3. Technical Foundations – how the Internet works and why technical remedies are of limited use

Authors: Anna Funk, Christian Hönig and Christian Munz
Academic supervisor: Tamás Szadeczky

DOI: 10.24989/ocg.v.342.3

3.1. Introduction

A probable cause why remedies applied by political and administrative bodies are not satisfactorily successful is that administrative staff and political deciders have limited knowledge of how both hate speech and fake news work from a technical perspective. One needs a sound understanding of how posting and disseminating hate speech and fake news or, generally spoken, the whole internet works. The goal of this chapter is to describe how it works. This does of course not include any judgment on whether this is good or bad – it is simply a description of mechanisms and the status quo.

The main message of this chapter is, that the internet is not, absolutely not comparable to any other media we know and to the legal setting we know from these other media. The main reasons for this are that the internet has no proprietor, organizer, authority whatsoever (1) and that a person or computer program which produces hate speech and fake news or any internet content is not located in the same country as the person affected (2) and hence not subject to the jurisdiction of this country. More than that, it is neither sure nor likely that the internet platform used is in either the country of the person producing hate speech and fake news or in the country of the person affected (3).

These three phenomena are different from a classic media setting like newspapers, radio, or television.

3.2. The Internet: A world without much Governance

The whole nature of the internet is that of a non-governed, self-administrated organism. As Leiner et al. have shown in their “A brief history of the internet” [3-1], the internet was not intended to host political discussions, hate speech, etc. "There would be no global control at the operations level." was one of four fundamental principles (called ground rules) stated by Robert E. Kahn [3-1, p. 24]. In 1969 the Requests for Comments (RFCs) were introduced by S. Crocker of UCLA, which were de facto standards but formally totally informal [3-1, p.28].

“The IETF now has more than 75 working groups, each working on a different aspect of Internet engineering. Each of these working groups has a mailing list to discuss one or more draft documents under development. When consensus is reached on a draft document it may be distributed as an RFC” [3-1, p. 28].

This quote describes why the internet itself cannot be measured by standards of sophisticated legislation like e.g., on press affairs: Because it was never intended nor “organized” to host such a quantity and quality of load like it does today. If those few academics from different universities over the USA, all distinguished scientists, everyone would have imagined that hate speech battles by millions of users would be fought on social media, they would likely have chosen a fundamentally different design.

3.2.1. The Postal Union and the Treaty of Bern on International Postal Services – A different approach and regime

The Treaty of Bern was signed on 9 October 1874. The treaty intended to standardize postal services and regulations to exchange international mail freely. It is the basis of global postal services. The signatories of the treaty form one postal area, to exchange shipments. Besides the definition of terms, the conditions are written down like costs, general shipping terms and more. The Treaty of Bern only regulates general conditions of the different types of shipments but details about the constitution and the handling. Another part of the treaty is instructions of shipping limitations, regulations of the post exchange with countries that have not signed the treaty and more. At the very end a special regulation for some signatories states, that no signatory country is bound to deliver a sending to an area, where the shipper can ship postal items into another member country and profit from their lower fees [3-2].

Article three of the treaty of Bern states that every member county has to make sure that every user has access to universal postal service. This service has to be area-wide and affordable. Another important article is article 12: the member countries have to take care of the acceptance, processing, transport and delivery of letters. Therefore, there are specific rules that every member country has to deliver every letter from any member country.

In 1874 the Universal Postal Union was founded and since then they regulate the international cooperation of the postal services and the basic parameters of the cross-border sending and the upcoming costs for the delivery. The main task of the Universal Postal Union is to secure worldwide, timely delivery of letters and packages.[140]

To ensure the delivery of letters there are four different bodies at the Universal Postal Union. First the Congress. It’s the supreme authority and gathers every four years. Diplomats from all 192 member countries are in Congress. They make decisions about the future of the postal sector; they also agree on new rules or policies for the international exchange. Another body is the Postal Operations Council, they are the technical and operational part. Its members are 40 member countries, which were elected by the last Congress. The main task of the Postal Operations Council is to help postal services around the world to modernize and upgrade postal products and services. This body also makes recommendations on standards for technological operational or further processes. The Council of Administration consists of 41 member countries and meets every year at the Universal Postal Union headquarter. This body has to ensure the continuity of the work between Congresses, conducts the activities and studies regulatory, administrative, legislative and legal issues. To be able to react in time to changes in the postal sector, the Council of Administration can approve proposals by the Postal Operations Council until the next Congress session. The promotion and coordination of all aspects of technical assistance among member countries is also a responsibility of the council. The last body, the International Bureau has a secretariat function. It supports the other bodies of the Universal Postal Union logistically and technically. It has taken a stronger leadership role in certain activities, like the application of postal technology through its Postal Technology Centre, the development of postal markets through potential growth areas such as direct mail and electronic mail services (EMS)[141], and the monitoring of the quality of service on a global scale. Through the Postal Technology Centre, the Universal Postal Union has entrenched some regional support centers all over the world to support information technology activities.[142]

[140] https://www.upu.int/en/Universal-Postal-Union (last accessed 17.12.2021)

[141] These services comprise, among others, sending electronic letters to a postal authority which prints it, puts it into an envelope and delivers it to the recipient. These services shall not be confused with e-Mail.

[142] https://www.upu.int/en/Universal-Postal-Union/About-UPU/Bodies (last accessed 17.12.2021).

Due to this treaty the signatories agreed to these standards and to establish an administration to control the postal services. Also, there is the Universal Postal Union with its bodies to ensure that agreements of the treaty are kept by the signatories. There are no rules like the Treaty of Bern on the internet, nor someone who can enforce any rules. So, there are no universally enforceable legal consequences on the internet.

3.2.2. IETF Recommendations[143]

Worldwide broadcasting and distribution of information is possible through the internet. It's also a medium for collaboration and communication between individuals [3-1, p. 22]. The internet can be divided into four historically developed aspects. First into the technological aspect which started with research on packet switching and the Advanced Research Projects Agency Network (ARPANET). The research also expands the current limits like scale and performance. The next is the social aspect, this formed a community of Internauts who work together to design and expand the current technology. The operations and management aspects are important for a global and complex operational infrastructure. And not to forget about the commercialization aspect where the research results and accessible information can be transitioned highly efficiently [3-1, p. 23].

Documentation is a very important part of the internet. It began with the constant growth of the internet through free and open access to basic documents like the specifications of the protocols. The academic traditions for open publication of ideas and results got promoted for the ARPANET and the Internet in the academic research community. But the usual way of an academic publication was too formal and slow to create a dynamic exchange. In 1969 S. Crocker established the Request for Comments (RFC) series of notes. The idea of the RFCs was to share ideas with other network researchers in an informal and fast way. In the beginning, the RFCs were printed documents, which were sent by snail mail. As soon as the File Transfer Protocol (FTP) was created and applied, the RFCs became online files and could be accessed through the network at many sites all around the world. RFCs should create a positive feedback loop through ideas or suggestions of another RFC with further ideas. The relevant ideas which belong together will be summed up in a specification document. Documents like this will then be used as a basis for the implementations of different research teams. Although the RFCs started as informational documents, they are more focused on protocol standards and "documents of record" now. The Internet is among other things constantly because of open access to the RFCs. Open access allows their usage for example in classes and for the development of new systems. Emails also changed the development of protocol specifications, technical standards, and Internet engineering. While at the beginning of RFCs the researchers from one place presented their ideas to the community, email enables joint authors with specific knowledge from all around the world to work together and come up with new and innovative ideas. Therefore, the IETF works with many mailing lists in each working group. In this mailing lists, the draft documents in progress can be discussed and improved. As soon as the working group has enough consensus researched the draft could be distributed as an RFC [3-1, p. 28].

Unlike a legal document, a draft of law or such an RFC is never voted on, never formally closed and hence its status can be described as "informal and permanently pending". The internet works because all actors design and develop their products like browsers, file services, etc. under strict observation of the RFCs on a voluntary basis.

[143] https://www.ietf.org/ (last accessed 25.10.2021)

The IETF (Internet Engineering Task Force) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of Internet architecture and the smooth operation of the Internet. The IETF operates in working groups to do the technical work. These groups are specialized in different areas, these are managed by Area Directors (ADs). The groups are supported via many programs of the Internet Society, another community "governing" the internet. A lot of the work gets done through mailing lists. There are IETF meetings and events three times a year, like the IETF Hackathons, which show practical implementations of IETF standards. The IETF aims to make the Internet work better by producing high quality, relevant technical documents that affect how people use and manage the internet. To reach this goal, the IETF established the following principles.[144]

- Open process: because of this principle the documents, the WG mailing lists, or attendance lists and the Meeting minutes of the IETF are publicly available on the internet. Therefore, any interested person can participate, inform themselves and make his or her voice heard.

- Technical competence: the IETF is willing to listen to technically competent input from any source. The IETF expects its output to be developed after strong network engineering principles, also called "engineering quality".

- Volunteer Core: people who work for the IETF want to make the internet work better.

- Rough consensus and running code: the standards are developed based on engineering judgement and real-world experience in applying their specifications.

- Protocol ownership: the IETF takes ownership of some protocols, so it accepts full responsibility, even if some aspects may not be seen on the internet. But if the IETF does not take the responsibility for a protocol it does not try to get control over it, even if it touches the Internet.

Note that the IETF is not responsible for the internet nor owns it. It is of limited legal nature, namely subpoenas and similar legal papers can be served under US law. Requests for authenticated documents and other information directly from the IETF may be made either informally or formally through a third-party subpoena.[145]

The most important documents from the IETF are the above-mentioned RFCs. There are more than 9,000 individually-numbered documents in the series. The RFCs address many aspects of computer networking, like technical foundations of the internet, addressing, routing and transport technologies. The RFCs furthermore specify protocols that are for services used by billions of people daily, like real-time collaboration, email and the domain name system.

RFCs may have different statuses, depending on their level and what they cover: Internet Standard, Proposed Standard, Best Current Practice, Experimental, Informational, and Historic.

RFCs start as Internet-Drafts (I-Ds). These are normally going to be improved and revised in different working groups. When RFCs get published, they are freely available. The described technical specifications are implemented and adopted voluntarily by software developers, hardware manufacturers, and network operators from around the world.

[144] https://www.ietf.org/about/mission/ (last accessed 24.01.2022)
[145] See https://www.ietf.org/about/administration/legal-request-procedures/ for the procedure (last accessed 24.1.2022).

Please note again that these documents are not binding and, if not obeyed, do not have legal consequences, but if everyone on the internet acts as they suggest, the internet is working better.
So RFCs are more like a recommendation for the users on what to do or not to do. The whole internet can be compared to a highway without any police or roadside assistance services. There are no binding rules which have to be followed because they can't be enforced or controlled. The RFCs recommend not to hack somebody but it's done despite this, simply because it's possible.[146]

"As the current rapid expansion of the Internet is fueled by the realization of its capability to promote information sharing, we should understand that the network's first role in information sharing was sharing the information about its own design and operation through the RFC documents. This unique method for evolving new capabilities in the network will continue to be critical to the future evolution of the Internet.". [3-1, p. 27]

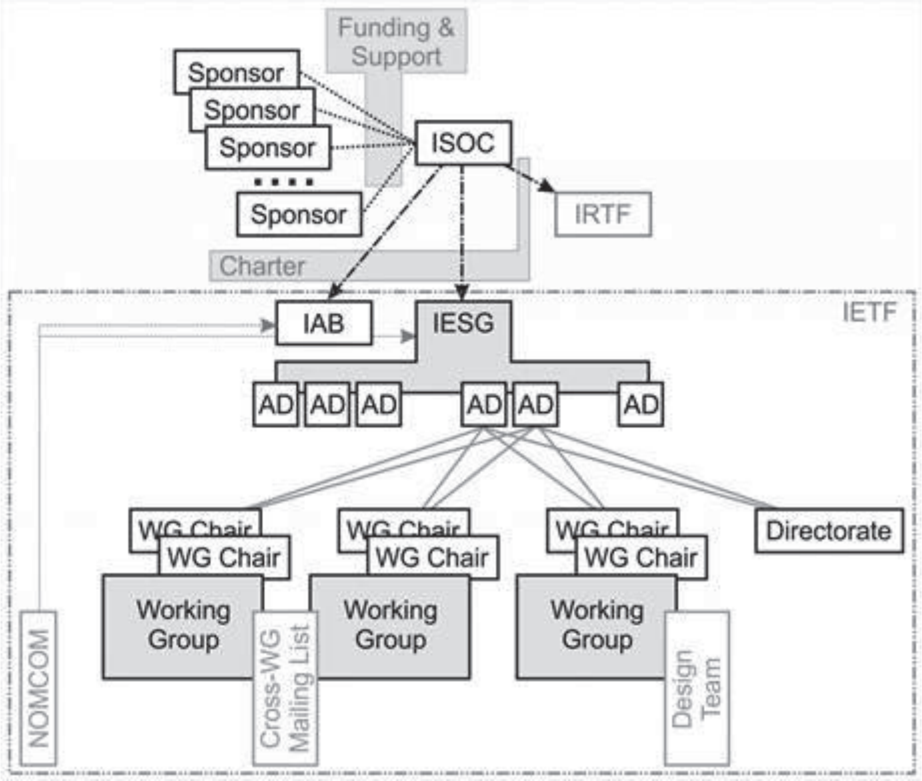


Figure 26: Organizational structure within IETF[147]

[146] https://www.ietf.org/standards/rfcs/ (last accessed 24.01.2022)
[147] https://devopedia.org/internet-engineering-task-force (last accessed 24.01.2022)

3.3. A brief introduction to how the internet works

3.3.1. Global Internet accessibility

Today, internet access is available in almost every country. Around 51 percent of the world's population is expected to have internet access as of 2019. Only the access rates may vary by country and region, depending on the local infrastructure. Even in areas that currently do not have the infrastructure to access the internet, there will most likely be the possibility to get a satellite connection in the near future. The technical availability of access to the internet also directly leads to steady growth of active users of social media, with an estimated 4.2 billion active users as of January 2021.[148]

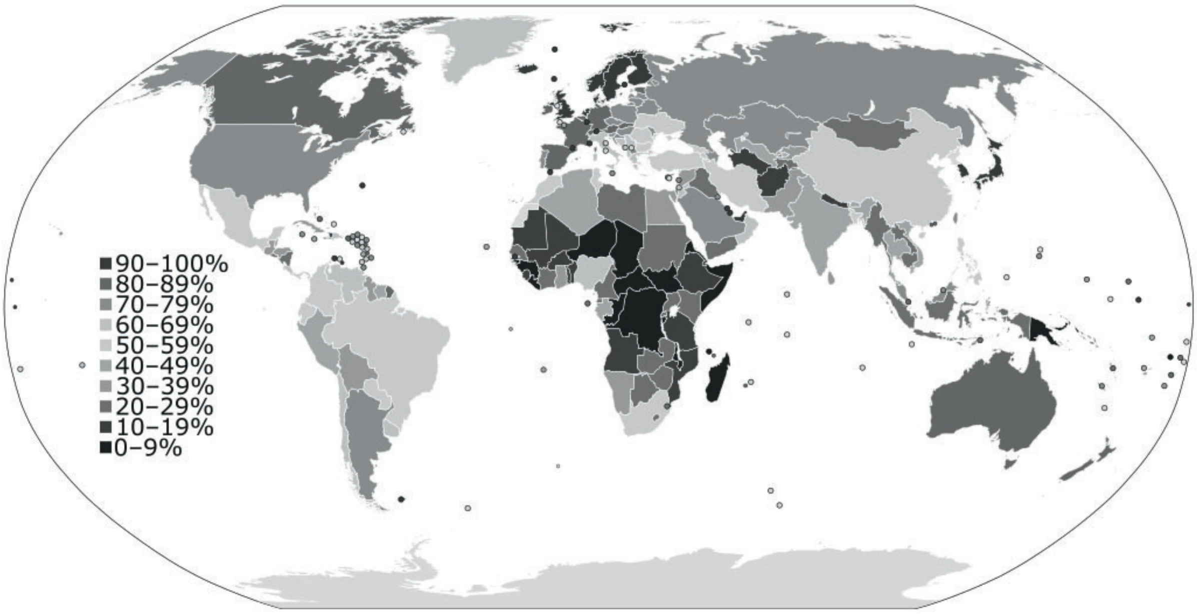


Figure 27: A world map colored to show the level of Internet penetration, by Jeff Ogden is licensed under CC-BY-SA 3.0[149]

3.3.2. Network Architecture Types

The internet itself is not one certain network but rather a collection of different networks and systems which are interconnected. In the early days of computing, the so-called mainframe architecture was one type of simple, local network. Multiple terminals were connected to a single mainframe system, that did all the calculations for all connected clients. In modern days it comes down to two major types of network architectures: Client-Server and Peer-to-Peer.

Most services on the internet (e.g., websites with social media functionality) are based on the client-server concept. On the client side, usually, the computer or smartphone of a user mainly shows data provided by a server. None of this data is stored permanently locally on the client. Instead, all the resources, information and data are stored and processed on the server. The owner of the server therefore technically owns the entire data stored on the server and may change or cancel the service he provides at any time. It is also possible to provide different versions or alternatives of data and services to different clients (e.g., for different countries or regions) ultimately leading to the possibility to create

[148] https://www.statista.com/statistics/617136/digital-population-worldwide/ (last accessed 09.01.2022)

[149] https://commons.wikimedia.org/wiki/File:InternetPenetrationWorldMap.svg (last accessed 08.02.2022).

different realities for each client. Those modifications to data by the server can only be noticed by users if they use multiple clients with different versions of data provided and do a side-by-side comparison. Despite the hierarchic composition, many sublayers of the ISO/OSI model, and connections between subnets are possible, which makes their analysis problematic [3-6, p. 52].

Another and less frequently used network architecture, is the so-called Peer-to-Peer. All clients work together on the same protocol level and each peer works in the network both as a server and as a client. Without one central server that provides certain services, it is not possible to simply shut down a Peer-to-Peer network via a single point. Additionally, it is not a single person alone responsible for the network. It is also not easy to provide certain functionalities like commenting on content which is a very important function in social media. However, Peer-to-Peer networks are perfectly fit for sharing large amounts of data (e.g., videos, music and archives). With the data being available redundant over multiple peers (users), it is almost impossible to stop the spread of peer-to-peer shared data.

Another reason why sharing platforms are rather peer-to-peer-organized is quite simple: If user A shares directly with user B and more clients, then there is no need for an actual platform hosting the content. Consequently, no one has neither a say nor any legal liability. The most used peer-to-peer network is BitTorrent.[150]

3.3.3. The IP-Protocol

A uniform language is required to communicate between client and server or between peers. For these networks, this is the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol family. Due to the setup of the Internet, instead of circuit-switching (direct, continuous communication), it uses packet-switching (sending smaller amounts of data, slicing the communication to fixed-sized packs). Large amounts of data such as videos and images are packed into small data packets and transmitted over the network. The receiver of the data packets reassembles them and processes the data and then displays the requested image in the client's browser, for example.

Similar to the address in the postal system, each participant in the network (whether client, server or peer) has its IP address via which it can be reached and is needed to send and receive the data packets defined by the internet protocol. An IP address is unique within each network and assigned only once at a time but might be reassigned any time to a different network device.

The assignment of an IP address to the client is performed by an Internet Service Provider. Internet Service Providers are usually private companies providing the network architecture for internet access to their customers. If the user does not log in with his data when using an Internet service, only the Internet service provider can say for sure which customer is behind which IP address since only the provider has the billing information of the user. Often, the Internet service provider does not permanently assign an IP address to a customer but instead assigns a new IP address from the Internet service provider's address pool to the customer after some time. If the Internet Access Provider does store the information which customer had which IP address at a certain time, it is possible to trace back certain actions on the internet (e.g., postings in social networks) to one exact customer or person.

However, only the owner of the connection is accessible in this way. In practice, several users are often connected within a local network and use the Internet connection offered by the Internet service provider. This works via so-called Networks Access Translation (NAT). If a computer in the local

[150] https://www.bittorrent.org/introduction.html (last accessed 24.01.2022)

network initiates a connection to a computer on the Internet, the data packets with the request are first transmitted to the router of the local network. This router performs the address translation of the sender address, i.e., exchanges the address of the internal computer with its IP address that gets routed through the internet, then transmits the request. The router thus presents itself to the Internet as the sender of the request. At the same time, the initiation of this network traffic is dynamically stored in a NAT translation table in the router to process the response from the Internet. When the response arrives, the table entry is used to determine the original initiator, the client in the local network. The computer in the local network now receives the data packets from the router and can process them.

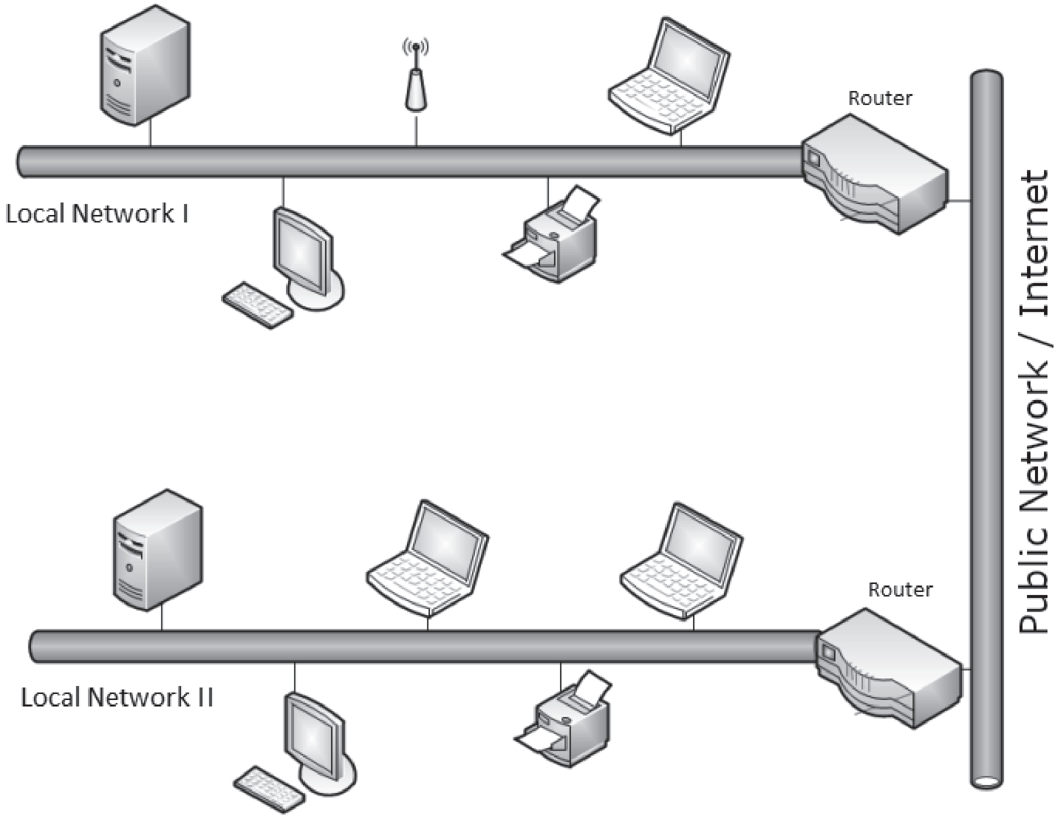


Figure 28: Structure of the internet, Alexander Prosser (2013)[151]

To assign data to individual clients on the local network, each client is assigned a local IP address. For this purpose, certain IP address ranges are not routed via the Internet but are only accessible within the local network.

Each network device has a unique MAC address (Media Access Control). The MAC address is often referred to as the physical address. It is assigned by the manufacturer of the network device and is unique in theory, but for many devices, it can be changed by the user through software manipulation. The router of the local network uses the MAC address of the network devices to assign them a local IP address, which is then used to handle the data traffic. If a user is located within a local network, the exact assignment to a person is only possible with the cooperation of the operator of the local network and only if the user does not regularly change the MAC address, e.g., of his laptop.[152]

[151] https://www.wu.ac.at/fileadmin/wu/o/evoting/Folien/LLM2013_01.pdf (last accessed 24.01.2022).
[152] https://standards.ieee.org/products-services/regauth/oui36/index.html (last accessed 24.01.2022.)

3.3.4. IP-Address assignment

An Internet service provider does not arbitrarily assign IP addresses to its customers. Instead, IP addresses are assigned hierarchically. The highest authority is the Internet Assigned Numbers Authority (IANA, iana.org), which controls the entire IP address space. It allocates IP address blocks to regional IP address allocators, the so-called Regional Internet Registries (RIR), which are responsible for IP address allocation in certain continents and regions. Those are:

- African Network Information Centre (AfriNIC) for the African continent.[153]
- Asia-Pacific Network Information Centre (APNIC) for the Asia-Pacific region.[154]
- American Registry for Internet Numbers (ARIN) for North America, North Atlantic and some Latin America & Caribbean Network Information Centre (LACNIC) for Latin America and the Caribbean islands.[155]
- Latin America & Caribbean Network Information Centre (LACNIC) for Latin America and the Caribbean[156]
- Réseaux IP Européens Network Coordination Centre (RIPE NCC) for Europe, Central Asia and the Middle East[157]

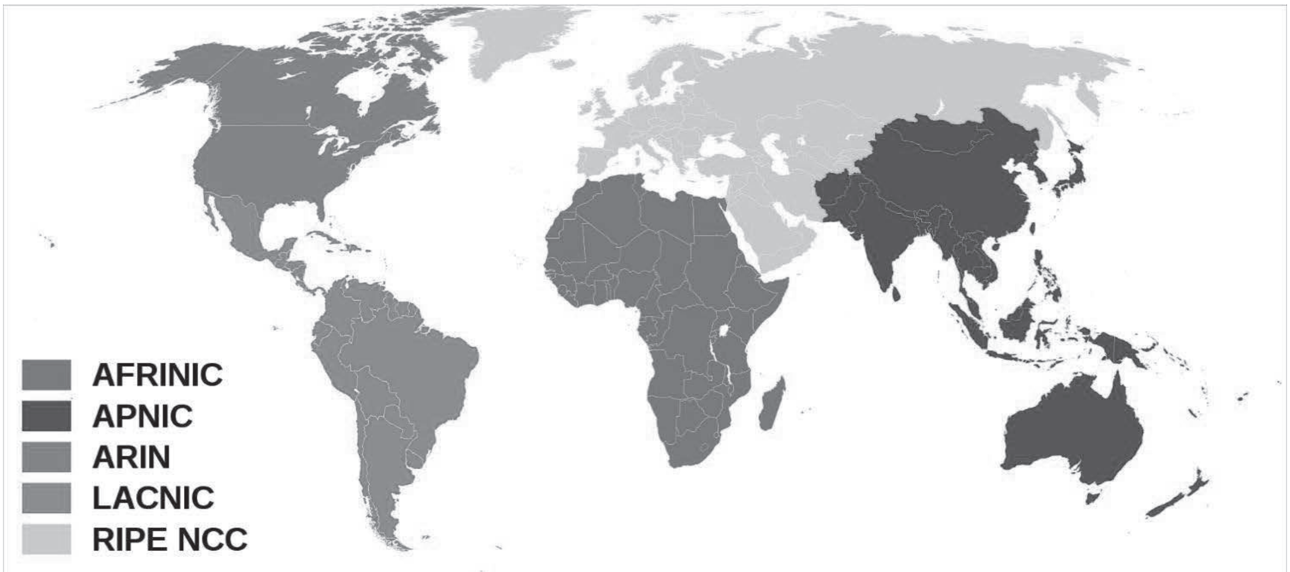


Figure 29: Regional Internet Registries world map, by Dork, Canuckguy, Sémhur is licensed under CC-BY-SA 3.0[158]

All Council of Europe member states are within the territorial jurisdiction of the RIPE NCC. Qualified Internet providers in the relevant regions can now apply to the Regional Internet Registries

[153] https://afrinic.net/about (last accessed 09.01.2022)
[154] https://www.apnic.net/about-apnic/organization/ (last accessed 09.01.2022)
[155] https://www.arin.net/about/welcome/region/ (last accessed 09.01.2022)
[156] https://www.lacnic.net/631/2/lacnic/coverage-area (last accessed 09.01.2022)
[157] https://www.ripe.net/about-us/what-we-do/ripe-ncc-service-region (last accessed 09.01.2022)
[158] https://de.wikipedia.org/wiki/Regional_Internet_Registry#/media/Datei:Regional_Internet_Registries_world_map.svg (last accessed 08.02.2022).

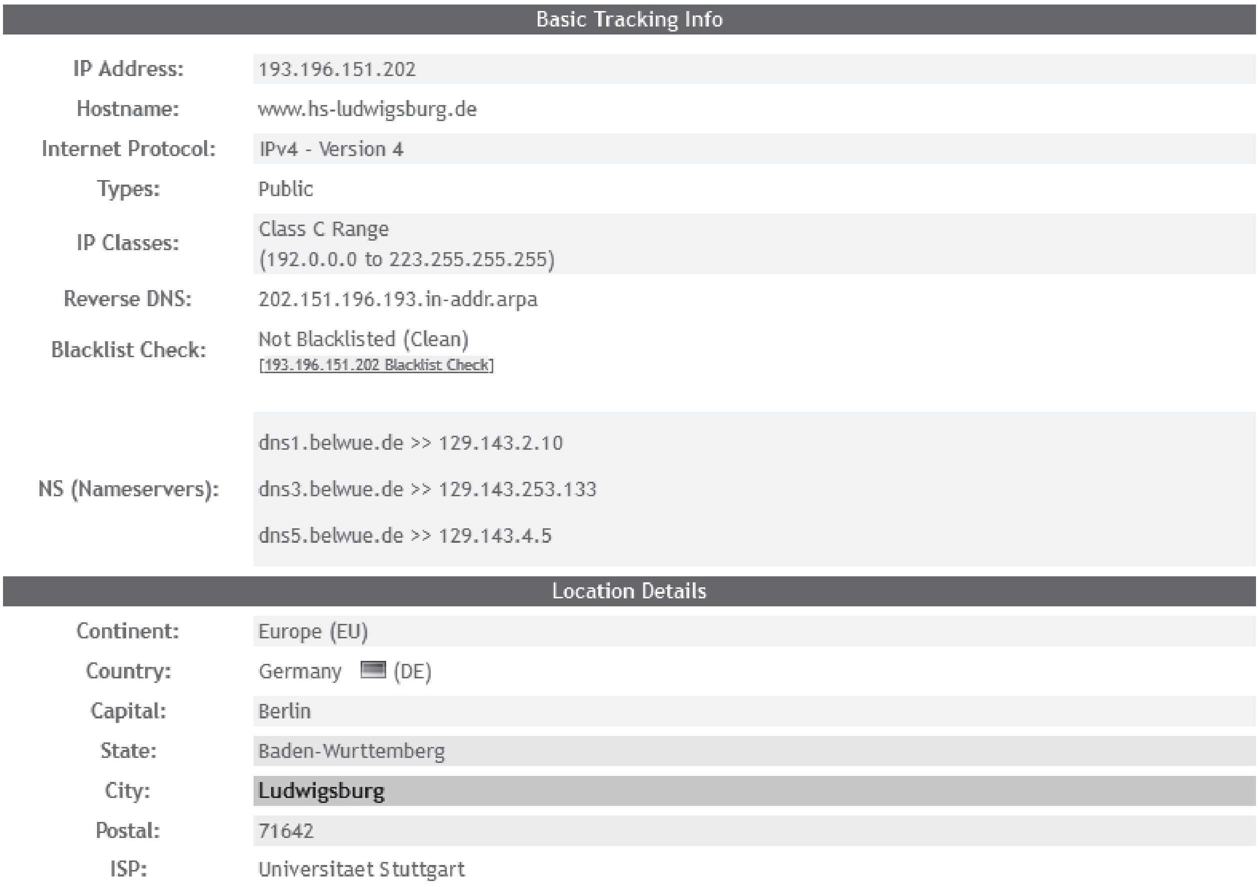
for their own IP address blocks, provided they meet the technical and administrative requirements and can demonstrate a need. Internet service providers are entitled to manage the address range allocated to them largely autonomously, but the allocation of IP addresses by these authorities to other providers and customers is nevertheless subject to extensive conditions: The request for necessary IP addresses must be precisely planned and justified, and the provider must ensure that accurate records are kept of the internal transfer of IP addresses. These two conditions in particular generate an enormous amount of administrative work for providers, even though the actual allocation of IP addresses by the authorities is traditionally free of charge.

Nevertheless, this documentation of IP address allocation is important so that it can be determined at any time to which provider or user a particular address block is assigned and so that future demand can be estimated.

Note that the IANA is also of a very limited legal nature, it is headquartered in California/USA and acts as a coordinator to make sure that neither an IP address nor a domain name is used more than once. For the concrete domains and addresses, the individual local authorities like the DENIC in Germany who controls the .de top-level domain are responsible. Of course, each of these individual authorities is liable to local law and law enforcement, e.g., the DENIC to German law only.

3.3.5. Tracing an IP-Address

Since the allocation of IP addresses to customers by the Internet service provider must be documented at the responsible regional Internet registry, the IP address of a homepage, for example, indicates the country in which it is hosted. The query is possible for everyone through IP tracking services, as these simply access the WHOIS services of the Regional Internet Registries.



Basic Tracking Info

IP Address:	193.196.151.202
Hostname:	www.hs-ludwigsburg.de
Internet Protocol:	IPv4 - Version 4
Types:	Public
IP Classes:	Class C Range (192.0.0.0 to 223.255.255.255)
Reverse DNS:	202.151.196.193.in-addr.arpa
Blacklist Check:	Not Blacklisted (Clean) [193.196.151.202 Blacklist Check]
NS (Nameservers):	dns1.belwue.de >> 129.143.2.10 dns3.belwue.de >> 129.143.253.133 dns5.belwue.de >> 129.143.4.5

Location Details

Continent:	Europe (EU)
Country:	Germany (DE)
Capital:	Berlin
State:	Baden-Wurttemberg
City:	Ludwigsburg
Postal:	71642
ISP:	Universitaet Stuttgart

Figure 30: Own image, Information from ip-tracker.org.
The IP-address shown provides the website of the „Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg“.

Based on the IP address of a client, the operators of a website can determine, for example, from which country and region the client is accessing the website. In this way, services are partially tailored to the respective user and relevant information is displayed first and foremost. Localization accurate to within a few meters based on the user's IP address is not possible. However, region or state can be determined with around 80 percent certainty.[159]

[159] https://www.if-so.com/geo-targeting/ (last accessed 08.01.2022)

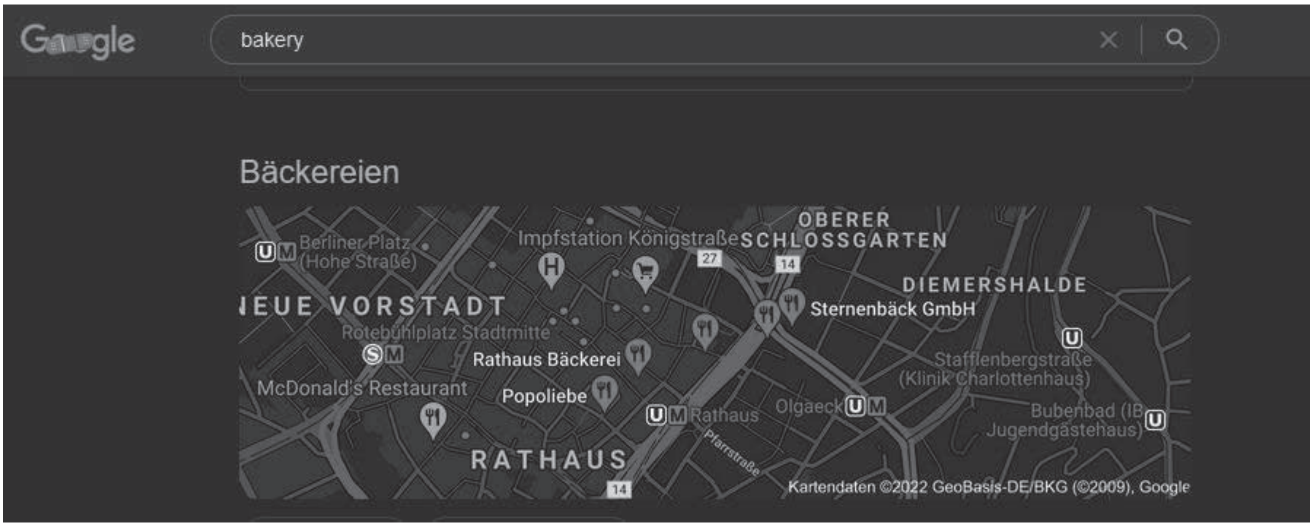


Figure 31: Own image, Google search for a bakery.
Except for the keyword, no other information was passed. Only the IP address was used for geolocation. The map extract shows a part of the city center of Stuttgart, Baden-Württemberg. The user's actual location is only about five kilometers away on the outskirts of the city.

3.3.6. Evade IP tracking

The easiest and fastest way to disguise one's own IP address and thus location when using Internet services is to use proxies. A proxy is a kind of intermediary between the client or user and an Internet resource, such as a website. If the proxy is appropriately configured not to forward the user's IP address to the website, but replaces it with its own and receives the website's data packets vicariously and forwards them to the user, the user's IP address is effectively disguised. The user needs to know that the data transmitted via a proxy can not only be read, stored, and evaluated by the proxy, but can even be manipulated. In addition, the loading time of websites is usually noticeably increased, since many proxy servers are used not only by one, but by hundreds of users, and all data packets of the website must take the "detour" via the proxy server.[160,161]

A proxy can also be used to filter data packets. Many companies use proxies to protect their employees' computers and other clients from dangerous websites. Web filters for pornographic, violent or similar content can also be set up for employees in this way. Another security aspect is the restriction of unwanted remote access to the client which goes beyond the response packets, since the contacted target system from the public network does not send its response packets directly to the client, but sends them to the proxy, which can actively control the connection.[162] End-to-end secure encryption between the website and the client (see 2.7) is essential when using a proxy to ensure the security and integrity of your data.

3.3.7. Website encryption and trust

The monitoring of network traffic by a wide variety of countries, institutions, companies, and others (see Section 3) creates the need for widely deployed, secure, encryption of websites and online services.

[160] https://www.ionos.de/digitalguide/server/knowhow/was-ist-ein-reverse-proxy/ (last accessed 09.01.2022)
[161] https://it-service.network/it-lexikon/proxy (last accessed 09.01.2022)
[162] https://tarnkappe.info/tarnkappe-guide-was-ist-ein-proxy/ (last accessed 09.01.2022)

In addition to personal data on social networks, the security of the ever-growing use of online banking is particularly at risk. Almost two-thirds of citizens in the euro area already use online banking.[163]

The Transport Layer Security (TLS) protocol, often also known by its predecessor name as Secure Sockets Layer (SSL), ensures encrypted transmission of data on the Internet. It is a hybrid encryption protocol that combines asymmetric and symmetric encryption (see paragraph 4.2). The encryption is intended to protect the transmitted data from unauthorized access by third parties and manipulation or forgery. In addition, TLS enables authentication of the communication participants and verification of identities of receiver or sender. TLS is often used for secure connections between a client with an Internet browser and a web server via HTTPS. But other protocols such as SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol) or FTP (File Transfer Protocol) can also use Transport Layer Security. Communication via TLS can be divided into two phases. First, a connection is established in which the client and server prove their identity to each other. Once a trusted connection has been established, the data is transferred using an encryption algorithm.

The so-called Transport Layer Security Record Protocol plays a central role in Transport Layer Security. Four other protocols of the standard build on this. These four protocols are:

- the Handshake Protocol
- the Alert Protocol
- the Change Cipher Spec Protocol
- the Application Data Protocol

The Handshake Protocol is responsible for negotiating a session and its security parameters. Among other things, the Handshake Protocol negotiates the cryptographic algorithms and key material used and authenticates the communication partners. The Alert Protocol is responsible for the error and alarm handling of TLS connections. It can initiate the immediate termination of a connection. The Application Data Protocol is used to split application data into blocks, compress, encrypt and transmit them. Finally, the Change Cipher Spec Protocol informs the receiver that the sender is changing to the cipher suite previously negotiated in the Handshake Protocol.

When a client establishes a connection to a server, the server authenticates itself with a certificate (see 2.7.1). The client verifies the trustworthiness of the certificate and that it matches the server name. Optionally, the client can authenticate itself to the server. In the next step, the communication partners derive a cryptographic session key with the help of the server's public key, which they then use to encrypt all messages to be transmitted. The authentication and identification of the communication partners are thus based on asymmetric encryption methods and public-key cryptography. The actual session key is a one-time-use symmetric key that is used to both decrypt and encrypt the data. Besides the TLS version, the exact used symmetric and asymmetric cryptographic algorithms, and also protocol settings determine the resultant security level [3-7, p. 128].

[163] https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15cbc&lang=en (last accessed 09.01.2022)

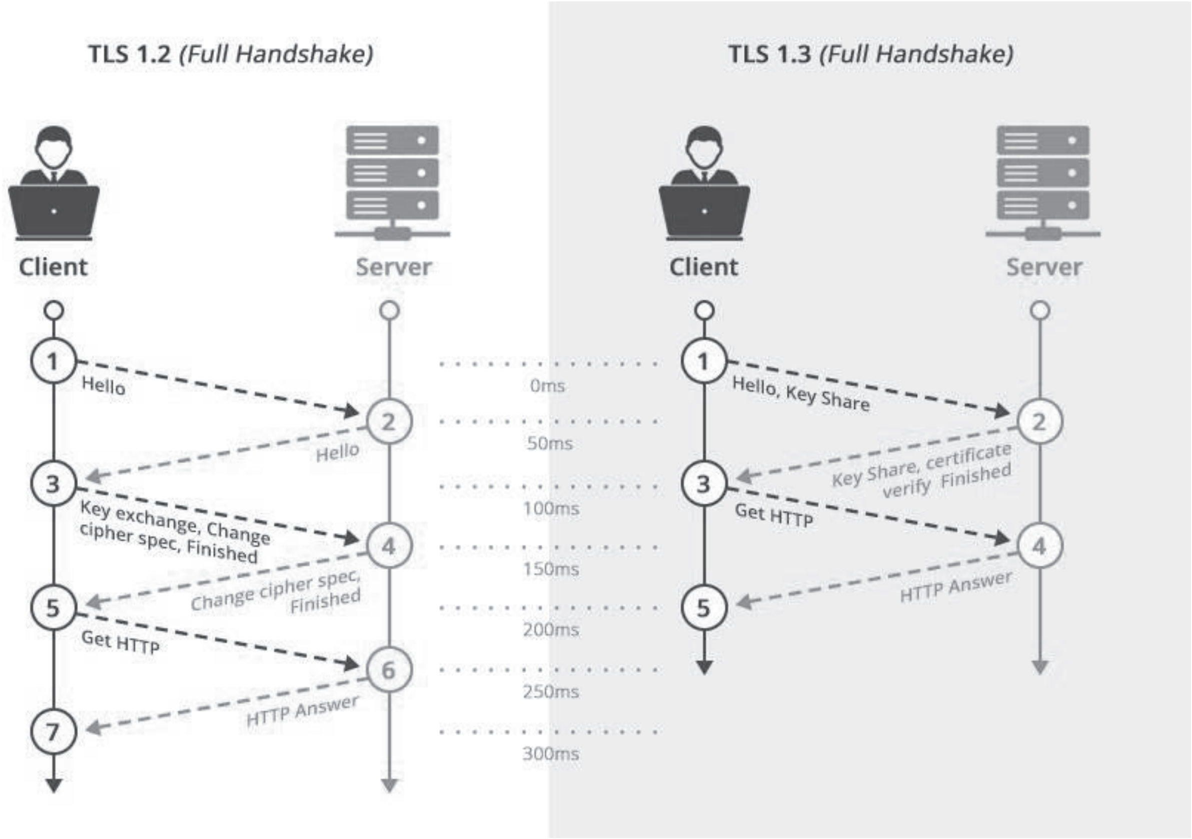


Figure 32: TLS 1.2 and 1.3 comparison by SSL2Buy.com[164]

3.3.7.1. Trustworthy certification authorities

The digital certificate is an electronic proof of authenticity issued by a certification authority (CA). On the Internet, certificates have the comparable function of an ID card in the offline world. With the help of a certificate, a public key can be securely assigned to a specific owner. The contents of the certificate include information about the name of the owner and the issuer of the certificate as well as about the validity period and the use of the certificate.

Together with the public key infrastructure (PKI), certificates enable information to be transmitted securely and encrypted on the Internet. The encryption is based on asymmetric cryptographic processes with private and public keys. The certificate reliably confirms to whom the public key belongs. Browsers and operating systems keep a list of trusted certification authorities. If a certificate is issued by such a certification authority, the computer considers it to be genuine.

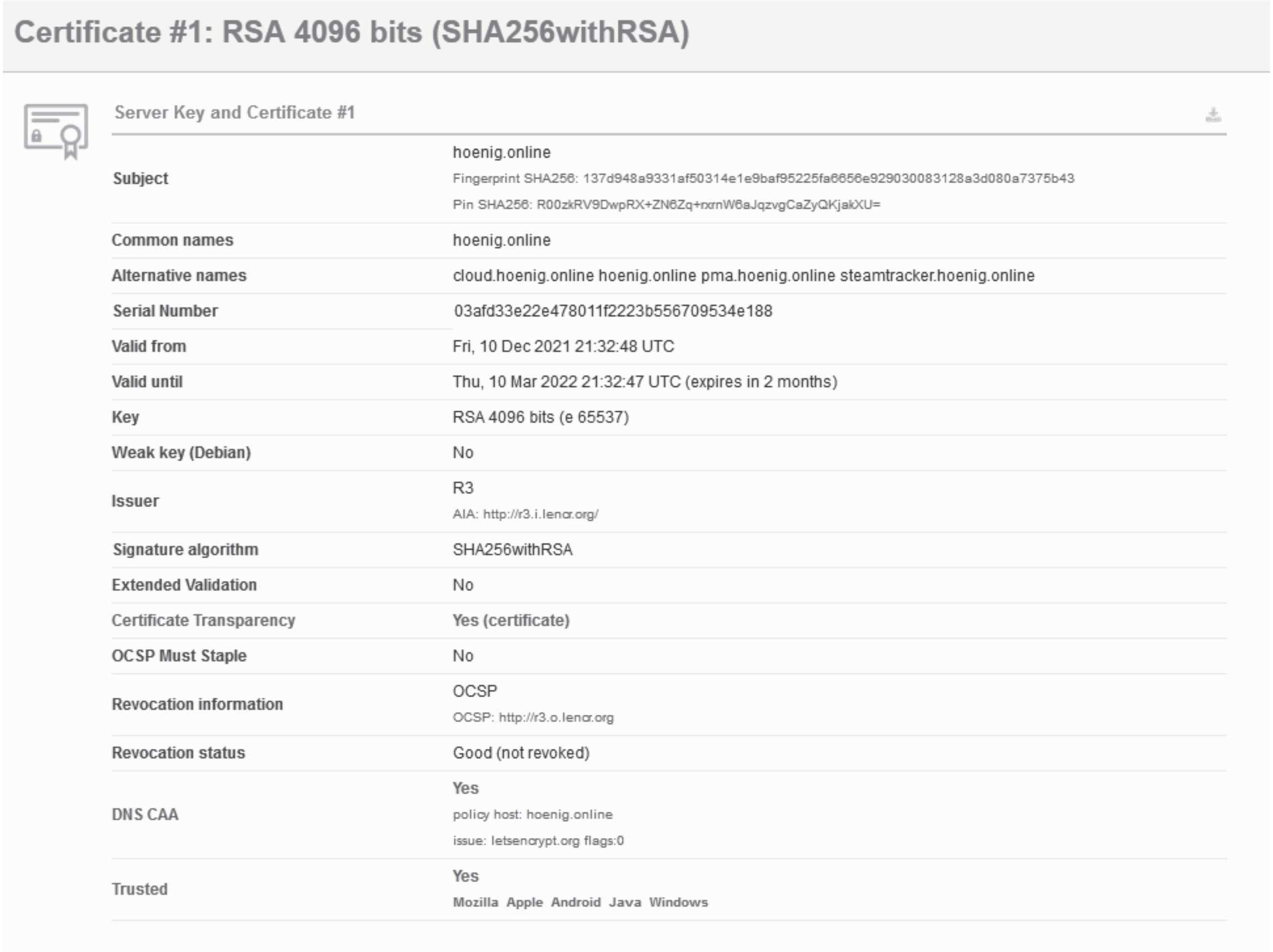
The X.509 standard specifies what content must be included in a certificate and what form. Some information is mandatory others are optional. X.509 certificates are used, for example, to encrypt websites using the HTTPS protocol or to sign and encrypt e-mails using the S/MIME standard.

Important information in an X.509 certificate includes:[165]

[164] https://www.ssl2buy.com/wiki/tls-1-3-protocol-released-move-ahead-to-advanced-security-and-privacy (last accessed 08.02.2022):
[165] https://datatracker.ietf.org/doc/html/rfc5280 (last accessed 09.01.2022)

- the version number
- the serial number
- the algorithms used to create it
- the name of the issuer
- the name of the holder
- the validity period
- information about the public key of the holder
- information about the intended use of the certificate
- the digital signature of the Certification Authority

Certification authorities (CA) or trust centers play an important role in the public key infrastructure and certificates. They check the details and identity of an applicant for a certificate and issue it if the details are correct. They can also take care of publishing the certificates and storing them in public directories. Other tasks of the CA include managing and publishing certificate revocation lists and recording all certification activities of the Certification Authority.



Certificate #1: RSA 4096 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	hoenig.online Fingerprint SHA256: 137d948a9331af50314e1e9baf95225fa6656e929030083128a3d080a7375b43 Pin SHA256: R00zkRV9DwpRX+ZN6Zq+rxrnW6aJqzvgCaZyQKjakXU=
Common names	hoenig.online
Alternative names	cloud.hoenig.online hoenig.online pma.hoenig.online steamtracker.hoenig.online
Serial Number	03afd33e22e478011f2223b556709534e188
Valid from	Fri, 10 Dec 2021 21:32:48 UTC
Valid until	Thu, 10 Mar 2022 21:32:47 UTC (expires in 2 months)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: hoenig.online issue: letsencrypt.org flags:0
Trusted	Yes Mozilla Apple Android Java Windows

Figure 33: Own image, Screenshot of an SSL test by qualys[166] for the domain hoenig.online.
The shown certificate was issued by Let's encrypt, a certificate authority provided by Mozilla, EFF and others.[167]

3.3.8. Domains and the Domain Name System

On the internet, data is always transferred between devices addressed by so-called IP addresses, which are the actual address instances of the internet protocol (for which the abbreviation IP stands). However, numbers are more difficult for people to remember than letters put together in a meaningful way, which is why a naming concept was devised for the internet that was based on the existing internet protocol, the Domain Name System (DNS).

The DNS has a hierarchical structure in order not to have to manage and process all DNS queries centrally, which would simply fail due to the number of domains and queries, but to be able to provide the DNS information in a distributed and heavily redundant manner. The so-called root servers form the top hierarchy. They contain information about the name servers that are responsible for the top-level domains on the Internet.[168]

The next hierarchy level is represented by the name servers of the top-level domains. Each of these top-level domains has its own name servers on the Internet, which contain information about the

[166] https://www.ssllabs.com/ssltest/ (last accessed 09.01.2022)
[167] https://letsencrypt.org/about/ (last accessed 09.01.2022)
[168] https://www.cloudflare.com/learning/dns/what-is-dns/ (last accessed 21.01.2022)

domains registered under the respective top-level domain. These name servers are administered by registries through which domain names can be registered within the respective top-level domain. As of January 2022, there are more than 2500 by ICANN officially accredited registrars over the world.[169] For example, GoDaddy, LLC is located in the US under US law or IONOS SE is located in Germany under EU and German law.

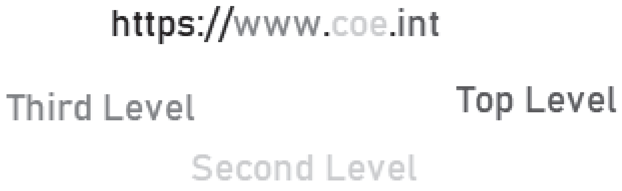


Figure 34: Domain levels

If we read this address from right to left, we first have the top-level domain “online”, the first visible DNS hierarchy level. From a technical point of view, this means that the domain name to the left was registered below the top-level domain “online”. The second part, i.e., “coe”, is the so-called second-level domain, i.e., the second visible DNS hierarchy level. In the case of the top-level domain "int", domain names can be registered directly under the top-level domain, which is not possible for all top-level domains. The domain “int” is also the only domain that is administered exclusively by IANA itself.[170] Within some other top-level domains, there is another level of hierarchy that identifies the category. For example, in the United Kingdom, domain names cannot be registered directly under the national top-level domain “uk”, but there are further levels of hierarchy, such as “co.uk” for commercial addresses or “ne.uk” for network-specific addresses. If there is such a further hierarchy level, this second hierarchy level is the second-level domain (for example, “co” in “co.uk”) and the actual domain name is the third-level domain, i.e., the third hierarchy level. Everything that now follows on the left after the actual domain name (in the example, “www” after “coe.int”) is the responsibility of the person who registered the domain name and can be used for individual computers. In the zone file for “coe.int”, therefore, an entry is created for the name "www" in the form which ensures that when “www.coe.int” is requested, the response is the IP address of the webserver on which the homepage of the Council of Europe is located.

In addition to the purely technical data, administrative information is also required during registration, which makes the ownership of the domain name clear. This necessary information is divided into the description and the contacts.

The description usually contains information about the owner of the domain and possibly other administrative information that is required during registration.

The contacts are divided into the different areas of responsibility that exist in the administration of a domain name:

- administrative contact ("admin-c")

[169] https://www.icann.org/en/accredited-registrars (last accessed 21.01.2022)
[170] http://www.iana.org/domains/root/db/int.html (last accessed 21.01.2022)

The administrative contact is the official owner of the domain name and the general contact for questions regarding the domain name or all entries under it.

- technical contact ("tech-c")

The technical contact is responsible for the technical handling of the domain name. Usually, a person from the IT department of the company concerned or the Internet provider is indicated here.

- billing contact ("billing-c")

The billing contact is found at registries of top-level domains, where a registered domain name must be paid directly to the registry. Usually, a person from the accounting department of the company concerned or also the Internet provider is specified here.

- zone contact ("zone-c")

The zone contact is required for some top-level domains and specifies a person who is responsible for entries within the zone file of the domain name. Usually, this is also a person from the IT department of the company concerned or the Internet provider.

Note that all these contacts are normally email addresses only. A physical address, where writs and civil papers can be served, is neither mandatory nor common.

3.3.8.1. Name resolution

Name servers have two tasks in the DNS: On the one hand, they can be authoritative for certain domains and hold zone information on the Internet, but on the other hand, they are also needed for name resolution. Domain names must be resolved if, for example, a user has entered a domain name in his web browser and the browser first needs the IP address of the target computer to contact it.

Name resolution on the Internet is also hierarchical:

In the introductory step of a name resolution, a client that needs the IP address of a certain resource on the Internet requests the name server responsible for it. The user usually does not need to worry about the address of the name server, since this data is usually supplied with the access parameters of the Internet access. If the name server has already recently performed a corresponding name resolution for the same domain name, it will immediately return the searched IP address. Otherwise, it will perform the following steps to be able to provide an answer.

The name server will resolve the domain name from right to left. So first it will determine which name server is responsible for the top-level domain “int”. The root servers are responsible for the information about the top-level domains, so the name server will contact a corresponding root server and ask if it knows which IP address “www.coe.int” points to. This is not authoritatively responsible for “www.coe.int” and will answer him, according to the DNS hierarchy, with the address of the name server for the top-level domain “int”, which can give more detailed information.

In the next step, the name server will contact the name server of the top-level domain “org” to obtain the information it is looking for. It will also send the same request to this server as to the root server. In this case, the name server for the top-level domain “int” is already authoritatively responsible for "coe.int" and will respond with the addresses of the name servers that are responsible for the domain. Normally, for other domains, these are the nameservers of the Internet provider in the next hierarchy level with which the domain is registered.

After the request to the name server responsible for the domain "coe.int", this looks in its zone file to see which IP address was registered and returns it.

After the name server has now determined the IP address of the desired query, it passes this on to the client. At the same time, the name server stores the result of this query in its cache for a certain period to be able to provide the answer immediately in the event of a possibly identical query.[171, 172]

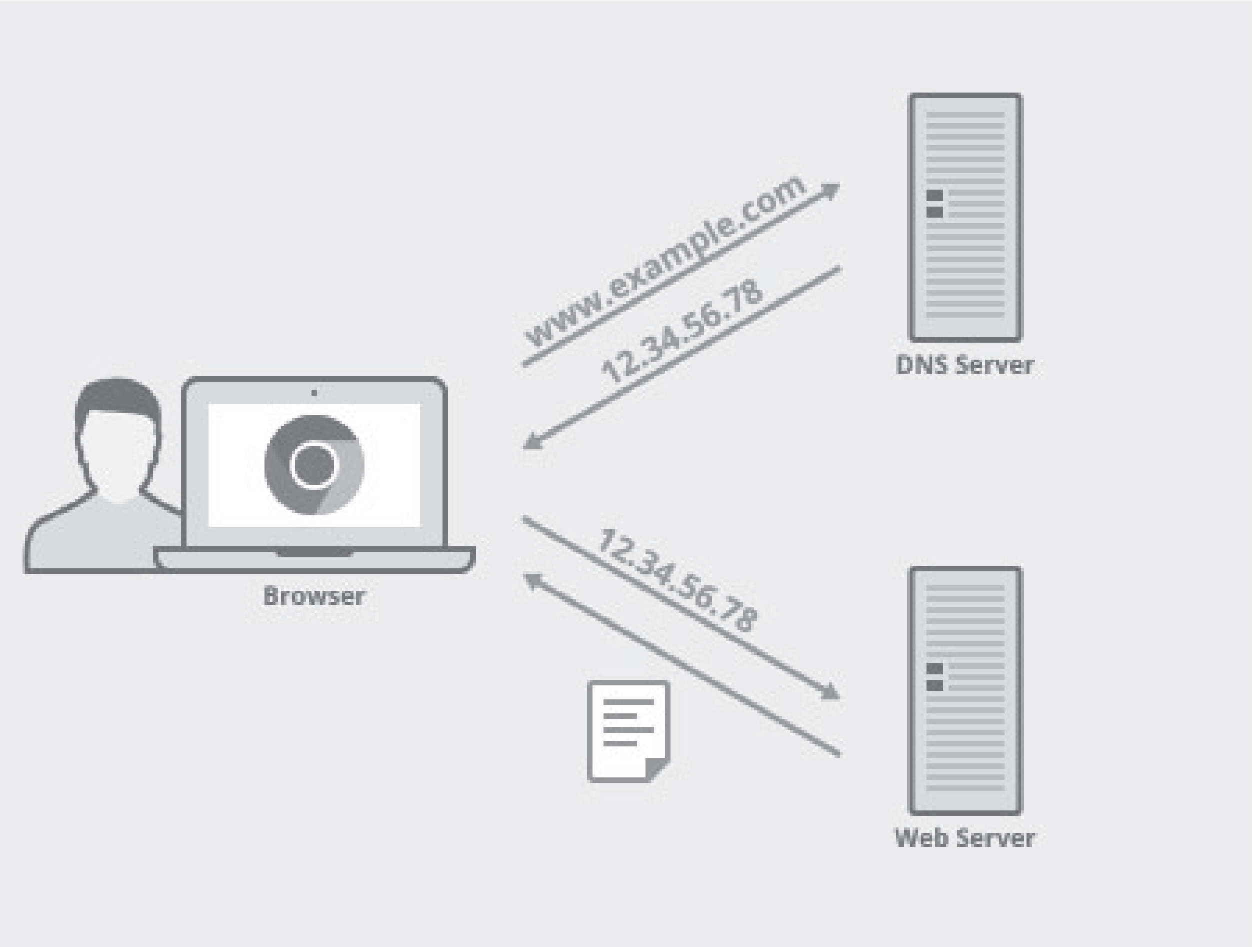


Figure 35: DNS-Server, by Seobility is licensed under CC-BY-SA 4.0[173]

3.3.8.2. Domain Blocking and Censoring

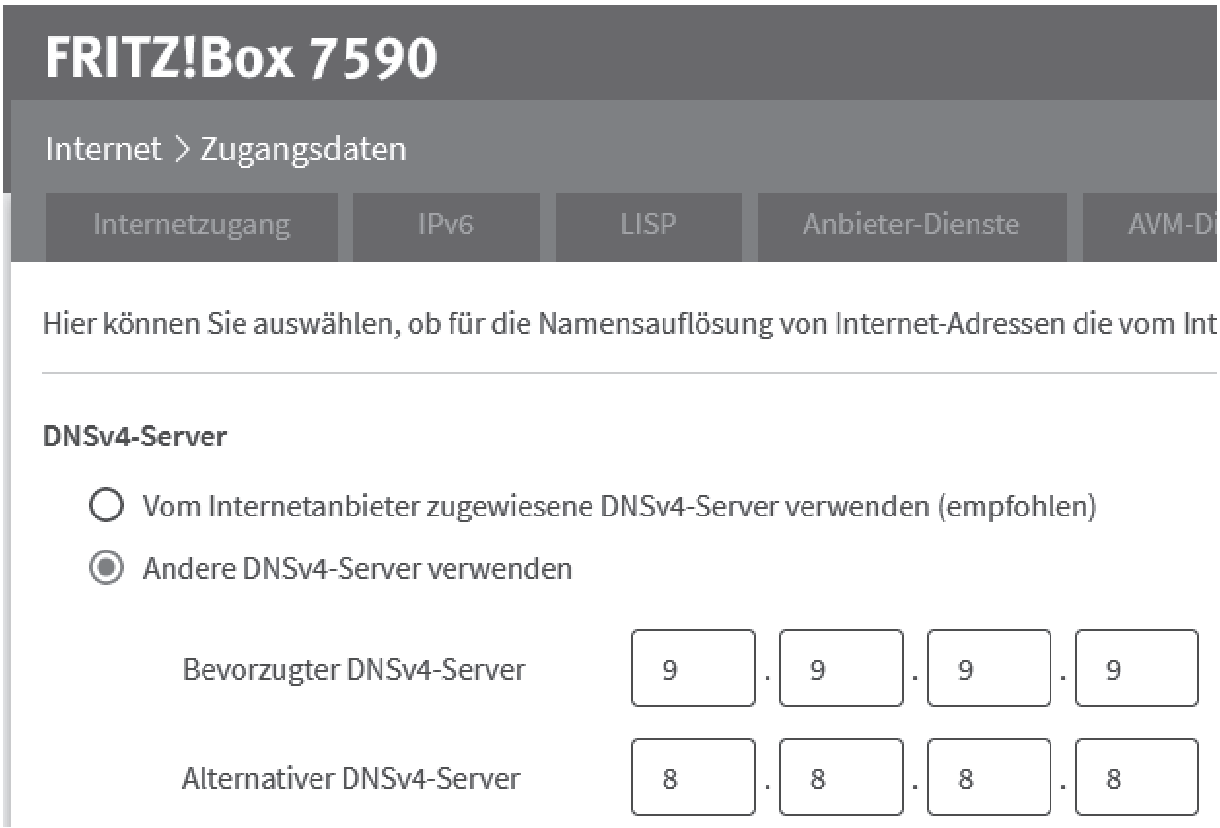
There are recurring demands to block certain websites with content that is prohibited by law in the respective country. These are often implemented with DNS blocks, as the website is hosted on servers abroad and the operators are not tangible. The name servers, which are operated by the customer's Internet service provider in the customer's own country, must then be configured accordingly so that

[171] https://www.techtarget.com/searchnetworking/definition/domain-name-system (last accessed 21.01.2022)
[172] https://www.seobility.net/de/wiki/DNS-Server (last accessed 21.01.2022)
[173] https://www.seobility.net/de/wiki/DNS-Server (last accessed 08.02.2022)

certain websites are not resolved. The customer will then not know the corresponding IP address of the website and will not be able to access it.[174,175]

However, this only affects the name servers in the customer's own country. The name servers that are located in the corresponding country of the website operator will continue to resolve the IP address of the website that is known to them.

If a customer is affected by the DNS blocking of his Internet service provider, he only has to adjust his configuration in such a way that a DNS server abroad is addressed for the resolution of a website domain. The time required for such a configuration change is limited to a few minutes.



Hier können Sie auswählen, ob für die Namensauflösung von Internet-Adressen die vom Int

DNSv4-Server

○ Vom Internetanbieter zugewiesene DNSv4-Server verwenden (empfohlen)

● Andere DNSv4-Server verwenden

Bevorzugter DNSv4-Server 9 . 9 . 9 . 9

Alternativer DNSv4-Server 8 . 8 . 8 . 8

Figure 36: Own image, DNS server settings of the author.
Instead of the "recommended" DNS servers of the Internet service provider, which would implement DNS blocks of the legislators in Germany, the DNS servers of Quad9, based in Switzerland[176], and Google, based in the United States[177], are addressed. Both outside the German legal jurisdiction.

3.4. Surveillance of network traffic

Data traffic on the Internet is continuously monitored by various, mostly governmental, agencies. The best-known example is probably the surveillance programs of the U.S. intelligence services, the nature and scope of which Edward Snowden reported to the Council of Europe in 2014.[178]

[174] https://tarnkappe.info/vodafone-muss-library-genesis-sperren/ (last accessed 21.01.2022)
[175] https://tarnkappe.info/boerse-to-teilweise-von-vodafone-gesperrt/ (last accessed 21.01.2022)
[176] https://www.quad9.net/about (last accessed 21.01.2022)
[177] https://developers.google.com/speed/public-dns (last accessed 21.01.2022)
[178] https://pace.coe.int/en/news/4960 (last accessed 25.01.2022)

The United States is mentioned first here because it enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) in response to the terrorist attacks of September 11, 2001. It provides U.S. law enforcement and intelligence agencies with extensive investigative, intercept, and surveillance capabilities aimed at deterring foreign terrorists and detecting and apprehending those in the country [3-3]. Part of the Patriot Act is the massive simplification for the issuance of a "National Security Letter". [3-4, p. 448] This enables law enforcement agencies to query personal data of users from banks, telecommunications providers or financial service providers, among others, without the need for judicial review of the order. The form in which intelligence agencies within the United States and around the world monitor telecommunications was revealed to the world in early summer 2013. Around 1.5 million previously secret documents were copied by whistleblower Edward Snowden, who had previously been an employee of various companies working for the National Security Agency intelligence service for 4 years, and made available to the press and thus to the world public. The impression was quickly created that the intelligence services of the United States were accessing, storing, and processing electronic data on a massive and warrantless scale [3-5, p. 36].

One of the first major surveillance programs of the U.S. intelligence services is "PRISM." With PRISM data was collected from U.S. companies Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple, including emails, chats, photos, telephone and video conferences, and even login data. While it is denied by the companies involved, it can be assumed that the National Security Agency has direct access to the servers of the affected U.S. companies. Depending on the exit interface through which the National Security Agency receives its data, real-time access to e-mails or chats is even possible.[179]

Whether this type of surveillance is necessary and justified by the threat of terrorist attacks does not need to be answered here. Other countries also have systems for monitoring the Internet traffic of the respective countries, be it at network nodes in Russia[180] or also at DE-CIX in Germany[181], one of the largest network nodes worldwide.

3.4.1. Implementing backdoors and weakening encryption

In addition to directly accessing unencrypted connections, a popular way for intelligence agencies is to deliberately implement vulnerabilities or backdoors in encryption software. Security solutions involving intelligence agencies have already been marketed with a backdoor or weakened encryption to eavesdrop on supposedly secure communications.[182]

However, the danger of weakened encryption algorithms or backdoors in network interfaces must not be underestimated under any circumstances. It can never be guaranteed that these access options to supposedly secure means of communication will not be abused, whether by governments of different countries or by criminal hacker groups that could misuse these options for their purposes. For example, the access data for a backdoor in the network software of a major manufacturer of

[179] https://www.washingtonpost.com/wp-srv/special/politics/prism-collectiondocuments/ (last accessed 25.01.2022)
[180] https://www.faz.net/aktuell/politik/ausland/russland-internet-wird-ab-jetzt-vom-staat-kontrolliert-16462733.html (last accessed 25.01.2022)
[181] https://netzpolitik.org/2015/klaus-landefeld-de-cix/ (last accessed 25.01.2022)
[182] https://www.zdf.de/nachrichten/politik/cryptoleaks-bnd-cia-operation-rubikon-100.html (last accessed 25.01.2022)

networking hardware was used by unknown third parties. With this login data, it was possible to monitor and read supposedly secure connections, such as VPN (see 4.2), in real-time.[183]

Note that the internet surveillance performed by US agencies is far more transparent than the surveillance probably and highly likely performed by agencies of other nations, who lack e.g. a Congress with public hearings, a Freedom of Information act and independent courts as well as civil society with powerful entities like the American Civil Liberties Union (ACLU).

We may assume that the whole internet is subject to far more surveillance, let aside the fact that big players like Facebook, Twitter, Google etc. are subject to US laws and jurisdiction and also to interventions from numerous US agencies.

3.5. Cryptographic basics and ways to remain anonymous in the net

For data being sent between two internet nodes via several unknown internet nodes where every single node can read – and probably alter – the data, the necessity arises, to encrypt the data sent. Sensitive data like credit card details or simple love letters do not need to be read by an unknown intermediary. The following chapter describes how basic cryptographical techniques work and how one of the most used tools, a so-called Virtual Private Network (VPN) works.

3.5.1. Basic cryptography

The usage of cryptography can be traced back to Gaius Iulius Caesar and his military campaigns in nowadays France and Belgium. He used a very simple but to that time a very effective way of cryptography. He put instead of the letter ‘a’ the letter ‘c’ and incremented the alphabet twice to encrypt his message (from the original word ‘apple’ to ‘crrng’). The decryption was also very easy for those who know the code. They decremented the alphabet twice backward (from the original word ‘crrng’ to ‘apple’) and had now the message from the original sender. The enemies on the way can’t read the message if they don’t get the encryption. [184]

Today's methods of encrypting messages are a lot more secure than the “old” one described above. The process to break encryption today by a brute force attack (a method who the hacker tries out all combinations that are possible) can take up to 7.5 million years. [185]

Encryption today is divided into two main parts. The so-called “symmetric encryption” and the “asymmetric encryption”. These have the same principle in encrypting the message with a key, but the accessibility of the key is handled differently.

3.5.1.1. Symmetric encryption

The encryption in the symmetric part works with an encryption key which is used to encrypt the message (plain text). Because of the encryption by the key, the text is now encrypted and for people who don’t have the key to decrypt it is illegible (cypher text). To decrypt the message from the cypher text the receiver uses the same key as the sender. The problem is: How does the sender send this key to the receiver without any risk of detection?

[183] https://www.rapid7.com/blog/post/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor/ (last accessed 25.01.2022)
[184] https://www.wu.ac.at/fileadmin/wu/o/evoting/Folien/LLM2013_02.pdf (last accessed10.12.2021)
[185] https://www.password-depot.de/know-how/brute-force-angriffe.htm (last accessed 13.12.2021)

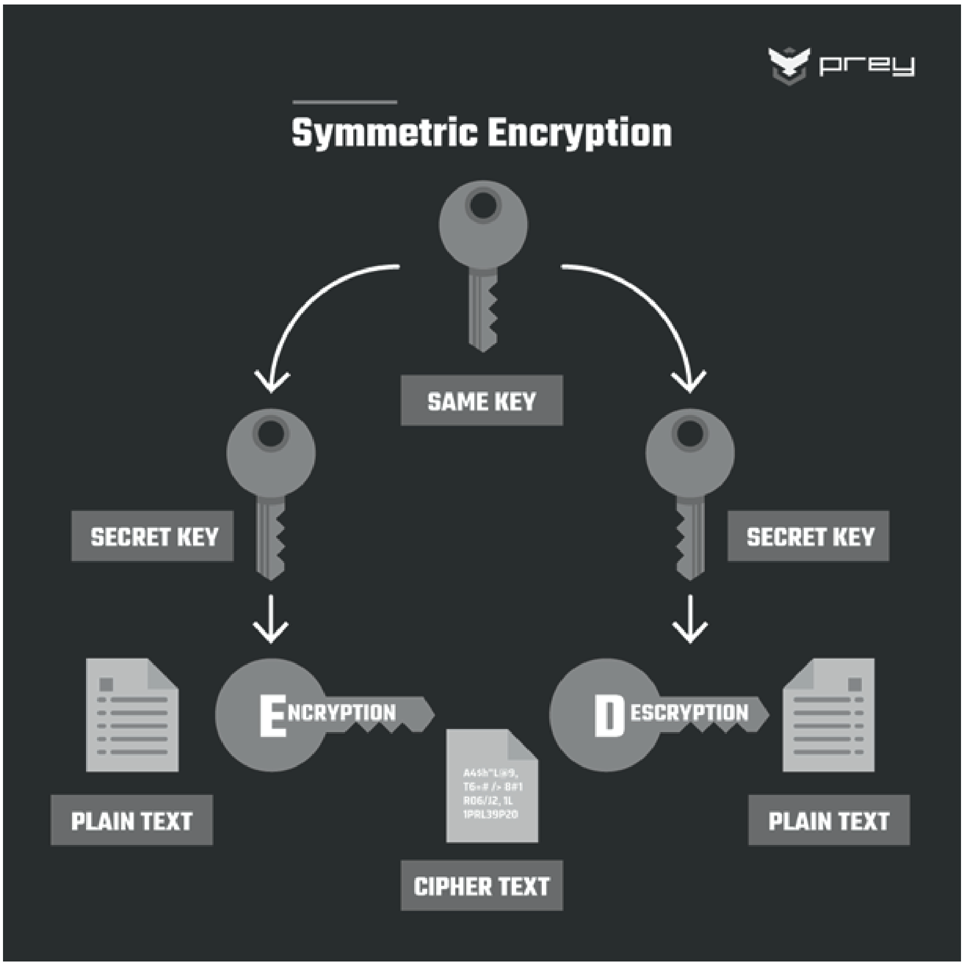


Figure 37: Symmetric encryption[186]

This is the only weakness of symmetric encryption. Some encryption programs solve the issue by assigning the two users that are communicating the keyway before the message is sent. Some others do it in an analog way by saving the key on an e.g., USB drive and deleting the key after the key file is implemented in the receiver's program.

In the following encryption method, this problem is non-existent because the keys to encrypt and decrypt are not the same.

3.5.1.2. Asymmetric encryption

The encryption in the asymmetric part works with a public encryption key which is used to encrypt the message (plain text). This key can be shared with anyone. It is, as its name says, accessible by the public. Because of the encryption by the key, the text is now encrypted and for people who don't have the key to decrypt it is illegible (cypher text). To decrypt the message from the cypher text the receiver uses a private key that only the receiver knows and owns. Only with that key, the message can be decrypted. From public key can't be inferred to the public key in any way. Now the receiver has the message with no risk that the private key is reviled in the transaction.

[186] https://preyproject.com/uploads/2020/09/rrss_01.png?resize=1024%2C1024&ssl=1 (last accessed 14.01.2022)

This method is today the mainly used one, because of its high standard of security.

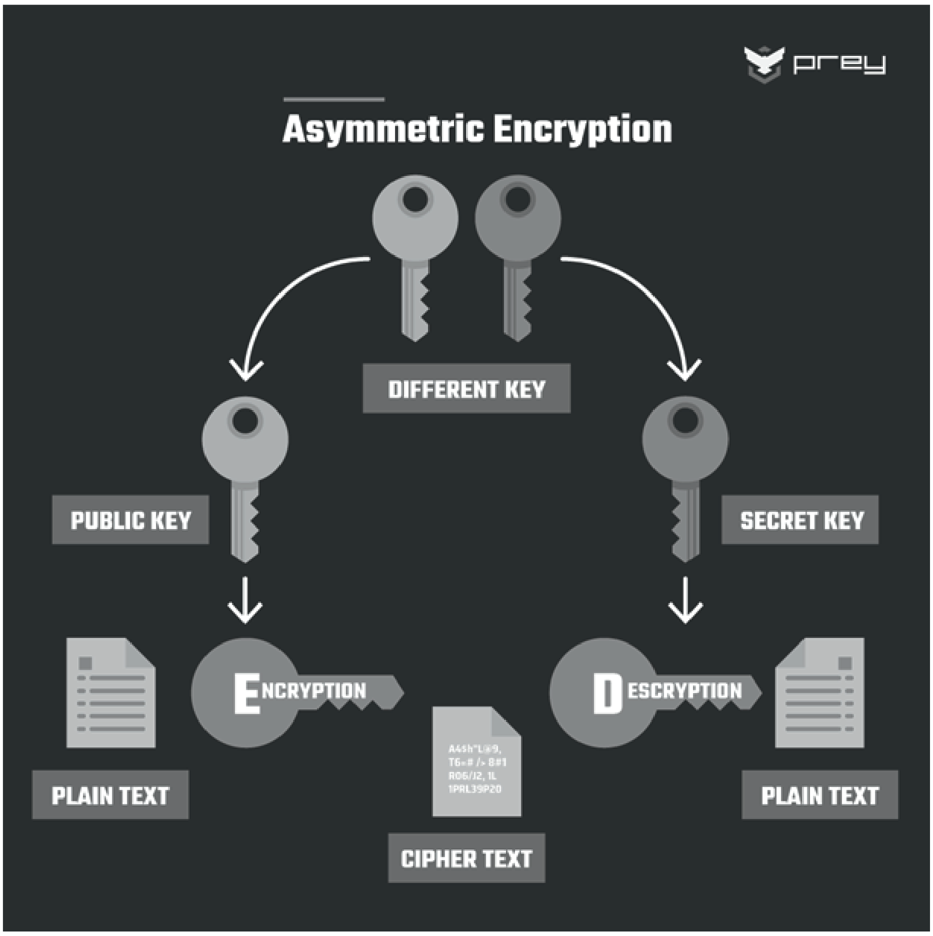


Figure 38: Asymmetric encryption[187]

3.5.2. Circumventing censorship by VPN

First of all, we need to determine what censorship is about. Censorship is an act of controlling or hiding a piece of information.[188] The topic of censorship is divided into two parts.

On the one hand, the pre-censorship is an occurrence of the publication mostly by media (books, movies, etc.) where the media is controlled by a governmental office. The governmental office decides whether there has to be a modification or the media is ready to publish it. This part of censorship is in Germany written in the constitution in Article 5.[189]

On the other hand, post-censorship is a mechanism that controls after the information is published. Everybody can have a free opinion but if it violates a law the person who breaks the law can be punished.[190]

[187] https://preyproject.com/uploads/2020/09/rrss_02.png?resize=1024%2C1024&ssl=1 (last accessed 14.01.2022)
[188] https://www.collinsdictionary.com/de/worterbuch/englisch/censorship (last accessed 23.11.2021)
[189] https://www.dwds.de/wb/Vorzensur (last accessed 10.12.2021)
[190] https://www.researchgate.net/publication/348871122_Wiemker-Dalg_-_Censorship (last accessed 10.12.2021)

The lack of uncensored information is perceived as a problem by the majority of the people, so they solve it by circumventing censorship.

The most common way to bypass censorship today is probably the VPN (virtual private network). A VPN is a technical application that disguises the data from the computer that the person uses by encrypting it and builds on that way a protected network connection. Mainly this function is a way to make it for third parties difficult to follow or to nab the data from the person's computer.[191]

The technical part of the VPN works as in the next paragraphs explained:

"A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data. This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless."[192]

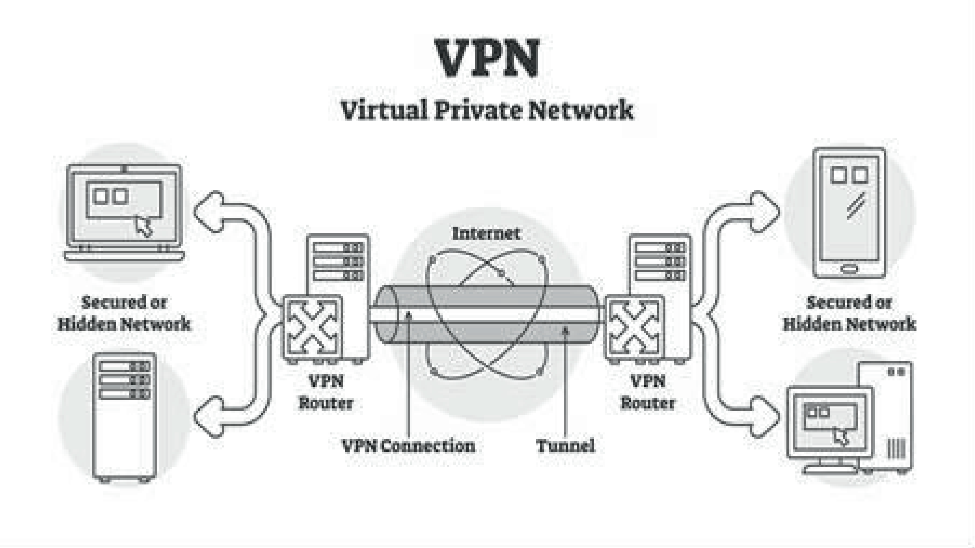


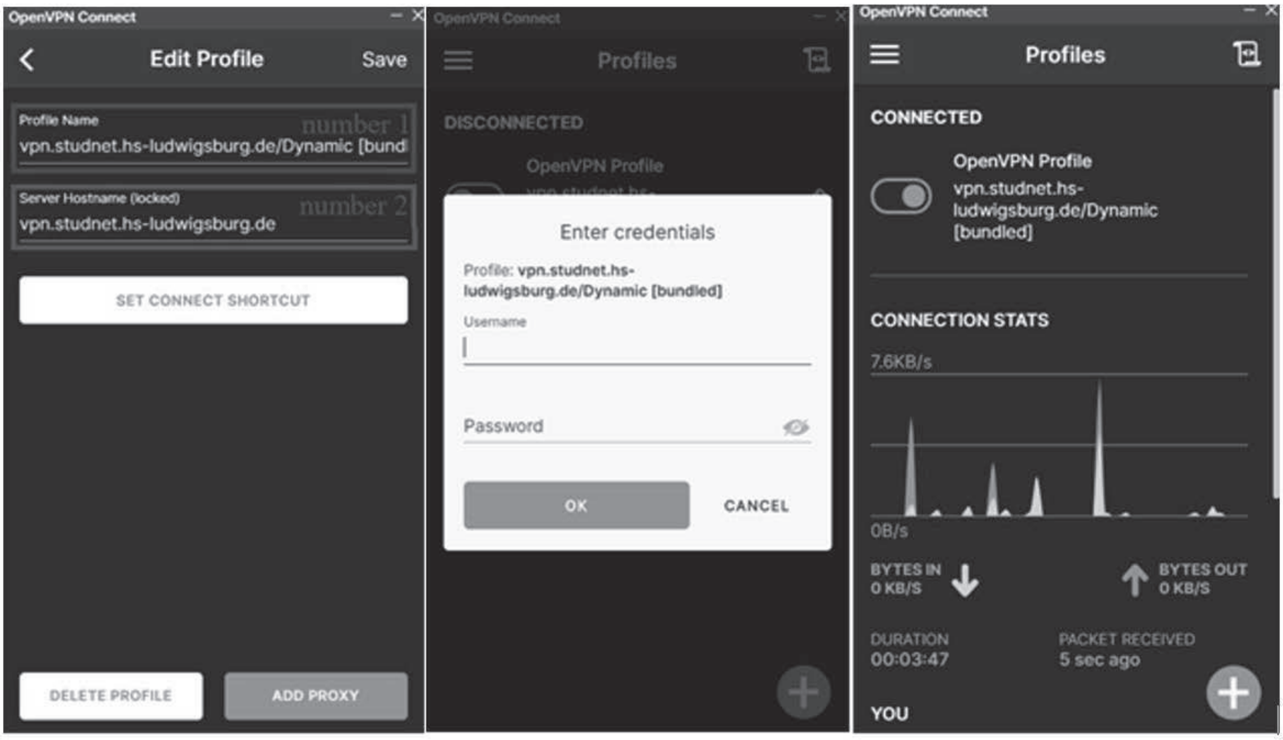
Figure 39: Virtual Private Network[193]

To prove its simplicity and usefulness, the following paragraphs describe how to connect to a VPN and one example of its value. The example is from the HVF Ludwigsburg and details the connection to the school's online library database.

The advantages of using the library database are the free access to a variety of academic/scientific sources and other types of literature. The first step is to download a VPN client, called 'OpenVPN'. In a browser of your choice search "OpenVPN", go to their website and download the VPN Client.

[191] https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn (last accessed 08.11.2021)
[192] https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn (last accessed 17.11.2021)
[193] https://10rgcev9tbx3hzifb27uulgw-wpengine.netdna-ssl.com/wp-content/uploads/2021/06/VPN-in-Online-Casinos.jpg (last accessed 14.01.2022)

When the download is completed, you open the OpenVPN and go to profiles to set up the connection to your university. As you see in the following picture below, only 2 fields have to be filled in: the name you assign to the connection (nr. 1) and the server-hostname (nr. 2).



Profile Name: vpn.studnet.hs-ludwigsburg.de/Dynamic [bund

Server Hostname (locked): vpn.studnet.hs-ludwigsburg.de

Enter credentials

Profile: vpn.studnet.hs-ludwigsburg.de/Dynamic [bundled]

Username

Password

OpenVPN Profile vpn.studnet.hs-ludwigsburg.de/Dynamic [bundled]

7.6KB/s

0B/s

BYTES IN 0 KB/S

BYTES OUT 0 KB/S

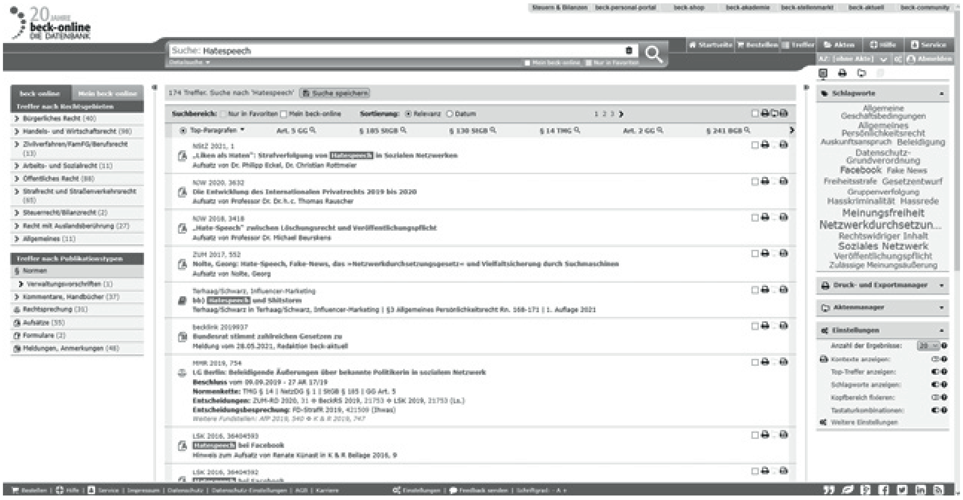
DURATION 00:03:47

PACKET RECEIVED 5 sec ago

Figure 40: Own recordings from the OpenVPN Connect

Following this step, you can save the connection and proceed to connect, as presented above. When pressing “Connect”, your client computer establishes a safe and encrypted TLS/SSL connection based on the public key of the server hs-ludwigsburg.de. The public key is a part of the asymmetric encryption used. It establishes an asymmetrically encrypted safe tunnel between the client (you) and the server (hs-ludwigsburg.de). All the work you must now do is to enter your username and your password to identify that you are a student or a teacher of the HVF and then you are connected to the university via an encrypted and safe VPN connection. Now you can use e.g., Beck Online with many features, that would otherwise be costly if not for the VPN connection.[194]

[194] https://www.hs-ludwigsburg.de/fileadmin/Seitendateien/einrichtungen/bibliothek/Dateien/OpenVPN_Stud.pdf (last accessed 20.12.2021)



Suche: Hatespeech

174 Treffer. Suche nach 'Hatespeech'

Treffer nach Rechtsgebieten
- Bürgerliches Recht (40)
- Handels- und Wirtschaftsrecht (98)
- Zivilverfahren/FamFG/Berufsrecht (13)
- Arbeits- und Sozialrecht (11)
- Öffentliches Recht (88)
- Strafrecht und Straßenverkehrsrecht (65)
- Steuerrecht/Bilanzrecht (2)
- Recht mit Auslandsberührung (27)
- Allgemeines (11)

Treffer nach Publikationstypen
- Normen
- Verwaltungsvorschriften (1)
- Kommentare, Handbücher (37)
- Rechtsprechung (31)
- Aufsätze (55)
- Formulare (2)
- Meldungen, Anmerkungen (48)

Suchbereich: □ Nur in Favoriten □ Mein beck-online Sortierung: ● Relevanz ○ Datum 1 2 3

● Top-Paragrafen Art. 5 GG § 185 StGB § 130 StGB § 14 TMG Art. 2 GG § 241 BGB

NStZ 2021, 1
„Liken als Haten": Strafverfolgung von Hatespeech in Sozialen Netzwerken
Aufsatz von Dr. Philipp Eckel, Dr. Christian Rottmeier

NJW 2020, 3632
Die Entwicklung des Internationalen Privatrechts 2019 bis 2020
Aufsatz von Professor Dr. Dr.h.c. Thomas Rauscher

NJW 2018, 3418
„Hate-Speech" zwischen Löschungsrecht und Veröffentlichungspflicht
Aufsatz von Professor Dr. Michael Beurskens

ZUM 2017, 552
Nolte, Georg: Hate-Speech, Fake-News, das »Netzwerkdurchsetzungsgesetz« und Vielfaltsicherung durch Suchmaschinen
Aufsatz von Nolte, Georg

Terhaag/Schwarz, Influencer-Marketing
bb) Hatespeech und Shitstorm
Terhaag/Schwarz in Terhaag/Schwarz, Influencer-Marketing | §3 Allgemeines Persönlichkeitsrecht Rn. 168-171 | 1. Auflage 2021

becklink 2019937
Bundesrat stimmt zahlreichen Gesetzen zu
Meldung vom 28.05.2021, Redaktion beck-aktuell

MMR 2019, 754
LG Berlin: Beleidigende Äußerungen über bekannte Politikerin in sozialem Netzwerk
Beschluss vom 09.09.2019 - 27 AR 17/19
Normenkette: TMG § 14 I NetzDG § 1 I StGB § 185 I GG Art. 5
Entscheidungen: ZUM-RD 2020, 31 ◆ BeckRS 2019, 21753 ◆ LSK 2019, 21753 (Ls.)
Entscheidungsbesprechung: FD-StrafR 2019, 421509 (Ihwas)
Weitere Fundstellen: AfP 2019, 540 ◆ K & R 2019, 747

LSK 2016, 36404593
Hatespeech bei Facebook
Hinweis zum Aufsatz von Renate Künast in K & R Beilage 2016, 9

LSK 2016, 36404592
Hatespeech bei Facebook

Schlagworte: Allgemeine Geschäftsbedingungen, Allgemeines Persönlichkeitsrecht, Auskunftsanspruch, Beleidigung, Datenschutz-Grundverordnung, Facebook, Fake News, Freiheitsstrafe, Gesetzentwurf, Gruppenverfolgung, Hasskriminalität, Hassrede, Meinungsfreiheit, Netzwerkdurchsetzun..., Rechtswidriger Inhalt, Soziales Netzwerk, Veröffentlichungspflicht, Zulässige Meinungsäußerung

Einstellungen:
Anzahl der Ergebnisse: 20
Kontexte anzeigen:
Top-Treffer anzeigen:
Schlagworte anzeigen:
Kopfbereich fixieren:
Tastaturkombinationen:
Weitere Einstellungen

Figure 41: Beck Online via VPN[195]

The advantages of using a VPN are diverse. To only name a few:

- Inaccessible data traffic
- Your VPN connection disguises and encrypts all data
- Secure connection
- The encryption of your VPN (depending on how reputable it is) can only be cracked with an encryption key. Without the key, it would take millions or billions of years.
- Disguise of your location
- Source of your data is after using a VPN the VPN-Servers so the location of the VPN is the only visible thing. All data that is transferred after this server is disguised so no one can trace it back to your location. And the IP address with which you access Facebook and post some hate speech is the one of the VPN – so authorities cannot catch you as long as the VPN provider does not deliver you to them.
- Access to regional content
- The source of your data is the location of your VPN, therefore you have access to the data in the region of your VPN server. Some VPN hosts offer the service of choosing the location of your VPN operations. This is called VPN-location-spoofing. A great example of the usage of this feature is Netflix accessibility in different regions. More series and films are available on Netflix in the USA than in Germany and the users circumvent it with a VPN.
- Secure data transfer
- The data that is transferred is safe from manipulation or spying. Most of the bigger companies use VPNs to transfer data between facilities.

[195] https://beck-online.beck.de/Search?pagenr=1&words=Hatespeech&st=&searchid= (last accessed 19.12.2021)

The only disadvantages are the minimal slower speed of your internet and the fact that you must trust the VPN host. If the VPN host is corrupted by the government or hijacked from a hacker attack this connection can be traced back to your position.

Besides that, the service (Chinese internet, Amazon, …) that you use can find out that you are using a VPN but not the exact data. Some governments that control the internet (e.g., China) can block the usage of a VPN via black lists. But they can’t block every usage of VPNs because most of the companies also use VPNs for communication. Therefore it would have a significant negative economic impact on the country.[196]

3.5.3. Government and VPN

If a government is confronted with VPN users, it has the following options to deal with the situation:

First of all, the government has to simply accept the usage of the VPN. This is the simplest solution and overall, the preferred one. This is the opinion of the majority of the internet community and civil society. It also is an issue in the business world because the VPN is also used to communicate and deliver confidential business information between branches.

The second option is to prohibit the usage of VPN by its citizens (and all other users worldwide using VPN) either by blocking all the VPN traffic with a negative/black list of server-IP-addresses from the VPN servers or by enabling access to social media, blogs and governmental sites only when the user is listed on a positive/white list (like publishing companies open their journals and repositories to users from listed university IP addresses only).

Using positive/white list would dramatically reduce the traffic on the respective websites, turning the effective traffic to zero in the worst case. If e.g., a newspaper with a forum only accepts postings from specific white-listed servers, its dissemination will likely diminish.

Note that the basic and underlying technology of a VPN, namely a Public Key Infrastructure with private and public keys and establishing a symmetrically encrypted VPN-tunnel is exactly the same technology, which is used in online banking, webmail services and many other services on the internet. So, prohibiting or abolishing this technology or the demands of digitally illiterate politicians “all cryptographic keys must be accessible to the government” would de facto disable any safe application on the internet and for example, open your online banking account to the government.

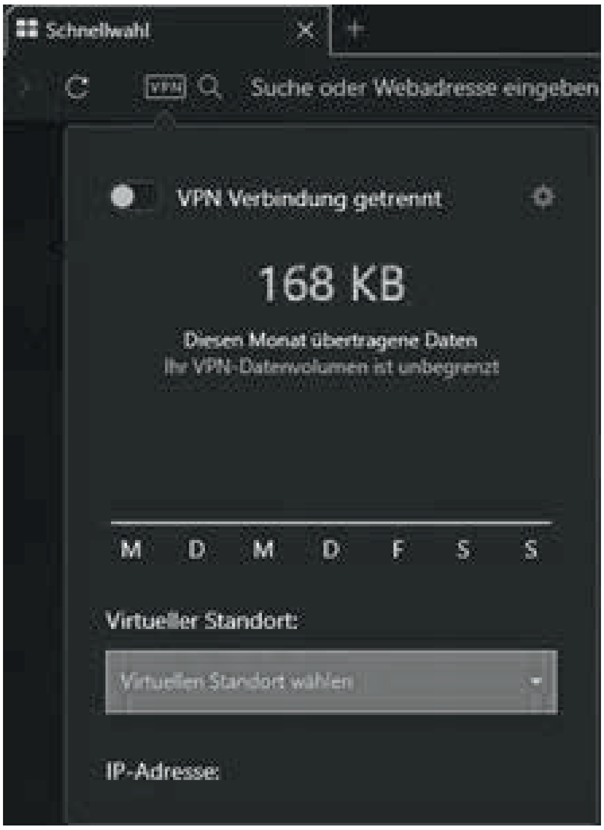
Using a black list is very inefficient because there are many providers that can offer easy access to the VPN servers.[197] There are also numerous browsers that provide a VPN function, e.g., Mozilla Firefox or Opera, either as an addon or build-in in the main browser (as shown in the picture below).

[196] https://www.dw.com/de/zensur-mit-vpn-umgehen-ist-das-überhaupt-sicher/a-56816688 (last accessed 17.11.2021)

[197] https://www.heise.de/download/specials/Anonym-surfen-mit-VPN-Die-besten-VPN-Anbieter-im-Vergleich-3798036 (last accessed 07.12.2021)

Mozilla VPN
Sicher, schnell und zuverlässig – auf jedem Gerät, egal wo du bist.
Ein Virtuelles Privates Netzwerk von den Machern von Firefox.
Jetzt Mozilla VPN nutzen
30 Tage Geld-zurück-Garantie *

Figure 42: Mozilla Firefox VPN[198]



VPN Verbindung getrennt

168 KB

Diesen Monat übertragene Daten
Ihr VPN-Datenvolumen ist unbegrenzt

Virtueller Standort:

Virtuellen Standort wählen

IP-Adresse:

Figure 43: Own recordings from Opera GX

3.5.4. Data protection

This chapter will explain the role of data protection for VPNs. First of all, what is the meaning of “data protection”?

[198] https://www.mozilla.org/de/products/vpn/ (last accessed 05.12.2021)

“It is the protection of the individual against impairments of his rights to informal self-determination, under which every citizen can in principle determine himself about the disclosure and use of his personal data. (BVerfGE 65, 1)”.[199]

This protection is on the legislative side granted in Europe because of the General Data Protection Regulation (GDPR). It regulates what personal data can be collected and processed. The scope of this regulation are organisations with the company headquarters in the EU and all organisations worldwide that process the personal data of EU citizens.[200]

The usage of a VPN is sometimes related to the lack of speech freedom. Often people in suppressed countries use VPNs or TOR (see next chapter) to communicate freely because otherwise, they face punishment. One example is a VPN provider in China, that was put in jail recently (December 2017) for five and a half years, just for providing users with a connection to the rest of the world.[201]

It is also a way to communicate freely without the risk of surveillance, which motivates people to use this communication channel. Such cases can be illustrated by whistleblowers such as Edward Snowden or Silver Meikar.[202]

3.5.4.1. Key escrow

Another approach to “controlling” the internet is a system called key escrow. It is also known as a “fair” cryptosystem. The mechanism behind this name is a simple agreement with a third party to store the keys that are used to decrypt the data. The keys stored by third parties can only be accessed by authorized persons or groups inside a business (e.g. head of the security) or in some cases the government itself. Note that the keys affected would also include keys for online banking and other very sensitive applications, therefore enabling a third party to trade your securities on the stock exchange, pretending to be you.

One of the downsides of key escrows is on the structural side. How is access granted only to authorised users? No system has been designed yet to overcome this challenge, mainly because the danger of abuse is very high. Many negative implications also arise from the use of this system on a national level. Many people don’t trust the government or have concerns regarding keys’ safety ensured by the government from a security perspective (e.g., hacker attacks).[203] Implementation of the system at the national level poses many struggles, one of the latest examples being France.[204]

3.5.4.2. NIS directive

The Network and Information Security Directive (NIS directive) is a part of the European cybersecurity strategy. The goal of this directive is to strengthen EU-wide cybersecurity. The main instrument is the enhancement of cooperation on more layers. This fits the timeline o the enforcement of EU cybersecurity: Regulation on establishing ENISA in 2004, EU Cybersecurity Strategy in 2013, the new

[199] https://wirtschaftslexikon.gabler.de/definition/datenschutz-28043 (last accessed 27.12.2021)

[200] https://www.atinternet.com/de/glossar/gdpr/ (last accessed 27.12.2021)

[201] https://www.heise.de/newsticker/meldung/Urteil-gegen-VPN-Dienst-Chinese-muss-fuenfeinhalb-Jahre-in-Haft-3926954.html (last accessed 03.01.2022)

[202] https://news.err.ee/104712/whistleblower-and-pm-put-scandal-in-perspective (last accessed 07.01.2022)

[203] https://jumpcloud.com/blog/key-escrow (last accessed 07.01.2022)

[204] https://www.icommercecentral.com/open-access/france-struggles-to-implement-worlds-first-trusted-third-party-infrastructure-with-key-escrow.php?aid=38879& (last accessed 07.01.2022)

regulation on ENISA in 2013, the NIS directive in 2016, and the Cybersecurity Act in 2019 [3-8, p. 84]. As a European Union directive, it has to be transferred into national law in all member states.

The NIS directive can be separated into three parts. These include the national capabilities, the cross-border collaboration and the national supervision of the critical sectors. National capabilities are cybersecurity capabilities of the individual countries, such as computer security incident response team (CSIRT), performing cyber exercises, etc. National supervision of critical sectors refers to the protection and supervision of the critical infrastructure cybersecurity, such as water, healthcare, energy, finances, and digital service providers, like online marketplaces or clouds.[205] It also refers to the Public Key Infrastructure and effectively hinders key escrow.[206]

3.5.5. A stronger alternative to VPNs: TOR

TOR is an abbreviation that stands for "The Onion Routing". This might seem a hilarious name, but if one understands the system and the procedures behind it, the name makes perfect sense.

Figure 44: TOR logo[207]

The origins of TOR are traced back to a project started by the US Navy. The network was developed for the US Navy and other military organisations to communicate online anonymously. It became popular because the project was public, to allow volunteers to work on it. Many users are choosing this browser nowadays because it is safe and has many functions that allow people to act without fear of being traced back or spied out.[208]

3.5.5.1. The technical structure of the TOR-browser

TOR provides safe operations because not even the browser knows your identity. The TOR browser builds tree "tunnels" to the destination. Instead of tunnels, these connections are like onion layers that are protecting and pile each other. That's why is called "The Onion Routing". These onion layers are not interconnected and no layer knows the destination and the identity of the user at the same time. Due to this structure, the TOR browser is secure - the internet cannot collect data if there is no data to collect. This type of procedure is called "privacy by design".[209]

[205] https://www.enisa.europa.eu/topics/nis-directive (last accessed 08.01.2022)
[206] https://digital-strategy.ec.europa.eu/en/policies/nis-directive (last accessed 25.01.2022)
[207] https://www.torproject.org/static/images/tor-project-logo-onions.png (last accessed 20.12.2021)
[208] https://vpnoverview.com/privacy/anonymous-browsing/tor/ (last accessed 25.11.2021)
[209] https://www.dw.com/de/zensur-mit-vpn-umgehen-ist-das-überhaupt-sicher/a-56816688 (last accessed 17.11.2021)

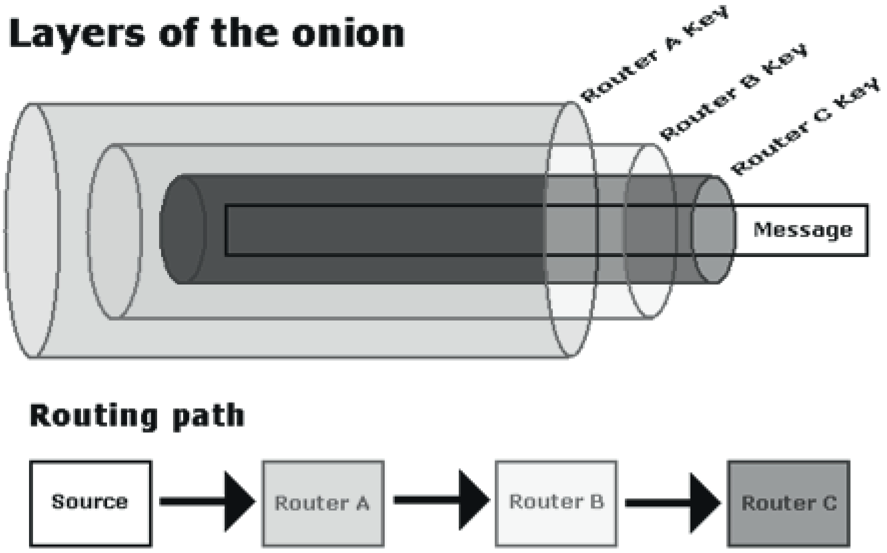


Figure 45: Onion routing[210]

As the picture below shows, the original data is encrypted and sent to a daisy chain of different servers. These encryptions are not edited but the encryption is added on top of the already existing encryption. Also, the servers that are used follow no strict pattern; they are randomly picked out. So, the users can surf and act anonymously. At the moment, this is the safest way to protect the identity of persons or to protect data.

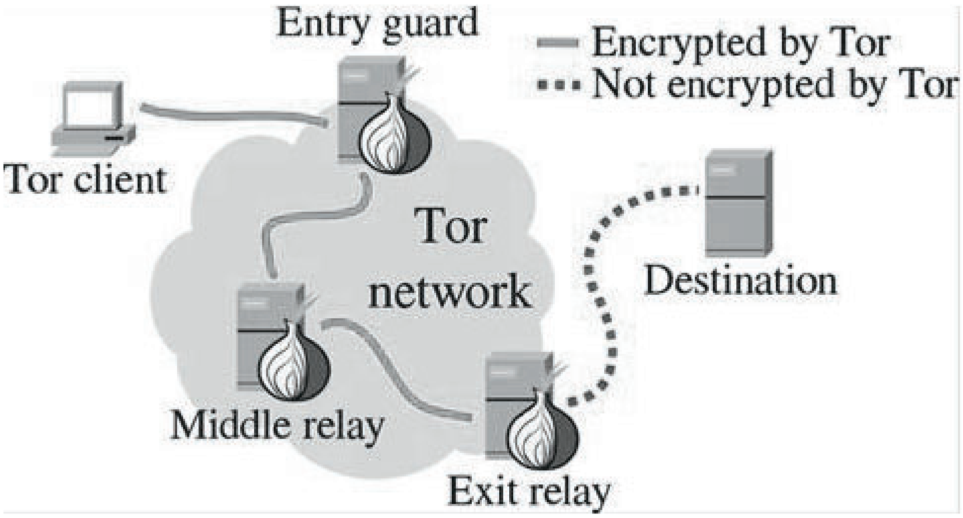


Figure 46. Onion routing (continued)[211]

The entry into TOR, namely the first TOR server or so-called entry guard can be any server whose administrator joins the TOR network. The government can of course blacklist such a server, but

[210] https://i3.moyens.net/de/images/2021/05/1621764758_981_Was-ist-Zwiebel-Routing-und-wie-koennen-Sie-Ihre-Privatsphaere-zurueckerhalten.png (last accessed 21.12.2021)
[211] https://br.atsit.in/de/wp-content/uploads/2021/06/download-tor-browser-fur-windows-mac-offline-installer.png (last accessed 21.12.2021)

millions of other servers could fill in. So, it is next to impossible to shut TOR down – and fully impossible for the government of a single state out of 194 states worldwide.

3.5.5.2. Advantages and disadvantages of TOR

The advantages of TOR are overwhelming and include:

- Inaccessible data traffic
    - TOR encrypts the data three times and covers its protection, so nobody can read the data except the addresses at the final destination.
- Secure connection
    - The way back to your final destination cannot be traced, because the existing encryption does not know your identity and the final destination simultaneously. Also, the brute-force attack to crack the encryptions used to secure the connection would take up billions of years.
- Disguise of your location
    - The source of your data when using TOR is the last used server of the TOR procedure, also known as the exit node, so the location of the TOR server is the only visible thing. All data that is transferred is disguised so no one can trace it back to your location. And the IP address you use to access Facebook and post hate speech is the address of the VPN – so authorities cannot catch you if you don’t make any mistakes.
- Access to regional content
    - The source of your data is the location of the last used TOR server TOR. So you have access to the data from the region of the TOR server, as well as websites and services, that can’t be found by regular browsers or search engines.
- Secure data transfer
    - The data that is transferred is safe from manipulation or spying because of the massive encryption.
- Absolute anonymity
    - Due to the encryption and the server structures, the identity of the person is protected, which benefits large groups of users.

TOR disadvantages are the slower speed of data connection, so streaming is possible at very low quality and the connection is more time-consuming, determined by the encryptions and the servers used. Another significant disadvantage is due to anonymity, which attracts many criminals. This is the consequence of making such a project public.[212]

[212] https://vpnoverview.com/privacy/anonymous-browsing/tor/ (last accessed 25.11.2021)

3.5.5.3. Users of TOR

The users of the TOR browser were originally the government agents and the military, employing it to communicate without fear of being intercepted or corrupted. But the user base has increased significantly. Today it is used by those who want to protect their confidentiality or profit from online anonymity, such as political activists, investigative journalists and whistle-blowers like Edward Snowden.

Another user group are the people in suppressed countries, where the authorities will punish you for certain opinions or online views. TOR allows them to communicate and enjoy more freedom because their statements cannot be traced back to a specific person. A third user group of TOR are individuals who bypass geo-restricted content or censorship and visit specific websites. TOR allows access to many web pages that are not visible for usual browsers because their addresses are not indexed by popular search engines Google or Bing.

Due to its anonymity, the browser also attracts criminals, that use it for communication, black markets trading illegal drugs and weapons and child porn. TOR browser is the only browser that lets you visit the dark web.[213]

3.6. Levels of the web

The *clear web* (also known as the *surface web*) is the section of the internet that can be publicly accessed from any browser. However, the other levels of the web, the so-called *deep web* and *dark web* are gaining more attention from the public. This chapter aims to deepen the understanding of these terms.

The differences between these levels of the web are determined by two attributes: indexing and encryption, which impact the transparency and visibility of the web and its content. The clear web is the visible part of the internet that gets indexed, meaning all search engines can scan these websites using crawlers and include the websites into a database of possible search results. The second characteristic, encryption is not usually found on the clear web, allowing users direct access. Some examples of the clear web are those accessible via search engines Google, Bing or online shops like Amazon. The ratio of the websites from the clear web to the whole internet is approximately 1 to 4%.[214]

Nowadays the borders of the clear internet and the deep web are fading. The deep web begins where websites are encrypted or not accessible via URL (free access hindered by means like mandatory logins, registration requirements, paywalls, etc.). So, when someone is buying from Amazon, to make the transfer via bank transactions on the online banking website, he transitions from the clear web (Amazon) to the deep web (bank websites). The deep web is mostly the source of the information about the clear web, accounting for cca. 90% of the websites, therefore without the deep web, the internet would be impossible. [215]

The deepest level of the web is the dark web or the darknet. The websites of the darknet are indexed and heavily encrypted, where URL is the first cryptographic key needed to decrypt the asymmetric encryption of a website. URLs don't include "http" or "https" or domain names like ".com"or ".org". Darknet accounts for cca. 6% of the total number of internet websites.[216]

[213] Ibid.

[214] https://techjury.net/blog/how-much-of-the-internet-is-the-dark-web/ (last accessed 30.01.2022)

[215] Ibid.

[216] https://www.anwalt.org/clear-web/ (last accessed 25.01.2022)

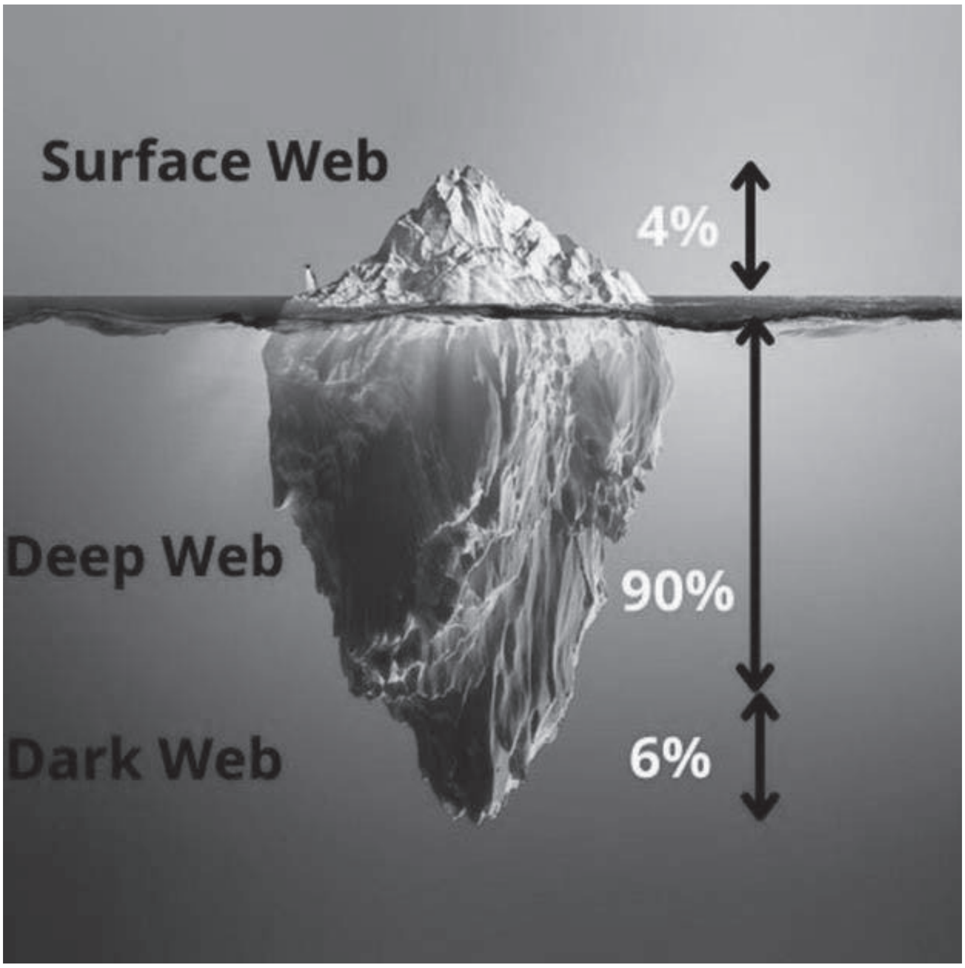


Figure 47: Web levels explained[217]

3.6.1. Domestic-only "Internet"

Most countries grant their subjects "free" use of the internet. "Free" in this case doesn't mean one can do anything on the internet, but rather the access to the internet is not restricted by the government or other groups of people. As usual, there are some exceptions, which will be exemplified in this chapter.

The first one is the Peoples' Republic of China, which runs a project called "The Great Firewall" or "Project Golden Shield". This project regulates the people's internet dramatically, with significant outcomes, like the limitation of information sources, blocking of internet tools like Google, Wikipedia, messengers, social networks (Meta (Facebook), Twitter, …) and mobile apps.[218] The censorship in China is implemented by modifying the search results and censoring the "wrong" opinions. Besides censorship, the PRC has influenced internet companies to provide the internal internet structure needed to diminish the effectiveness of other (foreign) companies.[219]

[217] https://postpear.com/wp-content/uploads/2021/06/Surface-Web-Deep-Web-Dark-Web-Internet-Explained.jpg (last accessed 24.01.2022)
[218] https://www.internetzensur.info/china/ (last accessed 30.01.2022)
[219] https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html (last accessed 30.01.2022)

The Chinese government has further plans to prohibit the usage of VPNs and TOR browser and make it punishable. In the recent past, a VPN provider received a five-year prison sentence.[220]

North Korea is another country with heavy network censorship established, resulting in a more restricted usage of the internet. Access to the internet, which is mostly used for governmental purposes, is only possible based on a special authorization.[221] These two countries are the biggest countries restricting access to the internet.[222]

3.6.2. Real name compulsory

Another approach to controlling the internet in some countries is the so-called real name compulsory system. Internet users are required to bind their virtual identity to their real one, using their legal name, including the government-issued e-ID.

The goal of this procedure is to prevent users from spreading false or denigrating information in internet forums, for example, because these people can then be identified and held accountable for their actions on the internet. But this procedure is only working when all internet providers require users to use their real name.[223]

There are various problems when it comes to real-name compulsory policy. First of all, at least in the CoE member states and the internet regime established there, it is easy to bypass this requirement via VPN. It means that even though a country may choose to enforce this policy, internet users can circumvent it by using a VPN server located in another country. Second of all, a vast majority is not using e-IDs provided by the government. Therefore, the Spiegel website, which only allows articles to be read by users with real names, would experience a huge decrease, by over 60% of their web traffic.[224] The consequences of such actions would be a significant decline in the company sales, eventually leading to its insolvency.

In conclusion, the real-name policy is not a viable approach to controlling the internet, at least not yet and not if enforced by only a small group of countries.

3.7. Social Media

Social media are mostly provided by big profit-oriented businesses, listed on the New York Stock Exchange, such as Meta Inc. or Twitter Inc. Social media provided by non-private entities are the rare exception, which raises the question of the business models behind them.

3.7.1. Business models and features

Social media business models vary greatly, all sharing the same end goal of gathering more traffic.

[220] https://vpntester.org/blog/china-statuiert-exempel-5-jahre-haft-geldstrafe-fuer-vpn-betreiber/ (last accessed 22.01.2022)
[221] https://www.bbc.com/news/world-asia-37426725 (last accessed 22.01.2022)
[222] https://www.wired.com/1997/06/china-3/ (last accessed 22.01.2022)
[223] https://www.golem.de/news/login-dienste-wer-von-der-klarnamenpflicht-profitieren-koennte-2002-146687.html (last accessed 29.01.2022)
[224] https://de.statista.com/statistik/daten/studie/777662/umfrage/nutzung-der-online-ausweisfunktion-des-npa-in-deutschland/ (last accessed 29.01.2022)

The “freemium model” offers several basic services for free and users need to upgarade to access other services. The providers have to figure out exactly how many services can be free so that the users are willing to upgrade, otherwise, the users may decide against it and only use the free services.

In the “affiliate model” a business makes money by guiding users to generate leads or sales on the websites of other affiliated companies. Nowadays many businesses rely on affiliated websites, to increase traffic to their websites and sell their products. Upon purchase or participation of users, the affiliated business receives a share of the transaction.

A “subscription model” requires users to pay a monthly or annual fee to access a product or service. It is common for monthly membership websites to have a high attrition rate because many users forget about the site after their first or second login and never visit it. Therefore, owners of such websites should make consistent efforts in keeping the site interesting and up-to-date.

“Virtual goods model” is another business model, where users pay for virtual goods like upgrades, points, or gifts on a website or a game. Three main categories of goods include functional, decorative and status items. The owners of such websites have to produce things that users want and need and that are relevant to the community, in order to be able to sell them.

The “advertising model” means the operator of a website sells advertisements, based on their internet traffic. The higher the traffic, the higher are the advertising charges. Therefore, users can still use the website for free while the operator can monetize it through advertising.[225]

There are also publishing and planning tools, which enable users to garner more attention for their content, especially if they post it at certain times when the engagement rate is higher. These tools are based on analytical features, that determine the peak engagement rates, most visited content items, competitors' activity levels etc. Based on such analyses, the users acquire more views, sell their products or have higher chances of becoming influencers.[226]

Besides the business model, a social media platform has to be appealing for the users. Hence it needs to have some essential features.

- *Simple and friendly user interface* – incorporating different elements, such as the content and media layout, input controls, navigation etc. user interface has to be simple and easy to navigate, regardless of the target audience.

- *Versatile and responsive* - user interface has to adapt and be responsive to different devices (smartphone, iPad or notebook) and screen sizes, without any loss of functionality or quality.

- *Visually appealing and accessible design* - the design elements have to be consistent and well-organized, so they don’t create sensory overload and are accessible to everyone, the fonts and colour schemes are carefully chosen to promote a cohesive and pleasant user experience.

- *Secure login* - social media platform should deliver safe procedures for a unique user account with personal login settings and identification methods, such as backup email or code authentication, to prevent malware attacks or identity theft. Users must have a choice of what

[225] https://mashable.com/archive/social-media-business-models (last accessed 17.12.2021)
[226] https://sproutsocial.com/insights/best-times-to-post-on-social-media/ (last accessed 17.12.2021)

personal information they are willing to share and make publicly available (name, contact information, location, occupation, etc).

- *Networking elements* – one of the most sought-after features, allowing users to create personal or professional networks of their choice, which may consist of friends, family, colleagues or people with similar interests. The app should allow users to add other accounts into their networks and follow each other.

- *Content sharing* is one of the best social media app features because it enhances communication between people and strengthens the feeling of connection. Content sharing may include posting and sending photos or videos and the possibility to comment on what other users are sharing.

- *Public and private messaging* is a very valuable feature, enabling an easier and cheaper communication channel with other people (group chats, video calls), as compared to long-distance calls or expensive text messages. Assuming the user is connected to a WiFi network, messaging will not affect the data plans.

- *The open forum* offered by social media platforms allows users to voice their opinions, rally together for a cause, or even discuss their hobbies, with like-minded individuals.

- *Real-time notification and an activity feed* keep people up-to-date and informed, therefore being an essential feature of social media.

- *Privacy settings* should be an essential feature of any social media platform. Users should be able to determine who can see their profiles, what personal information is shared and have the ability to opt-out of certain marketing tactics, like tracking inline browsing or shopping experiences.

These are the most important features of any social media platform, enabling them to gain users.[227]

3.7.2. Algorithms

Algorithms are usually defined as sets of rules or instructions focused on solving a problem or fulfilling a task. Algorithms are not inherent to the digital world, a recipe is also an algorithm, as it has instructions on how to perform the task of making a meal. Digital devices like computers or smartphones need algorithms to execute the functions of various hardware or software-based routines.[228]

Algorithms are essential for social media. But how do they work? Most social media providers consider their algorithms a business secret and it's often not known how exactly they work, because the algorithm is subsequently not published. They influence our use of the Internet and, especially our use of social media. The content shown on the internet depends on algorithms, which are run when the respective website is accessed. For instance, the shown content may depend on the browser version or the language setting of the individual user accessing the website with his device. To a certain extent, algorithms work similarly to a strong filter. Only a small part of all available information will be presented to the individual user, therefore influencing users' perceptions or opinions. Moreover, they are not transparent (only the creator and distributor of the software know

[227] https://www.koombea.com/blog/10-top-features-of-social-media-apps/ (last accessed 20.01.2022)
[228] https://www.investopedia.com/terms/a/algorithm.asp (last accessed 30.01.2022)

exactly how they function) and most of them are hidden, i.e. the source code is not published; hence it is unknown where they are used and how they influence the usage of the Internet.

Algorithms have a significant impact on social media. For instance, the algorithm decides what posts are shown on the front page, as they are considered more interesting and relevant for the user. This decision is based on certain statistics: how often the user has hovered, read, liked, clicked, shared and commented. The more two users interact with each other, the more the algorithm interprets them as belonging to the same group and their respective content being of interest. It also means that the rest of the content is not visible to and from the user. Algorithms are also strongly influenced by the activity level: users have to be very active to be seen. Subsequently, the user needs to spend as much time as possible on social media platforms if he wants to be seen, shared, followed and liked.

When algorithms define content as relevant for each user, a single user runs the risk of being incased in a "bubble" of content a group of others wants to see. This is quite risky, if a user gathers information through social media because the algorithm does not care if the news is true or fake, the number of likes, shares or comments is relevant. As a result, an emotional or provoking comment can become much more popular than an objective article, even if is more interesting or important.[229] The users interact mainly with users which think alike and block users they do not like or disagree with. Like-minded users support each other and encourage each other's opinions about who they are or what they do, fortifying each other in their opinion or actions.[230] The algorithms have a great impact on these internet bubbles.

Censorship also contributes to enforcing these bubbles, because people get banned or their posts and comments get deleted, making them think it must be true and the government wants to hide it. This also drives the shift towards other platforms. When people who used Facebook and WhatsApp get banned they will shift to Signal or Telegram, where they can communicate directly with like-minded people.[231]

3.7.3. Censorship

To figure out how censorship works, we must understand how the internet works. The connection to the internet is always through an Internet Service Provider (ISP). This ISP allocates an IP address to every computer, which is similar to a postal address, identifying the person and transport information. Everyone who knows this IP address can figure the address authority country and even municipality. When the computer is used at an internet café or office, it is possible to event determine the building, office and the exact computer that is used. This information is often available to government agencies.

[229] https://webcare.plus/algorithmen-social-media/ (last accessed 06.12.2021)

[230] https://webcare.plus/zwischen-wohlfuehl-oase-und-meinungsvielfalt-in-den-sozialen-medien/ (last accessed 23.12.2021)

[231] https://www.dw.com/de/meinung-facebooks-querdenker-zensur-geht-zu-weit/a-59216883 (last accessed 10.01.2022)

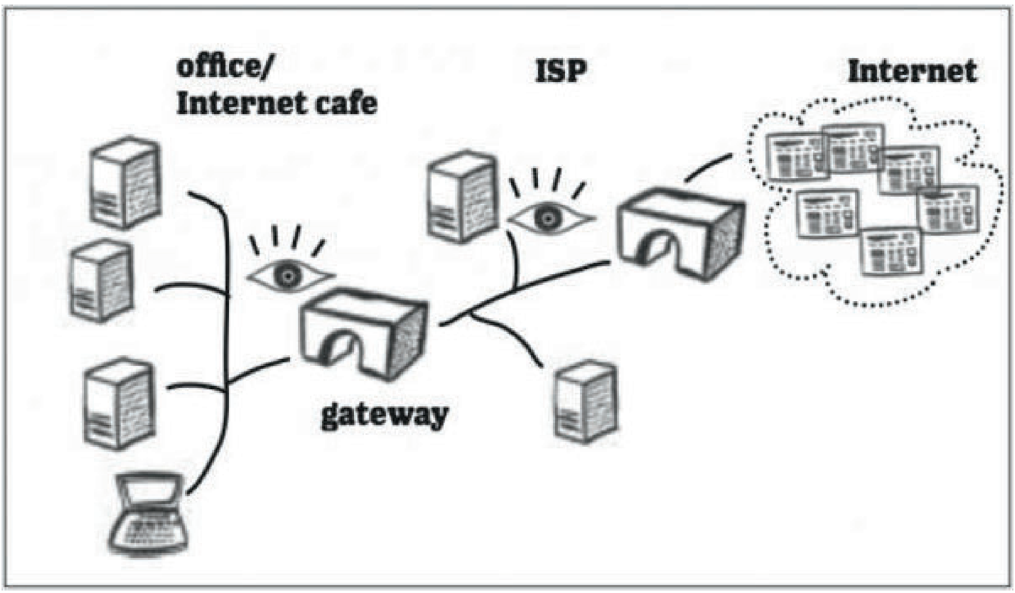


Figure 48: Internet connection[232]

However, not only computers have an IP address, websites also have them. To access a website, the IP address of the website can be entered in the address bar, not just the website address. Only, the IP addresses are convoluted and difficult to remember, so the Domain Name System (DNS) associates IP addresses with human-readable "domain names".

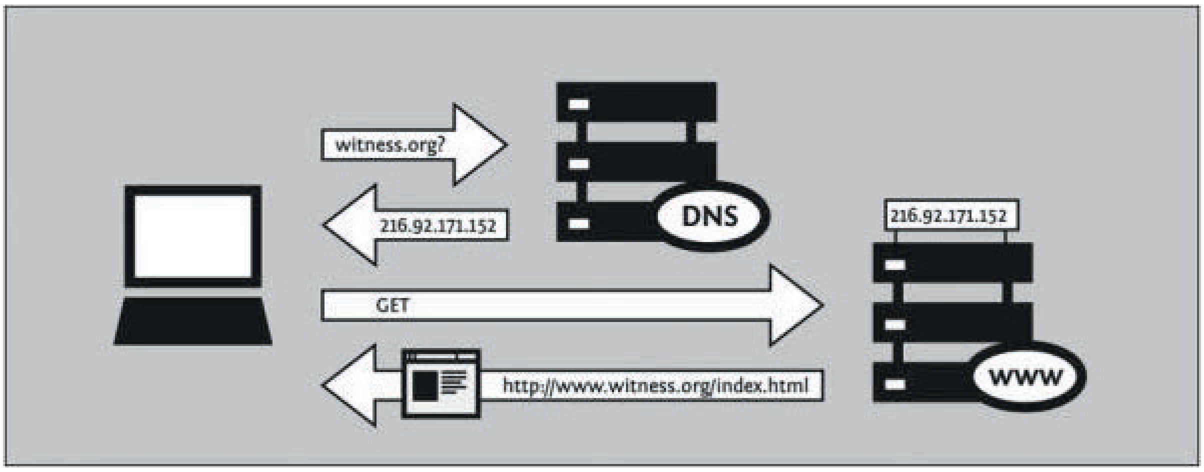


Figure 49: DNS[233]

To enable sending packets of information from server to server, the ISPs have to trust the established internet protocols on national and international infrastructure. This structure and conventions are normally referred to as the "backbone" of the internet. The backbone also consists of major network equipment installations that are interconnected via fiberoptic cables and satellites. Communication between internet users from different countries or even continents is enabled through these connections. Providers connect through routers, which are also known as gateways, which enable diverse networks to communicate with each other. But the gateways are also a point where the internet traffic can be monitored or even controlled.

[232] https://townsendcenter.berkeley.edu/blog/internet-censorship-part-1-technology-working-web (last accessed 04.01.2022)
[233] Ibid.

These complex processes are not seen by the average internet user. The understanding of these processes is necessary because they underline censorship on the internet. There are different types of censorship, that can be enforced at different levels of internet architecture.[234]

Censorship can be performed via different methods, such as DNS tampering or IP blocking. DNS tampering is one of the most common technologies, that can be used in countries where authorities control domain name servers. Officials can “deregister” the DNS to the censored content and these websites become invisible to the users because the DNS tampering will prevent the translation of domain names to website IP addresses.

IP blocking is enforced where governments have control over internet service providers, blacklisting specific IP addresses. When a user wants to access a certain website, the request is monitored by surveillance computers, that check the request with the blacklisted IP addresses. If the website is backlisted, the ISP will cancel the connection. This technology is frequently used in China, where international-gateway servers control the flow of internet information in and out of the country through mega-servers.

While IP blocking allows the government to block certain blacklisted websites, there are billions of websites with new ones created every second, making it impossible to keep updated blacklists. Keyword filtering could be a more powerful tool, it scans the Uniform Resource Locator (URL) string for keywords. If one of the forbidden words like “fascist” is encountered in the URL, the connection is cut. This also means that www.antifacist-initiative.org would subsequently be cut.

One of the newest and most sophisticated internet censorship techniques is packet filtering, meaning the actual contents of each page are scanned. Data sent via the internet is grouped in small units – packets - that are passed from one computer to another via routers. While IP address filtering only blocks websites based on where packets are going to or coming from, the packet filtering also inspects the content for banned keywords. If a forbidden keyword occurs in a packet, the connection is cut. The user may get an error message, without indicating he or she just got censored. It is important to note that packet filtering does not work when the content of the communication between the user and the website is encrypted – like in every online-banking session, which is encrypted via TLS/SSL.

Besides these wide-ranging internet censorship techniques, others like traffic shaping may be used. This is often used by governments or corporations, by delaying access to certain websites and simulating a slow-loading or unreliable website. A commonly used technique among companies is to blacklist individual port numbers, like Web or email, thus regulating certain employee behaviours, such as instant messaging.

Internet censorship is often disguised as a technical error or connection problem; therefore making it difficult to identify as censorship, which technology is used or who is blocking the website. This also makes it difficult to prevent censorship, but proxy servers or virtual private networks (VPN), filters can be bypassed, although not always rendering consistent results, as the following graph depicts.[235]

[234] https://townsendcenter.berkeley.edu/blog/internet-censorship-part-1-technology-working-web (last accessed 04.01.2022)
[235] https://townsendcenter.berkeley.edu/blog/internet-censorship-part-2-technology-information-control (last accessed 23.12.2021)

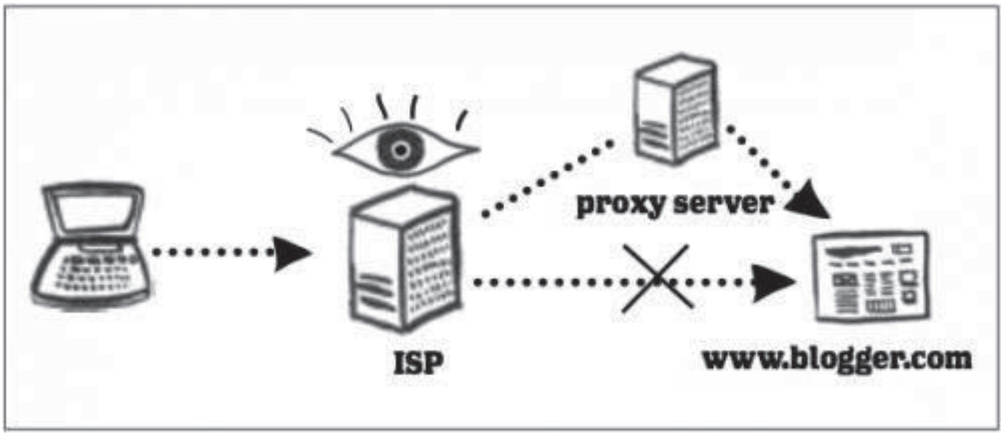


Figure 50: Avoiding internet censorship by using a proxy server[236]

Internet censorship has become an issue in countries with freedom of expression, mainly to the recent COVID-19-pandemic. In Germany many problems arose with the so-called "Querdenker".[237] This is an initiative hostile towards COVID-19 policies of the German government, which was blocked by Facebook. Following many demonstrations, these decisions were reversed, because the ban was not considered reasonable enough by administrative courts. This is a relevant case when because of a country's inability to tackle the issue, a private company became the real censor.

Facebook and other big social media providers are committed to taking action against those users on the internet who discriminate, insult, threaten other users or incite to violence. But it has to be reasonable. When 150 user profiles are banned because of "hate speech and inciting to violence" it's reasonable, but "publication of health-related misinformation" doesn't sound as reasonable. Many statements are covered by freedom of expression for good reason, no matter personal preferences.

These actions of the companies are not governed by law and arbitrated by courts, but by decisions based on property rights. When a company acts on its own, beyond the control of legislation and courts, just to satisfy the expectation of market demand, this is unacceptable. The current ban on the "Querdenker" was enforced on Facebook and Instagram but not on the WhatsApp messenger, although it also belongs to Facebook. The "Querdenker" already communicate and exchange via Telegram, as it's not forbidden to search for alternative channels to disseminate information, but everyone can file charges if they find discriminatory, violent or other criminal content there.[238]

The other social media giant Twitter got criticized when they banned the profile of the then-current president of the United States Donald Trump. Social media became a broadcast platform to reach out to the masses. And because the internet was based on the premise that, if you do not like it, you don't look, the government did not get involved or didn't impose regulations on the Internet. Most experts agree that this is not a censorship issue because the government is not the censor.[239]

[236] https://townsendcenter.berkeley.edu/blog/internet-censorship-part-1-technology-working-web (last accessed 04.01.2022)
[237] A German equivalent of QAnon, very similar.
[238] https://www.dw.com/de/meinung-facebooks-querdenker-zensur-geht-zu-weit/a-59216883 (last accessed 20.01.2022)
[239] https://www.forbes.com/sites/petersuciu/2021/01/11/do-social-media-companies-have-the-right-to-silence-the-masses--and-is-this-censoring-the-government/ (last accessed 20.01.2022)

References Chapter 3

[3-1] Leiner, Barry M., Cerf, Vinton G., Clark, David and Kahn, Robert E. (2009). A Brief History of the Internet. In: ACM SIGCOMM Computer Communication Review vol. 39 no. 5, pp. 22-31, https://dl.acm.org/doi/10.1145/1629607.1629613

[3-2] Treaty of Bern in the version Bukarest 2004 as published on the Austrian Federal platform as "Gesamte Rechtsvorschrift für Weltpostverein – Weltpostvertrag (Bukarest 2004), Fassung vom 5.10.2021", https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20006773 (last accessed 08.02.2022).

[3-3] H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (last accessed 08.02.2022).

[3-4] Bendix, W., & Quirk, P. J. (2016). Deliberating Surveillance Policy: Congress, the FBI, and the Abuse of National Security Letters, Journal of Policy History, 28(03).

[3-5] Deutscher Bundestag (2017), Beschlusempfehlung und Bericht des 1. Untersuchungsausschusses gemäß Artikel 44 des Grundgesetzes, Drucksache 18/12850, https://dserver.bundestag.de/btd/18/128/1812850.pdf (last accessed 08.02.2022).

[3-6] Bederna, Zsolt et al. (2021) Modelling computer networks for further security research, Security and Defence Quarterly 9(36) 16 p. doi: 10.35467/sdq/141572.

[3-7] Szadeczky, Tamás (2018), Security of E-Government Website Encryption in Germany and Hungary, Academic and Applied Research in Military and Public Management Science 17(2) pp. 127-138 doi: 10.32565/aarms.2018.2.9.

[3-8] Szádeczky, Tamás (2020) Governmental Regulation of Cybersecurity in the EU and Hungary after 2000, Academic and Applied Research in Military and Public Management Science, 19(1), pp. 83–93. doi: 10.32565/aarms.2020.1.7.