

adequate data protection: a metric used by the European Commission to measure the safety of data. Under the European Union’s General Data Protection Regulation, companies may transfer personal data to only those non-EU countries that offer essentially the same protection and rights as the EU does. There are only twelve countries or territories that the EU considers to have “data adequacy.”

Advanced Research Projects Agency Network (Arpanet): a closed computer network that transmitted its first successful message in 1969. It was developed jointly by the U.S. Department of Defense and the Massachusetts Institute of Technology during the Cold War as a closed, decentralized alternative to phone line networks, which were vulnerable to attack. Arpanet is considered to be the major precursor to the internet.

censorship: withholding of information, typically by a government or an authoritative body. Censorship comes in several forms, including blocking access to some websites or search terms deemed politically sensitive.

cloud: network of data centers, servers, and other physical infrastructure that store data online rather than on a physical hard drive attached to the user’s computer. The simplest difference between local storage and cloud storage is that users of cloud storage do not always know where their data is being stored. For example, Amazon stores its data at more than thirty-five data centers throughout the world.

CompuServe: an early commercial internet service provider. CompuServe was the first commercial service provider to offer internet connectivity; reached its peak in the 1990s.

cyberattacks: different types of code (such as computer viruses, worms, or Trojan horses) that harm computers and networks, and the people and organizations dependent on them. Cyberattacks are used for theft, espionage, and other purposes, and are typically offensive, asymmetric measures; and the perpetrators are difficult to identify.

cyber governance: the wide range of measures, institutions, and norms that guide, restrict, control, and otherwise shape online behavior and practices. Examples range from China’s Great Firewall to U.S. policies on

Glossary: Cyberspace and Cybersecurity

cyberbullying and bank guidelines on data integrity.

cyberspace: online virtual universe. Definitions vary, but the term cyberspace generally includes a range of services including online games, instant messaging, and the physical devices used to store information. The internet acts as the basis for cyberspace since it is publicly accessible and can be expanded by infinite data networks.

dial-up connection: a method of connecting to the internet through telephone networks (making simultaneous phone and internet use impossible). A dial-up connection is the cheapest but also the slowest means of internet access, and the only one available in areas where broadband and cable infrastructure do not exist.

domain name: a series of characters—letters or numbers—that represents a website, such as “cfr.org.” Domains are related to, but distinct from, URLs and IP addresses. URLs are also series of characters, but they identify the location of an item on the internet; for example, if you wanted to view a specific report on cfr.org, you would type the URL “www.cfr.org/nameofreport.pdf.” IP addresses are numbers assigned to websites that domain names represent.

domain name system (DNS): a collection of databases that assign IP addresses (numbers that a computer can read to reach a website) to website names (e.g., world101.cfr.org) that can be typed directly into a browser.

EU General Data Protection Regulation (GDPR): regulation enacted by the European Union in 2018 that codifies certain rights of EU internet users and certain responsibilities of businesses and other entities that collect and store those users’ data. GDPR is one of the first major bills of citizens’ rights on the internet and may become a global standard.

fiber optic cable: cable, made out of strands of glass as thin as hair, used to quickly transmit large volumes of internet traffic between locations all over the globe. These cables are laid beneath the surface of the earth; when laid on the seabed, they are called submarine cables.

Great Firewall: the system of strict censorship and internet regulation

Glossary: Cyberspace and Cybersecurity

enforced by the Chinese government within its borders. It is the largest system of censorship in the world, the foundations for which were laid in 1998. Since then, it has expanded to the blocking of most major international websites, including Facebook, Google, and Twitter, as well as controversial search terms and nearly all foreign news media.

intellectual property: original works created by an author, technological inventions, business marks and designs, and other “creations of the mind” that are protected by copyright, patent, and trademark laws.

international data centers: facilities that house data or online programs, established by companies that provide software over the internet (such as Microsoft). Data saved to the cloud is housed in such places. Companies typically establish data centers in high-volume data areas, but figuring out where to place one means balancing factors such as weather, number of submarine cables, and politics.

international waters: the parts of the ocean outside the jurisdiction of any particular state, theoretically belonging to everyone—as opposed to territorial waters, which extend to twelve nautical miles from a country’s coastline and constitute sovereign territory.

internet service provider (ISP): a company that provides internet access to subscribers. Initially public, ISPs have been almost entirely privatized in the United States. There are thousands of ISPs in the United States, but only about twelve reach more than a million users.

IP address: a unique series of numbers assigned to each website or device connected to the internet. Just like someone needs an address to send postal mail, computers need other devices’ IP addresses to communicate with them.

least developed countries (LDCs): low-income countries, mostly in sub-Saharan Africa and parts of Asia, that face substantial hindrances to development. The list of such countries is decided by the UN Economic and Social Council. People who live in LDCs often lack access to basic infrastructure, including the internet.

Morris worm: a computer virus released in 1988 by Robert Tappan Morris,

Glossary: Cyberspace and Cybersecurity

then a graduate student at Cornell University and now a professor at the Massachusetts Institute of Technology, that infected 10 percent of all networked devices in existence. Although he was prosecuted for transmitting the worm, Morris is also credited with revealing major vulnerabilities in networked computers and putting a spotlight on internet security.

Mosaic: an early web browser created by students in Illinois with funding from the National Science Foundation. Mosaic popularized internet use in the United States and let users view images and text on the same page for the first time.

Netscape: an internet browser popular in the 1990s. Developed by the creators of Mosaic, Netscape was faster and more functional than its predecessor but dwindled in use as other browsers, notably Internet Explorer, became available at the turn of the century. Netscape made its code available to everyone, a process called open-sourcing; the code was used to develop the browser Mozilla Firefox. Netscape was eventually bought by AOL and then Facebook.

Outer Space Treaty: a 1967 treaty, officially called the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, that defines space as a global commons, free for exploration and peaceful use by all. Drafted during the Cold War, the agreement is designed to limit the prospect of an armed conflict being started from space.

privatize: to transfer ownership of a public enterprise, controlled by a government, to a private entity, such as a company or individual.

right to be forgotten: a principle enshrined in the European Union's General Data Protection Regulation. Under the right to be forgotten, people can apply to have their personal data not appear on the internet if it meets certain conditions, such as if the data is no longer relevant or was unlawfully processed by an organization. The entity that holds the data (e.g., Google) gets to decide if these conditions are met. Currently, the right to be forgotten exists only in Europe, which means that unflattering search results that don't appear in a google.fr search in Paris would still show up in a google.com search in Chicago.

Glossary: Cyberspace and Cybersecurity

Secure Sockets Layer (SSL): a technology that securely connects devices operating over the internet, encrypting the information exchanged across them (e.g., credit card numbers) so it's harder for a third party to access. When SSL is in place, a website's address turns from http to https, the "s" standing for secure.

sovereignty: supreme or absolute authority over a territory. Eritrea, for example, makes laws that apply to Eritrea, not any other country; likewise, no other country can make domestic law for Eritrea. While sovereignty traditionally applies to a government's control of its land and sea borders, some countries argue that the principle also extends to cyberspace.

splinternet: the potential fragmentation of the internet into effectively separate networks based on a user's location and access, as opposed to a cohesive, universally available network. Censorship of websites by certain governments has been described as a potential first step toward splinternet, but even debates about net neutrality (the principle that an internet service providers should not determine, for example, whether users have access to certain content based on how much the users can pay) within a single country play a part.

Stuxnet: a U.S.-Israeli computer virus, discovered in 2010, that targeted Iran's nuclear weapons program. It was the first cyberattack to cause physical damage, and ended up infecting systems in more than 100 countries.

Sustainable Development Goals: seventeen global development goals, applicable to all countries, put forth by the United Nations in 2015. Countries seek to meet these wide-ranging goals (from the eradication of poverty to the protection of the planet and universal and affordable internet access) by 2030.

Telecommunications Act of 1996: a 1996 U.S. law that deregulated the communications market. The act was supposed to create more competition online, but it also allowed large communications businesses to buy smaller networks, leading to the dominance of just a few large corporations over the majority of U.S. broadband service.

Glossary: Cyberspace and Cybersecurity

UN Convention on the Law of the Sea (UNCLOS): a 1994 international agreement identifying what parts of the ocean countries control and how. The agreement defines the twelve nautical miles of ocean extending from the coastline as a country's sovereign territorial waters, waters in which foreign vessels may sail for transit purposes but may not fish, spy, or pollute. Maritime areas beyond territorial waters are international, but UNCLOS does place further restrictions on areas up to 200 nautical miles away from a country's shoreline.