
Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY
CYBER STATECRAFT
INITIATIVE
THE POLITICS OF INTERNET SECURITY
PRIVATE INDUSTRY AND THE FUTURE OF THE WEB
Justin Sherman

Scowcroft Center for Strategy and Security

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Cyber Statecraft Initiative

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

THE POLITICS OF INTERNET SECURITY

PRIVATE INDUSTRY AND THE FUTURE OF THE WEB

Justin Sherman

ISBN-13: 978-1-61977-125-3

Cover: Concept image of cables and connections for data transfer in the digital world. Credit: iStock.

October 2020

TABLE OF CONTENTS

Executive Summary 1

1: Introduction 2

2: Mapping Private Sector Influence on the Internet: Starting with Internet Protocols 4

3: Routing and the Border Gateway Protocol 8

- 3.1 How the BGP Works 8
- 3.2 How the BGP Malfunctions and Gets Exploited 9
- 3.3 Influencing the BGP's Security 13

4: Addressing and the Domain Name System 16

- 4.1 How the DNS Works 16
- 4.2 How the DNS Gets Exploited 16
- 4.3 Influencing the DNS's Security 18

Recommendations and Conclusion 22

About the Author 24

Acknowledgments 24

EXECUTIVE SUMMARY

The private sector's influence on the Internet's shape and behavior—and, therefore, its security—is enormous yet understudied. This infrastructural influence, spanning companies like Internet service providers and cloud services providers, is also underappreciated in US policy. The US government was the exclusive driver of Internet development for its first twenty-four years, and states continue to shape the Internet today through regulation, capacity-building, and direct participation in Internet processes. But Internet governance is now largely privatized. This report argues that the US private sector's unique influence on global Internet infrastructure gives it an opportunity and responsibility to improve Internet security, and that the US government should better collaborate with those actors and leverage that influence.

This argument matters because Internet insecurity is a national security issue for the United States and every other nation. Internet insecurity is also a selling point for the several authoritarian countries seeking to undermine trust in the free and open Internet model and replace it with a state-controlled, "sovereign" version. The US private sector, through its influence on the Internet's technology, protocols, standards, and operational practices, has an opportunity and responsibility to address these problems by reshaping the Internet to make it more secure—but many firms are not maximally using their influence to do so. It is critically important that US policymakers better understand this private sector influence on the Internet so it can help shape incentives for security.

This report examines two protocols as examples of private sector influence over presently vulnerable systems key to the Internet's function: the Border Gateway Protocol (BGP), used to route Internet traffic, and the Domain Name System (DNS), used to address Internet traffic. These two case studies detail how the protocols work, why they are vulnerable or error-prone, and what the private sector can do about it. This report uses empirical data on attacks and current protections.

This report concludes with a set of actionable recommendations for US policymakers. The US government should add Internet protocol security best practices to federal procurement rules, targeting major players with outsized influence on Internet infrastructure. The US government should also leverage its public-private partnerships to convene forward-looking discussions about the next set of Internet protocol security challenges. This report recommends that the US government require Internet protocol protections for federal agencies. It recommends private sector dialogues on threat data sharing for Internet protocol attacks. And it recommends a concerted US reinvestment in cyber diplomacy at the State Department to help establish state norms of nonaggression against key parts of the Internet's infrastructure.

1: INTRODUCTION

The private sector plays a crucial role in defining the changing shape of the Internet, especially its security. Any renewed US strategy to secure cyberspace must recognize and leverage this private sector influence, which spans everything from undersea fiber optic cables and the management of Internet exchange points to the definition of Internet standards and the management of cryptographic keys. Internet protocols for packet addressing and routing are a useful way to examine how the private sector and the US government can collaborate to improve global Internet security. Where the private sector may not maximally use its influence to shape these digital behaviors for security, the US government can incentivize firms to do so.

Governments influence the shape of the global Internet today by diverse means: laws around online content takedowns, commercial encryption, and data localization; interactions with standard-setting bodies like the Internet Engineering Task Force (IETF) and norm-setting bodies like the United Nations Group of Government Experts (UN GGE); and, more directly, via the procurement and construction of public infrastructure. Through regulation, standard-setting, diplomatic negotiations, overseas capacity-building and investment, trade agreements, and other mechanisms of statecraft, national governments can influence everything from the content flowing across the web to the undersea fiber optic cables that carry it.

But to an even greater degree, since the National Information Infrastructure (NII) plan of 1992, the Internet has been shaped by the private sector. Private corporations, especially those incorporated in the United States, are increasingly shaping the topology of the Internet (cables, servers, etc.) as well as its policies and procedures, like those that define how data traffic is routed from origin to destination. Multistakeholder Internet governance has in many ways become "the privatization of governance" with functions handled by the state in other domains overseen principally by the private sector in this one.[1] The private sector influences how the Internet is shaped and how it behaves through the design, construction, management, and ownership of Internet infrastructure and intellectual property. This is especially true where government regulation, norm-setting, or standard-setting in the technology sphere is slower than unilateral private sector action or is lacking altogether. All told, the private sector's role in this space is enormous yet incompletely studied and could be better leveraged in US government policy.

As some elements of the US government[2] work to increase the security of the Internet and its users—journalists, diplomats, businesses, citizens—they must address the influence of the private sector on global Internet security. Internet insecurity is a national security issue for the United States and every other nation. It has become even more important during the COVID-19 pandemic as citizens, businesses, and governments massively increase online activity that must be secured. Internet insecurity is also a selling point for many authoritarian countries which seek to promote a state-controlled replacement for the current Internet. Many private companies have influence over Internet infrastructure, and thus the power to improve Internet security, but are not maximally using it—which is where the US government can provide better incentives.

Internet protocols for packet addressing and routing are a prime point of this influence. They are defined by the Internet Engineering Task Force (IETF), a multistakeholder body composed of many different experts. That, in turn, tends to be mostly those companies which profit from new or improved standards: like Amazon and Google, AT&T and Verizon, Akamai and Cloudflare. How these companies help define and subsequently implement Internet protocols may seem obscure and geopolitically inconsequential, but it is quite the opposite. Packet addressing and routing protocols have profound impacts on the Internet—and so do their vulnerabilities. The National Institute of Standards and Technology (NIST) in 2019 called "BGP hijacking" attacks against the Internet's system of traffic routing "one of the greatest current threats to today's Internet."[3]

This report argues that the US government should collaborate with the private sector and integrate these firms' infrastructural influence over the Internet into a national strategy to bolster Internet security. US companies have a unique opportunity and responsibility to improve Internet security through their influence on Internet infrastructure, but many are not acting where they could. This report focuses on two protocols which are insecure and a considerable point of vulnerability on the global network, but which private companies can better protect and thus improve global Internet security—the Border

1 Laura DeNardis, Gordon Goldstein, and David A. Gross, *The Rising Geopolitics of Internet Governance: Cyber Sovereignty v. Distributed Governance* (New York: Columbia University, November 2016), 9.

2 For instance, see CISA (Cybersecurity and Infrastructure Security Agency), https://www.cisa.gov/.

3 William Haag et al. *Protecting the Integrity of Internet Routing: Border Gateway Protocol* (BGP) *Route Origin Validation*, NIST Special Publication 1800-14(2019): 2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-14.pdf.

Gateway Protocol (BGP) and the Domain Name System (DNS). This doesn't mean to suggest that these are the only protocols worth examining, nor that the discussed protections are the only ones—far from it—but that the BGP and the DNS are useful case studies.

- The first section examines the rising influence of corporations on the topology and digital rules of the Internet and the opportunity that provides to improve security. It examines Internet protocols as a case study.
- The next section is a case study of the BGP, its vulnerabilities, and one example of how companies can better protect it.
- The next section examines private sector influence on the DNS, major security vulnerabilities, and one example of how companies can better protect it.
- The final section makes five recommendations for the US government to build the private sector's influence on Internet infrastructure into a strategy for securing the Internet's digital rules.

2: MAPPING PRIVATE SECTOR INFLUENCE ON THE INTERNET: STARTING WITH INTERNET PROTOCOLS

It is a misconception to imagine that "the laws of cyberspace [are] immutable."[4] They are constantly evolving. The Internet's topology and digital rules are not a given, and government policy should not take them as such. Humans created the global Internet, from conceiving of the idea itself to building hardware and coding software to developing working groups on Internet standards. Today, private corporations increasingly influence the Internet's topology and digital rules.[5] These firms—Internet service providers (ISPs), content delivery networks (CDNs), cloud services providers, and social media companies—shape the Internet's topology by building server farms and laying fiber optic cables to connect their data centers to customers. They also shape the Internet's digital rules by implementing protocols that address and route Internet packets.

Where the US government was the principal architect and sole sponsor of Internet infrastructure from the inception of the ARPANET in 1968 to the implementation of the NII in 1992, subsequently, much network ownership and control has been in the private sector's hands. This means the firms controlling this Internet infrastructure can improve Internet security at scale by better protecting these protocols against manipulation. Broadly speaking, the digital rules by which Internet systems interoperate—including the BGP and the DNS, both discussed later—are developed, and maintained, by humans.

Companies routinely shape the Internet's topology and digital rules both of their own volition and in response to requirements or incentivization by governments. Google has recently participated in financing the construction of more than a dozen undersea cables.[6] Amazon, Facebook, Microsoft, and other companies have likewise invested in cable-building to enable faster Internet connectivity between population centers and their data centers.[7] Cloud service providers continue building Internet infrastructure, like data storage centers and the peripheral infrastructure to support them, as their customer bases and computing demands grow.[8] Cloud companies and content delivery networks may also use their own proprietary, internal traffic routing protocols to move data.[9] Companies beyond the United States are notably shaping the Internet's layout and rules in this way as well. For instance, China Telecom, the largest Chinese state-owned telecommunications company, continues to work with companies across the Philippines, Taiwan, Malaysia, Japan, and other countries in the Asia-Pacific region to develop undersea Internet cables to route global Internet data in a more Sino-centric way.[10]

Sometimes, this influence is deployed at the behest of governments. In China, the state maintains lists of keywords against which private companies must filter content—limiting the free flow of data.[11] The Iranian government requires Internet service providers to prioritize access to domestic

4 Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin Press, 2017), 90.

5 This, in turn, impacts information technology use. "The technology and human beings are continually adapting and mutually changing each other." Jeanette B. Ruiz and George A. Barnett, "Who Owns the International Internet Networks?" *Journal of International Communication* 21(1), 2015: 38-57, 38, https://www.tandfonline.com/doi/full/10.1080/13216597.2014.976583.

6 Adam Satariano, "How the Internet Travels Across Oceans," *New York Times*, March 10, 2019, https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html.

7 Satariano, "How."

8 See, for example, Gartner, Gartner forecasts worldwide public cloud revenue to grow 17% in 2020, press release, November 13, 2019, https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020.

9 For instance, Google was using its own proprietary QUIC protocol internally before governing bodies accepted the standard. Thanks to Trey Herr for further discussion of this point.

10 China Telecom, "How China Telecom is Connecting Countries Across Asia with the APG Line," accessed March 29, 2020, https://www.ctamericas.com/china-telecom-connecting-countries-across-apg/.

11 See, for example, Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, *Censored Contagion: How Information on the Coronavirus Is Managed on Chinese Social Media*, Citizen Lab, March 3, 2020, https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.

Internet resources over foreign ones.[12] India's Parliament is considering requiring local storage of data on Indian citizens and thus compelling foreign cloud providers to build local data centers.[13] The US National Security Agency has authority to compel ISPs, CDNs, and cloud service providers to provide real-time data collection for intelligence purposes and to maintain that access if requested.[14] In the European Union (EU), the General Data Protection Regulation (GDPR) forced companies to change data routing and storage practices to protect EU citizens' privacy and security.[15] All of these actions affect the flow of content around the Internet and directly or indirectly impact the Internet's topology. It is a stark reality that users in China have a different-looking and -behaving Internet than users in the United States, for example, in large part due to these technical changes and this infrastructural influence of the private sector.

How Internet data is addressed and routed is a prime example of this influence. Generally, Internet traffic needs two things to be sent around the world: it needs an address and a route to get there from its origin. It's companies that are often setting these addresses on their devices and systems and defining and choosing the routes. Put another way, firms controlling Internet infrastructure can influence the digital rules for how data flows through that infrastructure—and thus impact the Internet's behavior for billions of people. These name-resolution and traffic-routing decisions occur continuously, whether triggered by a user sending an email to a friend or a government agency communicating over encrypted messenger with a spy abroad. Where Internet data travels, and why, can have significant geopolitical effects.

This effectively makes some private firms foreign policy actors,[16] as their decisions about technology design, deployment, and operation can have global effects on politics, trade, and security. Faster and more reliable data routing enables faster business transactions. More secure data routing means it's safer for researchers to share proprietary data and for journalists to talk to sources. States, nonstate cyber proxies, and cybercriminals alike also spy and launch attacks over a physical Internet controlled by the often-overlooked parties operating "Autonomous Systems."

Each Autonomous System, or "AS," is one of the constituent networks of which the Internet is composed. An AS is uniquely identified by an Autonomous System Number (ASN), and is defined by having a unique, consistent, and centrally defined routing policy.[17] Internet users depend on the policies defined and enacted by these ASes every day to send emails, watch Netflix, collaborate on Google Drive, Zoom with friends and coworkers, and tweet the latest hot takes. These ASes are the "units" of routing on the global Internet, and they send Internet traffic both between servers in their network and externally to other ASes.[18] While often unrecognized, interconnection between ASes is a vital "inter" part of the Internet—traffic "hops" between these nodes when moving across the globe.

TABLE 1: Examples of Some Autonomous System (AS) Operator Services

Type of AS Operator	Examples of Services
Internet service provider (ISP)	Home WiFi, email hosting, corporate Internet services
Content delivery network (CDN)	Site hosting; music, video, video game streaming
Cloud providers	Site hosting, file sharing, renting memory and processing power to corporate clients

Source: Justin Sherman

12 See, e.g., Masha Alimardani, "After Iran Lifted a Ban on Telegram, It Continued to Throttle Access," *Slate*, March 9, 2018, https://slate.com/technology/2018/03/after-iran-lifted-a-ban-on-telegram-it-continued-to-throttle-access.html; and Collin Anderson, "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran," Arxiv.org, June 18, 2013, https://arxiv.org/pdf/1306.4361.pdf.

13 Reserve Bank of India, *Frequently Asked Questions*, https://m.rbi.org.in/Scripts/FAQView.aspx?Id=130; and Jennifer Daskal and Justin Sherman, *Data Nationalism on the Rise: The Global Push for State Control of Data*, Data Catalyst Institute, June 2020, https://datacatalyst.org/wp-content/uploads/2020/06/Data-Nationalism-on-the-Rise.pdf.

14 See, e.g., Sam Gustin, "NSA Scandal: As Tech Giants Fight Back, Phone Firms Stay Mum," *TIME*, July 3, 2013, https://business.time.com/2013/07/03/nsa-scandal-as-tech-giants-fight-back-phone-firms-stay-mum/. Since the leaks by Edward Snowden in 2013, investigative reporting has unveiled similar practices that are ongoing in the United States. See, for example, Ryan Gallagher and Henrik Moltke, "The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight U.S. Cities," Intercept, June 25, 2018, https://theintercept.com/2018/06/25/att-Internet-nsa-spy-hubs/.

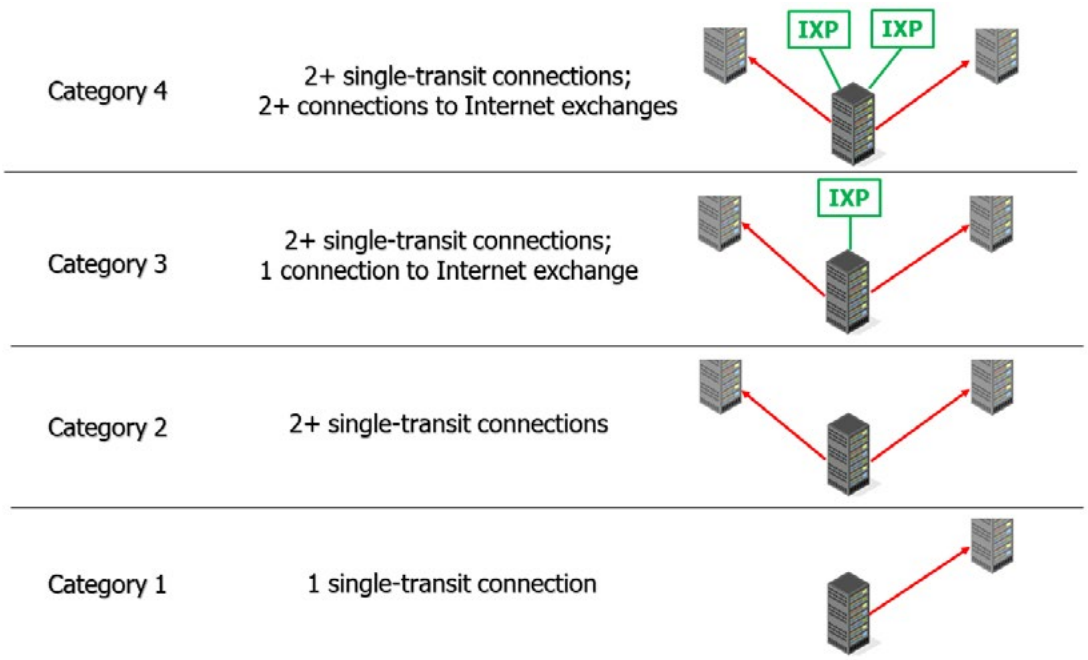
15 See, for example, Anu Bradford, "When It Comes to Markets, Europe Is No Fading Power," *Foreign Affairs*, February 3, 2020, https://www.foreignaffairs.com/articles/europe/2020-02-03/when-it-comes-markets-europe-no-fading-power.

16 Anne-Marie Slaughter, *The Chessboard and the Web: Strategies of Connection in a Networked World* (New Haven: Yale University Press, 2017), 23.

17 Thanks to Bill Woodcock for this definition.

18 Thanks to Bill Woodcock for this definition.

FIGURE 1: Four Categories of Network Operators Delineated by Their Connectedness



Source: Justin Sherman, adapted from Packet Clearing House, licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License

The three key categories of firms that manage these global network hubs are Internet service providers, content delivery networks, and cloud services providers. ISPs, like AT&T, CenturyLink, Comcast, and Verizon, transport Internet bandwidth from Internet exchange points to locations where users consume it, connecting devices like home routers and mobile phones to the web. CDNs like Akamai, Cloudflare, Limelight Networks, and Fastly provide servers that specifically deliver content, like streaming video, to end users.[19] Cloud providers like Amazon, Google, Microsoft, and Oracle rent out their digital resources (i.e., memory, storage, processing power) for customers to run applications and services, and are likewise responsible for routing large amounts of data and building some of their own Internet infrastructure.[20] These companies manage their own ASes and interconnect them with others to exchange traffic on the global Internet.

These firms—ISPs, CDNs, and cloud services providers—shape the Internet's topology by building server farms and laying fiber optic cables to deliver data to customers. They also shape the Internet's digital rules and substantially impact the security of the Internet by implementing protocols to address and route Internet packets.[21] These protocols determine where, when, and how data is routed, including if it is sent to the intended destination or on a safe path. They include, among others, the Border Gateway Protocol and the Domain Name System.

The BGP and the DNS help determine the outcome of major network failures, and their smooth operation across new or unexpected forms of failure helps determine the Internet's resilience. For instance, if a massive attack or technical disruption brings down servers in an Autonomous System, companies administering the DNS can maintain connectivity for users by rerouting queries to servers located away from the failure. If a major portion of the global network is jammed with traffic, to give another example, BGP implementors could change BGP policies to route traffic around the blockage. These are not just questions of security—for example, is the data encrypted or headed to the right destination—but also

19 "On the most basic level, a CDN is simply a network of servers used to deliver content." See: David Heidgerken, "Content Delivery Networks (CDN) Versus Cloud Computing: What's the Difference and Do I Need Both?" INAP, March 7, 2019, https://www.inap.com/blog/cdn-versus-cloud-computing-whats-difference-do-i-need-both/.

20 See, for example, "Google Cloud Infrastructure," Cloud.Google.com, accessed June 17, 2020, https://cloud.google.com/infrastructure.

21 Protocols may be commonly accepted, but varied implementations can have significant security effects. To use an analogy, many users might buy the same software, but some may configure the installation differently.

resilience, ensuring that Internet traffic moves from origin to destination even if there are failures in the network. This was a key component of the Internet's original design.

The BGP and the DNS are geopolitically significant because they are the mechanisms which link the Internet's constituent networks, and countries, together. These digital rules are implemented all around the world. The Internet exchange points (IXPs) at which inter-AS BGP connections occur, and at which most of the core DNS is hosted, are the centers of Internet bandwidth production—key to the Internet economy and locations where attackers can surveil, modify, redirect, or cut off Internet traffic.[22] Yet, it's not just about data security. The BGP and the DNS also affect this idea of resilience: failure to appropriately address or route traffic can lead to failure to keep users' data flowing. Vulnerabilities in the BGP and the DNS undermine security and resilience across the Internet ecosystem for the billions of users connected online every day: their flaws can have massively scaled effects on economic and national security.

Today, the BGP and the DNS are insecure because security was not a top priority when each was designed.[23] If anything, their core design principles, like many other protocols developed at the time, were interoperability—ensuring devices could communicate with one another—and resilience—ensuring that, in the event of a network failure, traffic would still reach its destination.[24] This gets to a broader point about the Internet and geopolitics, which is that companies that could hypothetically leverage their influence to improve Internet security, like with the BGP and the DNS, are often not doing so as much as they could.

Many of the companies maintaining Autonomous Systems today—ISPs, CDNs, and cloud services providers—are developing and updating services at the speed of a competitive market which struggles to incentivize good security practices. This leads to a recurring trend of features and performance being prioritized more highly than, or to the exclusion of, effective security. In 2018, for example, there was a campaign out of Iran to hack numerous DNS servers and steal information.[25] In June 2019, Verizon began using bad BGP routing information, diverting the traffic of other Internet companies away from its intended destination, because it hadn't implemented BGP safeguards even though it could have.[26] Numerous other examples are discussed in later sections of this report. Industry has engaged in work to fix some of these security problems.[27] But many aspects of the BGP and the DNS remain vulnerable to manipulation, leaving users, universities, businesses, and government agencies at risk.

The following sections build case studies of private sector influence on the security of the BGP and the DNS, demonstrating the reach and impact this influence can have on the security and resilience of the global Internet ecosystem. These protocols, and the protections subsequently discussed, are hardly the only examples of this phenomenon—but they are valuables ones. The principal argument is that companies with the potential to improve Internet security and resilience can do much more, which presents an opportunity and a need for governments, including in the United States, to introduce the right incentives.

22 This draws in part from the two forms of weaponized interdependence defined by Farrell and Newman: the panopticon effect, or the ability to "glean critical knowledge from information flows" concentrated at certain places, and the chokepoint effect, or the leveraging of power over hubs to penalize third parties. See: Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security*, 44(1), Summer 2019: 42-79, 55-56, 72, 74.

23 Many Internet pioneers have acknowledged this, and, in fact, David D. Clark, an MIT scientist, listed "security" as the first item in a 2008 list of new priorities for building a better Internet. Cited in: Craig Timberg, "A Flaw in the Design," *Washington Post*, May 30, 2015, https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

24 Robert Morgus and Justin Sherman, *The Idealized Internet vs. Internet Realities (Version 1.0): Analytical Framework for Assessing the Freedom, Openness, Interoperability, Security, and Resiliency of the Global Internet*, New America, July 26, 2018, 8, https://www.newamerica.org/cybersecurity-initiative/reports/idealized-Internet-vs-Internet-realities/.

25 Andy Greenberg, "Cyberspies Hijacked the Internet Domains of Entire Countries," *WIRED*, April 17, 2019, https://www.wired.com/story/sea-turtle-dns-hijacking/.

26 Liam Tung, "Amazon, Facebook Internet Outage: Verizon Blamed for 'Cascading Catastrophic Failure,'" *ZDNet*, June 25, 2019, https://www.zdnet.com/article/amazon-facebook-Internet-outage-verizon-blamed-for-cascading-catastrophic-failure/.

27 For instance, the issue of Domain Name System confidentiality has received much private sector discussion in the debates on DNS over TLS (DoT) versus DNS over HTTPS (DoH).

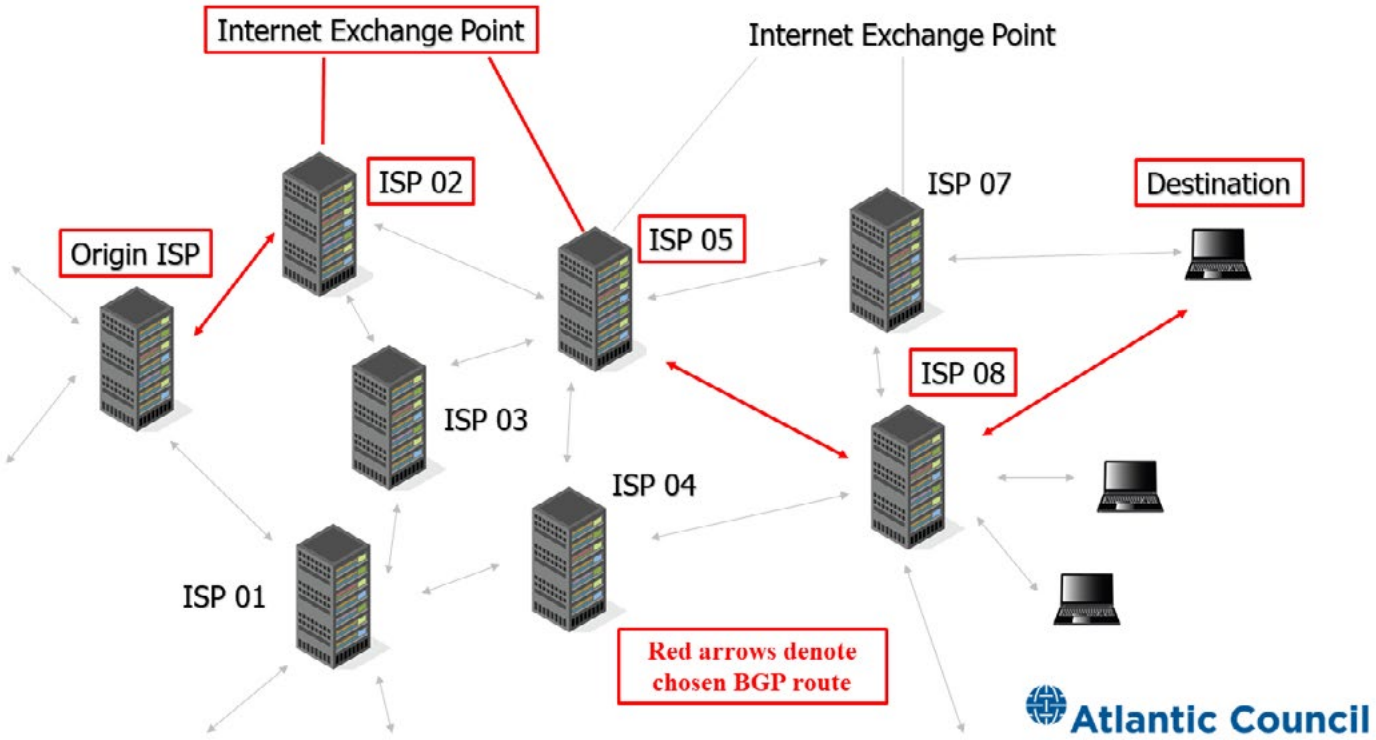
3: ROUTING AND THE BORDER GATEWAY PROTOCOL

3.1 How the BGP Works

The Border Gateway Protocol communicates potential paths that Internet packets can take from their origin to their destination. It's the Internet's "GPS" for traffic and a key part of the Internet's digital rules. There are multiple physical routes available to send an email from Washington, D.C., to a user in Berlin, because the Internet is made up of these meshed Autonomous Systems. But one of these paths must be picked and used. The BGP allows ASes like those operated by ISPs like Verizon, CDNs like Cloudflare, and cloud providers like Amazon and Google to communicate possible routes to each other. Then, for each packet which must be forwarded, each AS makes a routing decision—selecting a possible path it learned via the BGP from its neighboring ASes. These routing decisions typically prioritize the least-expensive or highest-performance routes.

Core to BGP routing is trust. ASes implicitly trust routing information received from neighboring ASes[28] because like many of the Internet's early protocols the BGP wasn't designed for security. Each time a packet moves from one AS to another (say, Verizon to Amazon), the sender assumes its own routing table (based on information from its neighbors, received via the BGP) reasonably approximates the actual topology of the

FIGURE 2: Visual of BGP Use Between Interconnected Autonomous Systems



Source: Justin Sherman

28 K. Sriram et al., "Problem Definition and Classification of BGP Route Leaks," Internet Engineering Task Force, RFC 7908, June 2016, https://tools.ietf.org/html/rfc7908#page-3.

Internet.[29] This blind trust problem explains the BGP's many malfunctions and exploitations.

3.2 How the BGP Malfunctions and Gets Exploited

ASes semi-regularly announce incorrect or inefficient paths—potentially forming a "route leak," where bad BGP data causes Internet traffic to move through unintended places, over highly inefficient routes, or to the wrong destination.[30] Companies may quickly correct them (shaping the Internet's behavior through real-time policy changes), but route leaks still disrupt traffic and produce unintended, sometimes disastrous, results. Human mistakes, like BGP misconfiguration, are a frequent cause of BGP routing errors.[31] And many ASes use BGP optimizers, which try to override other ASes' policies by taking advantage of their preference for specific routes—what one network engineer compared to prioritizing the destination "Buckingham Palace" over "London."[32] The problem is, this means that if any AS passes along a BGP route that's inefficient or incorrect but more specific, other ASes will typically blindly accept it.

These BGP errors occur daily, and they are not always innocuous. Route leaks can be malicious, where attackers abuse the BGP to hijack data along an unintended path or to an incorrect destination—allowing traffic to be blocked, modified, stolen, or spied upon. Attackers could break into an AS and change its BGP table's routing data. There's a good chance this maliciously designed route (i.e., sending traffic through a compromised midpoint) will be blindly accepted by neighboring ASes, leading to a propagation of the reroute. Alternatively, the legitimate operator of an AS could carelessly edit its routing information or policies, or could be compromised via an insider threat, achieving the same rerouting effects. The entire AS could also be malicious, set up for the sole purpose of injecting bogus routes.

The National Institute of Standards and Technology identifies five possible consequences of these hijacks: (1) denying access to Internet services; (2) redirecting Internet traffic through midpoints, either for eavesdropping at the midpoint or for adding in malicious code to attack the destination endpoint; (3) redirecting Internet traffic to the wrong endpoint; (4) undermining Internet Protocol-based reputation and filtering systems; and (5) undermining the Internet's routing stability.[33] The first and the third consequences are often connected, as delivering traffic to the wrong place is a way to deny a user access to services. The fourth and fifth consequences occur when incorrect or inefficient routes are propagated, as errors in and exploitations of the BGP undermine trust in the BGP itself and, more broadly, the Internet's ability to safely and reliably route data. In all cases of BGP route leaks, companies such as ISPs, CDNs, and cloud services providers using the BGP in an unsafe manner can undermine security across the global Internet.

29 J. Mauch, J. Snijders, and G. Hankins, "Default External BGP (EBGP) Route Propagation Behavior without Policies," Internet Engineering Task Force, RFC 8212, July 2017, https://tools.ietf.org/html/rfc8212.

30 Sriram, "Problem."

31 Barry Greene, "BGP Route Hijacking," *Akamai Blog*, November 5, 2018, https://blogs.akamai.com/2018/11/bgp-route-hijacking.html.

32 Tom Strickx, "How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today," Cloudflare, June 24, 2019, https://blog.cloudflare.com/how-verizon-and-a-bgp-optimizer-knocked-large-parts-of-the-Internet-offline-today/.

33 Haag et al., *Protecting*, 6.

TABLE 2: Snapshot of Major BGP Misrouting Incidents, 2015–20

Date	Duration	Affected Entities	Result	Security Effects (Using NIST Classification)
Nov. 2015	~9 hrs. (intermittent)	Akamai, TGP Telecom, Saudi Telecom, Tikona Digital Networks, Apple, Amazon, several other firms	Traffic routed through Bharti Airtel (India)[1]	Redirecting traffic through midpoint, undermining IP-based filtering, undermining routing stability
Apr. 2017	5-7 mins.	Symantec; EMC; MasterCard, Visa, Fortis, Alfa-Bank, Service Bank, several other financial services companies	Traffic routed through Rostelecom (Russia)[2]	Redirecting traffic through midpoint, undermining IP-based filtering, undermining routing stability
Dec. 2017	6 mins. (2x 3-min. events)	Google, Facebook, Apple, Microsoft	Traffic routed through Russian ISP[3]	Redirecting traffic through midpoint, undermining IP-based filtering, undermining routing stability
Apr. 2018	2 hrs.	Amazon	Some users redirected to phishing website[4]	Denying access to Internet services, redirecting traffic to wrong endpoint, undermining IP-based filtering, undermining routing stability
June 2018	2 hrs., 15 mins.	Hungarian ISP DoclerWeb Kft.	Traffic routed through Iran Telecommunication Company (Iran)[5]	Redirecting traffic through midpoint, undermining IP-based filtering, undermining routing stability
July 2018	45 mins. (1x 15-min., 1x 30-min. events)	Datawire, Vantiv, other payment processing firms	Traffic routed through Extreme Broadband (Malaysia)[6]	Redirecting traffic through midpoint, undermining IP-based filtering, undermining routing stability
Nov. 2018	1 hr., 14 mins.	Google	Traffic routed through MainOne Cable Company (Nigeria)[7]	Redirecting traffic through midpoint, undermining IP-based filtering, undermining routing stability
June 2019	2 hrs.	European networks, including Swisscom, KPN, Bouygues Telecom, and Numericable-SFR	Traffic routed through China Telecom (China)[8]	Redirecting traffic through midpoint, undermining IP-based filtering, undermining routing stability
June 2019	2 hrs.	Cloudflare, Amazon, Facebook, Linode, other Internet companies	Traffic routed through two small US firms whose systems crashed—rendering many websites unavailable[9]	Denying access to Internet services, redirecting traffic to wrong endpoint, undermining IP-based filtering, undermining routing stability
Apr. 2020	1 hr.	Google, Amazon, Facebook, Akamai, Cloudflare, over 200 CDNs and cloud service providers	Traffic routed through Rostelecom (Russia)[10]	Redirecting traffic through midpoint, undermining IP-based filtering, undermining routing stability

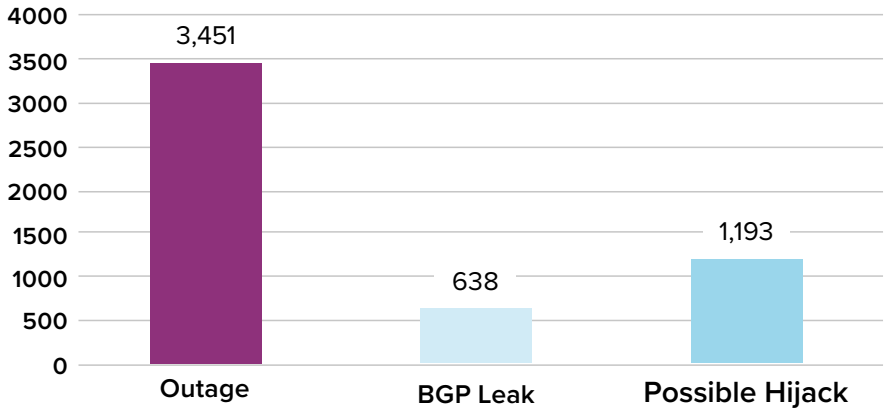
Source: Justin Sherman

1 Andree Toonk, "Large Scale BGP Hijack Out of India," BGPmon, November 6, 2015, https://bgpmon.net/large-scale-bgp-hijack-out-of-india/.
2 Dan Goodin, "Russian-Controlled Telecom Hijacks Financial Services' Internet Traffic," *Ars Technica*, April 27, 2017, https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-Internet-traffic/; and Andree Toonk, "BGPstream and The Curious Case of AS12389," BGPmon, April 27, 2017, https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/.
3 Dan Goodin, "'Suspicious' Event Routes Traffic for Big-Name Sites through Russia," *Ars Technica*, December 13, 2017, https://arstechnica.com/information-technology/2017/12/suspicious-event-routes-traffic-for-big-name-sites-through-russia/; and Andree Toonk, "Popular Destinations Rerouted to Russia," BGPmon, December 12, 2017, https://bgpmon.net/popular-destinations-rerouted-to-russia/.
4 Liam Tung, "AWS Traffic Hijack: Users Sent to Phishing Site in Two-Hour Cryptocurrency Heist," *ZDNet*, April 25, 2018, https://www.zdnet.com/article/aws-traffic-hijack-users-sent-to-phishing-site-in-two-hour-cryptocurrency-heist/.
5 Danny Adamatis et al., "Persian Stalker Pillages Iranian Users of Instagram and Telegram," Cisco Talos, November 5, 2018, https://blog.talosintelligence.com/2018/11/persian-stalker.html.
6 Doug Madory, "BGP / DNS Hijacks Target Payment Systems," August 3, 2018, Oracle Internet Intelligence, https://blogs.oracle.com/Internetintelligence/bgp-dns-hijacks-target-payment-systems.
7 Catalin Cimpanu, "Google Traffic Hijacked via Tiny Nigerian ISP," *ZDNet*, November 13, 2018, https://www.zdnet.com/article/google-traffic-hijacked-via-tiny-nigerian-isp/.
8 Catalin Cimpanu, "For Two Hours, a Large Chunk of European Mobile Traffic Was Rerouted through China," *ZDNet*, June 7, 2019, https://www.zdnet.com/article/for-two-hours-a-large-chunk-of-european-mobile-traffic-was-rerouted-through-china/.
9 Tung, "Amazon"; and Strickx, "How."
10 Catalin Cimpanu, "Russian Telco Hijacks Internet Traffic for Google, AWS, Cloudflare, and Others," *ZDNet*, April 5, 2020, https://www.zdnet.com/article/russian-telco-hijacks-Internet-traffic-for-google-aws-cloudflare-and-others/.

Route leaks occur with unsettling frequency. Data from BGPStream (an open-source BGP monitoring tool) indicates that in May 2020 alone, there were hundreds of BGP errors impacting ASes around the world.[34] These kinds of BGP events have impacted major technology firms like Facebook and Google, banking and financial services firms like MasterCard, and even US government agencies like the Department of Defense, a particularly frequent victim of inadvertent hijackings as a consequence of its broad holdings of IP addresses.[35] BGP route leaks can also vary in duration. Some last for hours and crash small companies' websites with misdirected traffic, like the second June 2019 incident in Table 2, or they could last for mere minutes but affect millions more people, compromising data from the likes of Google or Microsoft by routing traffic through a Russian state-owned telecom, as happened in April 2020.

These BGP incidents can have several, often overlapping effects, as noted using NIST's consequences of BGP events to code Table 2. Just one BGP routing error, like Google's traffic getting rerouted in November 2018 through MainOne Cable Company in Nigeria, can redirect traffic through an unanticipated midpoint, and undermine IP-based filtering systems and routing stability. BGP redirections, like Amazon user traffic going to a phishing website in April 2018, can send data to the wrong endpoint and compromise users' access credentials and identities. Malfunctions and exploitations of the BGP often go beyond just slightly delaying the delivery of traffic from one point to another. But again, these "major events" (Table 2) are just a snapshot; these protocol malfunctions and potential manipulations occur all the time. Global BGP incidents from January 1 through May 31 of 2020 can be seen in Figures 3 and 4.

FIGURE 3: Global BGP Incidents, January 1, 2020–May 31, 2020 (Count)

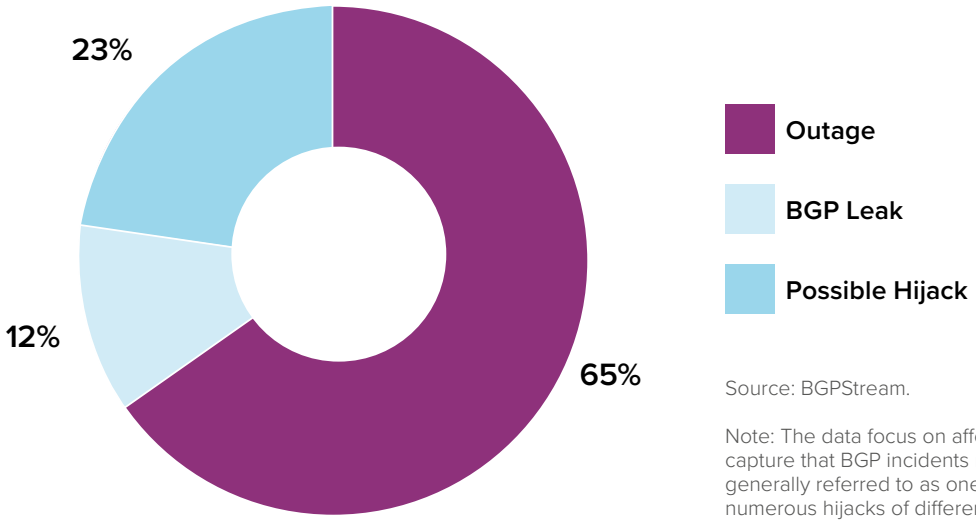


Source: BGPStream[1]

Note: The data focus on affected ASNs. They, thus, capture that BGP incidents reported in the press and generally referred to as one "hijack" may encompass numerous hijacks of different ASes' traffic.

1 Data from BGPStream. See: https://bgpstream.com/.

FIGURE 4: Global BGP Incidents, January 1, 2020–May 31, 2020 (Ratio)



Source: BGPStream.

Note: The data focus on affected ASNs. They, thus, capture that BGP incidents reported in the press and generally referred to as one "hijack" may encompass numerous hijacks of different ASes' traffic.

34 Data from BGPStream. See: https://bgpstream.com/.

35 Justin Sherman, "Hijacking the Internet Is Far Too Easy," *Slate*, November 16, 2018, https://slate.com/technology/2018/11/bgp-hijacking-russia-china-protocols-redirect-Internet-traffic.html.

Using the open-source BGPStream, data on BGP incidents from January 1, 2020, through May 31, 2020, show thousands of individual outages, BGP leaks, and possible BGP hijacks (Figure 3). The data are incomplete as different BGP monitoring tools have different perspectives on and visibility of the global network infrastructure, but BGPStream's data are a representative sample of the whole. Sixty-five percent of these events were outages, where BGP data transmission stopped working, but that still leaves 12 percent of incidents as BGP leaks (638 of them) and 23 percent as possible hijacks (1,193 of them). Many of these individual incidents may be collectively perceived by the media or analysts as one "event," but the data go to show that a single BGP malfunction or exploitation can impact numerous government agencies, companies, or end users.

There are many BGP routing incidents with difficult-to-establish causes, thus making them hard to sort into the category of malicious hijack or accident, and BGPStream's qualifying of hijacks as "potential" goes exactly to that point. Because of the implicit trust many ASes place in BGP route announcements, changes can propagate quickly and without malicious assistance.[36] It can be very difficult to discern intent. For example, in June 2019, traffic from multiple European networks was routed through China Telecom, the Chinese state-owned telecom, for two hours.[37] The BGP "route leak" occurred at Safe Host, a Swiss data colocation firm. It was possible for China Telecom to correct the BGP error once it received the traffic. Instead, China Telecom accepted the incorrect routes and began receiving traffic from European networks in the Netherlands, Switzerland, France, and more. "If any other ISP would have caused this incident, it would have likely been ignored," one journalist wrote.[38] But China Telecom's previous entanglement with BGP hijacks of long durations[39] meant this event raised some eyebrows.

TABLE 3: Five Autonomous Systems (Global) with Most Involvement in BGP Incidents, January 1, 2020–May 31, 2020

Autonomous System Operator	BGP Incidents, Jan. 1 2020–May 31 2020
Rostelecom (Russia)	132
DOD Network Information Center (United States)	99
Cafenet (Togo)	74
Uganda Telecom (Uganda)	57
Bangladesh Telegraph & Telephone Board (Bangladesh)	42

Source: BGPStream.

Note: The data focus on affected ASNs. They, thus, capture that BGP incidents reported in the press and generally referred to as one "hijack" may encompass numerous hijacks of different ASes' traffic.

TABLE 4: Five Autonomous Systems (Global) with Most Involvement in Potential BGP Hijacks, January 1, 2020–May 31, 2020

Autonomous System Operator	Potential Hijacks with AS Detected As Origin, Jan. 1 2020–May 31 2020
Rostelecom (Russia)	132
Angola Cables (Angola)	30
Wedare (Netherlands)	29
GigabitBank (Hong Kong)	27
CenturyLink (United States))	22

Source: BGPStream.

Note: The data focus on affected ASNs. They, thus, capture that BGP incidents reported in the press and generally referred to as one "hijack" may encompass numerous hijacks of different ASes' traffic.

36 Criticisms of existing attributions of BGP incidents as "hijacks" have focused on this difficulty. See, for example, Brenden Kuerbis, "The Folly of Treating Routing Hijacks As a National Security Problem," Internet Governance Project, November 29, 2018, https://www.Internetgovernance.org/2018/11/29/the-folly-of-treating-routing-hijacks-as-a-national-security-problem/.

37 Doug Madory, "Large European Routing Leak Sends Traffic Through China Telecom," Oracle Internet Intelligence, June 6, 2019, https://blogs.oracle.com/Internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom.

38 Cimpanu, "For Two."

39 Chris C. Demchak and Yuval Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," *Military Cyber Affairs* 3(1) Article 7 (2018): 1-9, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca; and Doug Madory, "China Telecom's Internet Traffic Misdirection," Oracle Internet Intelligence, November 5, 2018, https://blogs.oracle.com/Internetintelligence/china-telecoms-Internet-traffic-misdirection.

The suspicion of China Telecom is not unique, as the BGP has been abused by a handful of serial offenders over the past decade. China Telecom has already been the source of a dozen unique BGP incidents (leaks and possible hijacks) between January 1 and May 31 of 2020 alone. Russian state-owned telecommunications giant Rostelecom has been the source of numerous events over the past few years, including an April 2020 hijack that was one "incident" overall but encompassed the hijacking of dozens of different ASes' traffic (Table 2). AS operators in Angola, the Netherlands, and Hong Kong, and CenturyLink in the United States, were also detected by BGPStream as origins of numerous potential BGP hijacks in 2020 (Tables 3 and 4). Turla, widely believed to be a Russian state-sponsored espionage group,[40] has used BGP hijacks in tandem with other tools to deliver malware.[41] The Iranian government is no stranger to the BGP either, hijacking routes to target Iranian users of Instagram and the encrypted messaging app Telegram.[42] All this begs the question: if companies like AT&T and Verizon, Akamai and Cloudflare, Amazon and Google see BGP route leaks on the Internet every day, what can these Internet infrastructure operators do about it?

3.3 Influencing the BGP's Security

There are tools readily available to protect the BGP. One such tool is Resource Public Key Infrastructure (RPKI) for Route Origin Validation, used to sign and filter BGP origin data.[43] RPKI highlights the potential for the private sector to shape the Internet's digital rules for security and the reasons firms may not do so.[44] This makes it an exemplary case study for how the US government can help shape incentives—though just as the BGP is just one protocol that illustrates the private sector's influence on global Internet security, RPKI is just one mechanism for adding safeguards around the BGP.

RPKI is a way to cryptographically sign records that link IP addresses to their originating AS.[45] A regional Internet registry (RIR)—a nonprofit which manages Internet address space in different regions of the world—cryptographically signs assertions of IP address ownership. Then, the owner of said IP addresses signs a set of AS operators who can originate routes to those addresses. An AS operator like Amazon can download a local copy of the signed information.[46] Then, whenever Amazon receives new route announcements from neighboring ASes, it can check against this signed information to discard bad routes.[47] RPKI for Route Origin Validation only verifies legitimate destinations, not legitimate paths, but it builds more trust into Internet routing[48] and makes it easier for AS operators like Google and Cloudflare to route Internet data correctly.

It's up to the private sector to make these changes. AS operators can implement these protections to help secure Internet traffic routing at scale—improving security and resilience for every Internet user that needs traffic routed via the BGP, and protecting economic and national security in the process. The point is to raise costs: companies that put these safeguards around the BGP, the Internet's "GPS," make it harder for malicious actors to hijack the BGP and make it harder for those that still hijack the BGP to do so without detection. Keeping in mind that RPKI for Route Origin Validation is just one safeguard (just as the BGP is just one protocol), many other efforts, like machine learning to detect hijack patterns,[49] can further supplement Internet routing security.

This one illustrative solution isn't perfect; precisely because the Internet is human-made, from hardware cables to phone apps, it will always contain imperfections of human origin. Cryptographically signed routing tables can be compromised,

40 United States Computer Emergency Readiness Team, "NSA and NCSC Release Joint Advisory on Turla Group Activity," October 21, 2019, https://www.us-cert.gov/ncas/current-activity/2019/10/21/nsa-and-ncsc-release-joint-advisory-turla-group-activity.

41 *Diplomats in Eastern Europe Bitten by a Turla Mosquito*, ESET, January 2018: 8-9, https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf.

42 Danny Adamatis et al., "Persian Stalker Pillages Iranian Users of Instagram and Telegram," Cisco Talos, November 5, 2018, https://blog.talosintelligence.com/2018/11/persian-stalker.html.

43 Others include, for example, RPSL, BCP-38, and uRPF. RPKI, examined here, is merely one protection.

44 NIST lays out RPKI, BGP origin validation, and prefix filtering separately, but insofar as the last two leverage RPKI, I discuss all three at once here. Kotikalapudi Sriram and Doug Montgomery, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, NIST Special Publication 800-189, National Institute of Standards and Technology (2019): 2, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf.

45 Martin J Levy, "RPKI – The Required Cryptographic Upgrade to BGP Routing," Cloudflare, September 19, 2018, https://blog.cloudflare.com/rpki/.

46 Depending on its size, an AS operator may locally store one or multiple copies of a cached route. R. Bush and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol," Internet Engineering Task Force, RFC 6810, January 2013, https://tools.ietf.org/html/rfc6810.

47 R. Bush, "Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)," Internet Engineering Task Force, RFC 8481, September 2018, https://tools.ietf.org/html/rfc8481; and P. Mohapatra et al., "BGP Prefix Origin Validation," Internet Engineering Task Force, RFC 6811, January 2013, https://tools.ietf.org/html/rfc6811.

48 Levy, "RPKI."

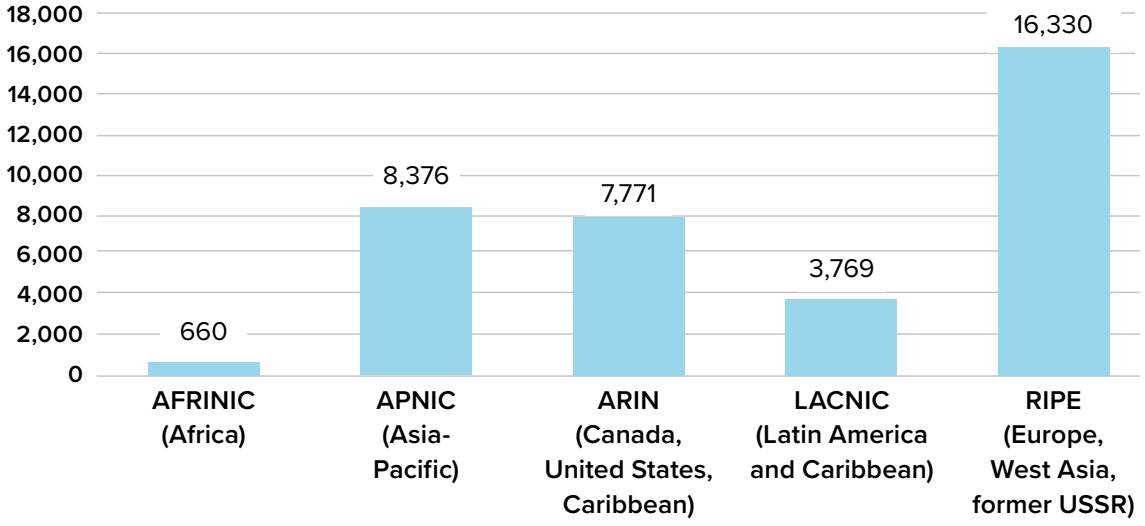
49 Liam Tung, "MIT: We've Created AI to Detect 'Serial Internet Address Hijackers,'" *ZDNet*, October 9, 2019, https://www.zdnet.com/article/mit-weve-created-ai-to-detect-serial-Internet-address-hijackers/; and Cecilia Testart et al., "Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table," *Internet Measurement Conference*, October 21-23, 2019, http://people.csail.mit.edu/ctestart/publications/BGPserialHijackers.pdf.

pattern detection systems can make errors, and malicious actors could pose as authorized AS operators to pass bad BGP routes to Google, for example, even with RPKI, hijacking content bound for a government service or large company.[50] But the private sector implementing these protections at scale would contribute massive improvements over the status quo. As one network engineer put it, "only a small specific group of densely connected organizations" needs to deploy RPKI on top of those already doing it "to positively impact the Internet experience for billions of end users."[51] More AS operators like AT&T or Verizon or Google or Cloudflare checking their BGP routes means a lower frequency of routing failures. This shapes the Internet's digital rules to improve security.

Yet, many have not signed and filtered routes with RPKI. Implementation of this protection on a regional basis—broken down by the five regional Internet registries which manage Internet address space for respective regions—varies as well, with the highest rate of adoption in Europe and the rate of adoption lagging within the North American region served by the American Registry for Internet Numbers (ARIN) (Figure 5).

FIGURE 5: Regional Internet Registries and RPKI Implementation

Route Origin Authorizations by Regional Intenet Registry (May 31, 2020 Snapshot)

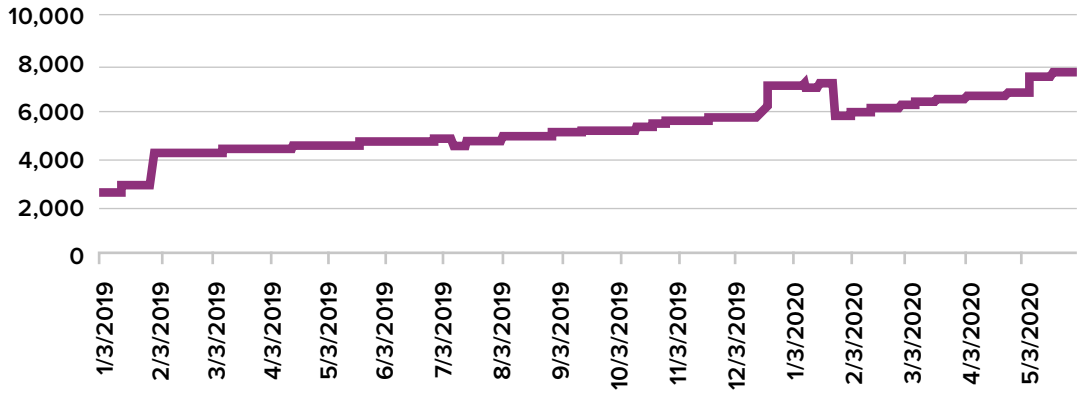


Source: RIPE.[1]

Note: Total number of resource certificates created under regional Internet registry trust anchor.

1 Downloaded from RIPE's Network Coordinate Centre, accessed July 7, 2020, https://certification-stats.ripe.net/.

FIGURE 6: American Registry for Internet Numbers (ARIN) and RPKI Implementation (through May 31, 2020)



Source: RIPE.

Note: Total number of resource certificates created under regional Internet registry trust anchor.

50 Jérôme Fleury and Louis Poinsignon, "RPKI and BGP: Our Path to Securing Internet Routing," Cloudflare, September 19, 2018, https://blog.cloudflare.com/rpki-details/.

51 Job Snijders of NTT Communications, quoted in: Madory, "BGP / DNS."

Routing security is a collective action problem; it takes more than one company to shape the Internet's digital rules. Benefits scale with the number of AS operators which implement routing security improvements. Marginal costs of implementation for one operator—including time and resources, concern about complexity and malfunctions, and concern about liability for those malfunctions—can outweigh perceived benefits if deployment is not widespread. And, clearly, deployment is not as widespread as it could be, though RPKI protections implemented by operators within ARIN have been rising (Figure 6). Firms might only partially employ this BGP safeguard,[52] and a lack of action at the global level illuminates the need for better government-private sector cooperation on this issue set. This is especially true in North America, where technology companies have an outsized influence on global Internet security.

Companies face several important disincentives to RPKI adoption which policymakers can help to address:

1. **Coordination:** RPKI must be implemented at scale, across many different AS operators, for it to effectively improve routing security. Telecommunications companies may privately say they support improvements to BGP security, for instance, but will not act if other companies won't either—the risks are not worth it. Coordinating this action at scale is difficult. Policymakers can help by putting RPKI into federal procurement rules, which is a way to incentivize security best practices in the industry without legislative regulation (see Recommendation 1). Policymakers can also invest more in cyber diplomacy to develop norms around the protection of and noninterference with the BGP (see Recommendation 5).

2. **Cost:** While many ISPs, CDNs, and cloud services providers are investing much more in security today than they were ten years ago, that investment has not focused on networking as heavily as other areas. Many companies still favor fast and resilient systems over deployment of more secure routing. Competition among firms, particularly for large operators, is a key part of the calculus as well. Policymakers could leverage public-private partnerships to explore other ways to incentivize firms and lower costs (see Recommendation 2). Policymakers can also push for RPKI protections on government systems to add another set of large AS operators to the list of those using RPKI (see Recommendation 3). Firms themselves can also share threat data from their insights into the Internet infrastructure (see Recommendation 4).

3. **Uptime:** BGP routing is key to the Internet's infrastructure. Network operators worry about RPKI causing even temporary errors in routing (or slightly slower routing), especially when scaled up for large operators where technical problems could have broader effects. This uptime issue affects other critical infrastructure, for example, delays in patching electrical power generation and distribution equipment which is operating near constantly. Industry and policymakers cultivating communities of knowledge among RPKI operators could help lower these risks (see Recommendation 2), as could pushing firms to implement protections at the same time via federal procurement rules (see Recommendation 1).

4. **Liability:** US network operators and ARIN, the regional Internet registry for North America, have conflicting risk tolerances for liability in the event of an RPKI malfunction. In other words, these entities have different stances on who should be liable for possible damages if an RPKI implementation malfunctions. Presently, many network operators maintain that they cannot or will not sign onto using RPKI with ARIN because of indemnification language in ARIN's services agreement, which they assert is too broad in its shielding of ARIN from liability.[53] ARIN, which recently made some revisions to the indemnification language, maintains that this language is necessary for an entity with a critical role in the global Internet and a significantly smaller budget than many network operators. This remains, in the words of one observer, a "logjam." The government can thus use its public-private partnerships and convening power to push further dialogue on this issue (see Recommendation 2).

AS operators can modify their processes to integrate RPKI and other routing security methods to better protect the Internet from routing attacks and errors. These operators wield tremendous influence over this infrastructure. But routing is just one example of poor incentives for firms to do as much as they can to shape the Internet for security, just as RPKI as discussed here is merely one protection for the BGP. The following section examines similar issues in another key Internet protocol—the DNS—to frame the paper's five recommendations in the final section.

52 This is indicated by data such as that from Cloudflare's IsBGPSafeYet dataset, downloaded from Cloudflare's IsBGPSafeYet.com, accessed on May 26, 2020, https://github.com/cloudflare/isbgpsafeyet.com/blob/master/data/operators.csv. Also based on IPinfo's list of AS operators in the United States. Accessed on May 26, 2020. https://ipinfo.io/countries/us. But classification isn't just a matter of considering the number of IP addresses in a single AS, for example, but considering other factors like AS interconnectedness.

53 Two legal scholars note that "our interviews with legal personnel have corroborated the view that indemnification is not typically an automatic deal-breaker, but rather acts as a weight on the scale." Christopher S. Yoo and David A. Wishnick, "Lowering Legal Barriers to RPKI Adoption," *Faculty Scholarship at Penn Law*, 2035, 2019, 14, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3037&context=faculty_scholarship.

4: ADDRESSING AND THE DOMAIN NAME SYSTEM

4.1 How the DNS Works

Before networks can route traffic around the world for Netflix or Skype or Facebook or Google Drive, they must know its address. The source of these addresses is the Domain Name System, often referred to as "the Internet's phone book," which translates domain names (i.e., atlanticcouncil.org) typed into a browser, or included in the right-hand side of an email address, to their respective Internet Protocol (IP) address (i.e., 104.20.20.178) to direct Internet traffic to its proper destination.[54] Like the BGP, the DNS is a protocol that is both critical to the Internet's digital rules and quite vulnerable to hacking and manipulation—and illustrates the potential for better government-private sector coordination on securing the Internet. It is again just one case study, and the protections for DNS integrity discussed within are only one protection available, like years-long government and industry efforts around DNS confidentiality.[55]

Speed and resilience were priorities for the Internet's design, and the DNS is no exception. The DNS does provide numerous benefits; users only have to remember website names, not IP addresses, and when IP addresses change, as when Google or Amazon physically relocate servers supporting their cloud services, website names stay the same while being mapped to new IP addresses. The DNS's abstraction layer also allows companies to link a single domain name to multiple IP addresses, and multiple domain names to single IP addresses, allowing a company like Verizon or Akamai to route data to users from the closest or fastest available server and to distribute the impact of large denial-of-service (DoS) attacks.[56]

Similar to the BGP, the DNS can be run internally to a network, like a firewalled corporate intranet, but the discussion here focuses on its use on the global Internet.

4.2 How the DNS Gets Exploited

The DNS is vulnerable to manipulation, and here this focuses on integrity (as opposed to, say, confidentiality). Attackers can intercept and maliciously edit DNS queries and responses to send users to malware-laden websites instead of their intended destination. Users might expect their banking website but instead be disclosing their banking credentials to a visually indistinguishable but malicious imposter. This could happen on the user's device, between the user and their recursive resolver, within the recursive resolver itself or, most commonly, between the recursive resolver and authoritative servers. This last attack is most broadly effective as it can change Internet packet addressing for all downstream devices.[57]

The DNS is also vulnerable because of a process called caching. Because it's costly (in time and resources) for computers to repeatedly request the same information from upstream servers, they store copies of the answers they receive in a local cache, thereby speeding up subsequent queries and vastly reducing demand on the network and servers. But cache maintenance requires many rules and policies, and this is another "attack surface" subject to exploitation. Using "DNS tunneling," hackers can also use channels of DNS communication between a computer and a DNS server to exfiltrate information or facilitate malware command-and-control through firewalls, which may not be able to validate DNS traffic.[58] It's a way to covertly steal data.

54 See, for example, "Public DNS," Google Developers, accessed May 20, 2020, https://developers.google.com/speed/public-dns.

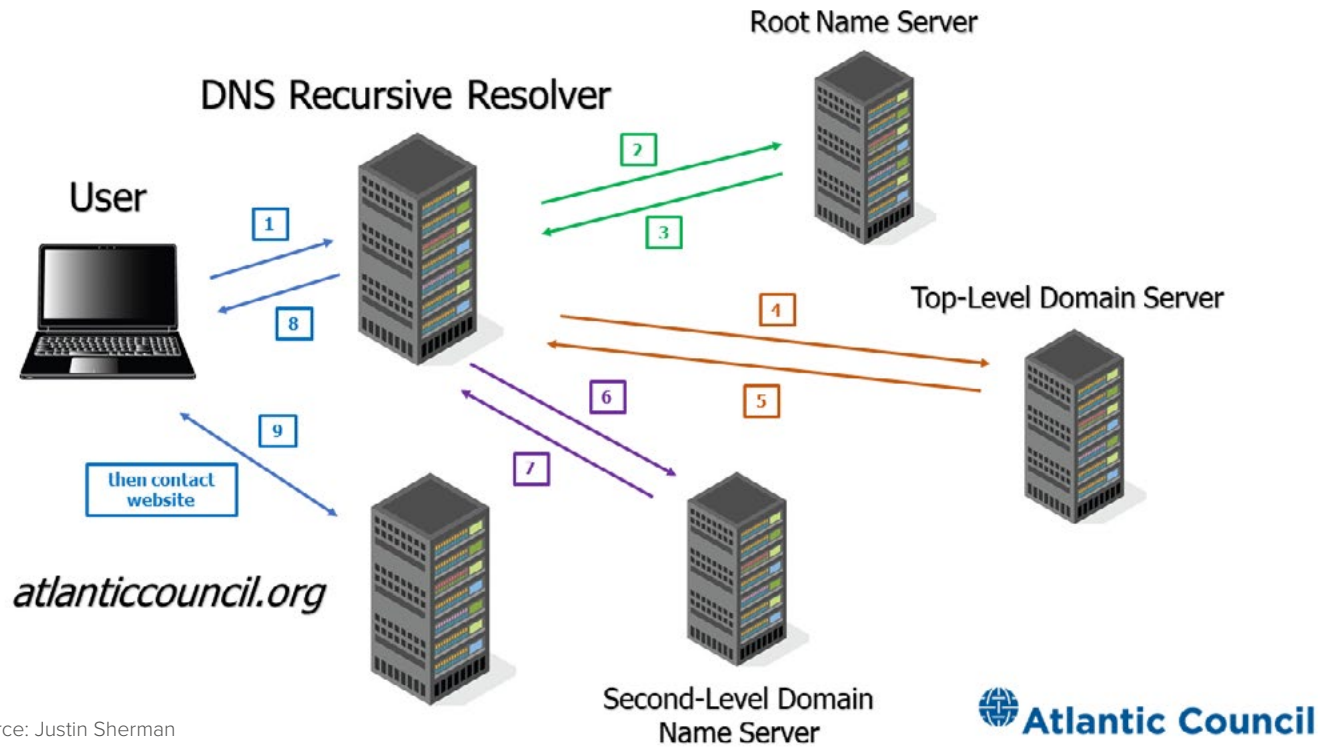
55 See, for example, Communications Security, Reliability, and Interoperability Council's work on DNS security, or IETF's work on the aforementioned DNS over TLS (DoT) versus DNS over HTTPS (DoH) issue.

56 J. Klensin, "Role of the Domain Name System (DNS)," Internet Engineering Task Force, RFC 3467, February 2003, https://tools.ietf.org/html/rfc3467.

57 Scott Fulton, "Top 10 DNS Attacks Likely to Infiltrate Your Network," *NetworkWorld*, February 20, 2015, https://www.networkworld.com/article/2886283/top-10-dns-attacks-likely-to-infiltrate-your-network.html; and Imperva, "Domain Name Server (DNS) Hijacking," accessed May 21, 2020, https://www.imperva.com/learn/application-security/dns-hijacking-redirection/.

58 Jeff Petters, "What Is DNS, How It Works + Vulnerabilities," *Inside Out Security Blog*, Varonis, March 29, 2020, https://www.varonis.com/blog/what-is-dns/.

FIGURE 7: DNS in Operation



Source: Justin Sherman

First, a user types a website name into a browser; second, the computer sends this name over the Internet to a DNS "recursive resolver"; and third, this recursive resolver queries a hierarchy of subsequent servers to fetch the Internet address information: a "root name server," a "top-level domain name server," and a "second-level domain name server."[1] Private companies have a notable hand in these digital rules. They can maintain mappings of website names to IP addresses. A few organizations can even filter DNS queries for security reasons.[2] Every day, private companies are implementing the DNS with geopolitical and security consequences.

1 Cloudflare, "What Is DNS?" accessed May 20, 2020, https://www.cloudflare.com/learning/dns/what-is-dns/; "What Is a DNS Query?" ClouDNS.net, accessed May 20, 2020, https://www.cloudns.net/wiki/article/254/; and Chris Gonyea, "DNS: Why It's Important and How It Works," Dyn, August 9, 2018, https://dyn.com/blog/dns-why-its-important-how-it-works/.

2 P. Hoffman, A. Sullivan, and K. Fujiwara, "DNS Terminology," Internet Engineering Task Force, RFC 8499, January 2019, https://tools.ietf.org/html/rfc8499.

There have been numerous DNS hijacks over the past few years, including a notable global DNS hijack campaign—dubbed "DNSpionage"—by actors with apparent links to Iran, that illustrate this problem. In November 2018, Cisco's Talos unit reported on "a new campaign targeting Lebanon and the United Arab Emirates" which impacted .gov domains and a Lebanese airline. The attackers also compromised the DNS of legitimate .gov and private domains in target countries, potentially redirecting traffic.[59] Yet this is hardly the only large-scale DNS hijacking incident. In April 2019, Cisco Talos published a report detailing another DNS hijacking campaign with public and private targets, "including national security organizations." Talos dubbed the operation, likely beginning as early as January 2017 and continuing into 2019, "Sea Turtle." It expressed concern that the operation's success would "lead to actors more broadly attacking the global DNS system."[60] However, these hijacks are not always as related to geopolitical and state security interests; other separate DNS hijacks have targeted individuals as well. For instance, cryptocurrency service MyEtherWallet was hit with a DNS hijack in August 2018 that stole more than $150,000 in cryptocurrency from the site's users.[61] In total, these incidents underscore poor security on the part of the DNS.

59 Warren Mercer and Paul Rascagneres, "DNSpionage Campaign Targets Middle East," Cisco Talos, November 27, 2018, https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html.

60 Danny Adamitis et al., "DNS Hijacking Abuses Trust in Core Internet Service," Cisco Talos, April 17, 2019, https://blog.talosintelligence.com/2019/04/seaturtle.html.

61 CoinDesk, "$150K Stolen From MyEtherWallet Users in DNS Server Hijacking," April 24, 2018, https://www.coindesk.com/150k-stolen-myetherwallet-users-dns-server-hijacking.

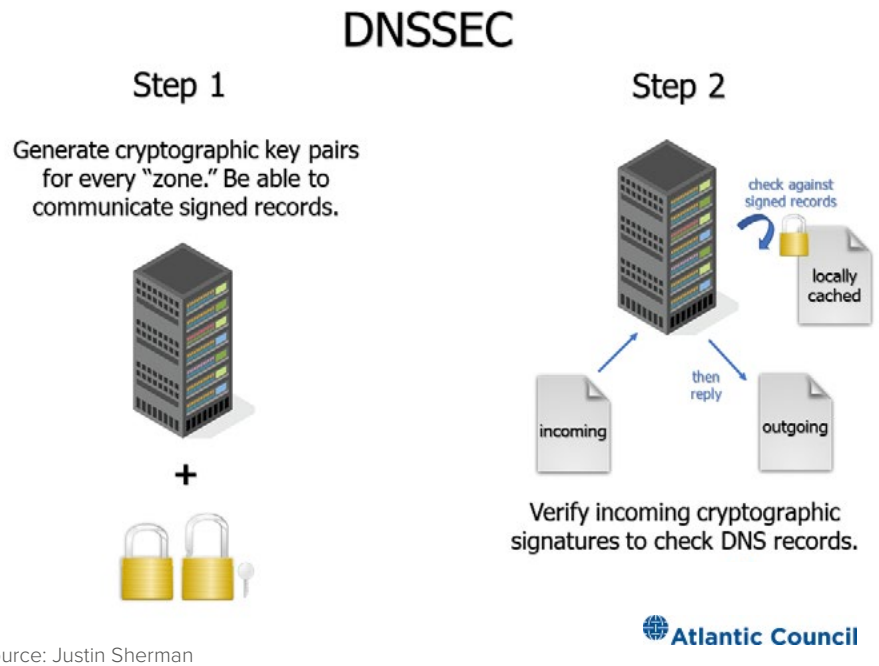
4.3 Influencing the DNS's Security

DNS hijacks and abuse hurt users and civil society organizations, businesses, and governments. Like other human-designed Internet rules, the DNS is not set in stone; in fact, companies with infrastructural influence over the Internet are rapidly reshaping the DNS protocol suite. To protect the DNS, AS operators, website hosts, and other companies or institutions that connect their constituents' systems to the Internet (e.g., for corporate and university networks) can implement DNS Security Extensions (DNSSEC). This is but one protection for the DNS, which is again one protocol—but collectively a valuable case study for private sector Internet influence.

DNSSEC uses public key cryptography to create a trust model for DNS records—it yields records that are verifiable by anyone receiving them.[62] This beneficially separates the data's integrity from the security of the servers and networks which handle it,[63] the equivalent of a detective sealing evidence in a tamper-evident bag.[64] A court can still verify the integrity of the evidence inside, regardless of whose hands it passed through between the detective and the court. Like RPKI, to implement DNSSEC, users must both create signatures and verify them.[65] One party signing the data is a necessary precursor to another party using the signature to verify the data's integrity—but the system as a whole is not secure until and unless both steps have been completed.

Just as the DNS is one protocol that highlights the private sector's overlooked, vital impact on global Internet security, DNSSEC is just one DNS protection. It doesn't solve all DNS security problems by itself. DNSSEC data is signed but not encrypted: computers can check a DNS record's authenticity (e.g., a user can verify the IP address they received for atlanticcouncil.org is the correct one), but the transaction's confidentiality is not protected (e.g., someone could see the user wants to connect to atlanticcouncil.org).[66] DNSSEC can also be implemented incorrectly,[67] and DNSSEC cannot

FIGURE 8: DNSSEC in Operation



Source: Justin Sherman

In the first step, the server operator must generate cryptographic key pairs for every "zone"—a portion of the Internet address space managed by a particular entity[1]—and then be able to communicate those signed records.[2] In the second step, the operator must be able to verify incoming cryptographic signatures from others to evaluate DNS record trustworthiness. Like with the BGP, the Internet's "GPS," companies can implement these protections for the DNS, the Internet's "phone book," to better protect Internet packet addressing.

1 Cloudflare, "What Is a DNS Zone?" accessed May 27, 2020, https://www.cloudflare.com/learning/dns/glossary/dns-zone/.

2 Internet Society, "DNSSEC Basics," accessed May 27, 2020, https://www.Internetsociety.org/deploy360/dnssec/basics/.

62 Verisign, "How DNSSEC Works to Provide the Protocol for a Secure Internet," accessed May 27, 2020, https://www.verisign.com/en_US/domain-names/dnssec/how-dnssec-works/index.xhtml.

63 R. Arends et al., "DNS Security Introduction and Requirements," Internet Engineering Task Force, RFC 4033, March 2005, https://tools.ietf.org/html/rfc4033.

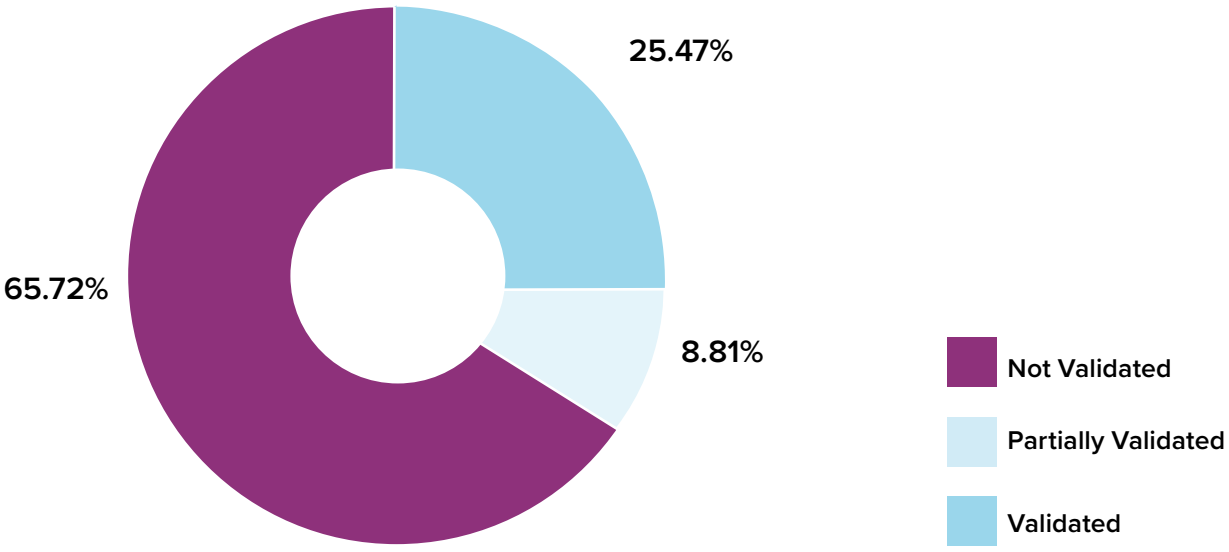
64 Credit goes to Bill Woodcock for this analogy.

65 Ramaswamy Chandramouli and Scott Rose, *Secure Domain Name System (DNS) Deployment Guide*, NIST Special Publication 800-81-2, Gaithersburg: National Institute of Standards and Technology, 2013, 9-1, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf.

66 Archana Kesavan, "Introduction to DNSSEC Monitoring," ThousandEyes, March 31, 2017, https://blog.thousandeyes.com/introduction-dnssec-monitoring/.

67 Site24x7, "DNSSEC Validation Results and Troubleshooting Tips," accessed June 22, 2020, https://support.site24x7.com/portal/en/kb/articles/dnssec-validation.

FIGURE 9: DNSSEC Validation Across Internet Users (Global)



Source: APNIC.[1]

Note: Users using DNSSEC-validating resolvers.

1 Downloaded from APNIC's DNSSEC Validation Rate dataset, accessed on May 26, 2020, https://stats.labs.apnic.net/dnssec. Also see methodology: Geoff Huston, "DNSSEC Validation (Revisited)," *ISP Column*, Potaroo.net, February 2020, https://www.potaroo.net/ispcol/2020-02/validating.html.

protect users from mistyping domain names; "typosquatting" is a frequent form of attack—for example, catching users who type "atlanticouncil.org" or "atlanticcouncil.com" instead of "atlanticcouncil.org."[68] It's up to the private sector to act, but that action is not widespread.

Globally, 65.7 percent of end users are neither performing DNSSEC validation nor trusting a recursive resolver to do it for them (Figure 9); they are still reliant on the DNS in its original and less-secure form. Once again, North America trails much of the world with only 28.5 percent of users seeing validated DNSSEC connections relative to 38.5 percent in Oceania and 29.5 percent in Europe. North America also lags in partial DNSSEC validation, with partial validation[69] much higher in Africa and Asia (Figure 10). Private industry plays a major arole in this, underscoring an urgent need for government action and government-private sector coordination on poor market incentives, collective action problems, and a lack of available tools, particularly for small firms. But even on the government side, North America is behind: for instance, the United Kingdom's National Cyber Security Centre offers up a Protective Domain Name System (implemented by Nominet UK, the .uk domain name registry) to make DNS protections easier in the UK,[70] whereas US government agencies are still lagging in DNSSEC adoption despite existing requirements for its implementation.[71]

68 Jesus Vigo, "Why Your Company Should Consider Implementing DNS Security Extensions," TechRepublic, March 2, 2018, https://www.techrepublic.com/article/why-your-company-should-consider-implementing-dns-security-extensions/.

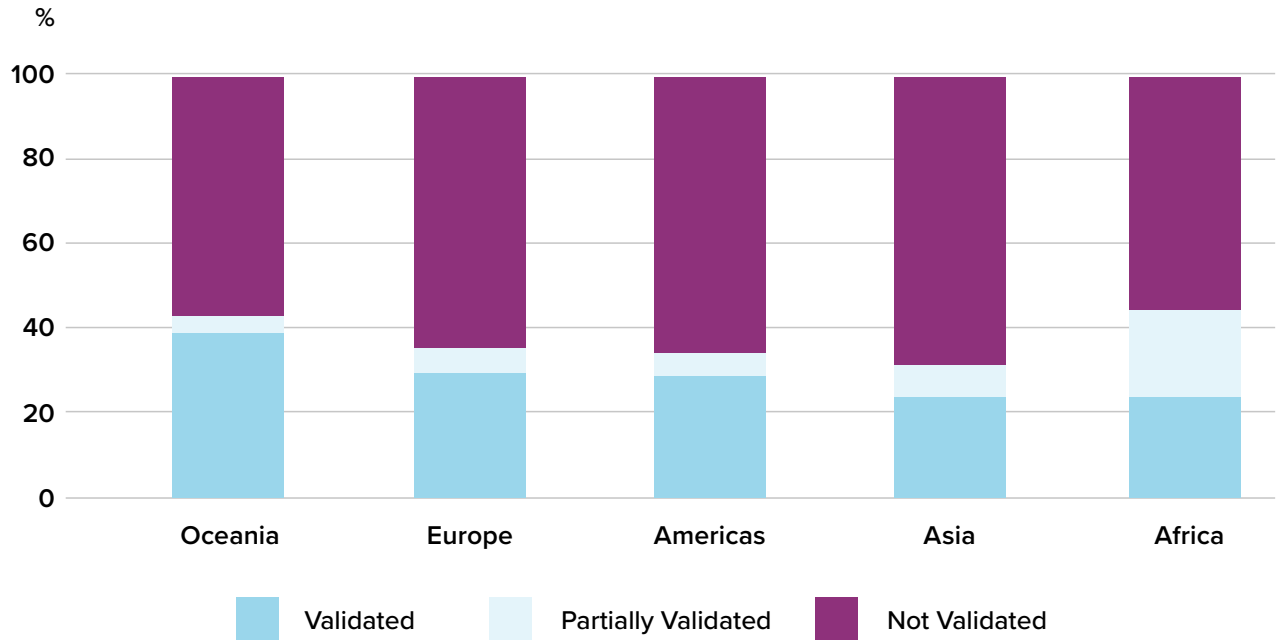
69 Partial validation describes when some of the user's resolvers validate and others do not. Thanks to Geoff Huston for providing this clarification.

70 United Kingdom National Cyber Security Centre, "Protective DNS (PDNS)," accessed June 22, 2020, https://www.ncsc.gov.uk/information/pdns.

71 NIST (National Institute of Standards and Technology), "Estimating IPv6 & DNSSEC External Service Deployment Status: Background and Methodology," accessed June 22, 2020, https://fedv6-deployment.antd.nist.gov/.

FIGURE 10: DNSSEC Validation Across Internet Users (Regional, Graph)

Estimated DNSSEC Validation by End Users, Regional (May 2020 Snapshot)



Source: APNIC.[1]
Note: Users using DNSSEC-validating resolvers.

1 APNIC's DNSSEC Validation Rate dataset.

Protections for the DNS, a key Internet protocol, are an example of a strong opportunity for the private sector to use its influence over the Internet to improve security for all. Yet, there are several barriers to wider action and adoption:

1. **Collective Action:** Like RPKI, the benefits of DNSSEC scale with the number of entities using it. Implementing DNSSEC does take work, yet more companies and individuals doing that work to implement DNSSEC measures on their end devices could add pressure on domain name server operators to implement DNSSEC themselves.[72] Policymakers could introduce federal procurement requirements here to encourage protections among large private sector operators (see Recommendation 1). They could also push the government to implement protections on its systems (see Recommendation 3).

2. **Cost:** Implementation of DNSSEC requires time and resources, like configuring signed addresses for one's domains. This is an obstacle for network operators and DNS providers in a constant race to maintain and improve network speed and stability.[73] Deploying protections at scale, like with many protocol protections, can also yield its own challenges and technical side effects. Policymakers can thus use the government's coordinating functions to convene public-private dialogues on this Internet protocol security challenge (see Recommendation 2).

3. **Stability:** DNSSEC implementations fail safe, by design. When anything goes wrong, the user cannot proceed because doing so would leave them open to compromise. For instance, nameservers might incorrectly sign records and thus prevent users from accurately validating DNSSEC-signed addresses.[74] Policymakers can use the government's coordinating and best-practice-sharing functions to help address stability issues when firms shape the Internet for security (see Recommendation 2). Policymakers can also invest in norm development for protecting and not interfering with the DNS (see Recommendation 5).

72 Nikolai Hampton, "Why Isn't Everyone Using DNSSEC?" APNIC, June 28, 2017, https://blog.apnic.net/2017/06/28/isnt-everyone-using-dnssec/.

73 See, for example, Matt Torrisi, "Is DNSSEC Adoption Worth It for Enterprises?," Dyn, September 18, 2018, https://dyn.com/blog/is-dnssec-adoption-worth-it-for-enterprises/.

74 Cloudflare, "Troubleshooting DNSSEC," last updated 2019, https://support.cloudflare.com/hc/en-us/articles/360021111972-Troubleshooting-DNSSEC.

4. **Tough to DIY:** Many users depend on third-party nameservers, like a cloud provider, to operate their website and resolve the DNS. This means relying on these third parties to adopt DNSSEC and to maintain it over time, including the necessary cryptographic signing process.[75] Policymakers can help lower barriers through convenings and public-private partnerships, for instance, like the UK's resources for DNSSEC implementation (see Recommendation 2).

There are structural challenges with companies using their infrastructural influence to protect the DNS (e.g., collective action problems) and weak market pressure for firms to implement DNSSEC and BGP RPKI. The two protocols are case studies in how private companies' infrastructural influence on the Internet gives leverage to shape the Internet's digital rules for security but underlines the need for more action from these companies. In this vein, the final section below develops five recommendations for the US government to help shape private sector incentives to better secure the Internet's digital rules.

75 Taejoong Chung, "Why DNSSEC Deployment Remains So Low," APNIC, December 6, 2017, https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/.

RECOMMENDATIONS AND CONCLUSION

The Internet's shape and behavior are not set in stone. The private sector continuously revises the Internet's topology and policies, changing its behavior for users, businesses, and governments across the world. Resulting effects on personal, economic, and national security are enormous, for these are not just decisions about a single database used by one company but about physical infrastructure and digital rules that impact millions if not billions of Internet users every day. The COVID-19 pandemic has underscored society's fundamental reliance on the Internet, and Internet dependence and connectivity will only grow in the years to come as more of the global population comes online; as the cloud market continues to expand in offering services to individuals and enterprise; as more work and learning becomes virtual; as government agencies turn to the cloud and to artificial intelligence for government functions; and as emerging technologies like 5G telecommunications empower the Internet of Things and autonomous vehicles to constantly connect and communicate data. Securing the addressing and routing of all of that data—making sure it arrives quickly, safely, securely, and via the right paths—is vital.

The US government has an opportunity to better integrate the unique influence the US private sector has on the Internet's topology and behavior, and thus its security, into a national policy for securing cyberspace. Yet, private firms must also recognize the opportunities and responsibility their influence gives them to improve Internet security and resilience at scale. Consequently, there is an urgent need not just for better government-introduced incentives for the private sector to act to the benefit of Internet security, but also for better government-private sector cooperation and coordination on these issues.

The BGP and the DNS show the poor pace of progress in driving these more secure Internet protocols to wide adoption—and underline the disconnect between private sector firms' influence and incentive to change. However, they are only two protocols, and the safeguards discussed in this report's case studies are only two of many safeguards for bolstering those protocols' security. Questions about BGP security have grown over the past few years, and the coming years will only bring new issues to the fore that will take on their own urgency. This is where leveraging this report's case studies on the BGP and the DNS—on the protocols, their vulnerabilities, the barriers to action—will help the government and the private sector build policy and strategy around incentives and coordinated action to tackle the next set of challenges. The United States should be looking ahead when building a strategy to secure the Internet with an appreciation of the private sector's influence.

To this end, this report makes the following five recommendations:

The US government should place Internet protocol security best practices in federal procurement rules. Incentivizing a few big players to change their behavior, especially ones in the United States with an outsized influence on Internet infrastructure, can have significant consequences for the Internet ecosystem and lower the barrier to collective action on the part of small and medium-sized network operators. This would compel ISPs, CDNs, cloud services providers, and other Internet infrastructure operators vying for federal contracts to adopt these safeguards. Those implementing these procurement rules should include the Departments of Defense, Veterans Affairs, Homeland Security, and Health and Human Services, which are the four biggest IT spenders in the US government. Looking beyond the case studies in this report, these rules could also draw from other security best practices for Internet addressing and routing, like those enumerated in Mutually Agreed Norms for Routing Security (MANRS),[76] or those laid out in previous work by the NIST.[77]

The US government should convene public and private stakeholders to tackle the next set of challenges on Internet protocol security. The US private sector's outsized influence on Internet infrastructure means the US government must better understand its security challenges and the incentives around them—which also presents an opportunity to be forward-looking. The key for any convening is to be voluntary, to have a well-defined scope, and to involve representatives with subject matter expertise as well as global stakeholders. Interagency buy-in from the government side is also essential for driving consensus on potentially coordinated or collaborative activities, and the involvement of a technical-expert agency like the NIST can help with the optics of a public-private convening on protocol modifications. Additionally, bringing operators to the table—those who technically work on these challenges that have business, policy, and geopolitical effects—could help drive substantive conversation at a convening spanning problems, how they can

76 See: "Mutually Agreed Norms for Routing Security," https://www.manrs.org/.

77 See, for example, Sriram and Montgomery, *Resilient*.

be addressed, and barriers to those solutions. There is also an educational role here insofar as some security issues with the Internet's digital rules come back to network operators' "hygiene" practices. Ensuring trust in a route's path, not just its origin, is one example of a "next big challenge."

The US government should require federal agencies to implement these Internet protocol security best practices in their own systems. While the US private sector has key influence on Internet topology and behavior worldwide, the US government maintains its own domestic networks that also should be secured. Government agencies, especially the Department of Defense, operate large networks that use many of the same digital rules as private operators. Policymakers should promote security best practices within these agencies,[78] such as through the Office of Management and Budget,[79] in coordination with the NIST. This can also include producing reports on the status quo within government agencies, building on previous work.

Large, private sector network operators should share and then leverage data on Internet protocol attacks. The US private sector's influence on global Internet topology and behavior provides key and unique insights into security threats around the world, such as attacks on the Internet's core digital rules. Some corporate aversion to naming and shaming is understandable, but ISPs, CDNs, and cloud services providers collectively have a depth and breadth of insight into the infrastructure that researchers cannot find elsewhere—meaning they also have insight into attacks and repeat offenders for, say, traffic routing malfunctions. Much like the public-private convening on future challenges in Internet protocol security, data sharing here would need buy-in not just from business leadership but also from operator-level personnel at those companies. A convening discussion about this issue should also address operator concerns about liability for increased data sharing, including with researchers who would greatly benefit from data on protocol attacks. This could occur through any number of existing private sector efforts to share threat information, such as through sector-specific information-sharing analysis centers (ISACs) or through nonprofit efforts like the Shadowserver Foundation.

The US government should invest more in the State Department's cyber diplomacy efforts to develop norms against manipulating core Internet protocols. Not only does the US private sector have enormous influence over global Internet infrastructure, but the United States has historically played a key leadership role in promoting and protecting practices around a relatively free and global Internet—which also means security is a critical issue. Existing intergovernmental and nongovernmental efforts to push these protections, like the Global Commission on the Stability of Cyberspace's "Call to Protect the Public Core of the Internet," already focus on this issue—developing norms around state and nonstate noninterference in Internet traffic addressing and routing protocols key to the Internet's functionality.[80] This could also involve the leveraging of private sector data on incidents like BGP hijacks. The United Nations Group of Governmental Experts (UN GGE) and UN Open-Ended Working Group (OEWG) are two forums through which this investment could occur, in addition to bilateral and multilateral engagements with allies and partners who share an interest in better securing the global Internet.

These recommendations are not a silver bullet. But they zoom out far beyond the illustrative case studies on the BGP and the DNS in this report and recommend the US government reassess its current strategy toward and relationship with the private sector with respect to Internet security. The private sector's role in Internet geopolitics on the infrastructural level cannot be ignored or sidelined any longer. Further, challenges that have plagued Internet routing and addressing security in the past can provide valuable lessons for the future.

On both of these points, Internet name resolution and packet routing protocols are exemplary case studies. The BGP and the DNS show how private sector influence over Internet infrastructure gives firms leverage to better protect Internet packet addressing and routing at scale—in ways that better protect personal, economic, and national security, as well as the overall resilience of the global Internet. This matters for global cybersecurity as well as for growing "cyber sovereignty" measures around the world, including the so-called fragmentation of the global Internet, which are driven in part by concerns about cybersecurity threats. Working to better secure the Internet will promote confidence in its continued viability as a global network of networks and, perhaps, slow the decline toward a fragmented and tribal information ecosystem.[81]

78 Legacy IP space maintained by government agencies may be one explanation for lagging best practices.

79 This OMB recommendation is borrowed from Yoo and Wishnick, "Lowering," 33.

80 Global Commission on the Stability of Cyberspace, *Definition of the Public Core, to Which the Norm Applies*, May 2018, https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf.

81 Justin Sherman, *Strengthening Democratic Internet Governance: The West Needs a Plan or Risks Getting Left Behind*, Atlantic Council, working draft; and Daskal and Sherman, *Data Nationalism on the Rise*.

ABOUT THE AUTHOR

Justin Sherman is a nonresident fellow at the Cyber Statecraft Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security. He is also a research fellow at the Tech, Law, & Security Program at American University Washington College of Law; a researcher in Lawfare's Trustworthy Hardware and Software Working Group; and a contributor at WIRED. He was previously a cybersecurity policy fellow at New America and a fellow at Duke Law School's Center on Law & Technology. He is currently earning his MA in security studies from Georgetown University's School of Foreign Service, and he earned his BS in computer science and his BA in political science from Duke University.

ACKNOWLEDGMENTS

The author would like to thank Trey Herr, Bill Woodcock, Stewart Scott, Tianjiu Zuo, Martin Levy, Jennifer Daskal, Megan Stifel, David Hoffman, Matthew Kroenig, and several other reviewers who requested anonymity for their feedback on earlier versions of this document. The author would also like to thank David Hoffman, Bill Woodcock, Frederick Douzet, Kavé Salamatian, Loqman Salamatian, Alissa Starzak, Josephine Wolff, Martin Levy, Louis Poinsignon, Jesse Sowell, Robert Morgus, Christopher Yoo, John Curran, and several others who requested anonymity for valuable discussions about the issues. Finally, the author would like to thank Simon Handler, Trey Herr, Nancy Messieh, and the broader Atlantic Council team for their support.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org