Governance Tier

Dimension	Description	Idealized Version	The Global Reality
Laws and Regulations	Laws and regulations are the primary tools used by states to shape behavior. They impose sanctions or punishment for (defined) undesirable actions or behaviors and/or provide incentives for (defined) desirable actions or behaviors. In the context of the internet, laws can both shape the behavior of internet users and provide guidelines on how internet architecture should operate.	Free: Laws and regulations that enable freedom of access to information and expression via the internet.	Free: All countries have some form of restriction on content, whether bans on child pornography or aggressive censorship of foreign press.[1]
		Open: Laws and regulations that enable or ensure openness ("oblivious" architecture).	Open: Some countries are not protecting net neutrality; many countries have laws that could allow ISPs to throttle traffic based on the content of that traffic.[2]
		Interoperable: Laws and regulations that do not negatively impact the network's interoperability.	Interoperable: Some nations mandate data localization and local data routing which can affect resilience.[3]
		Secure: Laws and regulations that criminalize/penalize (a) illicit use of computers (as we define it: computer network attacks, etc.), but do NOT criminalize (b) content and information, etc.	Secure: Most countries have laws that criminalize (a), but many also have laws that criminalize (b). In some cases laws criminalize behaviors that would otherwise positively impact the security of the global network.[4]
Social norms	Social norms are expectations about "appropriate behavior for actors with a given identity."[5] They regulate behavior through societal pressure. In the context of the internet, social norms typically guide how users interact	Free: Norms that enable freedom of access to information and expression via the internet.	Free: There are some norms in place to protect internet freedom,[6] but many countries challenge them within their own borders. Further, other nation-states push conflicting international norms to restrict internet freedom.[7]

	with the internet and with one another on the internet. However, social norms have in the past also shaped the way infrastructure owners and operators administer internet architecture.	Open: Norms that enable or ensure openness ("oblivious" architecture).	Open: Net neutrality was a norm, but some nations have already contested that fact.
		Secure: Norms that dictate responsible behavior of internet users (including individuals, states, and other organizations) to not undermine or exploit insecurity of the global network.	Secure: Much time and effort has gone into establishing norms, particularly for responsible behavior of states,[8] but despite these norms, actors persist in exploiting insecurities.
Standards	Standards give "specifications for products, services and systems to ensure quality, safety and efficiency."[9] In the context of the internet, standards provide guidelines primarily for using and configuring architecture.	Interoperable: Standards that ensure interoperability and that devices, systems, and networks are built to connect and interact.	Interoperable: The ideal is mostly the reality. Standards ensure most components of the internet can work with one another.
		Secure: Standards exist that promote security.[10]	Secure: Governments around the world can undermine national and international security standards.[11]
Markets	Markets regulate behavior through price. "Through the device of price, the market sets my opportunities, and through this range of opportunities, it regulates." [12] In the context of the internet, markets shape the creation, acquisition, and	Free: The market for internet access and content access is not artificially manipulated.	Free: Content laws artificially manipulate the market for information.
		Open: Net neutrality.	Open: ISPs violate net neutrality in some countries.[13]

configuration of architecture. They also impact the options available to internet users and the way users react to architectural changes.	Interoperable: Markets (global) provide economic incentives for developers/owners/ operators to build/manage interoperable infrastructure. Secure: People will understand what products are and are not secure and make purchases based on that judgment.	Interoperable: This appears to hold true. Devices that fail to work with other devices are typically not in great demand. Secure: This is not the case, as customers continually purchase products with minimal understanding of / care for the security implications.[14]

Architecture Tier

Element	Description	"Idealized" Version	The Global Reality
Content	The content element is the result of translating machine-readable code into human-interpretable information. Content is what is presented on the screen of most internet users. Examples of content include information on websites (not the websites themselves), email messages (not email protocols or applications), text messages, and Voice over Internet Protocol (VoIP).	Free: Universally, users can access and share any information they want at will. Open: Users are guaranteed free, immediate, online availability of information coupled with the rights to use that information fully in the digital environment.[15] Secure: Users can trust the validity of the content on the internet.[16]	Free: Countries and sometimes infrastructure operators put laws or policies in place to censor certain content. Open: Countries and sometimes infrastructure operators use technical measures to manipulate architecture to block or limit access to certain content. Secure: Fabricated content and manipulated content is rife on the internet. Users are often bereft of ways to verify the truth of a given piece of content.[17]
Application and Presentation	The application and presentation element serves to translate character code representations (machine-readable code, what is often referred to as "data") into physical windows, text, graphics, and other representations that are discernable to an average user. The result of this translation is content. Examples of application and presentation architecture include internet browsers, websites themselves (search engines, news sites, social media platforms, etc.),	Free: Any user can use and access any application. Open: Applications do not modify what a user of the application sees. Interoperable: Translation infrastructure needs to be able to take any coding language and turn it into something an internet user can read.	Free: Governments outlaw some applications. Open: Application owners, operators, and developers willingly design or are compelled by governments to design protocols to discriminate the content their applications present. Interoperable: This generally holds true. Files are fairly interoperable, although encryption can introduce complications.

	email and messaging applications, the Hypertext Transfer Protocol (HTTP), and others, as well as file types (JPG, .doc, .pdf, etc.), encryption protocols (RSA, PGP, etc.), and character code representations (ASCII, Unicode, etc.).	Secure: Applications are safe to use. In fact, security is built in (secure coding). Resilient: One type of application breaking doesn't cause all other types of applications to break.	Secure: Applications are vulnerable to cyber attacks. Files can easily be embedded with malicious code. Resilient: Sometimes applications break, but their failure has not yet led to the entire system failing. For example, a given web browser could break, but that would not prevent the world from accessing the global internet.[18]
Session	The session element is, for the purposes of the global internet, the interaction between an internet user and a host of internet content. A session is initiated by a user on the user's own device, sending a signal to a host via the transport element. The host then decides to accept or reject the request for access and sends that signal back to the user. The session remains open for as long as the user maintains access to the host's content. For example, when an internet user wants to access facebook.com, she enters the URL into her browser, ostensibly sending a session request to a Facebook server. The server chooses whether to accept or deny that request and sends it back to the user.	Free: Internet users are not blocked via legal or normative means from opening sessions on the global internet and do not need specific permissions to open specific sessions.[19] Open: Session architecture does not prevent internet users from opening sessions. Secure: Sessions are alterable only by authorized parties; information is kept secret from other sessions and parties. Resilient: Individual sessions can fail (causing failure for the user "up the chain"), but individual session failures do not cause global session failures.	Free: In some places, governments and/or infrastructure operators block users from opening sessions, usually through manipulations of the application element.[20] Open: In some places, infrastructure operators block users from opening sessions.[21] Secure: Hackers can compromise sessions through such actions as cross-site scripting (XSS) attacks[22] and attacks on mountable networked file system (NFS) shares.[23] Resilient: This generally holds true, but DDoS attacks can prevent users from opening sessions.[24]

Transport	The transport element consists of the processes and protocols that allow devices to communicate to one another over the network (see below). Transport protocols include TCP and UDP.	Open: Requests are not discriminated against.	Open: Governments and ISPs throttle traffic by delaying response times of transport protocols.[25]
		Secure: Message communications are encrypted; CIA is preserved.	Secure: Messaging is still vulnerable to attacks like three-way-handshake hacks,[26] TCP spoofing,[27] and others.
		Interoperable: It doesn't matter what device a user is using or what query a user is sending; the transport protocols can work with them all.	Interoperable: This largely holds true.
		Resilient: Messages are not dropped, duplicated, or corrupted, and arrive in a timely manner while making fair use of the network.	Resilient: Some failure occurs, but compared to other messaging protocols, and the central challenges that arise with networked messaging, TCP/UDP/etc. are relatively resilient.
Network	The network element is the processes and protocols that help internet traffic identify its intended destination. Network processes and protocols help assign identities to users and hosts. These most notable of these processes and protocols are the Internet Protocol (IP) and domain name service (DNS) registries.	Free: IP addresses are accessible[28] and the range of IPs from which a user can request information is not actively restricted.	Free: Countries control entire blocks of IP or restrict IP access.
		Open: The network does not discriminate (by limiting speed or bandwidth) when routing IPs.	Open: Government and ISPs identify what traffic to throttle based on IP addresses and other network characteristics.
		Interoperable: Protocols work coherently with one another.	Interoperable: ICANN governs a system which ensures that protocols largely do work coherently with one another.

		Secure: Routing infrastructure should not be vulnerable to attack.	Secure: The network element is vulnerable to some cyber attacks like DNS cache poisoning[29] and replay attacks,[30] which compromise IP and other protocols.
		Resilient: There are no SPOFs (single points of failure); systems are configured for redundancy.	Resilient: Heavy reliance on standard/universal protocols (IP, for example) creates potential single points of failure.[31] Single system failures can bring down entire subsections of the global internet (e.g., Mirai).[32]
Data Link	The data link element is oriented around packets themselves rather than users and hosts. The data link processes and protocols dictate how packets are sent and received and how they act when delivered to their destination. Data link processes and protocols play a basic role in ensuring the functionality of the internet by detecting and correcting basic errors in transmitted data. Data link processes and protocols include media access control (MAC) addresses.	Open: The protocols and access controls in this element will not identify or differentiate between traffic and treat it differently.	Open: This holds true in practice.
		Interoperable: An international system of standards weaves things together so that links (from/to different manufacturers) interact easily with one another (all of the others, in fact).	Interoperable: This is largely true, but as the need to secure the internet moves further from the end user and closer to the physical hardware, so too do challenges to interoperability.
		Secure: Data links uphold CIA.	Secure: Links are still vulnerable in their transmission of data, particularly on confidentiality and availability. Techniques for breaking or bypassing encryption (e.g., frequency attacks) also challenge this ideal.
		Resilient: Distributed data link infrastructure creates redundancy and resiliency.	Resilient: This largely holds true. Destroying one data link does not destroy all data links.

Physical	The physical element is the physical infrastructure and hardware that enables all the other elements. Physical elements of the global internet include servers, undersea cables, satellites, routers, Ethernet cables, internet exchange points (IXPs), cellphones, tablets, and computers themselves.	Free: Any user can plug into any component of the infrastructure and use it to access the global internet.	Free: Governments and corporations can and do purchase/own physical cables and exert control over how and by whom they are used.
		Open: The physical infrastructure does not identify or differentiate between traffic and treat it differently.	Open: The physical infrastructure itself does not breach openness.
		Interoperable: Physical components interact easily with one another.	Interoperable: Design standards for physical infrastructure ensure interoperability, for the most part.
		Secure: Physical components of the global internet are physically secured (e.g., strong access control), and physical infrastructure (hardware) is not hackable.	Secure: Physical security of physical infrastructure varies widely. Hardware is also hackable.[33]
		Resilient: If one wire fails, the system still survives.	Resilient: Because physical infrastructure is not necessarily equitably distributed, physical infrastructure failures have led to internet blackouts across entire nations.[34] However, one cable failing does not shut off the global network. The fact that 4 corporations account for 93% of CDN traffic poses potential challenges to the resiliency of the global internet.[35]

[1] This is not to say that all countries have equivalent laws; whereas the United States may ban the resale or redistribution of copyrighted content, China may punish any internet user criticizing a government policy online. It is to highlight, though, that virtually every country in the world has laws and regulations that limit or restrict the creation and/or dissemination of online content.

[2] Iran is a prime example of a nation-state that "throttles" (slows) traffic based on the nature of the traffic itself. This violates an open internet architecture. See: Collin Anderson, "Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran," June 18 2013, https://arxiv.org/abs/1306.4361, 1.

[3] Laws and regulations that require internet service providers and other administrators of internet architecture to store citizens' data locally (data localization) and/or prioritize domestic internet traffic (local data routing) violate the non-discriminatory nature of an open internet. For examples of data localization laws see: Bret Cohen, Britanie Hall, and Charlie Wood, "Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy," 2017, https://www.americanbar.org/content/dam/aba/publications/antitrust_magazine/anti_fall2017_cohen.authcheckdam.pdf. For discussion on how routing protocols can influence internet resilience on technical levels, see: Government of France, "Internet Resilience in France: 2015," 2015, https://www.ssi.gouv.fr/uploads/2015/06/internet-resilience-in-france-report_2015_anssi.pdf.

[4] For instance, see the United States' so-called Computer Fraud and Abuse Act: Legal Information Institute, "18 U.S. Code § 1030 - Fraud and Related Activity in Connection with Computer," n.d., https://www.law.cornell.edu/uscode/text/18/1030.

[5] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," 1998, https://www.jstor.org/stable/2601361, 891.

[6] United Nations Human Rights Council, "The Promotion, Protection and Enjoyment of Human Rights on the Internet," https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/082/83/PDF/G1408283.pdf?OpenElement.

[7] United Nations General Assembly, "International Code of Conduct for Information Security," January 9 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

[8] See earlier endnote regarding international norms.

[9] This definition is taken from the International Organization for Standardization (ISO). See: International Organization for Standardization, "About ISO," n.d., https://www.iso.org/about-us.html.

[10] Widely-implemented internet protocols such as HTTPS and TCP are continually updated with stronger encryption and more robust security processes.

[11] Governments often expect law enforcement and intelligence agencies to maintain some violation of security standards under the banner of fighting crime and protecting national security. This could also be argued in an intelligence-gathering context (e.g., breaking an adversary's security standards for espionage purposes). In other words, policymakers around the world permit or even encourage the violation of internet security standards for assorted reasons.

[12] Lawrence Lessig, "The Laws of Cyberspace," 1998, https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf, 3.

[13] As previously referenced, the United States federal government just officially repealed its protections of net neutrality.

[14] This reality is the impetus for numerous organizations working to provide security metrics for software and/or hardware products, such as the Cyber Independent Testing Lab (CITL) and Consumer Reports. See: Cyber Independent Testing Lab, "About Us," n.d., http://cyber-itl.org/about-us/; and Consumer Reports, "Consumer Reports to Begin Evaluating Products, Services for Privacy and Data Security," March 6 2017, https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/.

[15] This definition is an adapted version of the Open Access definition. See: SPARC, "Open Access," n.d., https://sparcopen.org/open-access/.

[16] From the "idealized" perspective of liberal-democratic policymakers, the value of the internet relies on this notion.

[17] This is perhaps one of the most accepted characteristics of the "internet reality" in recent years.

[18] More blatantly, the global internet is not reliant on a single web browser for end user communication just as all users do not rely on a single messaging app.

[19] In the context of freedom and the session element, it's important to recall that we are concerned with the global (i.e., the publicly-accessible) internet. Thus, while some networked technology (like corporate networks) will require certain permissions to open certain sessions, in essence posing a prohibition as described in the framework above, this is not within the purview of our discussion of the publicly-facing, global internet.

[20] In China, for instance, the government has explicitly banned certain VPNs as well as prohibited citizens from using those VPNs. Thus, service providers cannot allow Chinese citizens to open sessions with an outlawed VPN. See: Freedom House, "Freedom on the Net 2017: China," 2017, https://freedomhouse.org/report/freedom-net/2017/china. Similar practices, as previously referenced, occur in Russia.

[21] See previous endnote, which also implicates the openness of the internet architecture.

[22] Cross-site scripting attacks occur when "an untrusted source is allowed to inject its own code into a web application," after which point the malicious code seeps into another session on the device. See: TechTarget, "Cross-Site Scripting (XSS)," n.d., https://searchsecurity.techtarget.com/definition/cross-site-scripting.

[23] Attacks on mountable NFS shares occur when a user gains unauthorized, remote access to a networked file system without administrative privileges. See: Beyond Security, "Finding and Fixing Mountable NFS Shares, a High Risk Vulnerability," n.d., https://www.beyondsecurity.com/scan_pentest_network_mountable_nfs_shares_vulnerability.html.

[24] There are many examples of DDoS attacks preventing users from opening sessions with a given service, perhaps most notably the Mirai botnet that struck American service provider Dyn in 2016. See: Ben Herzberg, Dima Bekerman, and Igal Zeifman, "Breaking Down Mirai: An IoT DDoS Botnet Analysis," October 26 2016, https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

[25] See previous reference to Iran, which provides a potent example of internet traffic throttling.

[26] "Three-way handshakes" occur when two devices initiate a network connection (through the transport element). Because this process can often reveal information about the devices, however, it can be used by attackers to later compromise the devices' connection.
[27] While perhaps less common than it was several years ago, TCP spoofing enables a malicious actor to send seemingly-legitimate traffic to a victim through masking or "spoofing" their machine's identity. See: Matthew Tanase, "IP Spoofing: An Introduction," March 11 2003, https://www.symantec.com/connect/articles/ip-spoofing-introduction.
[28] Again, this does not mean free of financial cost. There are certainly financial costs involved with the acquisition and use of IP addresses.
[29] DNS cache poisoning occurs when an attacker compromises the database of a Domain Name System (DNS) server. This can lead the server to inadvertently reroute traffic to malicious destinations through seemingly-legitimate means. See: Veracode, "DNS Cache Poisoning Attack Solutions," n.d., https://www.veracode.com/security/cache-poisoning.
[30] Replay attacks occur when an attacker duplicates and resends a stream of legitimate traffic already sent between two parties. This can cause assorted failures and/or security complications. See: Microsoft Corporation, "Replay Attacks," March 30 2017, https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/replay-attacks.
[31] The Internet Protocol has not broken to date, but such an event would mean failure in a fundamental building block of the global internet. Dan Geer discusses this general idea in a 2018 paper, citing the Domain Name system root as an example of a critical service "which by the very definition of [its] mission must create a single point of failure." See: Dan Geer, "A Rubicon," 2018, https://www.hoover.org/sites/default/files/research/docs/geer_webreadypdfupdated2.pdf, 2.
[32] See earlier endnote on the Mirai botnet, which rendered numerous internet services completely unavailable along the eastern coast of the United States.
[33] Israeli cybersecurity researchers have developed numerous attack techniques to compromise computer hardware through physics, such as reading computer data through the heat generated from a processor. See: Jesse Emspak, "A Computer's Heat Could Divulge Top Secrets," July 1 2015, https://www.scientificamerican.com/article/a-computer-s-heat-could-divulge-top-secrets/.
[34] In 2011, for instance, Egypt cut off nearly all access to the global internet from within its borders. See: Matt Richtel, "Egypt Cuts Off Most Internet and Cell Service," January 28 2011, https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html?mtrref=www.google.com.
[35] Figure from: Dwayne Winseck, "The Geopolitical Economy of the Global Internet Infrastructure," 2017, https://www.jstor.org/stable/10.5325/jinfopoli.7.2017.0228, 242.