What if the internet failed?

Since the 1960s, when work on its development began, internet infrastructure has become almost as important as the electricity and transport infrastructure in modern societies. More and more key services, such as banking, food retail and health care, rely on internet connections. Despite the internet's original resilient decentralised design, the increasing importance of a few central players and the shift towards greater centralisation have made the internet more susceptible to failure. This would have severe repercussions: people would not be able to withdraw cash or pay by card, supermarkets and large retailers would not be able to bill and sell products, and managing digital certificates (such as the Covid-19 vaccination certificate) would no longer be possible.

© TheDigitalArtist / Pixaby

Internet-dependent solutions promise greater efficiency and ease of use as well as enhanced control and communication. On a European level, such solutions concern, for instance, the establishment of a European health data space and the European data infrastructure initiative, Gaia-X. All EU Member States increasingly rely on internet-based solutions for many aspects of government, such as taxation, managing citizens' official documents and registering their personal information. The internet is already integral to the functioning of some of the most important sectors of the European economy, such as financial services, transport and tourism, but also to security and border management. The role the internet plays is likely to further increase in significance, especially in the context of the coronavirus pandemic and the subsequent lasting transformations of work and consumption.

The internet has been designed for extraordinary resilience. Its decentralised structure as a network of networks is meant to ensure that, should one or multiple nodes fail, information could still be transmitted, even in the event of a nuclear war. However, with the widespread adoption of the internet and its increased importance in all areas of social life, economic dynamics that incentivise centralisation have become more important. This development implies that the failure of nodes that are more centralised will have more severe, more likely, and more wide-ranging impacts.

There are several ways in which the internet could fail. There could be physical disruption to the connections making up the internet or the crucial nodes in the network where most of the data are exchanged, for instance, through the destruction of cables. Such physical disruption occasionally occurs by accident, but the impact is usually limited. To significantly affect the network, one would have to mount a large-scale, coordinated attack on a high number of nodes. Some natural phenomena, such as solar storms, may cause more severe physical damage. More important are the non-physical disruptions, as they can relatively easily affect larger parts of the network. These include distributed denial of service (DDoS) attacks or the rerouting of traffic through the Border Gateway Protocol (BGP), both explained below. Depending on the scale and target of these attacks, they can lead to important internet outages. Due to the increasingly centralised structure of the internet, even single end-user errors may have significant effects. This was the case in June 2021, when a customer of cloud computing company Fastly, while changing his settings, inadvertently forced several major websites offline as a result of a bug in the company software.

DDoS attacks attempt to overload a service by sending a large number of requests from many different devices, often infected with malware, simultaneously. The targets of these attacks can range from individual websites, which are frequently forced offline as a result of the attack, to more central parts of the internet's infrastructure. In 2016, a large-scale DDoS attack forced Dyn, which at the time was managing significant parts of the domain name system (DNS) infrastructure, offline. This caused disruption to services for many large websites, such as the BBC, and to websites related to the Swedish government. In May 2021, a similar attack targeted Belnet, a Belgian internet service provider on which much of the Belgian government institutions rely for internet connectivity. This attack caused important services to be inaccessible for universities, hospitals, and even the federal parliament. The advent of the internet of things will likely trigger a drastic surge in the number of devices capable of connecting to the internet, often with poor security standards, which would increase the vulnerability to and the severity of DDoS attacks.

'BGP hijacking' refers to the illegitimate corruption of internet routing tables and the subsequent redirection of traffic. In 2008, a Pakistani telecommunications company, in an effort to block the country's access to YouTube, changed the routing tables and accidentally claimed to be the legitimate address for YouTube. Global traffic was thereby rerouted

Author: Lieve Van Woensel with Carl Pierer, Scientific Foresight Unit (STOA)

PE 690.044 – September 2021

from YouTube to Pakistan, causing internet failure in the country and rendering YouTube inaccessible. This vulnerability touches upon a key element in the functioning of the internet, namely, the way traffic is directed, and has been known for more than a decade. Despite increased efforts by the private sector to remedy this problem, it has continued to lead to important security breaches and has been recognised by ENISA.

Potential impacts and developments

In societies that increasingly rely on internet-based services, disruptions to the internet can have many severe consequences. They would likely affect many more domains than can be covered here.

At a more general level, any data stored off-site (in the cloud) may become inaccessible. More importantly, this data may well be difficult to recover: cloud service providers may struggle to identify the exact server on which the data is physically stored. Without this kind of traceability, it might be impossible to physically recover the data for the duration of the internet outage. This is particularly meaningful for data that are time-sensitive, as is the case with health data kept by hospitals, which are increasingly reliant on cloud solutions (in the EU, Sweden's hospitals are at the forefront of this trend).

Importantly, a general internet outage would severely affect monetary transactions. Payments by card would no longer be possible, and cash machines, unable to connect to central banking servers, would not dispense any cash. Without access to cash, individuals would not be able to perform even their most basic daily activities such as buying a cup of coffee or food. Many ticketing services for events, travel or transport connect to the internet to authorise the purchase or verify the authenticity of a ticket. Without such a connection, these tickets could neither be bought nor validated. More topically, app-based solutions for controlling the digital Covid certificate are functional as long as they have an operational internet connection. Severing it could endanger the strategies for containing the coronavirus pandemic.

Software providers today increasingly rely on the software-as-a-service (SaaS) business model, where clients acquire access to centrally hosted software on a subscription basis, while the software is owned, managed and delivered remotely. For their correct functioning and/or maintenance, such services rely on an internet connection. Consequently, disruption to this connection will severely impact businesses and industries relying on such software. The SaaS-model has been widely adopted in many business applications.

Finally, the internet also plays a crucial role in cloud-based solutions in the domains of logistics, inventory and supply-chain. If this means of communication is disrupted, retailers would struggle to fill their shelves and know when to order what product. Without the possibility of billing, consumers would not be able to buy any groceries or other products from supermarkets and large retailers.

Anticipatory policy-making

While many services have only recently adopted or are currently switching to internet-based solutions, the impacts of internet failure, whenever it occurs, are exacerbated by the fact that it is very difficult, if not impossible, to simply go back to the old ways of doing things. Moreover, efforts to correctly and precisely assess and increase the resilience of the internet are currently hampered by a lack of knowledge about the exact configuration, key players and the very structure of the internet.

The European Parliament (EP) is in a position to address these issues by means of a three-pronged approach. First, in a general vein, it can work towards counteracting the centralisation of internet infrastructure, especially in forthcoming discussions on the Digital Markets Act. In these discussions, it can push for more stringent implementation of the EU's competition legislation, and at the same time emphasise the importance of distributed internet infrastructure, for instance by repatriating systems, servers, and storage to the EU, and urging the EU and Member States to invest in such infrastructure. It can furthermore support greater diversity of platforms and operating systems. In the meantime, the EP can mandate the monitoring, by the relevant bodies at EU and Member State level, of existing back-up solutions for sensitive systems, such as law enforcement, to constantly evaluate the feasibility of offline back-up solutions for essential services. Second, as the ongoing trend of centralisation of the internet increases its vulnerability, deepened awareness of the potential failures of any internet-based solution is required, for example, when making risk assessments. It is in this context that ongoing efforts to establish a common European security certificate have to be understood. The EP could call for this certificate to be required for any device destined for sale in the single market and capable of connecting to the internet. Third, the EP could support a coordinated effort to research and map the information lacking about what economic practices and developments may negatively affect the resilient structure of the internet, and what alternatives are available to prevent this.