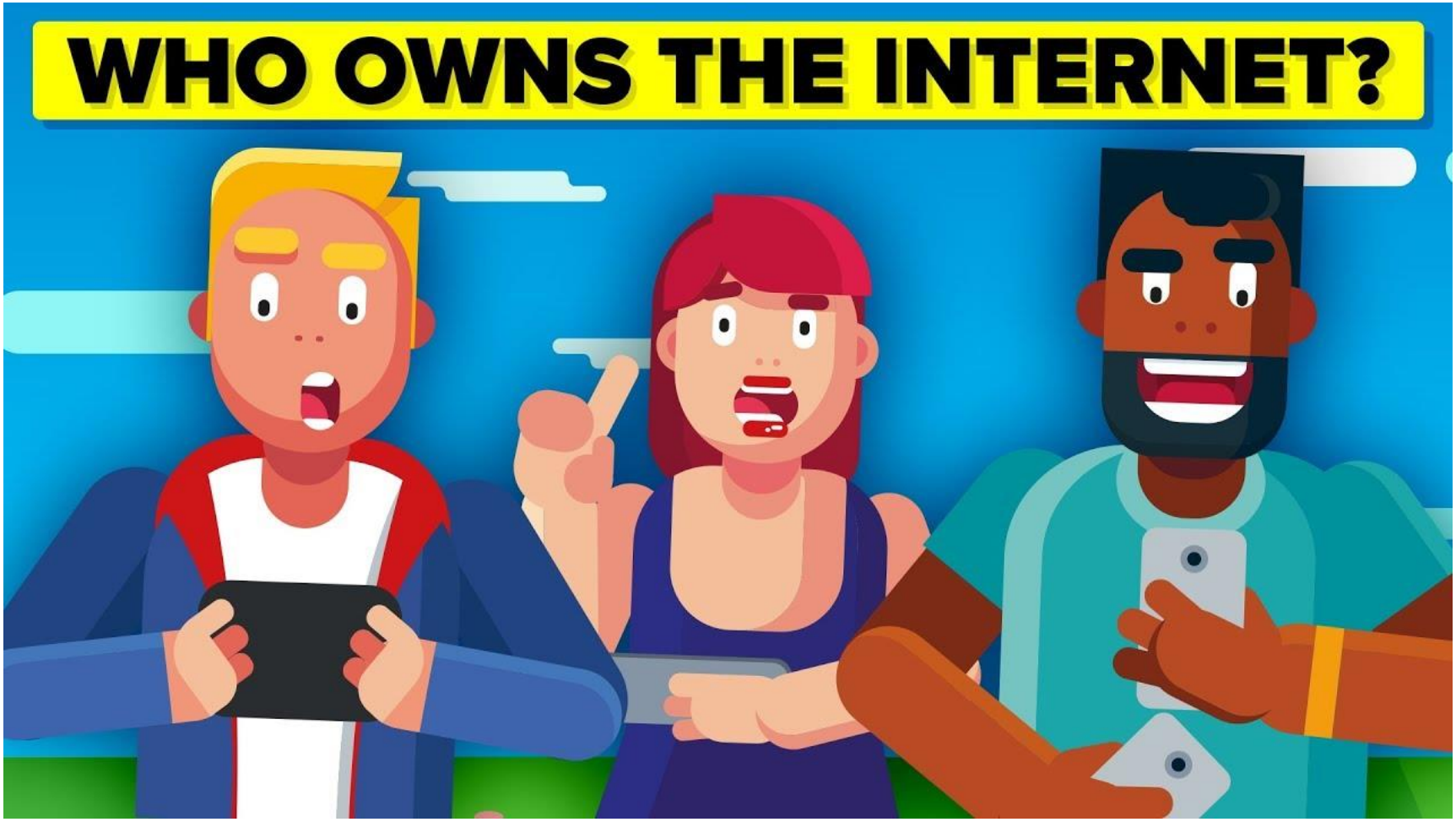
Chapter 5
Governance of the Internet

Table of Contents

Introduction

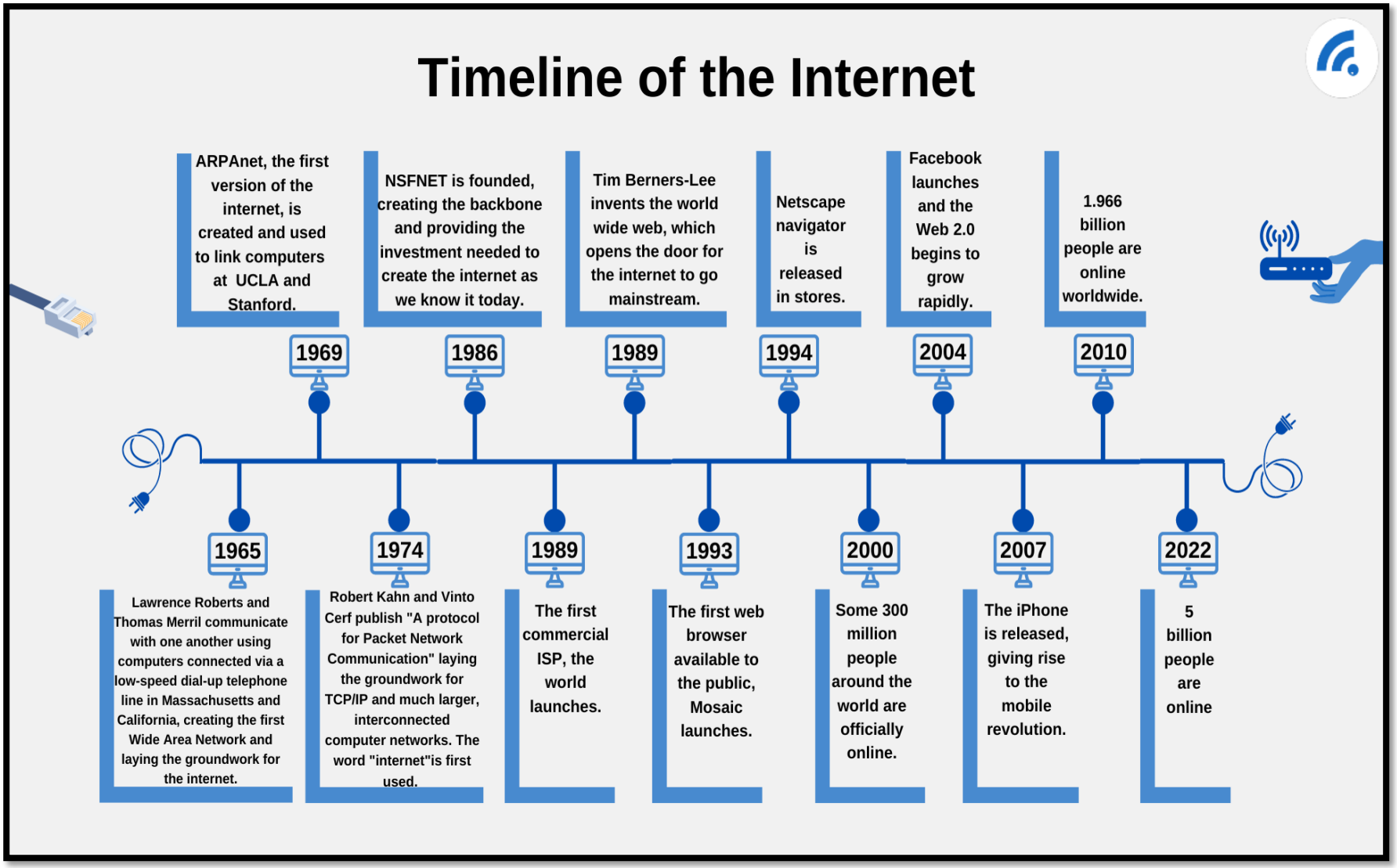


Introduction

The governance of the internet is a complex and evolving topic that encompasses the policies, rules, and processes by which the internet is managed and operated.

As the internet has become an integral part of modern society, questions regarding its governance and control have become increasingly important. The governance of the internet involves various stakeholders, including governments, private organizations, technical experts, civil society, and internet users.

The Origin of Internet

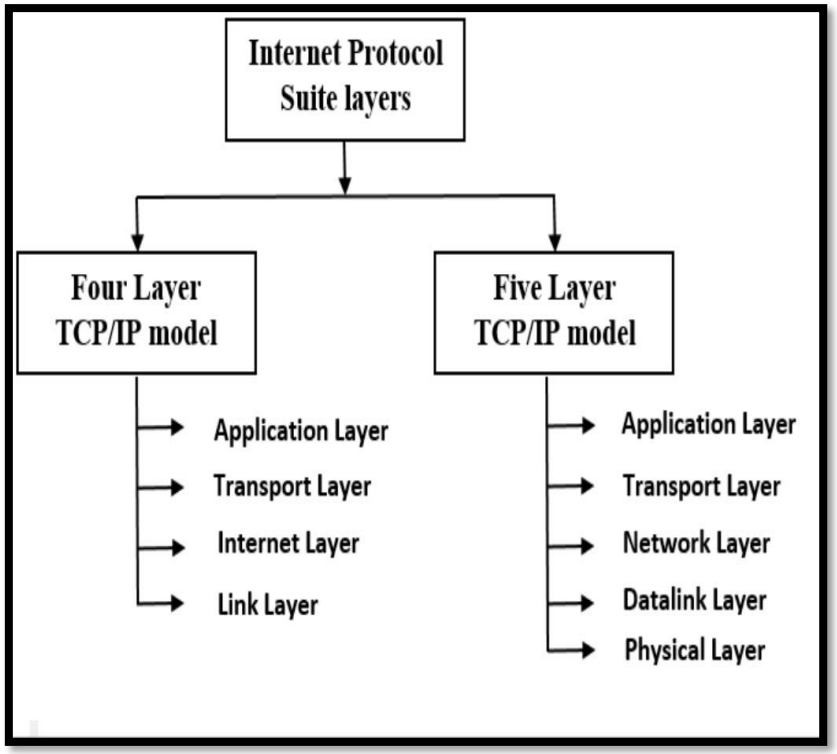


The Internet Protocol

The Internet Protocol (IP) is a fundamental protocol that serves as the backbone of the internet. It is responsible for the addressing and routing of data packets across networks, enabling communication and data transfer between devices connected to the internet.

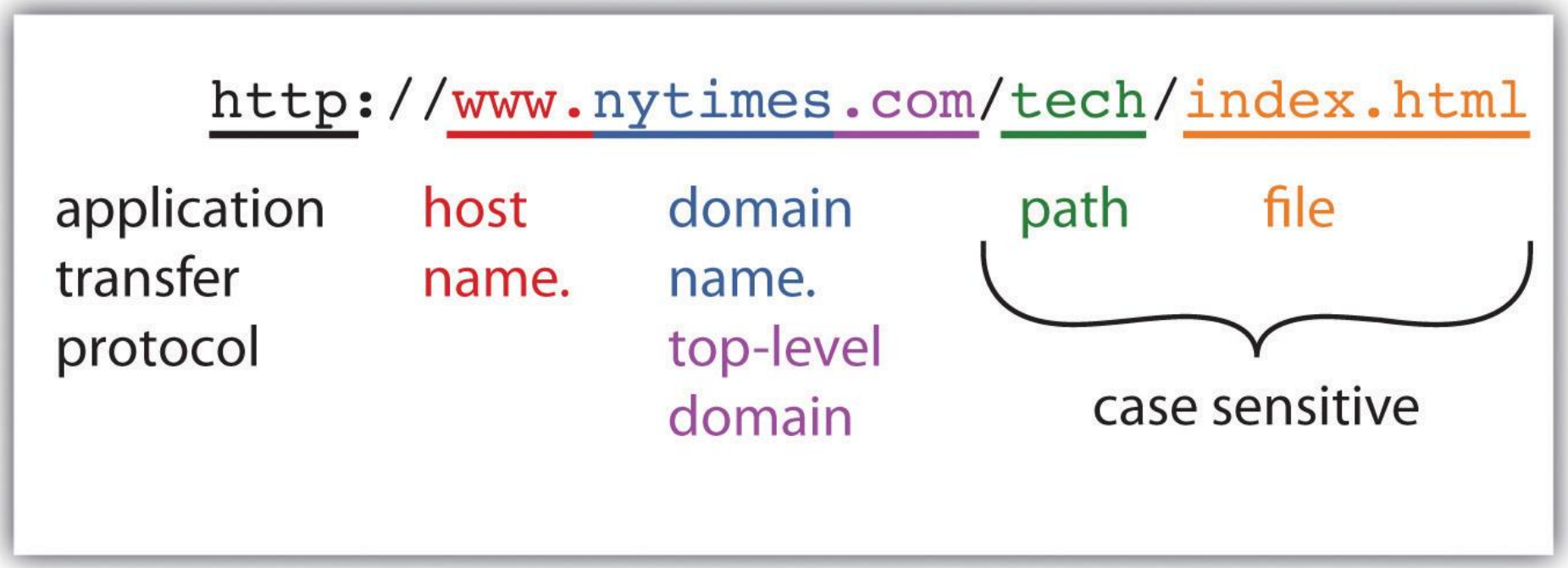
IP operates at the network layer of the internet protocol suite, known as the TCP/IP (Transmission Control Protocol/Internet Protocol), and works in conjunction with other protocols to facilitate data transmission.

Internet Protocol

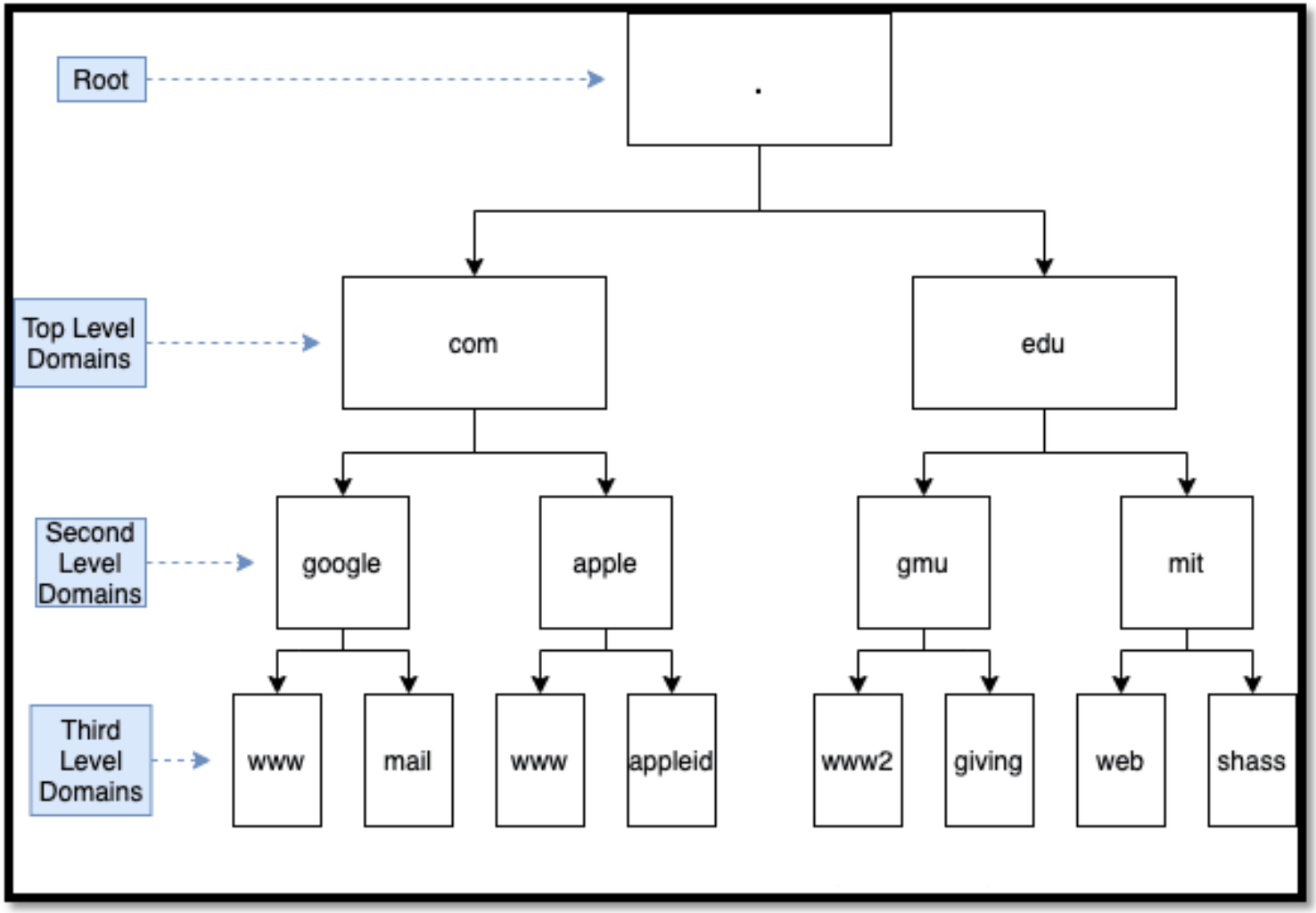


TCP/IP Layers	TCP/IP Prototocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP		UDP		
Network Layer	IP		ARP	ICMP	IGMP
Network Interface Layer	Ethernet		Token Ring	Other Link-Layer Protocols	

Domain Name


http://www.nytimes.com/tech/index.html
application transfer protocol
host name.
domain name.
top-level domain
path
file
case sensitive

Internet Protocol



Types of Domain Name

Domain types examples

Protocol	Sub-domain (third-level domain)	.	Domain name (second-level domain)	.	Domain ending (top-level domain)	Description
https://	www	.	example	.	org	Address with generic top-level domain (gTLD) for non-profit organizations (.org)
https://	www	.	example	.	de	Address with country code top-level domain (ccTLD) for Germany (.de)
https://	www	.	example	.	blog	Address with new generic top-level domain (.blog)
https://	example	.	co	.	uk	Address with country-specific, second-level domain (.co) – the actual domain name (example) becomes the third-level domain here, an additional sub-domain would become the fourth-level domain
https://	en	.	example	.	org	Address with sub-domain (.en) for an English-language website

Domain name Hijacking

Domain name hijacking refers to the unauthorized and malicious act of taking control over someone else's domain name without their permission or rightful ownership. It typically involves an individual or entity manipulating the domain name registration process or gaining unauthorized access to the domain owner's account.

Once hijacked, the perpetrator may redirect the domain's traffic to their own website, alter the domain's settings, or hold it for ransom. Domain name hijacking can have severe consequences, such as disrupting online business operations, damaging brand reputation, and causing financial losses.

It is essential for domain owners to take proactive measures to protect their domains, such as using strong passwords, enabling two-factor authentication, and regularly monitoring their domain registrar accounts for any suspicious activity.

Reverse domain name hijacking

Reverse domain name hijacking refers to a situation where a complainant, typically a trademark owner or individual, maliciously or unfairly attempts to acquire a domain name by wrongly accusing the legitimate domain owner of infringement or cybersquatting.

It involves filing a baseless complaint or dispute resolution proceeding, misusing legal procedures and misrepresenting facts to coerce the rightful owner into surrendering their domain.

In reverse domain name hijacking, the complainant knowingly disregards the rights of the domain owner and aims to obtain the domain through deceptive or abusive means.

This unethical practice undermines the principles of fair play and the rights of legitimate domain owners.

Reverse domain name hijacking

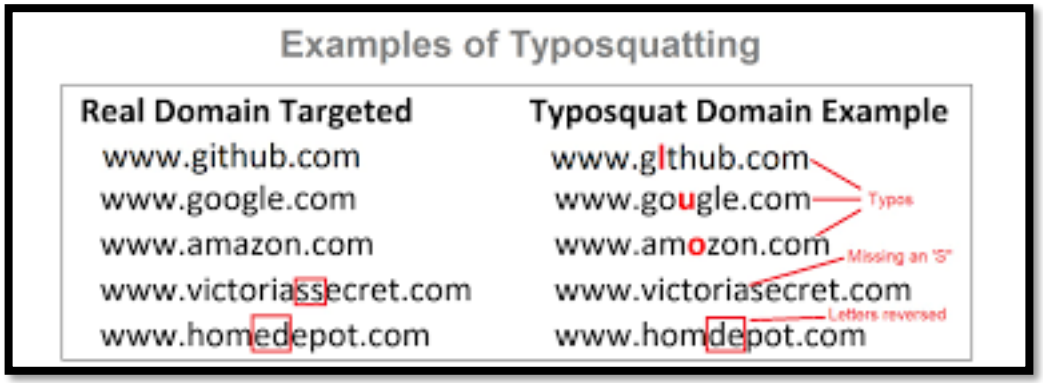
Reverse domain name hijacking refers to a situation where a complainant, typically a trademark owner or individual, maliciously or unfairly attempts to acquire a domain name by wrongly accusing the legitimate domain owner of infringement or cybersquatting.

It involves filing a baseless complaint or dispute resolution proceeding, misusing legal procedures and misrepresenting facts to coerce the rightful owner into surrendering their domain.

In reverse domain name hijacking, the complainant knowingly disregards the rights of the domain owner and aims to obtain the domain through deceptive or abusive means.

This unethical practice undermines the principles of fair play and the rights of legitimate domain owners.

Typosquatting



Typosquatting, also known as URL hijacking or domain mimicry, refers to a deceptive practice where individuals or entities intentionally register domain names that closely resemble popular or well-known domains but contain typographical errors or slight variations. The purpose of typosquatting is to take advantage of users' typing mistakes or misspellings when entering a website's URL.

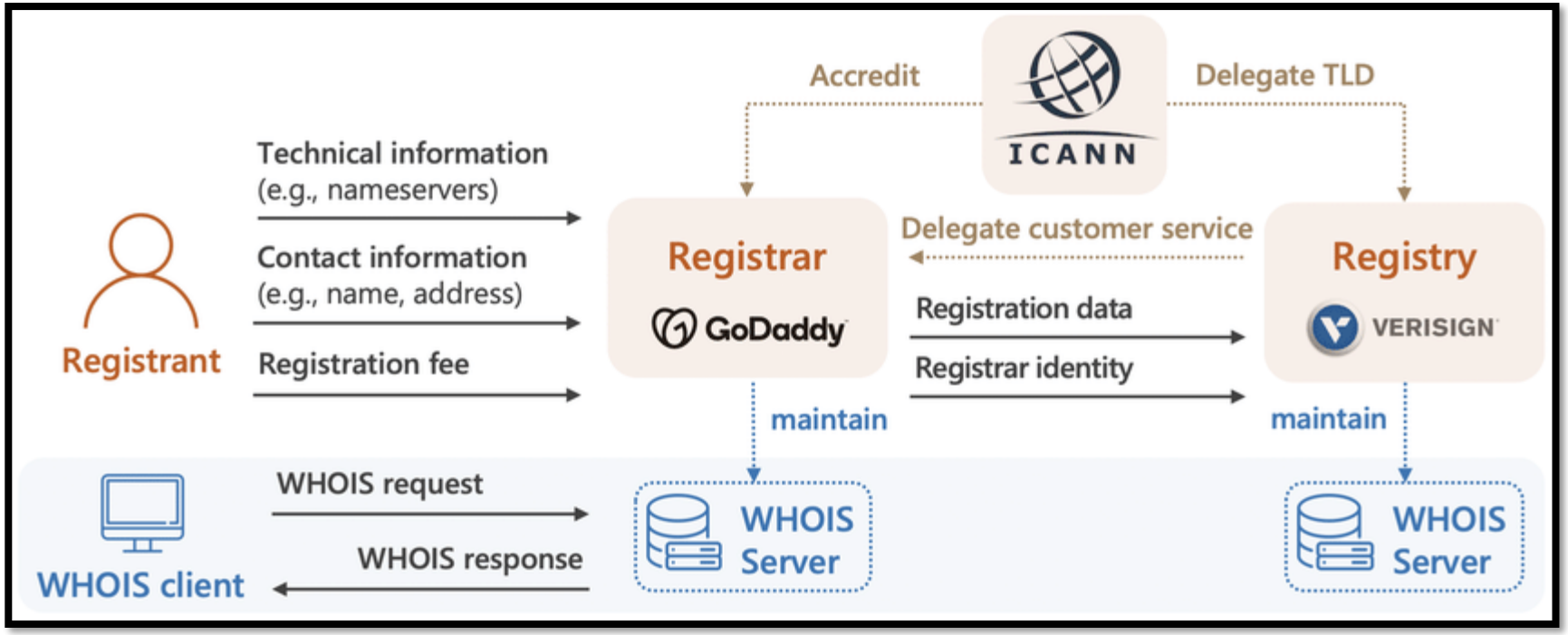
By registering these deceptive domain names, typosquatters seek to redirect traffic intended for legitimate websites to their own sites for various reasons, including financial gain, spreading malware, or conducting phishing attacks.

What is ICANN?

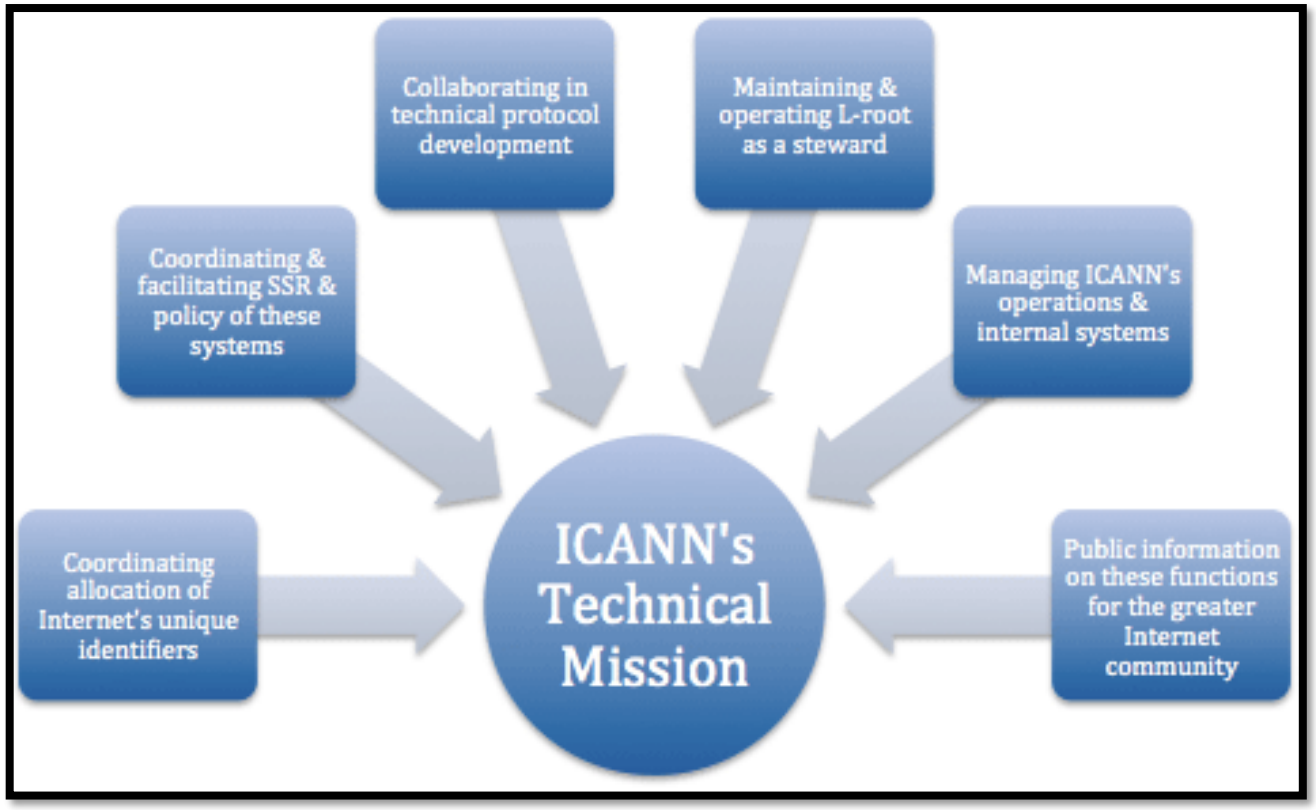
ICANN (Internet Corporation for Assigned Names and Numbers) is a nonprofit organization that plays a crucial role in the governance and coordination of the global Domain Name System (DNS).

It is responsible for managing and overseeing the allocation of domain names, IP addresses, and other unique identifiers that enable the functioning of the internet.

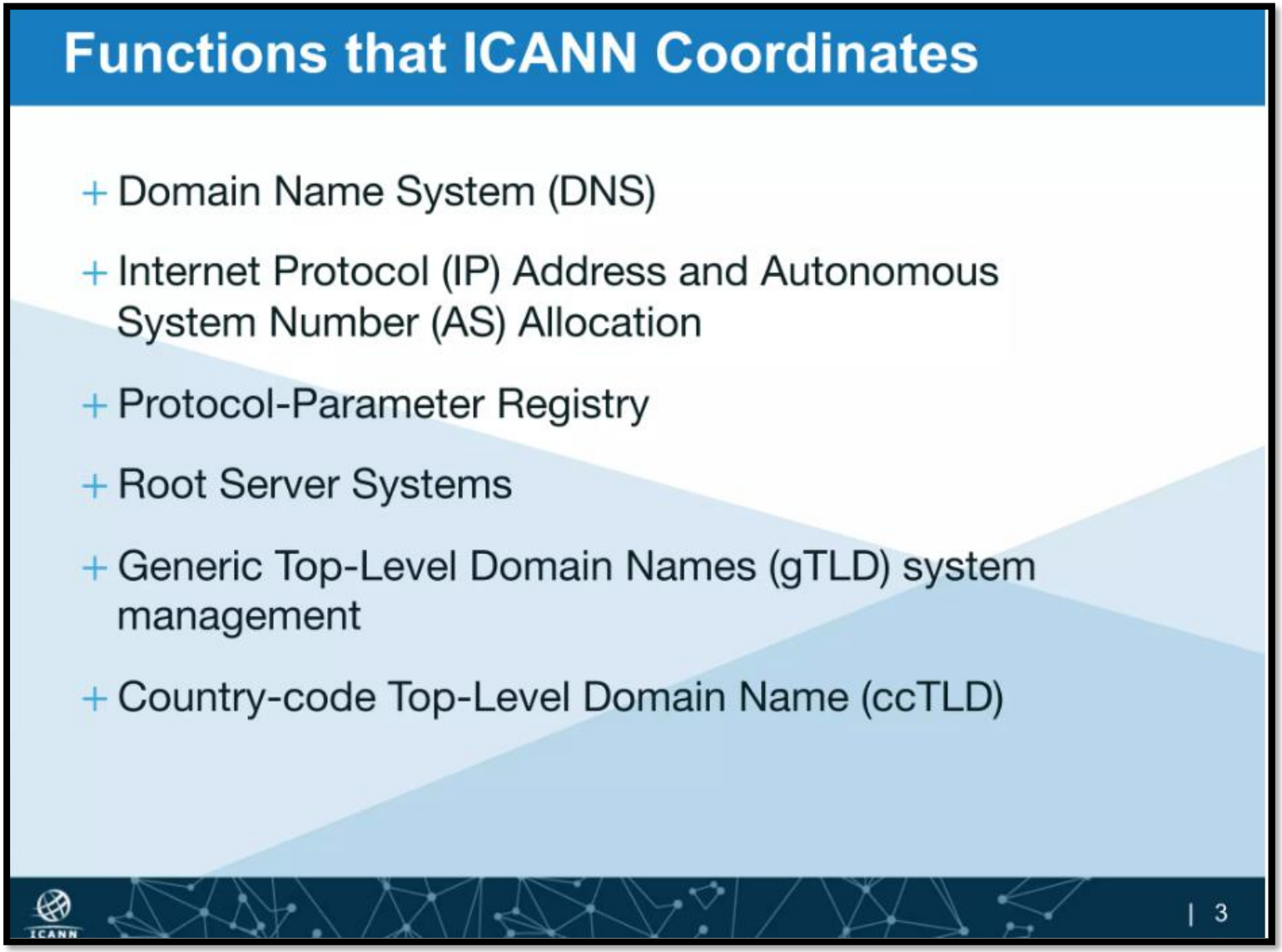
Root of all evil: ICANN



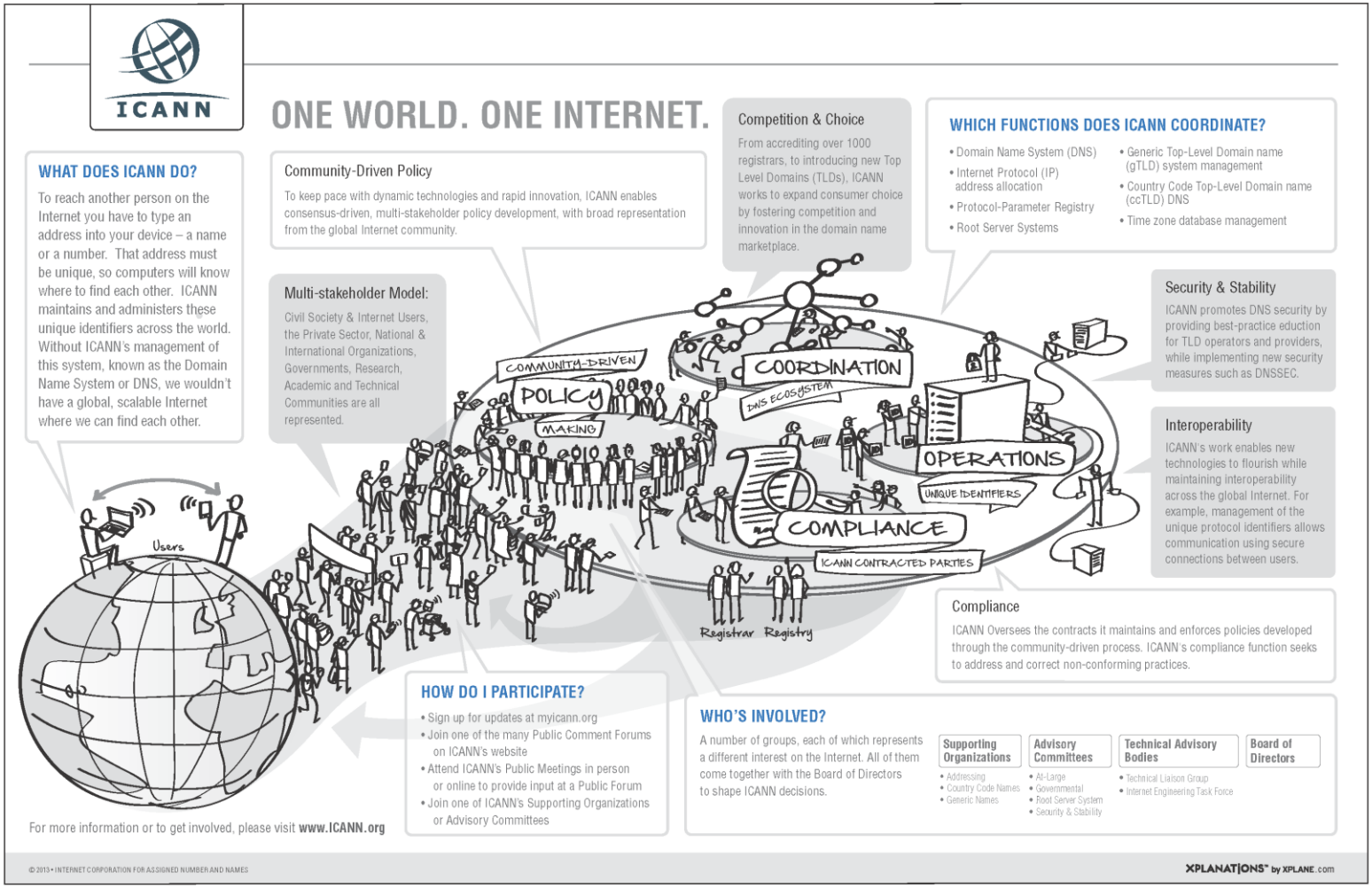
Root of all evil: ICANN



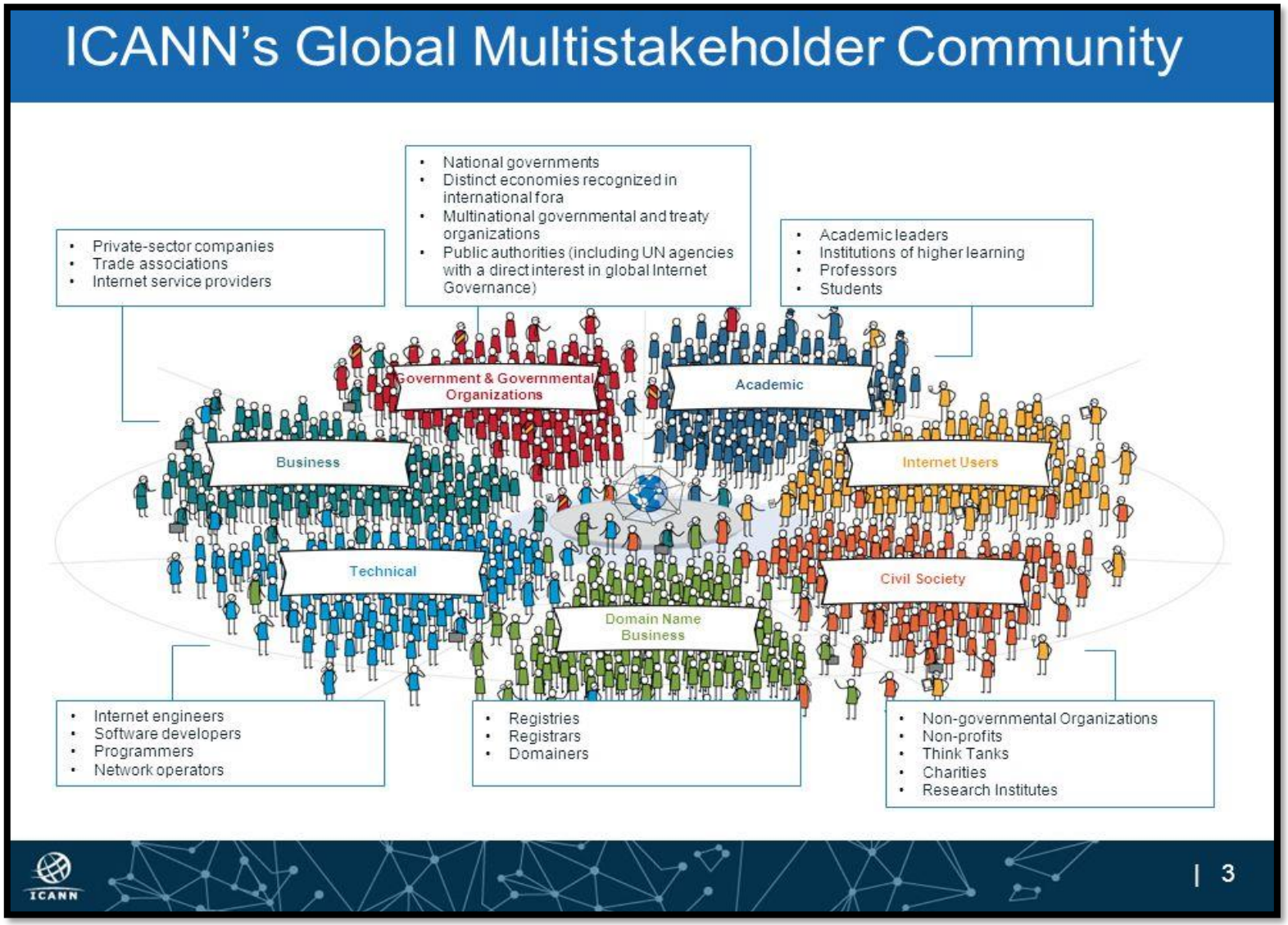
Root of all evil: ICANN



Root of all evil: ICANN

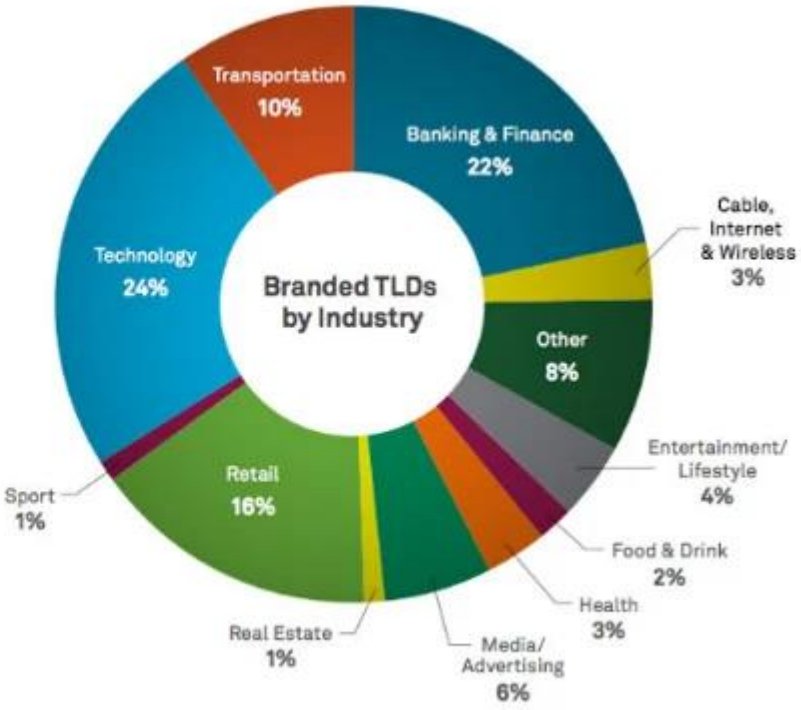


Multi-Stakeholder Model



ICANN: Commercialization

Banking & Finance	139
Cable, Internet & Wireless	19
Other	53
Entertainment/Lifestyle	27
Food & Drink	12
Health	21
Media/Advertising	37
Real Estate	7
Retail	99
Sport	7
Technology	154
Transportation	60
Total	**635**



ICANN (Internet Corporation for Assigned Names and Numbers) has faced discussions and criticisms regarding the commercialization of domain names and the domain name system (DNS).

This refers to the increasing commercial interests and market-driven dynamics surrounding the registration, management, and monetization of domain names.

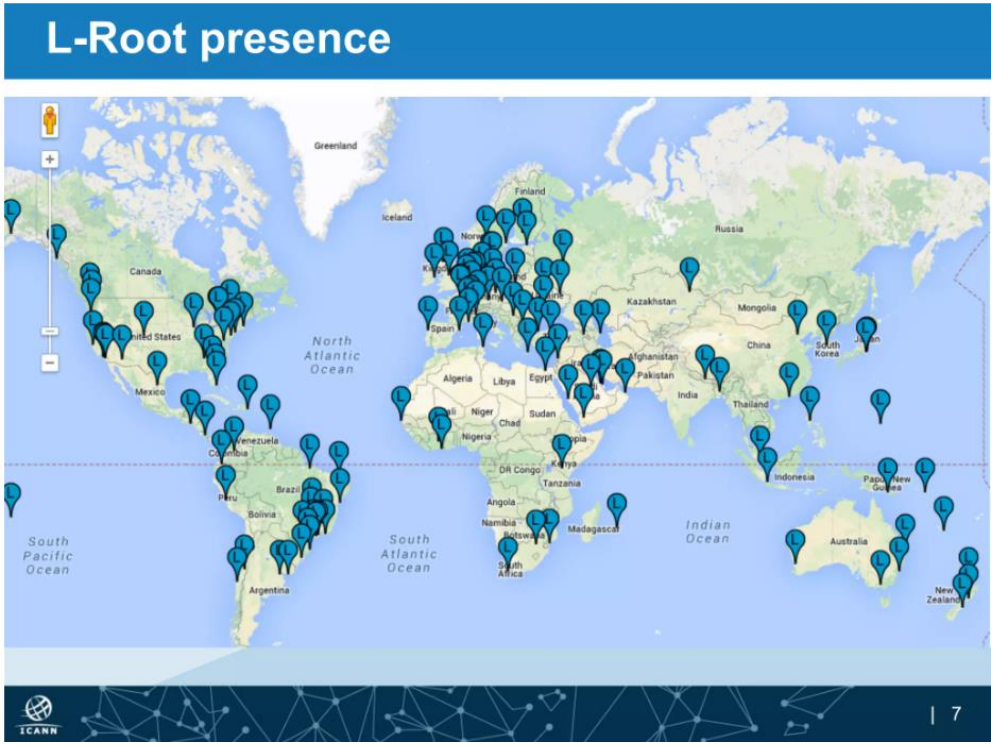
ICANN: Ownership

ICANN (Internet Corporation for Assigned Names and Numbers) is a nonprofit organization and does not have traditional ownership in the sense of private ownership or shareholders. Instead, ICANN operates under a unique multistakeholder governance model that involves various stakeholders from different sectors.

ICANN: Corporate Identity

CANN (Internet Corporation for Assigned Names and Numbers) has its own corporate identity that represents its mission, values, and role in governing the internet's unique identifiers.

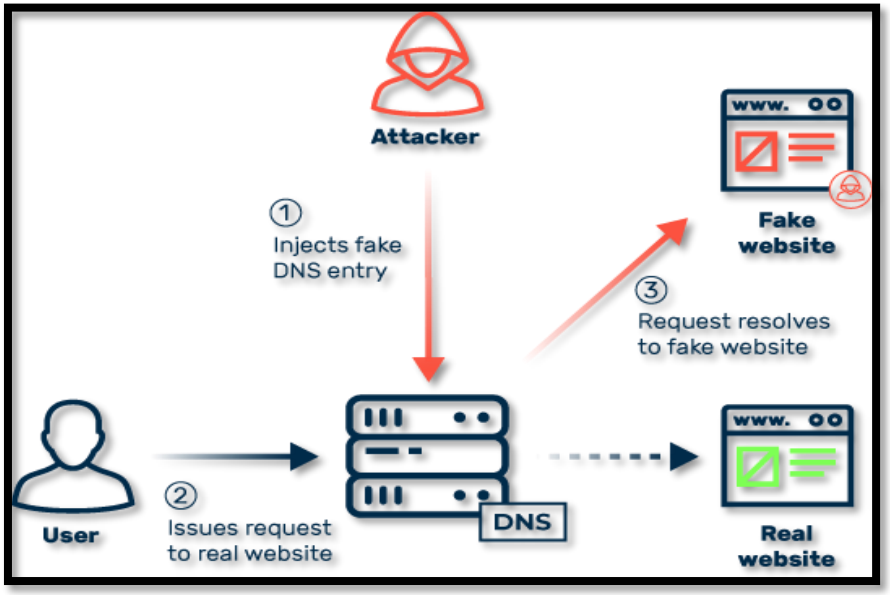
ICANN's corporate identity emphasizes its commitment to serving the global internet community and fostering collaboration among stakeholders from different regions and backgrounds.



ICANN: The future

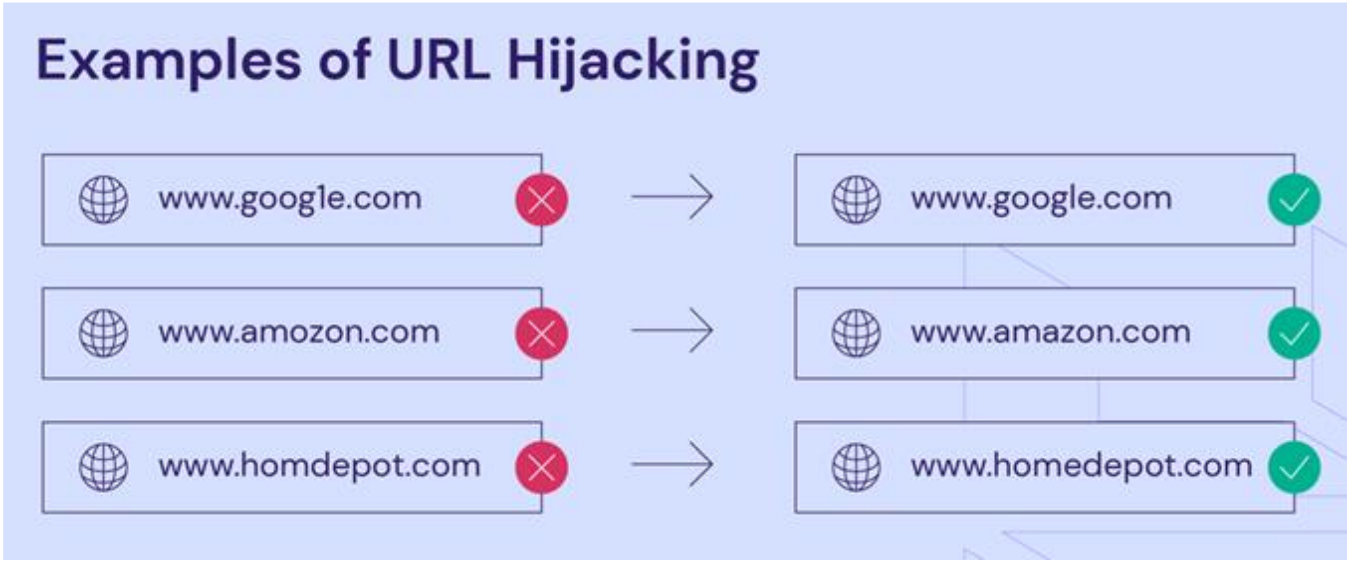
Domain Name System (DNS) Security: ICANN continues to work on enhancing the security and stability of the DNS. This includes initiatives to combat domain abuse, strengthen DNS infrastructure, and improve measures to prevent cyber threats such as DNS attacks and domain hijacking.

DNS attacks



ICANN: The future

Domain Name hijacking/ Domain Hijacking



Domain name hijacking refers to the unauthorized and malicious act of taking control over a registered domain name without the legitimate owner's consent. It involves gaining unauthorized access to the domain registrar account or manipulating the domain registration settings to transfer the domain name to another party.

ICANN: The future

Internet Governance and Policy Development: ICANN facilitates discussions and policy development on a wide range of internet governance issues.

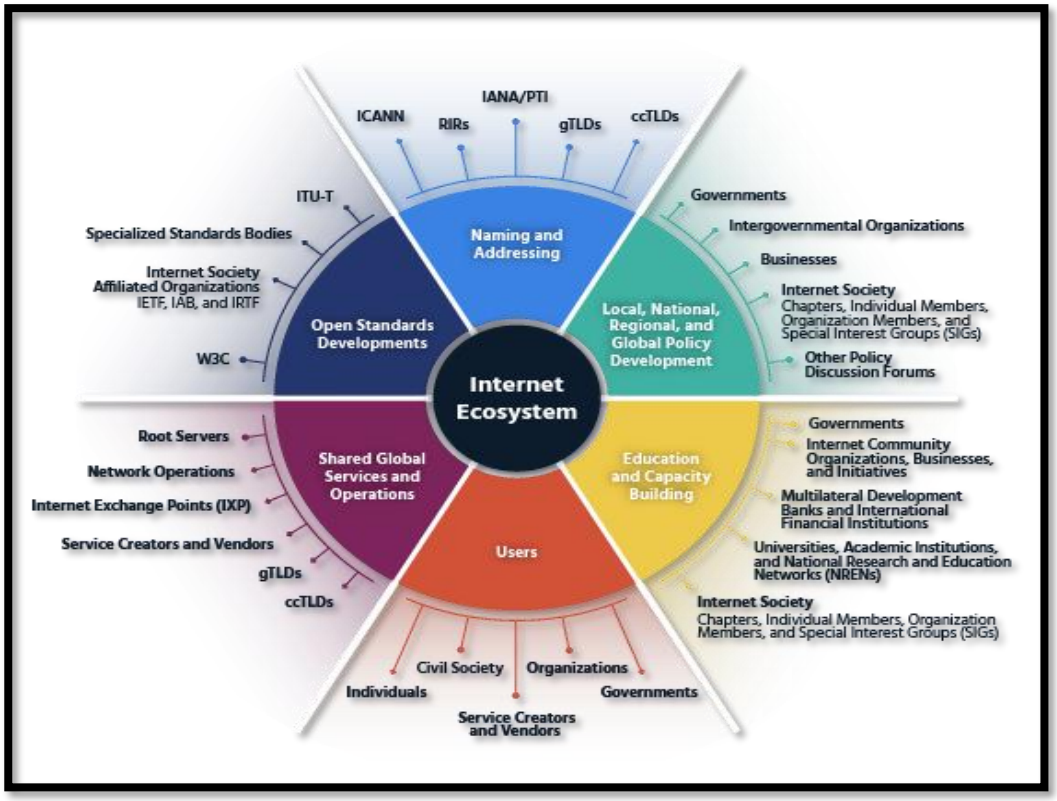
This includes ongoing efforts to engage stakeholders in addressing topics like privacy, data protection, intellectual property rights, online content regulation, and access to the internet.

ICANN: The future

New Generic Top-Level Domains (gTLDs): ICANN introduced a significant expansion of gTLDs to promote competition and innovation in the domain name industry. ICANN may continue to evaluate the success and impact of this program and consider further additions or modifications to the gTLD space.

gTLD	From	To
.dad	2 April 2023	1st May 2023
.esq	2 April 2023	1st May 2023
.foo	2 April 2023	1st May 2023
.mov	2 April 2023	1st May 2023
.nexus	2 April 2023	1st May 2023
.phd	2 April 2023	1st May 2023
.prof	2 April 2023	1st May 2023
.zip	2 April 2023	1st May 2023

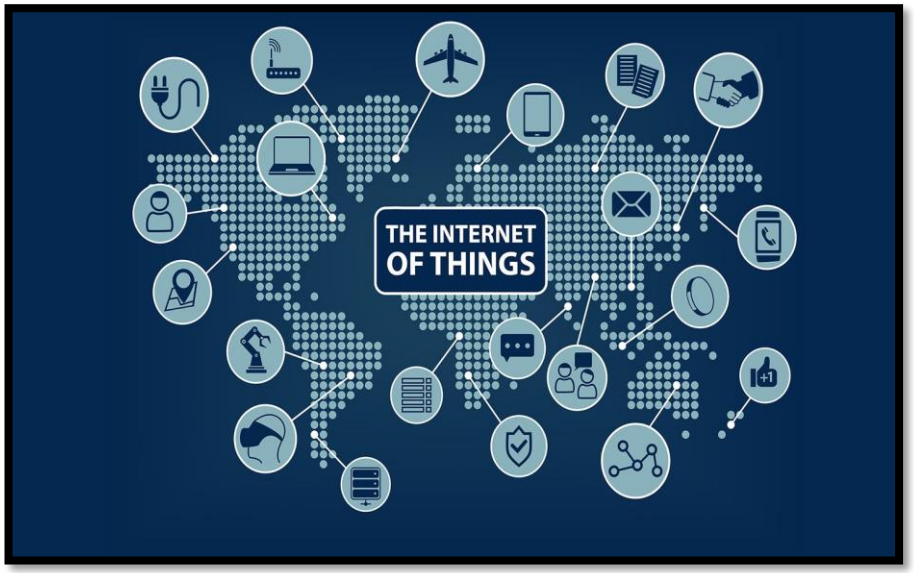
ICANN: The future

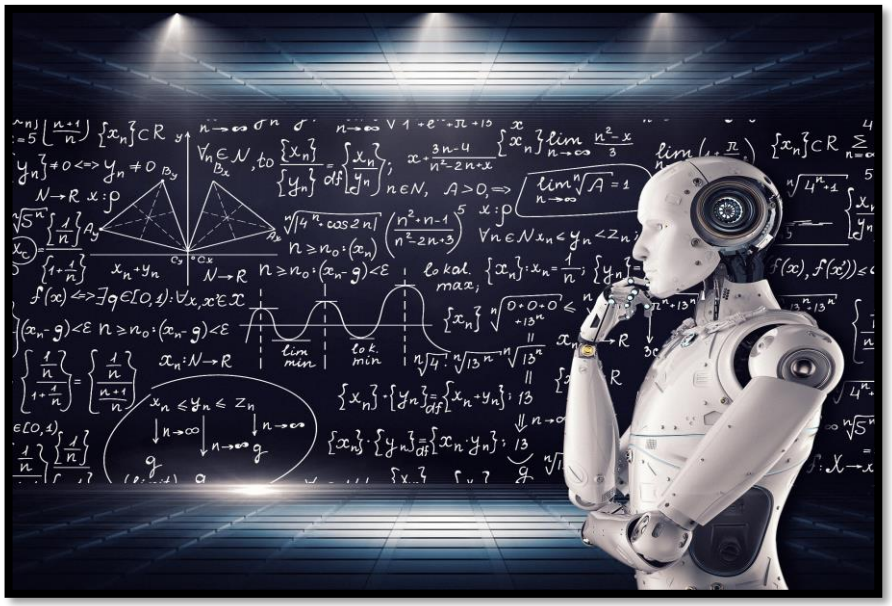


International Engagement: ICANN strives to foster international collaboration and engagement, working with governments, organizations, and stakeholders worldwide to ensure a globally inclusive and diverse internet governance ecosystem. ICANN may further expand its outreach efforts and partnerships to strengthen global participation and representation.

ICANN: The future

Emerging Technologies: ICANN keeps a close eye on emerging technologies that could impact the internet's unique identifier systems, such as the Internet of Things (IoT), blockchain, and artificial intelligence. It may explore the implications of these technologies on DNS management and identify any necessary adaptations or policy considerations.





End