



UNIDIR

PRIMER

Internet Fragmentation and Cybersecurity

SAMUELE DOMINIONI

Summary of Key Points

- The promotion of an open, secure, stable, accessible, and peaceful ICT environment is a recurrent objective in the multilateral processes relating to international and ICT security at the United Nations. The OEWG itself represents a significant milestone in international cooperation towards such an ICT environment.
- The Internet remains stable and generally open and secure in its foundations. However, Internet fragmentation is a growing and concerning phenomenon. Fragmentation can be understood in different ways according to the nature of the stakeholders. Nevertheless, it is possible to identify a technical dimension of it. Here, fragmentation may affect critical components of the Internet that guarantee the interoperability of networks and devices.

- Three main areas of concern exist in the technical dimension of Internet fragmentation, namely regarding addressing, naming, and routing. Some of these concerns relate to necessary innovations that the multi-stakeholder community had to elaborate to address the increasing use of ICT technologies but that are not still fully implemented (e.g., IPv4 and IPv6); others concern emerging trends in the development of technical critical components that diverge from the current international standards and protocols (e.g., in the domain name system); and finally, others refer to technical flaws or limitations in the design and development of critical components of the Internet (e.g., routing).
- These areas of fragmentation not only impair the openness, stability, and accessibility of the global Internet but also have cybersecurity implications. Some of these relate to the cybersecurity of standards and protocols themselves (e.g., routing protocols), which can be affected by a wide variety of malicious ICT activities. Others refer to the endangered reachability, availability, and security of data (e.g., alternative name systems). Overall, because of the complexity and interdependence of the Internet's structure, the fragmentation of the technical dimension can pose complex, multifaceted risks (the so-called 'wicked problems') for cybersecurity.
- Future research will look at how the areas of risks and trends identified in this primer might have an impact on the implementation of the framework for responsible State behaviour in cyberspace, and thus on international peace and security.

Introduction

The promotion of an open, secure, stable, accessible, and peaceful ICT environment is a recurrent objective in the multilateral processes relating to international and ICT security at the United Nations. For example, the final report of the 2021 Group of Governmental Experts (GGE) on advancing responsible State behaviour in cyberspace in the context of international security affirmed that “an open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security”.¹ The final report of the Open-ended Working Group (OEWG) on developments in the field of information and

telecommunications in the context of international security recalled that “[t]he OEWG represents a significant milestone in international cooperation towards an open, secure, stable, accessible and peaceful ICT environment”.² Moreover, both reports stressed the importance of protecting technical infrastructure essential to the general availability and integrity of the Internet.³ The General Assembly resolution that established the current OEWG (2021–2025) confirmed: “the conclusions of the Group of Governmental Experts, in its 2013 and 2015 reports, that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability

1 General Assembly, 2021, A/76/135, <https://undocs.org/Home/Mobile?FinalSymbol=A%2F76%2F135>.

2 General Assembly, 2021, A/75/816, <https://undocs.org/Home/Mobile?FinalSymbol=A%2F75%2F816>.

3 The GGE 2021 report claims, “to the general availability or integrity of the Internet”. See General Assembly, 2021, A/76/135, para. 10.

and promoting an open, secure, stable, accessible and peaceful information and communications technology environment”.⁴ However, the fragmentation of the ICT environment, and more specifically of the Internet, has become an increasingly troublesome possibility, which is already occurring in certain settings. Indeed, the fragmentation of the Internet can have effects at different and sometimes intertwined levels, including the political, commercial, and technological.⁵ A growing number of States and other stakeholders are raising concerns over an Internet fragmentation scenario. The Secretary-General’s document, Our Common Agenda, lists avoiding Internet fragmentation as an action to be considered, and it is one of the main topics to be included in the upcoming Global Digital Compact.

This primer is the first outcome of a broader project on Internet fragmentation and international security, and it aims to introduce the

topic of Internet fragmentation and outline the main challenges that can be posed to cybersecurity broadly understood. Building on this first outcome, the second part of the research project will look at how Internet fragmentation impacts international security and, in particular, the implementation of the framework of responsible State behaviour for cyberspace (henceforth the Framework). This primer is intended to provide policymakers, diplomats, and other non-technical interested parties with an introductory overview of Internet fragmentation developments and their cybersecurity implications. The material presented here is drawn from publicly available sources, expert interviews (conducted between September and November 2023), and a multi-stakeholder dialogue with speakers from the private sector, academia, and civil society held online on 17 October 2023.

What is Internet Fragmentation?

Internet fragmentation is a contested concept that may have different interpretations according to the nature of the stakeholder. Nevertheless, according to certain scholarship, it is possible to identify a trend in the tripartite understanding of Internet fragmentation, which can refer to technical, commercial,

and governmental fragmentation.⁶ Others conceive of tripartite fragmentation with a slightly different understanding.⁷ Since this primer focuses on the cybersecurity impact of Internet fragmentation it centres the analysis on the technical dimension.⁸

4 General Assembly, 2020, A/RES/75/240, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/25/PDF/N2100025.pdf>.

5 William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, “Internet Fragmentation: An Overview”, Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

6 Ibid.

7 For example, the IGF Policy Network on Internet Fragmentation discussion paper on Internet fragmentation uses the following dimensions: fragmentation of the user experience, fragmentation of the Internet’s technical layer, and fragmentation of Internet governance and coordination; PNIF, 2023, PNIF Discussion Paper (input to IGF 2023), 15 September, https://www.intgovforum.org/en/filedepot_download/256/26218.

8 The effects of political and commercial fragmentation on cybersecurity will be considered in future publications.

According to a World Economic Forum (WEF) white paper on Internet fragmentation, technical fragmentation occurs when there are “conditions in the underlying infrastructure [i.e., the Internet layers] that impede the ability

of systems to fully interoperate and exchange data packets and of the Internet to function consistently at all end points”.⁹ Box 1 provides a brief overview of the Internet layers and their functions.

Box1: The Internet Layers

The Open System Interconnection (OSI) and the Transmission Control Protocol/Internet Protocol (TCP/IP) models are among the most used methods to classify the Internet’s layered structure. These models are usually represented as a vertical stack. Each layer is tasked with different but interconnected functions that transform a piece of information (e.g., a text query into a browser) into data packets to make communication between two (or more) devices possible.

The **OSI model** contains seven layers: application, presentation, session, transport, network, data link, and physical.

1. The **application layer** provides services for network applications that use the Internet, such as browsers, email, and telecommunication applications.
2. At the **presentation layer**, the information from the application layer is formatted for display (in case it is receiving) or to be processed further (in case it is sending).
3. At the **session layer**, the authentication and authorization processes occur. For example, authentication (i.e., logging into an application) makes the connection between the user and the application server, thereby initiating a session.
4. The **transport layer** ensures the reliability of communication among devices and networks. There are two main protocols that allow for this ‘transportation’, the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The first protocol is used to establish connections that reliably transfer information among devices, yet it can be slow. The second, UDP, is used for connections that require greater speed but less accuracy in data transfer (e.g., streaming videos).
5. The **network layer** facilitates data transmission between devices in different networks. One of the functions of this layer is logical addressing, which attaches each user’s IP address to the data packet to ensure it can reach the correct destination. This data is then transmitted through routers from one network to another. This layer uses path determination which is used to find the best possible path for data delivery.

w9 William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, “Internet Fragmentation: An Overview”, Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, p. 14.

- 6. The **data link layer** helps to prepare the information to be sent between different networks and tries to avoid errors that may occur in transit in the subsequent layer.
- 7. At the last layer of the OSI model, the **physical layer**, the data is converted into binary code which is in turn transformed into signals to be transmitted over local media (or the other way round in case it is receiving the packets), which are the physical connection between devices (e.g., copper wire, optical fibre or air for radio signals).

TCP/IP is similar to the OSI model but synthesizes the application, presentation, and session layers from the OSI model into one layer which is called the application layer in the TCP/IP model. The remaining layers are given the same name as those in the OSI model, namely transport, network, data link and physical.

Table 1: The Two Models

OSI	TCP/IP
Application (human-computer interaction)	Application (data presentation, encoding and session control)
Presentation (data representation and encryption)	
Session (interhost communication)	
Transport (TCP and UDP)	Transport (TCP and UDP)
Network (routing and IP addresses)	Network (routing and IP addresses)
Data Link (error recovery and retransmission)	Data Link (error recovery and retransmission)
Physical (sends data electronically, optically, or as radio waves)	Physical (sends data electronically, optically, or as radio waves)

As a matter of fact, the Internet can function as an open and global public good because of several infrastructures and properties that allow communication and exchange of information (in the form of data packets) regardless of

where you are, who you are, and through which devices you are connecting to the Internet. Among these, there are critical components that guarantee the interoperability of networks and devices (see Box 2).

Box 2: The Critical Components of the Internet

The following initiatives have contributed to highlighting what constitutes the critical components of the Internet.

The Global Commission on the Stability of Cyberspace crafted the concept of the Public Core of the Internet, which includes:

1. Packet routing and forwarding
2. Naming and numbering systems
3. The cryptographic mechanisms of security and identity
4. Transmission media
5. Software
6. Data centres¹⁰

The Internet Society has proposed five critical properties that define the essential functions of Internet networks:

1. An accessible infrastructure with a Common Protocol that is open and has low barriers to entry.
2. Open Architecture of Interoperable and Reusable Building Blocks based on open-standards development processes voluntarily adopted by a user community.
3. Decentralized Management and a Single Distributed Routing System which is scalable and agile.
4. Common Global Identifiers which are unambiguous and universal.
5. A technology-neutral, General-Purpose Network that is simple and adaptable.¹¹

The discussion paper of the Internet Governance Forum Policy Network on Internet Fragmentation (PNIF) claims that the fragmentation of the Internet's technical infrastructure relates to "a range of challenges to this interoperability at the technical transport layer that makes the Internet work".¹² Indeed, the global Internet

is "basically rooted in the design of the Internet transport layer and the common use of the same technical protocols (TCP/IP, DNS, BGP, HTTP, IPv4&6, etc.), based on a unified, but decentralized root server system for all kinds of Internet communication".¹³ Therefore, because of the essential features pertaining to critical

10 Global Commission on the Stability of Cyberspace, "Advancing Cyberstability", November 2019, <https://hcss.nl/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf>.

11 Internet Society, "The Internet Way of Networking: Defining the Critical Properties of the Internet", September 2020, <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>.

12 PNIF, 2023, PNIF Discussion Paper (input to IGF 2023), 15 September, https://www.intgovforum.org/en/filedepot_download/256/26218, p. 12.

13 Wolfgang Kleinwächter and Alexander Klimburg, 2023, "Fragment or Not Fragment – Is This the Question? Will the "One World-One Internet" Survive Today's Geopolitical Stress Test?", CircleID, 6 June, <https://circleid.com/posts/20230606-fragment-or-not-fragment-is-this-the-question-will-one-world-one-internet-survive-todays-geopolitical-stress-tests>.

components of the Internet, actions aimed at fragmenting this technical dimension would

constitute a most serious threat to its openness and interoperability.

Areas of Risks for Internet Fragmentation at the Technical Level

Technical fragmentation is a recurrent concern, especially for the multi-stakeholder community that deals with critical components of the Internet. The WEF white paper on Internet fragmentation published in 2016 claimed that “the internet remains stable and generally open and secure in its foundations”.¹⁴ Almost eight years later, which for technology is a span of time, these foundations are still solid even if there are growing fragilities and risks.¹⁵ For the sake of consistently building on the existing literature and, in particular, on the WEF white paper, this brief uses the same areas of risks, namely addressing, naming (the Domain Name System), and routing (interconnection) of the Internet,¹⁶ to determine current trends that are weakening the foundations of the Internet.

Addressing

Addressing relates to the unique identifiers, otherwise called IP addresses, expressed in decimal values, that designate unique points on the Internet. Two main issues concern IPs and

fragmentation. The first relates to the adoption and compatibility of two versions of IP (IPv4 and IPv6), and the second relates to the management of IP numbers.

There are currently two main versions of IP addresses: IPv4 and IPv6. The first is composed of a 32-bit address space and can generate up to around 4.3 billion addresses. Because of the enormous increase of endpoints (e.g., devices) on the Internet in the last decades, IPv4 has now exhausted its possible combinations. Therefore, to respond to this need for more unique identifiers, a new version of IP (IPv6) with 128-bit address space was introduced. IPv6 can cover up to 340 trillion trillion trillion endpoints.¹⁷ However, IPv4 and IPv6 are not directly interoperable. This means that devices on IPv4 networks cannot communicate with devices on IPv6 networks.¹⁸ The compatibility is achievable only through transition technologies, such as dual-stacked networks. Fragmentation can occur in case of discrepancies in IP

14 William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, “Internet Fragmentation: An Overview”, Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, p. 8.

15 Author interview with Dr. Vinton G. Cerf, one of the authors of the WEF White Paper on Internet fragmentation, 26 October 2023.

16 A simple way to understand addressing, naming, and routing is to look at these terms as “The name of a resource indicates what we seek, an address indicates where it is, and a route tells us how to get there”; John F. Schoch, 1978, “A Note on Inter-Network Naming, Addressing, and Routing”, Internet Experiment Note # 19, Notebook Section 2.3.3.5, <https://www.rfc-editor.org/ien/ien19.txt>.

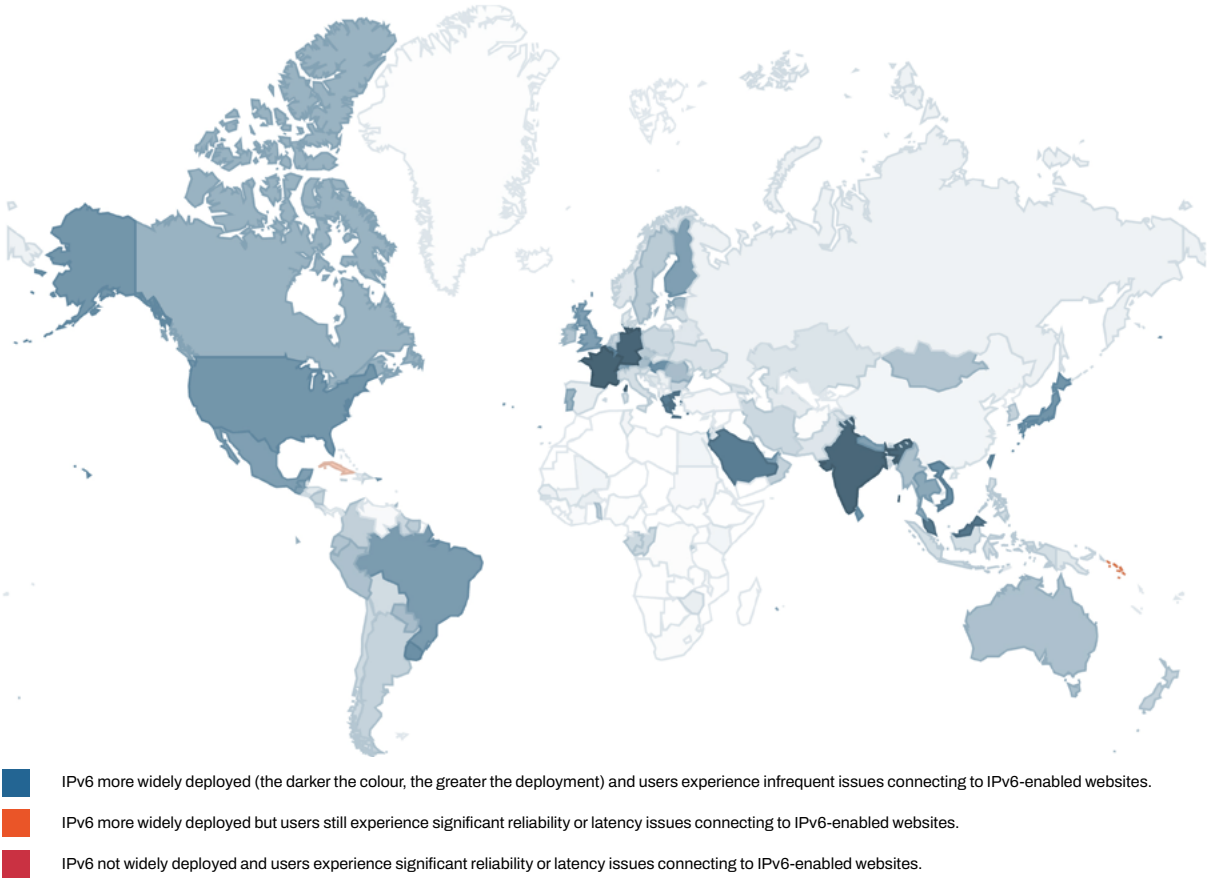
17 William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, “Internet Fragmentation: An Overview”, Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

18 Erik Bais, “IPv4 vs IPv6: What Security Professionals Should Know”, Prefix Broker, <https://www.prefixbroker.com/news/ipv4-vs-ipv6-what-security-professionals-should-know/>.

versions not sustained by transition technologies among countries and regions of the world.

The level of IPv6 adoption is steadily increasing¹⁹ with variations among countries.

Figure 1: Per-Country IPv6 Adoption



Source: Google Statistics (Google collects statistics about IPv6 adoption in the Internet on an ongoing basis.)

Therefore, fragmentation along the lines of this facet of the digital divide is possible and poses risks to the overall interoperability of the networks and devices across countries and regions.

The second aspect of IP fragmentation concerns the management of IP numbers used for IP addresses. In the current state of the Internet, this task is managed by the Internet Assigned Number Authority (IANA, an affiliate of the

Internet Corporation for Assigned Names and Numbers—ICANN), along with the Regional Internet Registers (RIR), and it is implemented in broad regions because Internet structures are not contained within national borders. It is key that there is a system responsible for the global uniqueness of IPs; otherwise, there is the risk of creating alternative and uncoordinated IP addresses that complicate, or even make impossible, compatibility with the existing deployed IPv4- or IPv6-based infrastructure.²⁰

19 At the time of the publication of the WEF White Paper, IPv6 connectivity counted only for 4 per cent of the Internet, whereas in October 2023, it is around 40 per cent (source <https://www.google.com/intl/en/ipv6/statistics.html>).

20 See, for example, the debate around the proposal for the ‘New IP’: Alain Durand, 2020, “New IP”, ICANN Office of the Chief Technology Officer, <https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf>.

Naming

Naming refers to the Domain Name System (DNS), which translates names into IP addresses (e.g., for UNIDIR's website the DNS is <https://unidir.org> and its corresponding IP is 34.x.y.z).²¹ To ensure this feature, it is essential that the management of this unique mapping and pairing task (performed by ICANN) remains stable, consistent, and legitimate. Attempts to set up alternative name systems (including the management of the root zone)²² would be one of the worst possible forms of fragmentation²³ because unique DNS translations would be lost. This would result in inconsistencies and potential DNS look-up errors; for example, different users typing <https://unidir.org> could open other pages than the one intended.

Routing

Routing refers to protocols used to ensure that

information follows the right and optimum track when traveling through a network. In case information needs to travel from one network to another (the Internet is composed of many different networks often managed individually by a single service provider), Border Gateway Protocols (BGP) serve to connect them, therefore enabling the global routing system of the Internet. As pointed out in the WEF white paper, “it is still technically possible for deliberate or accidental corruption of the routing data to occur”.²⁴ The security of the routing system still needs improvements, for example, by implementing the so-called Resource Public Key Infrastructure (RPKI), a public key infrastructure framework designed to secure the Border Gateway Protocol.²⁵ Overall, if the BGP is not adequately protected, fragmentation can occur because of the inability of the network to guarantee the confidentiality, integrity, and availability of data.

Areas of Concern for Cybersecurity

The focus of this primer is not only to understand Internet fragmentation and its current state but also to identify possible cybersecurity implications. This primer looks at cybersecurity from a very comprehensive standpoint, which

relies on the so-called cybersecurity triad²⁶ and authenticity. In general, the fragmentation of the Internet can entail multiple risks for cybersecurity that may encompass the so-called ‘wicked problems’.

21 Full IP address is hidden.

22 The root zone is the top-level part (tld) of the DNS hierarchy (e.g., in <https://unidir.org> the tld is “.org”).

23 Multi-stakeholder dialogue on Internet Fragmentation and Cybersecurity, 17 October 2023; William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter, 2016, “Internet Fragmentation: An Overview”, Future of the Internet Initiative White Paper, World Economic Forum, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

24 Ibid., p. 23.

25 Author interview with Dr. Vinton G. Cerf, one of the authors of the White Paper, 26 October 2023.

26 The triad focuses on the security of data, and it refers to its confidentiality, availability, and integrity. Availability refers to the fact that data must be available to authorized users whenever needed; any event that might delay their access is affecting the availability of the data. Confidentiality refers to the accessibility of data; only authorized users should have access to specific data, which otherwise must be kept secret or private. Integrity concerns the authenticity, reliability, and trustworthiness of data; this means that data should not be tampered with. See Samuele Dominioni and Giacomo Persi Paoli, 2022, “A Taxonomy of Malicious ICT Incidents”, UNIDIR, <https://unidir.org/publication/a-taxonomy-of-malicious-ict-incidents/>.

Table 2: Types of Problems

TYPE	CHARACTERISTICS	SOLUTION PATH
Simple	Solutions, or design approaches for solutions, are known	Cooperation: awareness-raising and information-sharing, typically through Network Operator Groups
Complex	No known solution exists; the problem spans multiple parts of the Internet	Consensus: open, consensus-based standards development
Wicked	No solution exists in any domain; general lack of agreement on existence or characterization of the problem	Collaboration: moving beyond existing domain and organization boundaries and set processes for determining problems and solutions

Source: Leslie Daigle, Konstantinos Komaitis and Phil Roberts “Keys to Successful Collaboration and Solving Wicked Problems”, *Internet Society*, 2016.

These problems arise especially in composite, interconnected, multi-stakeholder fields or domains (e.g., the Internet) and can be extremely complex and multifaceted.²⁷

A multi-stakeholder approach, which includes collaboration among different actors, sectors, and countries, is often needed to cope with wicked problems (see table 1).²⁸ Therefore, “a fragmented Internet prevents any possible opportunity to address cybersecurity because it dismisses the many interdependent factors and closes down the venues for any potential collaboration”.²⁹ Moreover, fragmenting the Internet into smaller networks may result in reducing the overall resilience of the networks. This is because the Internet’s strength is that

it is decentralized and built on interoperable components (e.g., standards and protocols, devices, etc.), which allow the technical community, in case of need, to address issues without compromising the entire network.³⁰

The following headings highlight what are the security concerns of each of the fragmentation areas identified.

Addressing

There are two main cybersecurity implications for the fragmentation of addressing. First, the scattered adoption of IPv6 across the world not only may foster fragmentation due to the direct incompatibility of the two IP models but also inconsistencies in different levels of

27 Most critical malicious ICT incidents have a transborder nature, involving multiple assets and actors of different sectors and geographical provenance.

28 Leslie Daigle, Konstantinos Komaitis, and Phil Roberts, 2016, “Keys to Successful Collaboration and Solving Wicked Internet Problems”, *Internet Society*, <https://www.internetsociety.org/resources/doc/2017/keys-to-successful-collaboration-and-solving-wicked-internet-problems/>.

29 Konstantinos Komaitis, 2023, “Internet Fragmentation: Why It Matters for Europe”, *Research in Focus*, EU Cyber Direct – EU Cyber Diplomacy Initiative, <https://euclid.s3.eu-central-1.amazonaws.com/euclid/assets/10yLip90/internet-fragmentation-why-it-matters-for-europe.pdf>, p. 8.

30 Author’s interview with Konstantinos Komaitis, November 9, 2023.

exposure to ICT threats. IPv6 has key characteristics, including the integration of Internet Protocol Security (IPsec),³¹ which would offer better security.³² However, the implementation and configuration of IPv6 can be more challenging than IPv4 and require specific technical knowledge and skills. Errors in configuring IPv6-enabled devices could introduce vulnerabilities and, therefore, make the devices more prone to compromise.³³ Moreover, devices and networks that are dual-stack (i.e., that run IPv4 and IPv6 simultaneously) may have additional security concerns because of the increased attack surface.³⁴

Second, the remote, yet possible, development of national IPs with no coordination or in contrast to the existing system would seriously disrupt both global reachability and the security of national networks. Indeed, in this case, States would need to work on establishing bilateral agreements with Internet service providers and ensuring security standards and protocols for their own networks. Not all States have the same capabilities to achieve the same level of security. Currently, each State can rely on an open multi-stakeholder community devoted to developing, discussing, and updating standards and protocols for all.

Naming

Fragmentation at the naming level, mostly occurring through the development of alternative name systems, would cause enormous cybersecurity failures. In this scenario, for example, when typing the name of a website, the user may not be able to reach the intended site or may end up on a different one. Overall, in the case of alternative name systems, users will not be able to access data, which, in turn, will not be available. Moreover, efforts undertaken by the multi-stakeholder community to bridge the DNS to alternative name systems can lead to “unpredictable results, user frustration, rising support costs, and in the end, a less secure and stable Internet”.³⁵

Routing

Border protocols are vulnerable to hacks that may tamper with data flows. Indeed, the BGP has limited internal mechanisms that protect against malicious acts that modify or even delete data and, therefore, disrupt overall network routing behavior.³⁶ Indeed, BGP is susceptible to severe and different ICT threats, including route hijacking,³⁷ which may result in Internet fragmentation and disruptive or exploitative

31 IPsec is a standard that provides channel security at the Internet layer. IPsec is mandatory for IPv6, whereas it was optional for IPv4. See Internet Engineering Task Force (IETF), 2011, “IPv6 Node Requirements, Request for Comment 6434”, <https://www.rfc-editor.org/rfc/pdf/rfc6434.txt.pdf>.

32 Emre Durda and Ali Buldu, 2010, “IPV4/IPV6 Security and Threat Comparisons”, *Procedia—Social and Behavioral Sciences* 2, www.sciencedirect.com/science/article/pii/S187704281000902X, pp. 5285–5291.

33 National Security Agency, 2023, “IPv6 Security Guidance”, U/OO/105622-23 | PP-22-1805 , ver. 1.0, https://media.defense.gov/2023/Jan/18/2003145994/-1/-1/0/CSI_IPV6_SECURITY_GUIDANCE.PDF.

34 Ibid.

35 Alain Durand, 2022, “Challenges with Alternative Name Systems”, OCTO-034, ICANN, <https://www.icann.org/en/system/files/files/octo-034-27apr22-en.pdf>.

36 IETF, 2006, RFC#4272, “BGP Security Vulnerabilities Analysis”, <https://datatracker.ietf.org/doc/html/rfc4272>.

37 This scenario occurs when perpetrators maliciously reroute Internet traffic by falsely announcing an IP address, which in fact leads Internet traffic to another one. In other words, “BGP hijack is much like if someone were to change out all the signs on a stretch of freeway and reroute automobile traffic onto incorrect exits”; Cloudflare, What is BGP Hijacking”, <https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/>.

effects.³⁸ Most of the time, such effects have limited impact and scope; however, other times, they may produce devastating communications

failure.³⁹ Implementing the RPKI can be an effective cybersecurity measure.

Conclusion and Next Steps

The Internet remains stable, generally open, and secure in its foundations. However, there are growing fragilities and risks at all levels. Internet fragmentation at the technical level could potentially break down an open, secure, stable, accessible, and peaceful ICT environment, with overwhelming implications for cybersecurity.

Worrisome trends exist, and they showcase a possible increase in practices and policies aimed at contrasting primarily technical international standards and protocols, posing several challenges for cybersecurity. Therefore, any arbitrary and unilateral attempts to tamper with the critical components of the Internet may further aggravate the already ongoing fragmentation and impoverish the overall security of the network of networks and beyond. Indeed, Internet fragmentation might have implications not only for cybersecurity but also for international security. Future research will look at how the areas of risks and trends identified in this primer might have an impact on the implementation of the framework, and thus on international peace and security.

In conclusion, to ensure an open, secure, stable, accessible, and peaceful ICT environment, the multi-stakeholder community—including Member States—should consider protecting the integrity, availability, and interconnectedness of the critical components of the Internet. To do so, it is key to appraise the interdependences of these components and the ripple effects that tampering with these complex and interconnected systems would entail for this global, human-made commons. This primer is an effort to that end.

38 Each cyber incident produces an effect on a target, and there are two main types of primary effects: disruptive, which refers to interfering with ICT function, and exploitative, which relates to stealing information. See Samuele Dominiononi and Giacomo Persi Paoli, 2022, “A Taxonomy of Malicious ICT Incidents”, UNIDIR, https://unidir.org/files/2022-08/UNIDIR_Taxonomy_of_Malicious_ICT_Incidents.pdf; Charles Harry and Nancy Gallagher, 2018, “Classifying Cyber Events”, *Journal of Information Warfare*, vol. 17, no. 3, <https://www.jstor.org/stable/26633163>, pp. 17–31.

39 “For example, critical applications such as online banking, stock trading, and telemedicine run over the Internet”; Kevin Butler et al., 2010, “A Survey of BGP Security Issues and Solutions”, *Proceedings of the IEEE*, Vol. 98, No. 1, <https://ieeexplore.ieee.org/abstract/document/5357585>, pp. 100–122.

Acknowledgements

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This publication was funded by the European Union as part of UNIDIR's Security and Technology Programme, which is supported by the governments of Czech Republic, Germany, Italy, the Netherlands and Switzerland, and by Microsoft. The author extends his thanks to the diverse body of experts from across industry, government, and academia who provided substantive feedback on different iterations and sections of this paper and participated in the multi-stakeholders' workshop, including Ang Benjamin, Jaya Baloo, Vinton Cerf, Alain Durand, Marie Humeau, Tommy Jensen, Konstantinos Komaitis, Allison Mankin, Kevin Reifsteck, Rob Spiger, Bill Woodcock, Michael Zappa. Elia Smith, a graduate professional in the Security and Technology Programme, contributed to the research project.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Author




Dr. Samuele Dominioni is a researcher in the Security and Technology Programme at UNIDIR. Before joining UNIDIR, he held research positions in both academic and think tank settings. He holds a PhD in international relations and political history from Sciences Po, France, and the IMT School for Advanced Studies, Italy.

Citation

S. Dominioni. *Internet Fragmentation and Cybersecurity: A Primer*. Geneva, Switzerland: UNIDIR, 2023.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual author. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, European Union, its staff members or sponsors.

-  @unidir
-  /unidir
-  /un_disarmresearch
-  /unidirgeneva
-  /unidir



Palais des Nations
1211 Geneva, Switzerland

© UNIDIR, 2023

WWW.UNIDIR.ORG