meta should be grateful to us for enabling their rapid rise to global dominance.

To come?

I can't help being very pessimistic about the coming years. The attempt to coopt private enterprises to work in a manner that safeguards the public interest in our common public telecommunications realm has failed, again. It reminds me of Theodore Vail's efforts in the early 20th century to come to an understanding with the US Congress to bestow on AT&T a monopoly in national telephone services in exchange for an undertaking that the company would act with restraint as an enlightened private sector entity that would act in the national public interest[15]. As it turned out, AT&T could not resist itself from exploiting its monopoly position for any more than a decade!

It looks like national pressures are calling for an end to multistakeholderism in Internet Governance, hastened by a tectonic shift in the position of the US in international circles. The most likely direction we will now pursue in Internet Governance is a shift to multilateralism and an increased role for the United Nations and the World Trade Organisation for the middle-ranked nation states, accompanied by a tumultuous period of US unilateralism.

Is this situation caused only by the outcome of the 2024 US Presidential election? If there had been different candidates and a different election outcome, would the position we find ourselves in today be materially different?

It seems to me that there are much larger social forces at play that transcend individuals and their actions, however erratic they may be! We are embarking on changes in our society that are as dramatic—and even as traumatic—as the industrial revolution of the nineteenth century. Such revolutions leave a trail of social dislocation and uncertainty in their wake, and this information revolution is no exception. It is perhaps unsurprising that nation states tend to be more assertive in such situations as they try to mitigate some of the worst excesses of such social disruptions. One side effect of this increasing nationalistic stance is that various international institutions, both regional and global, tend to be regarded with increasing levels of distrust from these national regimes and from populist national fora. In times of uncertainty and stress, nations naturally try to raise the drawbridge and attempt to insulate themselves from such disruptions by asserting greater levels of control within their own national realm. The root cause of all social dislocation is attributed to the actions of foreign bodies, and they claim that greater levels of national determinism will restore some aspect of a myth of prior national greatness and prosperity.

The industrial revolution was certainly triggered by the refinement of the steam engine, but the social revolution was far larger in scope than the invention of a simple mechanical device. In a similar line of thought, maybe it's not the Internet or its governance that lies at the heart of many of today's problems. Maybe it's the broader challenges of our enthusiastic adoption of computing and communications that have formed a propulsive force for widespread social dislocation in today's world.

Disclaimer

The views expressed in this opinion piece do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

Further Reading

[1] World Summit on the Information Society (WSIS): **https://www.unesco.org/en/wsis**

[2] Internet Assigned Numbers Authority (IANA): **https://www.iana.org/**

[3] Internet Corporation for Assigned Names and Numbers (ICANN): **https://www.icann.org/**

[4] National Telecommunications and Information Administration (NTIA): **https://www.ntia.gov/**

[5] Château de Bossey, "Report of the Working Group on Internet Governance," June 2005, **https://www.wgig.org/docs/WGIGREPORT.pdf**

[6] Internet Governance Forum (IGF): **https://www.intgovforum.org/en**

[7] Daniel Karrenberg, Gerard Ross, Paul Wilson, and Leslie Nobile, "Development of the Regional Internet Registry System," *The Internet Protocol Journal*, Volume 4, No. 4, December 2001.

[8] *The Internet Engineering Task Force* (IETF): **https://www.ietf.org/**

[9] NetMundial Initiative: **https://netmundial.br/2014**

[10] T. Sridhar, "Cloud Computing—A Primer: Part One," *The Internet Protocol Journal*, Volume 12, No. 3, September 2009.

[11] T. Sridhar, "Cloud Computing—A Primer: Part Two," *The Internet Protocol Journal*, Volume 12, No. 4, December 2009.

[12] European Commission, "Data Protection in the EU," **https://commission.europa.eu/law/law-topic/data-protection_en**

[13] International Telecommunication Union (ITU): **https://www.itu.int/**

[14] A Technical Community Coalition for Multistakeholderism (TCCM): **https://www.tccm.global/**

[15] Wikipedia article: "Theodore Newton Vail," **https://en.wikipedia.org/wiki/Theodore_Newton_Vail**

GEOFF HUSTON AM, B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region. He has been closely involved with the development of the Internet for many years, particularly within Australia, where he was responsible for building the Internet within the Australian academic and research sector in the early 1990s. He is author of numerous Internet-related books, and was a member of the Internet Architecture Board from 1999 until 2005. He served on the Board of Trustees of the Internet Society from 1992 until 2001. At various times Geoff has worked as an Internet researcher, an ISP systems architect, and a network operator. E-mail: **gih@apnic.net**

Counter-Opinion: Multistakeholderism Is Not Ending; Rather, It Is Moving to a Next Stage

Avri Doria, Technicalities

Multi-stakeholderism is not ending, but the honeymoon is over. No more handwaving about what multi-stakeholderism, also written as multistakeholderism, is and what it isn't—without a deeper dive and a few definitions. However, as is so often the case in *Internet Governance*[1], where we cannot even all agree on how to write relevant terms like "multistakeholderism," we cannot agree on how to define them either. I will try to indicate the definitions I choose to use as I go along. Accounting for the fractal nature of definition, where every word used blossoms into its own definitional frond, I will endeavor to be frugal.

Multistakeholderism, a History

I define the term multistakeholderism as: the study and practice of participatory models in decision making. These participatory models are often referred to as *multistakeholder models*, though other terms are sometimes used. I think that both the understanding and use of participatory models in decision making are the keys to the origin story of the Internet. As I expect that Geoff[0] is not making any claims about the study of such models, I will concentrate on the use and abuse of multistakeholderism in the Internet[2]. In some ways I believe he is referring more to a general multistakeholder environment that existed before and that can be seen as no longer existing. While the environment in 2025 is not that of the 1970s, neither the advent of TCP/IP, nor that of 2005—the time at which the *World Summit on the Information Society* (WSIS) agreed on the *Tunis Agenda*—nor even the same as it was in 2014 around the time of *WSIS+10*, I believe the opportunities for multistakeholder models of governance remain in the present and are increasing. Not only is the study of multistakeholder models increasing, but the applications of multistakeholder models and methods are increasing as well. The environment is one in which discussion of multistakeholder methodologies is growing despite the number of people claiming to "no longer believe in multistakeholderism." This disbelief applies not only to the digital divide, cyber security, and the spread of governance to other layers of Internet technical policy such as content, but it also applies to any and all decisions that need to be made in dealing with the Internet and Internet technologies, whether global, regional, or local.

I think Geoff gives a very good description of one perspective, a political perspective, on the history of Internet Governance and its relation to the term multistakeholderism.

I have no real disagreement with the coherence of that description, and will not offer an alternative political perspective as counter balance, though there are several ways of looking at the history of Internet Governance, possibly enough for a full semester's study on the subject of history and philosophy of Internet Governance; practically everyone I discuss the issue with has a somewhat different view of the history, depending on their perspective. I am more concerned with the interpretation of where the application of multistakeholder models to Internet Governance is at the moment and where it is headed. Beyond the technology itself and activities that the Internet enables, it is the sustainability and evolution of multistakeholderism, with its methods and modalities for finding consensus among nations and the stakeholders of the Internet, that seem most important.

In one sense, I agree with Geoff, that the laissez-faire multistakeholderism that rejects "kings, presidents, and voting"[3a, 3b], and declares its independence from governments[4] no longer exists. If it ever existed, it did so before the Tunis Agenda, before governments started to care, though it takes a stretch of imagination to believe that a network being built with government money is ever free of government influence. In a strong sense, the early developers did not think in terms of being multistakeholders; they were engineers and scientists working on a difficult and interesting problem, cooperating with each other to get the job done. The term multistakeholder was not part of common vocabulary until the WSIS process with its notions of an open, inclusive, just, and democratic process, began using the term. In retrospect, the group of engineers and scientists who invented the protocols found a way to cooperate in building the Internet that can easily be defined as having been one of the foundational examples of a multistakeholder model. They gave us, and continue to give us, a model that can hopefully be followed and improved.

Multistakeholderism Today

In the 20 years since WSIS, gradually more and more institutional entities have declared themselves to be supporters of multistakeholderism, if not actually multistakeholder entities themselves. At the same time, we have seen support for multistakeholderism grow and then ebb in popularity with the cognoscenti. Yet, today pretty much for any topic related to internets, data, or AI governance, multistakeholderism is a term of art that many use to describe the governance they want.

As the scope and reach of WSIS grew, more and more processes declared themselves to be multistakeholder. None of them necessarily meant the same thing that the Tunis Agenda meant, nor did they necessarily mean the same thing that anyone else meant. More and more participants began to group themselves into clubs they called "stakeholder groups" in a process that I refer to as "multistakeholder groupism." In Internet Governance, as defined by the Tunis Agenda, there were originally three Stakeholder groups—*Governments*, *Business*, and *Civil Society*—with at least two cross-cutting groups, the *Academic* and *Technical* communities.

Neither of these cross-cutting groups was defined as a stakeholder group in their own right because the people in those groups were often also members of the primary three defined stakeholder groupings. It was important to the technical community to be recognized as a stakeholder group in itself. They finally were recognized as such at the time of WSIS+10. It is very good to see the *Technical Community Coalition for Multistakeholderism* (TCCM) active, and participating successfully in today's policy tussles[5]. Since WSIS, many different groups have been defined as stakeholder groups in a variety of fora, without having been included in the Tunis Agenda model.

The Tunis Agenda's notion of a multistakeholder model is a top-down model with fixed roles and responsibilities for all the stakeholder groups defined 20 years ago, in a member states–only decision process. Only a few entities qualify as multistakeholder in the sense defined by the Tunis Agenda, such as the *Internet Governance Forum* (IGF), and to a partial, and hopefully only-incipient extent, the *International Telecommunication Union* (ITU), which led the prototype of a Tunis Agenda–based multistakeholder model in the way it ran the ITU's WSIS. These groups are top-down groups that have been given a definition and view that they must follow and for which they are accountable to the *United Nations* (UN) system. And if they behave, they are given a consultative voice. At the ITU, decisions are still made at councils that exclude all but state actors, whereas the IGF is barred from making decisions because there are no purely state actor councils. Still, a little bit at a time, the UN-dominated bodies allow more and more stakeholders to approach the table and to have a voice. It is a start that should be encouraged.

Many of the other groups that have referred to themselves as following a multistakeholder model have developed their models more organically, usually from a bottom-up perspective. I include groups like the *Internet Engineering Task Force* (IETF), the *Internet Corporation for Assigned Names and Numbers* (ICANN), the *Regional Internet Registries* (RIRs), and others. Though often related to each other, each of these organizations developed its own model. For example, the IETF was always dedicated to the individual stakeholders, no matter what Tunis Agenda–style stakeholder group they belonged to, company they worked for, or nationality. While they may have grouped themselves into siloes based on technology or operational principles that were practical and mutable over the years, these siloes have changed as the technology and structure of the Internet changed. They are very different in nature from the silo-based stakeholder groups defined by the Tunis Agenda and imitated by most every other organization.

Policy Making: Unilateral, Multilateral, or Multistakeholder?

Where are actual policies to be made? In multilateral political caldrons, or in the work done within multistakeholder organizations that design and deploy the networks? If multistakeholderism is dead, does that mean that governance will come only from the multilateral processes of states?

It is a simplification to believe that the state, or a multilateral collection of states like the UN, can develop a set of directives that spell the end of multistakeholder governance. On the contrary, every regulation, every rule comes with its own emergent set of opportunities, for crime and for simply working the rule to get around the rule. These effects are often extra juridical, or perhaps just pre juridical, and are within the purview of the multistakeholder policy makers who are responsible for keeping the networks working and the users happy. More multilateral rulings bring greater need for multistakeholder remediation. Just look at the amount of multistakeholder effort that has gone into dealing with the requirements of the trans-jurisdictional *General Data Protection Regulation* (GDPR). I shudder to think of all the multistakeholder efforts, with corresponding staffing and expenditures, that go into dealing with all of the output of unexpected results arising from the European Commission's NIS2 Directive: *Securing Network and Information Systems*. And though the decisions that come out of the WSIS+20 deliberations will be made by governments after consultations that are giving all stakeholders a chance to comment, making these decisions work will require great amounts of multistakeholder "sweat and tears." The more the states do, the more work is required from the multistakeholder multitudes who make the Internet what it is. Some body has to figure out how to cope with the regulatory fuss so that the Internet can continue to function and grow. Some multistakeholder groups invest time and effort into self-governance they hope will sate the eagerness of regulators. Whether it is work to dissuade the creation of regulations, or work to survive them, regulations help motivate the need for more multistakeholder efforts.

But it then comes back to the question: what does multistakeholder governance mean, and how is it to be done? Is it just a reaction to the dictates of the states? Or does it have an importance and power of its own?

Multistakeholderism Moving Forward

A major development in the lifecycle of global multistakeholder models is the work that was done in the *NETmundial* and the *NETMundial+10* events. "Convened in São Paulo, Brazil, in April 2014, stakeholders from academia, civil society, governments and International Organizations, private sector, and technical community around the world asserted the need for improvements to Internet Governance and digital policy processes. The event spelled out how to bring all stakeholders, people, cultures, countries, and distinct economies together to solve the common challenges we face"[7]. It was quite a daring move, but one that has given a pointer on a way to move forward with the model. NETmundial established principles for multistakeholder processes, giving a good basis for a definition of governance within a multistakeholder environment.

NETmundial+10 reaffirmed the principles from 2014 and went beyond them in two important ways: The event established guidelines and process steps ("Guidelines") for multistakeholder collaboration, consensus-building, and decision-making, and for how multistakeholder and multilateral efforts could coexist and cooperate.

Figure 1: NETmundial 2014 Internet Governance Process Principles[6].

- Multistakeholder
- Open, participative, consensus driven
- Transparent
- Accountable
- Inclusive and equitable
- Distributed
- Collaborative
- Enabling meaningful participation
- Access and low barriers
- Agility

The "São Paulo Multistakeholder Guidelines," with its 13 specific guidelines and the dozen process steps, goes beyond the general feeling of the original undefined notions of multistakeholder cooperation in Internet building and maintenance, and the strict top-down regimentation of the Tunis Agenda for Internet Governance. They also recognized that "one size would *not* fit all;" in fact, it turns out that every instantiation of a multistakeholder model or creation of a multistakeholder environment will be unique. See Figure 2 and Figure 3.

As time goes on, there is a good chance that newly formed and existing organizations committed to a multistakeholder model will take heed of these guidelines, and perhaps discover a few more along the way. Now let's consider a second manner in which the development of the model continues. In a multistakeholder-based organization, especially one with some degree of bottom-up modelling, there is almost always a stakeholder group advocating for improvement. Many have processes to organize continuous improvement, while some lurch from one improvement campaign to another, but all spend some part of the time trying to improve themselves. While some disparage these efforts sometimes as "navel-gazing" or as "wastes of time and bandwidth," they are nearly ubiquitous and are a necessary ingredient in the improvement and proliferation of multistakeholderism in contributing to both understanding and process development.

Another notion is developing in the evolution of multistakeholder models—that is the idea of "multistakeholder all the way up and multistakeholder all the way down." That means that a multistakeholder model can be applied at every organizational layer. At every level of organization, separate stakeholder types can be defined with their own set of process-specific roles and responsibilities. Both of these types bring their own concerns and principles to the discussions, and the basic rules of democratic inclusion, fairness, and consensus are applied to decisions, whether it is decisions on technology or policy. When a multistakeholder model can be applied at every layer of an enterprise, the power of the model comes to the fore. As a student of multistakeholderism, I would argue that most decision processes are improved by a multistakeholder modality.

Figure 2: NETmundial Guidelines[7]

1. Multistakeholder processes should be mindful of power asymmetries between diverse stakeholders, and empower stakeholders by providing them with the necessary information, resources, and skills to participate effectively, meaningfully and sustainably. Transparency measures should aim for making policy processes known, accessible, comprehensible and actionable.

2. Multistakeholder processes should involve informed and deliberative discussion among stakeholders. Meaningful dialogue is a conflict-preventing mechanism throughout all steps of the process.

3. Multistakeholder processes should strive to treat all stakeholders fairly and equitably, considering their respective needs, capacities, realities, and vulnerabilities. Stakeholders should participate on equal footing, treat one another with mutual respect, recognizing the value of diverse viewpoints and contributions and the different nature of their roles and responsibilities in an issue-specific manner.

4. Multistakeholder processes should be governed by the rule of law and respect to international human rights principles, including economic, social, cultural, civic and political rights.

5. Multistakeholder processes should respect and value the linguistic diversity of participants, and be accessible to all stakeholders, regardless of their background, status, or level of expertise.

6. All stakeholders should share responsibility and uphold accountability and transparency in their respective roles for the outcomes of the multistakeholder process, with legal and political accountability for protection of human rights remaining the primary responsibility of governments, also recognizing the private sector's responsibility to respect human rights in line with the *United Nations Guiding Principles on Business and Human Rights*.

7. Internet governance and digital policy processes should be agile and adaptable to changing circumstances, evolving technologies, emerging issues, and changing geopolitical dynamics.

8. Mechanisms for resolving conflicts among stakeholders within collaborative multistakeholder processes should be in place to enable decision-making.

9. A global multistakeholder approach to Internet governance and digital policy processes should recognize the need for collaborative action across national borders and stakeholder groups, while duly considering and leveraging local and regional perspectives.

10. Decisions should consider the long-term implications and sustainability of outcomes for human rights, and inclusive and sustainable development, as per the Tunis agenda.

11. Capacity-development efforts that enhance the understanding and skills of stakeholders, particularly those from developing countries and underrepresented communities, should be in place throughout all steps of a multistakeholder process[11].

12. Cooperation and dialogue should actively be sought with other governance fora and processes, in order to avoid duplication of efforts and to share outcomes, best practices and lessons learned.

13. Collaboration processes should be oriented towards practical, actionable outcomes that lead to tangible results and positive changes for Internet governance and digital policy processes.

Figure 3: NETmundial Process Steps Oriented Guidelines

Recommended process steps for an open and inclusive multistakeholder process:

1. Scope the issue/s: define the issue or set of issues to be considered by the multistakeholder collaboration process, considering, as much as possible, all affected perspectives.

2. Identify stakeholders: Identify all relevant stakeholders as inclusively and flexibly as feasible, including individuals, groups, organizations, and communities affected by the decision or collaboration.

3. Engage stakeholders: Actively engage all interested stakeholders throughout the process consistently and in a sustained fashion, through methods such as public consultations, surveys, workshops, and fora to gather input and feedback.

4. Share information: Provide clear and full information about the process, objectives, and outcomes to ensure transparency and understanding among stakeholders, making full use of accessible digital records including related process documentation.

5. Ensure equitable participation: Ensure equitable participation of all relevant diverse perspectives and interests, including marginalized or underrepresented groups.

6. Facilitate dialogue: Facilitate open dialogue, collaboration and deliberation among and between relevant stakeholders, encouraging respectful communication and consensus-building.

7. Prepare draft outcomes: develop draft outcomes for consultation on the basis of dialogues between relevant stakeholders, and consult the wider community of all interested stakeholders over results.

8. Factor in feedback from wider community: adapt the draft outcomes taking into account the inputs stemming from the consultation, transparently reporting on how inputs were considered, and the corresponding reasons.

9. Open decision-making: use collaborative decision-making processes that involve all the relevant stakeholders in identifying solutions, exploring trade-offs, and reaching agreements.

10. Community powers: submit final outcomes to the consideration of the wider community, providing for mechanisms empowering the wider community to react to outcomes that are inconsistent with the wider community interests.

11. Implementation and accountability in decision-making: Establish mechanisms for implementing decisions and holding stakeholders accountable for their commitments.

12. Monitor and adapt: Monitor progress, evaluate outcomes, and be willing to adapt the process based on feedback and changing circumstances.

When I first saw the title of Geoff's essay, I wondered: "what about multilateralism, is it ending too in this age of unilateralism," as hinted in Geoff's writings. While not the topic of this comment, it may be relevant to the discussion. Multistakeholder methods may actually be one element of salvation for the multilateral model. An example can be found in the São Paulo Multistakeholder Guidelines.

While the guidelines focus mostly on maintaining and furthering the use of multistakeholder models in Internet Governance, it also accounts for the necessity of cooperating instead of competing with or ignoring the multilateral processes. Unless replaced by deterioration into competing unilateral models, the multilateral model will persist as long as nation states persist, because it is their intrastakeholder group way of governance, and very few state-based organizations use a multistakeholder-based model for their internal governance. The only possible exception that comes to mind is Switzerland.

The question of whether governments belong inside the multistakeholder models occasionally comes up. Some believe the states are too important to waste their time with stakeholders. Some believe that including states constitutes a category error in that stakeholders are subject to states. Others believe that states rarely have unity of purpose and are themselves made of stakeholders, such as executives, parliamentarians, judicial, and others like regulators and enforcers. Some believe that including states in multistakeholder models is confusing at best and a profanity at worst. But, if only to protect people from other people with law enforcement activities and to be dutiful shepherds of Human Rights as defined in the set of treaties and covenants termed the *International Bill of Human Rights*[8], nation states are necessary stakeholders. Some other stakeholders who see no reason to include governments as stakeholders sometimes dispute this idea. I cannot think of a stakeholder group whose existence is not disparaged on occasion by those from other stakeholder groups. Among civil society, I know stakeholders who disparage government, and I know many who despair at the participation of industry, not remembering that industry and government have cooperated for as long as capitalism has been society's primary economic religion.

Some, members of the technical community, but certainly not all, have no use for civil society and their references to human rights, believing that is just a form of gaming, and they maintain that old fallacy that engineering and science are value-free. Some users strive to be considered stakeholders, while others refuse to recognize them as relevant, even though each of us is a user when we go home at night. While there are many who are devoted to multistakeholder principles and who respect the growing types of self-defined stakeholder groups, we still have a long way to go in identifying the relevant stakeholder for each issue. We also have a long way to go in understanding the roles and responsibilities of each stakeholder group in the various phases of decision making.

The first phase of laissez-faire, undefined multistakeholderism, may indeed be ending. In its place a new generation of multistakeholder models, built for specific purposes, is just emerging. These models include considerations such as determining the relevant stakeholder mix, and having varied decision-making processes depending on roles and responsibilities that correspond to the types and phases of programs. It is not a dead movement; it is a young movement that is evolving. There is still so much to understand about the nature and power of multistakeholder governance.

Multistakeholderism and Current Affairs

Over time, some people have become disillusioned by the current model because it cannot deliver the nirvana of perfect participatory governance. Over time, people may rename the stakeholder environment and the multistakeholder model, but neither the study of such participatory models nor their deployment is over—it's not even close.

During the last year, much of the governance community, if it can be called that, has been discussing governance of the Internet in all of its multilayer richness, fragmented networks, massive data, and AI everywhere. In the *Pact for the Future*[9], specifically in the *Global Digital Compact*[10], a key governmental motivation describing a multilateral future, we find:

> "Governments, the private sector, civil society, the technical community, academia and international and regional organizations, in their respective roles and responsibilities, are essential to advance an inclusive, open, safe and secure digital future. Our cooperation will be multi-stakeholder and harness the contributions of all;"[10]

The next step in the movement of governance of the Internet and all the emerging new issues and technology developments are all being discussed in terms of a multistakeholder future in a multilateral world. Its methods and ways of finding agreement are becoming part of mainstream decision making. There are still many arguments about who makes decisions for a specific issue during a phase of public policy development, but for the most part there is recognition, often grudging, that no stakeholder group is capable of making the best decisions alone. In many deliberations, there is the beginning of the realization that multistakeholder methods are often necessary for finding the best solution, or at least an adequate solution, for a problem in its time.

As I write this, there are ongoing discussions on the WSIS+20 Outcomes that will come out later this year. While this process is controlled by governments to develop a document that is a government outcome and not a multistakeholder one, it has done better stakeholder consultations than the UN usually does. The current *Zero Draft*[12] contains support for the use of multistakeholder models in the areas of Internet, Data, AI governance, and human rights in the Information society. It remains to be seen how much is retained in the final draft when it is finalized in mid December 2025.

Multistakeholder governance is not ending; it is entering its next stage of development, implementation, and deployment.

References

[0] Geoff Huston, "Opinion: The End of Multistakeholderism?" *The Internet Protocol Journal*, Volume 28, No. 3, December 2025.

[1] In terms of the Internet/internet controversy, the usage rule I follow is that when speaking of the one unfragmented, for some definition of unfragmented, network based upon one of two revisions of the *Internet Protocol* (IP) packets with addressing as standardized by the IETF, I use the proper name Internet. On the other hand, when using it as an adjective to refer to a type of technology, policy, or politics, etc., I use the lower case as is appropriate for an adjective. I thank the editors for allowing my usage. The specific use of *Internet Governance* is as the capitalized proper name of a discipline, for the various definitions of that discipline.

[2] Avri Doria, "Use and Abuse of Multistakeholderism in the Internet," Reprint from *The Evolution Of Global Internet Governance — Principles and Policies in the Making*, ISBN 978-3-7255-6908-3, 2013.

[3a] Andrew L. Russell, "'Rough Consensus and Running Code' and the Internet-OSI Standards War," *IEEE Annals of the History of Computing*, Volume 28, Issue 3, July–September, 2006.

[3b] David D. Clark, "*A Cloudy Crystal Ball — Visions of The Future*," Presentation given at IETF 24, July 1992, Slide 19: **https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf**

[4] John Perry Barlow, "A declaration of the Independence of cyberspace," *Electronic Frontier Foundation*, 1996. **https://www.eff.org/cyberspace-independence**

[5] *Technical Community Coalition for Multistakeholderism*, **https://www.tccm.global/**; As an independent member of the technical community, I currently consider myself a fellow traveler with the TCCM, where membership is reserved for organizations (a fine example of multistakeholder-groupism) though individuals are allowed to participate in their activities. I have been advocating for robust technical community participation since the days of WSIS and am happy to see that TCCM has arrived on the scene.

[6] NETmundial Multistakeholder Statement, São Paulo, Brazil 2014, page 6: **https://netmundial.br/2014/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf**

[7] NETmundial+10 Multistakeholder Statement São Paulo, Brazil, 2024: **https://netmundial.br/netmundial-10-multistakeholder-statement-strengthening-internet-governance-and-digital-policy-processes**; page 12.

[8] International Bill of Human Rights, 1948: **https://documents.un.org/doc/resolution/gen/nr0/043/88/pdf/nr004388.pdf**; formally including *Universal Declaration of Rights* (UDHR), the *International Covenant on Economic Social and Cultural Rights* (ICESCR) 1966, and the *International Covenant on Civil and Political Rights* (ICCPR) 1966. Over time it has come to informally include many other treaties and covenants on related human rights, such as the rights of the child and rights of disabled persons.

[9] *UN Pact for the Future: A Vision for Global Collaboration*, 2024: **https://unric.org/en/pact-for-the-future/**

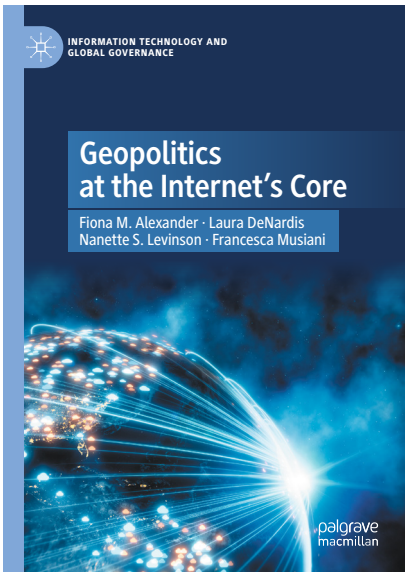
[10] Global Digital Compact, 2024, A/79/L.2, page 3: **https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf**

[11] *Capacity Development or Capacity Building* are general terms used throughout Internet Governance and many development programs. The terms can refer to any skill necessary for participation in the technological or policy aspects of the Internet and related areas like Internet Governance or Human Rights on the Internet as well as the skills needed to build a community network in a rural unserved location or maintain a network in an urban region. In most any forward-looking document on Internet Governance, one can expect to find many references to the necessity for enabling capacity development. It can be used in reference to individuals, but is most often used in reference to enabling populations of groups, regions, or nations.

[12] Zero draft of the WSIS+20 Outcome Document: **https://www.itu.int/md/S25-CWGWSIS43-INF-0004**

AVRI DORIA is a researcher based in Providence, RI, USA, who served on the UN *Working Group on Internet Governance* (WGIG), the UN *Working Group on Enhanced Cooperation I* (WGEC), as a member of the *Internet Governance Forum* (IGF) Secretariat, and later as a member of the *IGF Multistakeholder Advisory Group* (IGF MAG). As a technologist, she has been involved in the development of Internet protocols and architectures for over 30 years; was chair of the *Internet Research Task Force Routing Research Group* (IRTF-RRG), was a founder and co-chair of the *Research Group on Human Rights Protocol Considerations* (IRTF-HRPC), and has served on the *Internet Research Steering Group* (IRSG). She is active in ICANN policy development, was chair of the GNSO Council, served on the ICANN Board, and continues as an active At Large participant of ICANN. Avri is also a member of the *Freedom Online Coalition Advisory Network*. Blog at **https://m17m.is** E-mail: **avri@doria.org**

Book Review: Geopolitics at the Internet's Core



Geopolitics at the Internet's Core, by Fiona M. Alexander, Laura DeNardis, Nanette S. Levinson, and Francesca Musiani, ISBN 978-3-031-89477-0, Springer Nature, 2025[0].

The book *Geopolitics at the Internet's Core* is a most unusual and very helpful effort by four co-authors who have long been involved in shaping technology policy and governance: Fiona M. Alexander and Nanette S. Levinson, who both hold various research positions at American University in Washington, DC; Laura DeNardis, a professor at Georgetown University and author of numerous books on tech governance; and Francesca Musiani, a researcher at the French National Center for Scientific Research.

While I consider myself well-read and steeped in Internet technologies and have some technical understanding of the underlying Internet protocols, this is a unique, useful, and educational book that should have wide appeal.

The book concerns itself with the evolution of Internet protocols as it relates to its governance and technological history. It traces this path from the Internet's beginnings as a U.S. science experiment to the underlying worldwide phenomenon that we know today. That link may seem a well-visited side issue, especially for a network engineer or someone who has written numerous *Requests for Comments* (RFCs), but *Internet Governance* is becoming increasingly important, and having that context should be a critical part of anyone's job today. For example, most readers of *The Internet Protocol Journal* are familiar with *Distributed Denial of Service* (DDoS) attacks, how they are caused, and their consequences in terms of systemic outages or data corruption. But behind that technical layer is a deeper failure of the trust and geopolitics of the compromised IP addresses, and how these attacks can be prevented with particular security and political changes. "As geopolitical strategies are increasingly embedded in technology, IP addresses will certainly continue to be a bone of contention in terms of security," the authors write.

The authors take us behind the scenes to numerous cross-country border conflicts that demonstrate the shifting winds of geopolitics and ways that Internet infrastructure and design have been co-opted for various political and economic purposes. They write, "The Internet Protocol has been born out of conflict since its inception. One remarkable feature of its evolution is that, as each issue becomes resolved, geopolitical tensions seem to only escalate." They show how IP has been at the center of these conflicts and show how it is a lens that can help explain some of these issues, even though, as they point out, "who is doing the governing and what is being governed have often been over-simplified or just grossly incorrect."

Many of the events dissected in this book will be familiar to IPJ readers, some of whom directly participated in them, such as the transition of the *Internet Corporation for Assigned Names and Numbers* (ICANN) from a US-owned entity to an international standards and multi-stakeholder body, the rocky transition to IPv6, or the fight to select TCP/IP over *Open Systems Interconnection* (OSI) protocols. The authors' treatment, however, delves into the central governance issues that might not be as familiar as the technical arguments for these choices, showing the influence of various institutional controls and public policies. "If design is governance, the process matters. And design going forward matters," they write. This is part of the book's unique perspective.

Indeed, the notion of multistakeholderism might be a new term for you. The authors take pains to demonstrate how "government top-down mandates were not the decider" in the development of TCP/IP, which adopted many innovations thanks to consensus and more bottom-up approaches. (See Geoff Huston's and Avri Doria's essays on multistakeholderism in this issue of IPJ[3,4].) To dive further into this concept, the authors devote a chapter on embracing more inclusive audiences. The authors document several ways to measure this inclusion:

If we look at how IP protocols are distributed across the globe, we'll see that their U.S.-based *Defense Advanced Research Projects Agency* (DARPA) origins are still very much in evidence. There are several ways to measure this distribution. One is by counting *Internet Exchange Points* (IXPs)—the places where large ISPs can connect to each other. These places are still mostly congregated in western countries, and many countries have either no IXPs or a single place[1]. The absence or paucity of an IXP means that residents of that country will have longer latencies, less local content, and higher cost of Internet access.

There is also measuring the number of available IP address ranges in any given locality. We know that the IPv4 "classic" address ranges have been consumed, but in Africa there are still many available address ranges. And then there are the distributions of *Domain Name System* (DNS) servers, because having one logically "nearby" also affects traffic latency and resiliency of digital networks. It took until 2022 before Africa had its own managed DNS cluster, meaning that prior to then most of the DNS traffic had to transit to another continent.

If we move our lens to a wider angle to examine the actual languages used online, we see that English dominates, and despite there being thousands of different languages spoken and written, 82% of online content is represented by ten languages: English, Chinese, Spanish, Arabic, Portuguese, Japanese, Russian, German, French, and Malaysian[2]. For much of the Internet's early years, non-*American Standard Code for Information Interchange* (ASCII) characters for domain names were not supported, and today there are still gaps in having local character set domain support.

Let's move our lens to a still wider angle to Internet Governance. This exercise is also instructive in showing the unequal distribution of resources. The various standards bodies that determine Internet policy still have a very western bias, which can cloud any cross-national decisions, because who is on these various governing bodies can be significant. The result of this situation is that the distribution and control over Internet resources have become entangled in various political conflicts, such as the Russia/Ukraine and Israel/Hamas wars and various sanctions against Iran. These events are examined in detail from the geopolitical points of view, and they show how IP addresses can become political proxies and form a basic social resource. The authors ask, "Do [the Internet governing] organizations most people have never heard of hold the power to unplug an entire country from the Internet? In part, yes." Protocols have become a proxy for political purposes, and now outages, whether directed from inside a country by authoritarian purposes or requested from the outside by well-meaning humanitarian actors, are now the new norm. The governance is murky, and cutting off Internet access could support less freedom of expression, because "one country's illegal hate speech is another country's protected speech," as they write. "It is true that the experience of the Internet in one part of the world—whether as a user, government official, or developer—is quite different than in other parts of the world. There is uneven distribution, uneven filtering and censorship, and uneven economic opportunity."

Another chapter concerns how Internet protocols will evolve to adapt to future technologies. I recall when the web was still fresh and text-based, when video streams were still a technical challenge, when blockchain was just a thought experiment, and when a firewall was just connecting two networks and not an essential Internet security appliance. All of these technologies have been influenced greatly by TCP/IP protocols. This is also the case for what is now happening with the influence of Artificial Intelligence. "AI and the Internet are entangled in every way. AI has diffused into the Internet's architecture at all layers. Machine learning techniques are at the heart of many cybersecurity mechanisms detecting DDoS attacks and other irregular patterns that indicate the presence of malware or unauthorized network intrusions."

They distill the Internet's possible future into five broad themes:

- Tension between bordered nations and how a borderless Internet will influence data governance decisions and regulations,
- Governments will seek economic or political objectives by co-opting various pieces of Internet infrastructure,
- There will be attempts to modify TCP/IP design through political means, such as overlaying security features,
- A move towards more privatization efforts on Internet infrastructure, and
- Changes in the multistakeholder governance that will be shaped by a variety of factors.

Other chapters address content moderation issues and security innovations. Each chapter could serve as the touchstone for a college class on the subject, and with excellent footnotes, a useful source document if a professor were so inclined to create one. I don't mean to give these chapters short shrift, because each one contains a series of insights that I found refreshing and thought-provoking—such as an observation that content moderation has moved down the tech stack into more infrastructure controls. Another set of observations is showing where trust fails in compromised certificate authorities and DNS servers or IP address blocks used for DDoS attacks—and why these failures must be front and center of any governance and policy efforts.

The book occupies a useful place for many different audiences:

- Academics who may want to use it as a text for a course in IP history or geopolitics or some combination,
- Engineering staff at digital technology vendors, who may want to understand where their role is in a wider governance context,
- ICANN groupies (both pro and con), which could include the IPJ readership,
- GenZ and other youngsters, who were born after most of the action depicted in this book took place and are tired of reading low-content online articles, and
- Policy wonks in major national capitals who are about to embark on formulating changes to their country's Internet Governance.

The authors point out that while Internet Governance has changed over time, sometimes quite radically, "life did not change for the average Internet user." That perhaps is testament to the Internet's resilience and design. Many of us know how the Internet routes around outages or breaches. This book is perhaps the first one I have read that shows how it also routes around many policy changes that impact its basic core protocols.

References

[0] Springer Nature Link:
https://link.springer.com/book/10.1007/978-3-031-89478-7

[1] Packet Clearing House, "Internet Exchange Directory,"
https://www.pch.net/ixp/dir

[2] Meital Kupfer, "A more inclusive Internet for who? Non-English speakers in digital spaces," *Internet Society Foundation Blog*, February 20, 2023.

[3] Geoff Huston, "Opinion: The End of Multistakeholderism?" *The Internet Protocol Journal*, Volume 28, No. 3, December 2025.

[4] Avri Doria, "Counter-Opinion: Multistakeholderism Is Not Ending; Rather, It Is Moving to a Next Stage," *The Internet Protocol Journal,* Volume 28, No. 3, December 2025.

—David Strom
david@strom.com

In Memoriam: Fearghas McKay: October 15, 1963 – October 1, 2025

Ed.: Fearghas was an active member of several Internet communities. Included here are reactions to his passing from a few of them.

The North American Network Operators' Group (NANOG)

Fearghas McKay was a remarkable individual known for his ability to forge connections worldwide. His impact was particularly evident within the NANOG community, where he attended over 25 NANOG conferences and dedicated more than 7 years of service on various NANOG Committees. The relationships he built and the community he fostered are reflected in his work on the Program Committee, Hackathon Committee, Elections Committee, and, most recently, the Workshop Committee.

The European Peering Forum (EPF)

We are deeply saddened to hear of the passing of a beloved figure in our industry. Fearghas McKay was more than a pioneer—he was a mentor, a sharer of knowledge, and a source of inspiration to countless colleagues and friends. His passion, generosity, and unwavering commitment to our industry left a mark on all of us. As we mourn this profound loss, we also celebrate the orange legacy he leaves behind—one that will continue to shape and uplift our community for years to come. Our thoughts are with his family, friends and colleagues across the industry. Fearghas, you will be greatly missed.

The European Internet Exchange Association (Euro-IX)

We are deeply saddened to learn of the passing of our friend and colleague, Fearghas McKay. As a founder member of Euro-IX and a Director on its first Board, Fearghas played an important role in shaping the interconnection community in its early days. He was an enthusiastic and long-standing supporter of Euro-IX, *Internet Exchange Providers* (IXPs) and the wider industry, contributing tirelessly to the growth and collaboration that define our community today.

Fearghas also served for many years on the Forum Programme Committee, both within Euro-IX and for other industry events, committed to the highest quality of knowledge sharing and discussion with a deep passion for presentations that really brought more knowledge and insights to the community. His presence was well known across the globe—a very familiar face, a trusted voice and a generous contributor of technical insight.

Beyond his professional contributions, Fearghas was a steadfast supporter of NOGs, IXP events and the broader networking community. He brought people together, encouraged new ideas and championed the work that IXPs do to strengthen the Internet.

Our thoughts are with his many friends and colleagues across the industry especially his colleagues in Flexoptix and with those who stood by him and especially after the loss of his beloved Susan Forney in 2021.

Fearghas will be remembered with deep respect and fondness. In the spirit of his Scottish heart, we will raise a glass to him—a dram of peaty whisky with just the smallest drop of water, exactly as he liked it. He will be greatly missed.

The Global NOG Alliance

It is with heavy hearts that we learned on October 1, 2025, that an important member of our international community has passed away. This has hit all of us at the Global NOG Alliance very hard. Each and every one of us worked closely with Fearghas McKay, and the grief runs deep and the loss is painful.

Fearghas was a builder of communities, a believer in open communication, and one of those people who quietly kept the global NOG world turning. He didn't just show up to meetings—he changed the tone of the room. If things were stuck, he'd unstick them. If people were drifting, he'd bring the conversation back to what mattered.

Sometimes that meant producing a bottle of whisky to get the discussion moving. Other times it meant sitting back and, with a single comment, cutting through the nonsense with more common sense than most committees can muster in a week. He gave his time freely—to programme committees, working groups, IXPs, and anyone who needed a steer—and he did it across regions, time zones, and years.

Fearghas was direct in the way only someone who genuinely cares can be. Say what matters, fix what's broken, move on. He did not waste time, and he did not let others waste it either. He didn't suffer fools, but he gave generously to people who were trying. That mix—sharpness and generosity—made everyone around him a little better, a little clearer, and a little braver.

For those of us who worked with him, he was the honest voice in the room and the steady hand behind the scenes. Thank you, Fearghas, for the clarity, the time, the advocacy, the late-night fixes, the dry humour, and the straight talk. We'll keep the channels open—you'd expect no less.

For anyone who didn't cross paths with him: he gave years to the community through roles like Euro-IX Forum Programme Committee Chair, RIPE working groups, and NOGs around the world. Most recently, at Flexoptix, he kept doing what he always did—connecting people, ideas, and networks.

We extend our sincere condolences to friends, mentees, colleagues, and above all, the family.

On October 25, 2025, we said goodbye to Fearghas in Copenhagen together with family and friends from the community. On behalf of everyone in the international community, we would like to thank Paddy, Magnus, and the family for organizing a memorial service in Copenhagen.

With shocked regards,
The Global NOG Alliance Team

RIPE

We were all very saddened yesterday to learn that Fearghas McKay had passed away. No doubt this will come as a shock to his family and those of us who knew him from his work in the community.

Fearghas has been an active participant in the RIPE community for many years. He served as Chair of the *European Internet Exchange* (EIX) Working Group from 1998–2013, and has been a part of programme committees and steering groups for a number of Network Operator Groups and peering forums, including the *African Peering and Interconnection Forum* (AfPIF), the *Central Asia Peering and Interconnection Forum* (CAPIF) and the *United Kingdom Network Operators' Forum* (UKNOF), often taking the role of co-chair within these groups. He was also a RIPE Atlas Ambassador for several years, helping to introduce Internet measurements to network operators around the world.

His contributions have helped shape the RIPE community and the interconnection world more broadly. We will miss his energy, his humour, and his friendship.

On behalf of the RIPE community we wish to extend our condolences to Fearghas's family and friends.

Kind regards,
Mirjam Kühne, RIPE Chair

Fragments

Our Privacy Policy

The *General Data Protection Regulation* (GDPR) is a regulation for data protection and privacy for all individual citizens of the *European Union* (EU) and the *European Economic Area* (EEA). Its implementation in May 2018 led many organizations worldwide to post or update privacy statements regarding how they handle information collected in the course of business. Such statements tend to be long and include carefully crafted legal language. We realize that we may need to provide similar language on our website and in the printed edition, but until such a statement has been developed here is an explanation of how we use any information you have supplied relating to your subscription:

- The mailing list for *The Internet Protocol Journal* (IPJ) is entirely "opt in." We never have and never will use mailing lists from other organizations for any purpose.
- You may unsubscribe at any time using our online subscription system or by contacting us via e-mail. We will honor any request to remove your name and contact information from our database.
- We will use your contact information only to communicate with you about your subscription; for example, to inform you that a new issue is available, that your subscription needs to be renewed, or that your printed copy has been returned to us as undeliverable by the postal authorities.
- We will never use your contact information for any other purpose or provide the subscription list to any third party other than for the purpose of distributing IPJ by post or by electronic means.
- If you make a donation in support of the journal, your name will be listed on our website and in print unless you tell us otherwise.

Read Any Good Books Lately?

Then why not share your thoughts with the readers of IPJ? We accept reviews of new titles, as well as some of the "networking classics." In some cases, we may be able to get a publisher to send you a book for review if you don't have access to it. For more information, contact us at **ipj@protocoljournal.org**

Check your Subscription Details!

Make sure that both your postal and e-mail addresses are up-to-date since these are the only methods by which we can contact you. If you see the words "Invalid E-mail" on your printed copy, this means that we have been unable to contact you through the e-mail address on file. If this is the case, please contact us at **ipj@protocoljournal.org** with your new information. The subscription portal is located here:
https://www.ipjsubscription.org/

Thank You!

Publication of IPJ is made possible by organizations and individuals around the world dedicated to the design, growth, evolution, and operation of the global Internet and private networks built on the Internet Protocol. The following individuals have provided support to IPJ. You can join them by visiting **http://tinyurl.com/IPJ-donate**

Kjetil Aas
Fabrizio Accatino
Michael Achola
Martin Adkins
Melchior Aelmans
Christopher Affleck
Scott Aitken
Jacobus Akkerhuis
Antonio Cuñat Alario
William Allaire
Nicola Altan
Shane Amante
Marcelo do Amaral
Matteo D'Ambrosio
Selva Anandavel
Jens Andersson
Danish Ansari
Finn Arildsen
Tim Armstrong
Richard Artes
Michael Aschwanden
David Atkins
Jac Backus
Jaime Badua
Bent Bagger
Eric Baker
Fred Baker†
Santosh Balagopalan
William Baltas
David Bandinelli
A C Barber
Benjamin Barkin-Wilkins
Ryan Barnes
Feras Batainah
Michael Bazarewsky
Robert Beckett
David Belson
Richard Bennett
Matthew Best
Hidde Beumer
Pier Paolo Biagi
Arturo Bianchi
John Bigrow
Orvar Ari Bjarnason
Tyson Blanchard
Axel Boeger
Keith Bogart
Mirko Bonadei
Roberto Bonalumi
Lolke Boonstra
Cente Cornelis Boot
Julie Bottorff Photography
Gerry Boudreaux
Leen de Braal
Stephen Bradley
Kevin Breit
Thomas Bridge
Ilia Bromberg
Lukasz Bromirski
Václav Brožík
Christophe Brun
Gareth Bryan
Ron Buchalski
Paul Buchanan
Stefan Buckmann
Caner Budakoglu
Darrell Budic
BugWorks
Scott Burleigh
Chad Burnham
Randy Bush
Colin Butcher
Jon Harald Bøvre
Olivier Cahagne
Antoine Camerlo
Tracy Camp
Brian Candler
Fabio Caneparo
Roberto Canonico
David Cardwell
Richard Carrara
John Cavanaugh
Lj Cemeras
Dave Chapman
Stefanos Charchalakis
Molly Cheam
Christof Chen
Pierluigi Checchi
Greg Chisholm
David Chosrova
Marcin Cieslak
Lauris Cikovskis
Brad Clark
Narelle Clark
Horst Clausen
James Cliver
Guido Coenders
Robert Collet
Joseph Connolly
Steve Corbató
Brian Courtney
Beth and Steve Crocker
Dave Crocker
Kevin Croes
John Curran
Sergio Danelli
André Danthine†
Morgan Davis
Jeff Day
Nicholas Dean
Fernando Saldana Del Castillo
Rodolfo Delgado-Bueno
Julien Dhallenne
Freek Dijkstra
Geert Van Dijk
David Dillow
Richard Dodsworth
Ernesto Doelling
Michael Dolan
Eugene Doroniuk
Michael Dragone
Joshua Dreier
Lutz Drink
Aaron Dudek
Dmitriy Dudko
Andrew Dul
Joan Marc Riera Duocastella
Pedro Duque
Holger Durer
Karlheinz Dölger
Mark Eanes
Andrew Edwards
Peter Robert Egli
George Ehlers
Peter Eisses
Torbjörn Eklöv
Jacobus Gerrit Elsenaar
Y Ertur
ERNW GmbH
ESdatCo
Steve Esquivel
Jay Etchings
Mikhail Evstiounin
Babatunde Faluyi
Bill Fenner
Paul Ferguson
Ricardo Ferreira
Kent Fichtner
Ulrich N Fierz
Armin Fisslthaler
Michael Fiumano
The Flirble Organisation
Jean-Pierre Forcioli
Gary Ford
Susan Forney†
Christopher Forsyth
Andrew Fox
Craig Fox
Fausto Franceschini
Erik Fredriksson
Valerie Fronczak
Tomislav Futivic
Laurence Gagliani
Edward Gallagher
Andrew Gallo
Chris Gamboni
Xosé Bravo Garcia
Osvaldo Gazzaniga
Kevin Gee
Rodney Gehrke
Radu Cristian Gheorghiu
Greg Giessow
John Gilbert
Serge Van Ginderachter
Greg Goddard
Tiago Goncalves
Ron Goodheart
Octavio Alfageme Gorostiaga
Barry Greene
Jeffrey Greene
Richard Gregor
Martijn Groenleer
Geert Jan de Groot
Ólafur Guðmundsson
Christopher Guemez
Rafael Leon Guerrero
Gulf Coast Shots
Galen Guyer
Sheryll de Guzman
Rex Hale
Jason Hall
James Hamilton
Darow Han
Handy Networks LLC
Stephen Hanna
Martin Hannigan
John Hardin
David Harper
Edward Hauser
David Hauweele
Marilyn Hay
Headcrafts SRLS
Hidde van der Heide
Johan Helsingius
Robert Hinden
Michael Hippert
Damien Holloway
Alain Van Hoof
Edward Hotard
Bill Huber
Hagen Hultzsch
Kauto Huopio
Asbjørn Højmark
Kevin Iddles
Mika Ilvesmaki
Karsten Iwen
Joseph Jackson
David Jaffe
Ashford Jaggernauth
Thomas Jalkanen
Jozef Janitor
Martijn Jansen
John Jarvis
Dennis Jennings
Edward Jennings
Aart Jochem
Nils Johansson
Brian Johnson
Curtis Johnson
Don Johnson
Richard Johnson
Jim Johnston
Jose Enrique Diaz Jolly
Jonatan Jonasson
Daniel Jones
Gary Jones
Jerry Jones
Michael Jones
Amar Joshi
Javier Juan
David Jump
Anders Marius Jørgensen
Merike Kaeo
Andrew Kaiser
Vladislav Kalinovsky
Naoki Kambe
Akbar Kara
Christos Karayiannis
Daniel Karrenberg
David Kekar
Stuart Kendrick
Robert Kent
Robert Kerman
Thomas Kernen
Jithin Kesavan
Jubal Kessler
Shan Ali Khan
Nabeel Khatri
Dae Young Kim
William W. H. Kimandu
John King
Russell Kirk
Gary Klesk
Anthony Klopp
Henry Kluge
Michael Kluk
Paul Knight
Andrew Koch
Ia Kochiashvili
Carsten Koempe
Richard Koene
Alexader Kogan
Matthijs Koot
Antonin Kral
Robert Krejčí
John Kristoff
Terje Krogdahl
Bobby Krupczak
Murray Kucherawy
Warren Kumari
George Kuo
Dirk Kurfuerst
Mathias Körber
Darrell Lack
Andrew Lamb
Richard Lamb
Yan Landriault

Edwin Lang
Sig Lange
Markus Langenmair
Fred Langham
Tracy LaQuey Parker
Christian de Larrinaga
Alex Latzko
Jose Antonio Lazaro Lazaro
Antonio Leding
Rick van Leeuwen
Simon Leinen
Anton van der Leun
Robert Lewis
Christian Liberale
Mark Lieu
Martin Lillepuu
Roger Lindholm
Link Light Networks
Art de Llanos
Mike Lochocki
Chris and Janet Lonvick
Mario Lopez
Sergio Loreti
Eric Louie
Adam Loveless
Josh Lowe
Guillermo a Loyola
Hannes Lubich
Dan Lynch†
David MacDuffie
Sanya Madan
Miroslav Madić
Alexis Madriz
Carl Malamud
Jonathan Maldonado
Michael Malik
Tarmo Mamers
Yogesh Mangar
John Mann
Bill Manning†
Diego Mansilla
Harold March
Vincent Marchand
Normando Marcolongo
Gabriel Marroquin
David Martin
Jim Martin
Ruben Tripiana Martin
Timothy Martin
Carles Mateu
Juan Jose Marin Martinez
Ioan Maxim
David Mazel
Miles McCredie
Gavin McCullagh
Brian McCullough
Joe McEachern
Alexander McKenzie
Jay McMaster
Bruce McNamara
Mark Mc Nicholas
Olaf Mehlberg
Carsten Melberg
Kevin Menezes
Bart Jan Menkveld
Sean Mentzer
Eduard Metz
William Mills
David Millsom
Desiree Miloshevic
Joost van der Minnen
Thomas Mino
Rob Minshall
Wijnand Modderman-Lenstra
Mohammad Moghaddas
Charles Monson
Andrea Montefusco
Fernando Montenegro
Roberto Montoya
Joel Moore
Joseph Moran
John More
Maurizio Moroni
Brian Mort
Soenke Mumm
Tariq Mustafa
Stuart Nadin
Michel Nakhla
Mazdak Rajabi Nasab
Krishna Natarajan
Naveen Nathan
Ryan Nelson
Darryl Newman
Mai Nguyen
Thomas Nikolajsen
Paul Nikolich
Travis Northrup
Marijana Novakovic
David Oates
Ovidiu Obersterescu
Jim Oplotnik
Tim O'Brien
Mike O'Connor
Mike O'Dell
John O'Neill
Carl Önne
Packet Consulting Limited
Carlos Astor Araujo Palmeira
Gordon Palmer
Alexis Panagopoulos
Gaurav Panwar
Sujith Madathil Parambath
Chris Parker
Alex Parkinson
Craig Partridge
Manuel Uruena Pascual
Ricardo Patara
Dipesh Patel
Dan Paynter
Leif-Eric Pedersen
Rui Sao Pedro
Juan Pena
Luis Javier Perez
Chris Perkins
Michael Petry
Alexander Peuchert
David Phelan
Harald Pilz
Derrell Piper
Rob Pirnie
Jorge Ivan Pincay Ponce
Marc Vives Piza
Victoria Poncini
Blahoslav Popela
Andrew Potter
Ian Potts
Eduard Llull Pou
Tim Pozar
David Preston
David Raistrick
Priyan R Rajeevan
Balaji Rajendran
Paul Rathbone
William Rawlings
Mujtiba Raza Rizvi
Bill Reid
Petr Rejhon
Robert Remenyi
Rodrigo Ribeiro
Glenn Ricart
Justin Richards
Rafael Riera
Mark Risinger
Fernando Robayo
Michael Roberts
Gregory Robinson
Ron Rockrohr
Graziano G Rodegari
Carlos Rodrigues
Magnus Romedahl
Lex Van Roon
Marshall Rose
Alessandra Rosi
David Ross
William Ross
Boudhayan Roychowdhury
Carlos Rubio
Rainer Rudigier
Timo Ruiter
RustedMusic
Babak Saberi
George Sadowsky
Scott Sandefur
Sachin Sapkal
Arturas Satkovskis
PS Saunders
Richard Savoy
John Sayer
Phil Scarr
Gianpaolo Scassellati
Elizabeth Scheid
Jeroen Van Ingen Schenau
Carsten Scherb
Ernest Schirmer
Benson Schliesser
Philip Schneck
James Schneider
Peter Schoo
Dan Schrenk
Richard Schultz
Timothy Schwab
Roger Schwartz
SeenThere
Scott Seifel
Paul Selkirk
Andre Serralheiro
Yury Shefer
Yaron Sheffer
Doron Shikmoni
Tj Shumway
Jeffrey Sicuranza
Thorsten Sideboard
Greipur Sigurdsson
Fillipe Cajaiba da Silva
Andrew Simmons
Pradeep Singh
Henry Sinnreich
Geoff Sisson
John Sisson
Helge Skrivervik
Terry Slattery
Darren Sleeth
Richard Smit
Bob Smith
Courtney Smith
Eric Smith
Mark Smith
Tim Sneddon
Craig Snell
Job Snijders
Ronald Solano
Asit Som
Ignacio Soto Campos
Evandro Sousa
Fredrik Söderblom
Peter Spekreijse
Thayumanavan Sridhar
Paul Stancik
Ralf Stempfer
Matthew Stenberg
Martin Štěpánek
Adrian Stevens
Clinton Stevens
John Streck
Martin Streule
David Strom
Colin Strutt
Viktor Sudakov
Kathleen Summers
Edward-W. Suor
Vincent Surillo
Terence Charles Sweetser
T2Group
Roman Tarasov
David Theese
Rabbi Rob and Lauren Thomas
Douglas Thompson
Kerry Thompson
Lorin J Thompson
Jerome Tissieres
Fabrizio Tivano
Peter Tomsu Fine Art Photography
Joseph Toste
Rey Tucker
Sandro Tumini
Angelo Turetta
Brian William Turnbow
Michael Turzanski
Adam Tuxbury
Phil Tweedie
Steve Ulrich
Unitek Engineering AG
John Urbanek
Martin Urwaleck
Bart Vanautgaerden
Betsy Vanderpool
Surendran Vangadasalam
Ramnath Vasudha
Jose Luis Couto Vázquez
Randy Veasley
Philip Venables
Buddy Venne
Alejandro Vennera
Luca Ventura
Scott Vermillion
Tom Vest
Peter Villemoes
Vista Global Coaching & Consulting
Dario Vitali
Marc Vives
Rüdiger Volk
Jeffrey Wagner
Don Wahl
Michael L Wahrman
Lakhinder Walia
Laurence Walker
Randy Watts
Andrew Webster
Jd Wegner
Tim Weil
Westmoreland Engineering Inc.
Rick Wesson
Peter Whimp
Russ White
Jurrien Wijlhuizen
William Willaford
Joseph Williams
Derick Winkworth
Pindar Wong
Brian Woods
Makarand Yerawadekar
Phillip Yialeloglou
Janko Zavernik
Bernd Zeimetz
Muhammad Ziad Ziayuddin
Tom Zingale
Matteo Zovi
Jose Zumalave
Romeo Zwart
廖 明沂.

Call for Papers

The *Internet Protocol Journal* (IPJ) is a quarterly technical publication containing tutorial articles ("What is...?") as well as implementation/operation articles ("How to..."). The journal provides articles about all aspects of Internet technology. IPJ is not intended to promote any specific products or services, but rather is intended to serve as an informational and educational resource for engineering professionals involved in the design, development, and operation of public and private internets and intranets. In addition to feature-length articles, IPJ contains technical updates, book reviews, announcements, opinion columns, and letters to the Editor. Topics include but are not limited to:

- Access and infrastructure technologies such as: Wi-Fi, Gigabit Ethernet, SONET, xDSL, cable, fiber optics, satellite, and mobile wireless.
- Transport and interconnection functions such as: switching, routing, tunneling, protocol transition, multicast, and performance.
- Network management, administration, and security issues, including: authentication, privacy, encryption, monitoring, firewalls, troubleshooting, and mapping.
- Value-added systems and services such as: Virtual Private Networks, resource location, caching, client/server systems, distributed systems, cloud computing, and quality of service.
- Application and end-user issues such as: E-mail, Web authoring, server technologies and systems, electronic commerce, and application management.
- Legal, policy, regulatory and governance topics such as: copyright, content control, content liability, settlement charges, resource allocation, and trademark disputes in the context of internetworking.

IPJ will pay a stipend of US$1000 for published, feature-length articles. For further information regarding article submissions, please contact Ole J. Jacobsen, Editor and Publisher. Ole can be reached at **ole@protocoljournal.org** or **olejacobsen@me.com**

Follow us on X and Facebook **@protocoljournal** **https://www.facebook.com/newipj**

Supporters and Sponsors

Supporters

Internet Society

CISCO

Diamond Sponsors

Your logo here!

Ruby Sponsors

APNIC FOUNDATION

Sapphire Sponsors

ICANN

Emerald Sponsors

Akamai

amsix

APRICOT Asia Pacific Regional Internet Conference on Operational Technologies

.auDA

DE CIX

EQUINIX

FLEXOPTIX

GÉANT

Google

identity digital

JPRS

RIPE NCC RIPE NETWORK COORDINATION CENTRE

lacnic

LinkedIn

linx

NTT DATA

WIDE PROJECT

VERISIGN

TEAM CYMRU

Corporate Subscriptions

AFRINIC The Internet Numbers Registry for Africa

COMCAST

DNS-OARC

ISC Internet Systems Consortium

IWL

NSRC Network Startup Resource Center

qa cafe

For more information about sponsorship, please contact **sponsor@protocoljournal.org**

The Internet Protocol Journal
Link Fulfillment
7650 Marathon Dr., Suite E
Livermore, CA 94550

CHANGE SERVICE REQUESTED

The Internet Protocol Journal is published quarterly and supported by the Internet Society and other organizations and individuals around the world dedicated to the design, growth, evolution, and operation of the global Internet and private networks built on the Internet Protocol.

Email: ipj@protocoljournal.org
Web: www.protocoljournal.org