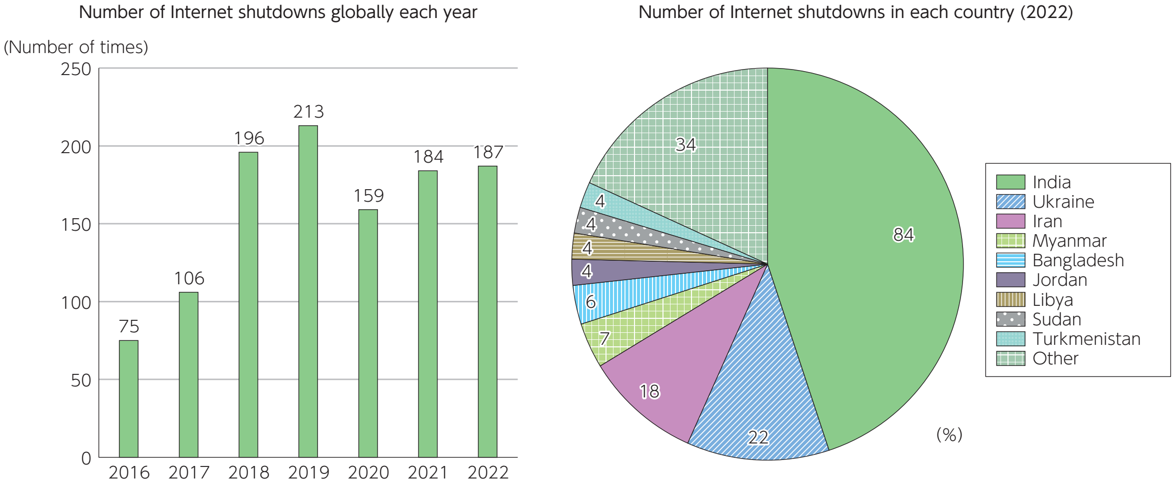
Column Maintaining and promoting a free and open Internet

The Internet originated as a communications network between universities and research institutes under the ARPANET program[1] in the U.S., and it started to be used commercially in the 1990s. With the widespread adoption of personal computers and the development of broadband networks, it has expanded worldwide. The Internet has developed into a free and open space accessible to all in accordance with the basic principles of autonomy, dispersion, and cooperation, and it has become the foundation that supports our socioeconomic activities, where all kinds of people share knowledge and information, and a range of digital services and businesses are created by various stakeholders.

As a governance framework supporting a free and open Internet, the Internet Corporation for Assigned Names and Numbers (ICANN) has played a major role in the management and coordination of resources, such as domain names and IP addresses, and the Internet Engineering Task Force (IETF) has played a major role in the standardization of internet-related technologies. ICANN and the IETF operate according to the principle that governments are just one of the parties involved in decision-making and that democratic decision-making involves multiple stakeholders, including researchers, companies, engineers, and civil society. In addition, the Internet Governance Forum (IGF) was established in 2006, following the consensus statement of the United Nations-sponsored World Summit on the Information Society (WSIS). The IGF also adopts a multi-stakeholder approach in which various parties, including industry, government, academia, and the public, participate in discussions, based on the idea that a wide range of participants share their wisdom to solve problems.[2]

As a threat to this kind of free and open Internet, the movement towards a "splinternet" has become apparent. The term splinternet is a combination of "splinter" and "Internet," and it refers to a situation in which the Internet becomes fragmented due to government regulations and interventions, technological factors, and business activities.[3] According to a report by Access Now, an international NPO, 35 countries experienced at least 187 internet shutdowns in 2022, with both figures up from the previous year **(Figure 1)**.

Figure 1 Internet shutdowns in the world



Number of Internet shutdowns globally each year

Number of Internet shutdowns in each country (2022)

(Source) Created based on "WEAPONS OF CONTROL, SHIELDS OF IMPUNIT"[4]

Fragmentation caused by government regulation and intervention includes state control and management of the Internet that is based on China and Russia's claim of cyber sovereignty.[5]

Since the 1990s, China has been censoring and fragmenting the Internet under a national strategy called the Golden Projects. To protect its interests being negatively affected by information from other countries, it has created an internet censorship system called the Great Firewall (Golden Shield), which blocks access to Google, Facebook, YouTube, and other sites in China. A survey carried out by Freedom House in 2022 found that of the 65 countries surveyed, China had the least amount of freedom on the Internet.

In addition, in recent years, China has proposed positioning the International Telecommunication Union (ITU), a specialized agency of the United Nations, as an internet management organization, and it has begun to

[1] It is a network program between universities and research institutes that is funded by the Advanced Research Projects Agency of the U.S. Department of Defense. The world's first packet communication was realized in 1969.

[2] https://japanigf.jp/about/igf

[3] See Section 2 in Chapter 2 for information on the concentration of digital data with platform providers, etc. and Section 3 in Chapter 2 for information on the algorithmic selection and restriction of data on the Internet.

[4] https://www.accessnow.org/wp-content/uploads/2023/03/2022-KIO-Report-final.pdf

[5] Unlike the idea espoused by Western countries and Japan, etc. that governments and public authorities should not intervene in internet governance and that the Internet should develop outside of government regulations, China and Russia advocate the concept of cyber sovereignty, which states that active control of cyberspace within their borders should be internationally recognized as a national interest.

strengthen its influence in the ITU. As an intergovernmental organization, the ITU is based on a one-country, one-vote system, and private organizations are not expected to be involved in ITU decisions. It is considered that the aim of China's insistence on centralizing discussions on internet governance in the ITU is for countries to take the lead in managing the Internet and for international agreements to be managed on a one-country-one-vote system that includes developing countries so that China's opinions are more strongly reflected.[6]

In September 2019, China's Huawei, together with the Ministry of Industry and Information Technology (a government agency) and two Chinese state-owned telecommunications companies, proposed to the ITU "New IP." This would form the basic technology of a new Internet on the basis that the quality of the current internet protocol (IP) (best effort type) cannot cope with the introduction of cutting-edge technology in the future. This proposal was strongly opposed by Western countries and the IETF, which argued that New IP is incompatible with the existing IP and would compromise interconnectivity. In December 2020, the ITU concluded that New IP would not be discussed further.

The Russian government has also begun to regulate and intervene in the Internet, and in November 2019, a federal law (commonly known as the Sovereign Internet Law) came into effect to block or restrict internet communications with foreign countries in the event of an emergency, etc. The law requires telecom operators to install technical tools on their networks to counter threats to internet traffic and to restrict access to prohibited websites. It also stipulates that the Federal Service for Supervision of Communications, Information Technology and Mass Media centrally manages communications networks when the Internet in Russia is threatened.

In addition to these developments regarding cyber sovereignty by China and Russia, the current complex international situation has led to new fragmentation. Specifically, four days after Russia invaded Ukraine in February 2022, the Ukrainian government requested ICANN to revoke the Russian domain .ru and to suspend DNS root servers in Russia. As discussed above, the Internet is a global platform that is used under the unwritten law that it is accessible to people all over the world, so this request from the Ukrainian government attracted the attention of various countries as it shook the foundation of the Internet. In response, ICANN refused to accept the Ukrainian government's request, saying the "unilateral disconnection of a domain is not stipulated in ICANN policy." Regarding the invasion of Ukraine, not only governments but also companies are taking actions, and in March 2022, two major U.S. telecom operators cut off their connections to Russian networks.[7]

So far, the Internet has supported the creation of digital services, the expansion of innovation, and active communications as a universal infrastructure that is accessible to all without the influence or intervention of any particular state. In order to avoid the fragmentation of the Internet and to maintain and promote a free and open Internet, it is important to maintain the management and operation of the Internet based on a multi-stakeholder framework rather than national initiatives.

For this reason, in April 2022, the U.S. issued the Declaration for the Future of the Internet[8] together with 60 countries and regions, including Japan, Australia, and countries in Europe. The declaration expresses concern that "Access to the open Internet is limited by some authoritarian governments, and online platforms and digital tools are increasingly used to repress freedom of expression and deny other human rights and fundamental freedoms." It also calls for support for an open, free, global, interoperable, reliable, and secure Internet in the future. Furthermore, with regard to the future of the Internet and the Internet and digital technologies, the declaration presents the following principles: (1) protection of human rights and fundamental freedoms, (2) a global Internet (with no fragmentation), (3) inclusive and affordable access to the Internet, (4) trust in the digital ecosystem, and (5) multi-stakeholder internet governance.

In addition, the G7 Digital and Tech Ministers' Meeting in Takasaki, Gunma, held in April 2023, reaffirmed the importance of maintaining and developing internet governance through a multi-stakeholder framework to ensure open and free access to the Internet. The ministers also expressed their opposition to excessive government intervention that unreasonably restricts the distribution of data on the Internet and their continued commitment to ensuring Data Free Flow with Trust (DFFT).

In October 2023, the annual meeting of the Internet Governance Forum (IGF) will be held in Japan. It is expected that the multi-stakeholder discussions, which included the government, the private sector, and the technical and academic communities, will yield meaningful results that support a free and open Internet.

[6] In February 2022, China and Russia issued a statement stating they share the position that "[Both countries] support the internationalization of internet governance, affirm that countries have equal rights to governance, and any attempt to limit the sovereign right to ensure domestic security by regulating domestic segments of the Internet is unacceptable" and that they were "interested in greater ITU participation in addressing these issues."
https://www.digitalpolicyforum.jp/column/220902/

[7] As the trends and nature of the splinternet itself have changed significantly over time, there are indications that Splinternet 1.0, which is defensive in nature to protect a country's own information environment from other countries, has shifted to Splinternet 2.0 in which specific countries are strategically and aggressively disconnected from global networks in order to exclude them. Professor Toshiya Jitsuzumi of Chuo University stated that in the so-called Splinternet 1.0 stage, internet disruptions were done by national governments, but the Splinternet 2.0 stage is characterized by disruptions being done not only by national governments but also by private companies.

[8] Provisional translation: https://www.soumu.go.jp/main_content/000812030.pdf