The G7 Research Group presents the

2022 G7 Elmau Summit Interim Compliance Report

28 June 2022 to 6 January 2023

Prepared by
Keah Sharma and Malhaar Moharir
and the G7 Research Group
7 March 2023 (updated from 22 February 2023)
www.g7.utoronto.ca • g7@utoronto.ca • @g7_rg

"We have meanwhile set up a process and there are also independent institutions monitoring which objectives of our G7 meetings we actually achieve. When it comes to these goals we have a compliance rate of about 80%, according to the University of Toronto. Germany, with its 87%, comes off pretty well. That means that next year too, under the Japanese G7 presidency, we are going to check where we stand in comparison to what we have discussed with each other now. So a lot of what we have resolved to do here together is something that we are going to have to work very hard at over the next few months. But I think that it has become apparent that we, as the G7, want to assume responsibility far beyond the prosperity in our own countries. That's why today's outreach meetings, that is the meetings with our guests, were also of great importance."

Chancellor Angela Merkel, Schloss Elmau, 8 June 2015

G7 summits are a moment for people to judge whether aspirational intent is met by concrete commitments. The G7 Research Group provides a report card on the implementation of G7 and G20 commitments. It is a good moment for the public to interact with leaders and say, you took a leadership position on these issues — a year later, or three years later, what have you accomplished?

Achim Steiner, Administrator, United Nations Development Programme,
in *G7 Canada: The 2018 Charlevoix Summit*

Contents

11. Digital Economy: Empowering Citizens

"We affirm our commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely."

G7 Leaders' Communiqué

Assessment

	No Compliance	Partial Compliance	Full Compliance
Canada			+1
France			+1
Germany			+1
Italy		0	
Japan		0	
United Kingdom			+1
United States			+1
European Union			+1
Average	+0.75 (88%)		

Background

The digital economy was first introduced as an issue area at the 2000 Okinawa Summit with the milestone introduction of the Digital Opportunities Task Force (DOT force).[1783] The digital economy has been described through various terms including 'information technology' (IT), 'information and communications technology' (ICT), 'the Internet' and 'cyberspace.' Over the last two decades, the importance of commitments in this issue area has remained consistent. The G8 Communiqué Okinawa 2000 recognised the role that IT played in the process of globalisation and IT's ability to empower, benefit and link the global population. The Communiqué also stated the large potential of IT to expand economies, enhance public welfare, promote stronger social cohesion and flourish democracy. The Communiqué determined that access to digital opportunities must be open to all, creating a goal to bridge the international information and knowledge divide by maximising the benefits of IT and ensuring its availability to people with limited access. On 13 June 2021, the Cornwall Summit communiqué emphasised the importance of the digital economy for economic recovery, jobs and future frontiers.[1784] The 2016 Ise-Shima Summit reiterates the importance of cyberspace being accessible, open, interoperable, reliable and secure as a key pillar for economic growth and prosperity as well as freedom, democracy and respect for privacy and human rights.[1785]

At the 2000 Okinawa Summit, G8 leaders committed to spreading IT to locations with limited internet access with the help of the private sector including the World Economic Forum's Global Digital Divide Initiative and the Global Business Dialogue on Electronic Commerce (GBDe).[1786] Leaders also committed to setting up the DOT force, which would research and recommend global action that would bridge the international information and knowledge divide.

[1783] G8 Communiqué Okinawa 2000, G7 Information Centre (Toronto) 23 July 2000. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2000okinawa/finalcom.htm
[1784] Carbis Bay G7 Summit Communiqué: Our Shared Agenda for Global Action to Build Back Better, G7 Information Centre (Toronto) 13 June 2021. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2021cornwall/210613-communique.html
[1785] G7 Ise-Shima Leaders' Declaration, G7 Information Centre (Toronto) 27 May 2016. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html
[1786] G8 Communiqué Okinawa 2000, G7 Information Centre (Toronto) 23 July 2000. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2000okinawa/finalcom.htm

At the 2001 Genoa Summit, G8 leaders began to refer to IT as ICT and tasked the DOT force with training teachers on best practices and strengthening education strategies using ICT.[1787] Leaders also called on the private sector to seek new investment opportunities in ICT and learning materials.

At the 2011 Deauville Summit, G8 leaders committed to an annual e-G8 Internet meeting with leading internet players.[1788] The meetings would establish imperatives and duties in terms of security, intellectual property and digital taxation that are compatible with developing innovation and maintaining the free and open nature of the Internet.

At the 2014 Brussels Summit, G7 leaders committed to supporting the global economy by completing an expanded Information Technology Agreement to help support and encourage consistency with current and future multilateral deals.[1789]

At the 2015 Elmau Summit, G7 leaders tasked nations and societies with promoting good governance and respect for human rights by confronting the proliferation of hatred and intolerance through the internet.[1790] The promotion of good governance would combat the spread of hateful ideology and extremism online.

At the 2016 Ise-Shima Summit, G7 leaders stated that an accessible, open, interoperable, reliable and secure cyberspace is a key pillar for economic growth and prosperity that also supports freedom, democracy and respect for privacy and human rights.[1791] Leaders committed to cooperating with each other to prevent the malicious use of cyberspace by states and non-state actors. Leaders also reaffirmed the applicability of international law in cyberspace and committed to promoting a strategic framework to apply existing international law to state behavior in international cyberspace. Additionally, leaders reaffirmed that countries should not conduct or knowingly support theft of intellectual property that is enabled by ICT. Leaders also committed to supporting an open, transparent, free, fair, and equally accessible cyberspace while respecting privacy, data protection, and cyber security. Finally, leaders committed to maximising the potential of the digital economy, addressing global challenges, bridging digital divides and realizing inclusive development.

At the 2017 Taormina Summit, G7 leaders recognised the Next Production Revolution's (NPR) ability to provide the benefits of innovation and digitalization for people across all sectors and regions and support women's opportunities in careers in science, technology, engineering and mathematics.[1792] The NPR aims to inform governments of science and technology-driven innovations that can be used to create economic opportunities.[1793]

At the 2018 Charlevoix Summit, G7 leaders committed to addressing the use of the internet as a tool for terrorism, including recruitment, training, propaganda and financing, by working with partners including the Global Internet Forum to Counter Terrorism.[1794] Leaders recognised that digitalization of the economy

---

[1787] Communiqué, G7 Information Centre (Toronto) 22 July 2001. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2001genoa/finalcommunique.html

[1788] The G8 Deauville Summit, G7 Information Centre (Toronto) 26 May 2011. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2011deauville/2011-sarkozy-0526-en.html

[1789] G7 Brussels Summit Declaration, G7 Information Centre (Toronto) 5 June 2014. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2014brussels/declaration.html

[1790] Leaders' Declaration: G7 Summit, G7 Information Centre (Toronto) 8 June 2015. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2015elmau/2015-G7-declaration-en.html

[1791] G7 Ise-Shima Leaders' Declaration, G7 Information Centre (Toronto) 27 May 2016. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html

[1792] G7 Taormina Leaders' Communiqué, G7 Information Centre (Toronto) 27 May 2017. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2017taormina/communique.html

[1793] Enabling the Next Production Revolution, Organisation for Economic Co-operation and Development (Paris) n.d. Access Date: 9 October 2022. https://www.oecd.org/sti/ind/next-production-revolution.htm

[1794] The Charlevoix G7 Summit Communiqué, G7 Information Centre (Toronto) 9 June 2018. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2018charlevoix/communique.html

impacted the international tax system and welcomed the interim analytical report by the Organisation for Economic Co-operation and Development on the impact of digitalization of the economy on the international tax system. Leaders also committed to seeking a consensus-based solution for this issue by 2020. Leaders also endorsed the Charlevoix Commitment to End Sexual and Gender-Based Violence, Abuse and Harassment in Digital Contexts with the goal of protecting individuals' human rights online.

At the 2019 Biarritz Summit, G7 leaders recognised artificial intelligence's (AI) transformation of societies, the global economy and the future of work in positive capacities regarding human wellbeing and in negative capacities regarding the economy, privacy and data protection, and implications for democracy.[1795] Leaders also acknowledged the need for responsible AI development grounded in human rights and innovation.

At the 2021 Cornwall Summit, G7 leaders committed to preserving an open, interoperable, reliable and secure internet which innovates and supports freedom, trust, and empowerment of people.[1796] Leaders committed to cooperate to further a shared understanding of existing international law applications to cyberspace. Leaders also committed to collaboratively address the rising shared threat from criminal ransomware networks.

Commitment Features

At the 2022 Elmau Summit, leaders committed to "empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely." This commitment can be interpreted as having one main target, which is empowering citizens through their use of the internet and digital technologies. This target includes two dimensions: empowering "vulnerable groups" and ensuring that citizens can use the internet and digital technologies "safely" and "securely."

"Empower" is understood to mean giving official authority or legal power to an entity.[1797] In the context of this commitment, it refers to promoting the self-actualization of citizens through their use of the internet and digital technologies.

"Vulnerable groups" is understood to mean a body of people who are at a greater disadvantage or at a greater risk of being harmed relative to the general population.[1798] In the context of this commitment, it refers to the inexperienced group of people who face a greater risk of harm online because they are only now gaining access to the internet or will soon do so.[1799] This particularly includes low-income users.

"Digital technologies" refers to electronic tools, systems and devices that generate, store, or process data.[1800] Examples of digital technologies include, but are not limited to: mobile phones, computers, social media, automated banking machines and AI.

"Safely" and "securely" are understood to mean protected from danger or harm.[1801] In the context of this commitment, it refers to protecting citizens' digital technologies and internet networks against unauthorized

---

[1795] Biarritz Strategy for an Open, Free and Secure Digital Transformation, G7 Information Centre (Toronto) 26 August 2019. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2019biarritz/biarritz-strategy-for-digital-transformation.html

[1796] Carbis Bay G7 Summit Communiqué: Our Shared Agenda for Global Action to Build Back Better, G7 Information Centre (Toronto) 13 June 2021. Access Date: 26 September 2022. http://www.g7.utoronto.ca/summit/2021cornwall/210613-communique.html

[1797] Empower, Merriam-Webster (Springfield) n.d. Access Date: 25 September 2022. https://www.merriam-webster.com/dictionary/empower

[1798] Vulnerable, Merriam-Webster (Springfield) n.d. Access Date: 25 September 2022. https://www.merriam-webster.com/dictionary/vulnerable

[1799] Global Risks Report 2022: Chapter 3. Digital Dependencies and Cyber Vulnerabilities, World Economic Forum (Geneva) 11 January 2022. Access Date: 6 January 2023. https://www.weforum.org/reports/global-risks-report-2022/in-full/chapter-3-digital-dependencies-and-cyber-vulnerabilities/

[1800] Digital Technology, Dictionary.com (Detroit) n.d. Access Date: 5 October 2022. https://www.merriam-webster.com/dictionary/digital

[1801] Secure, Merriam-Webster (Springfield) n.d. Access Date: 25 September 2022. https://www.merriam-webster.com/dictionary/secure

access or attack.[1802] On the one hand, cyber safety refers to citizens' safe practices while using the internet to protect against online harm.[1803] On the other hand, cyber security refers to the collection of tools and safeguards that protect the "cyber environment."[1804]

Full compliance, or a score of +1, will be given to G7 members that demonstrate strong action in fulfilling both dimensions of the target to empower citizens through their use of the internet and digital technologies. G7 members must ensure the safety and security of the internet and digital technologies and empower vulnerable groups. Strong actions may include developing secure networks, improving infrastructure that increases access to a reliable internet connection, reducing the cost of digital services, creating new committees or funding existing committees that are dedicated to improving cyber security, promoting safe practices to bolster cyber safety and joining international organizations dedicated to expanding internet access.

Partial compliance, or a score of 0, will be assigned to G7 members that demonstrate strong action in one of the target dimensions while demonstrating weak or no action in the other dimension. This may include strong action in empowering vulnerable groups but weak action in ensuring the safety and security of the internet and digital technologies or vice versa. Weak actions may include attending meetings that speak on the importance of increasing cyber security, reaffirming the commitment to empower vulnerable groups and denouncing countries, organizations or individuals that engage in cyber-attacks.

Non-compliance, or a score of −1, will be assigned if the G7 member demonstrates weak action in both dimensions or fails to demonstrate any action in both dimensions.

Scoring Guidelines

−1	The G7 member has NOT taken any action to empower vulnerable groups or to ensure the safety and security of the internet and digital technologies OR has only taken weak action in empowering vulnerable groups and ensuring the safety and security of the internet and digital technologies.
0	The G7 member has taken strong action to empower vulnerable groups but has taken weak or no action to ensure the safety and security of the internet and digital technologies OR the G7 member has taken strong action to ensure the safety and security of the internet and digital technologies but has taken weak or no action to empower vulnerable groups.
+1	The G7 member has taken strong action to empower citizens and vulnerable groups AND to ensure the safety and security of the internet and digital technologies.

Compliance Director: Arees Chooljian
Lead Analyst: Joy Chan

Canada: +1

Canada has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely.

On 19 August 2022, Public Safety Canada concluded an eight-week public consultation on Canada's approach to cyber security in advance of the renewal of Canada's National Cyber Security Strategy.[1805] Conducted via email, the survey sought to realize public attitudes relating to the following three goals: (1) secure and resilient

---

[1802] Cybersecurity, Merriam-Webster (Springfield) n.d. Access Date: 25 September 2022. https://www.merriam-webster.com/dictionary/cybersecurity

[1803] Cybersafety, Merriam-Webster (Springfield) n.d. Access Date: 6 January 2023. https://www.merriam-webster.com/dictionary/cybersafety

[1804] Definition of Cybersecurity, International Telecommunication Union (Geneva) n.d. Access Date: 6 January 2023. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[1805] Consulting on Canada's Approach to Cyber Security, Public Safety Canada (Ottawa) n.d. Access Date: 5 November 2022. https://www.publicsafety.gc.ca/cnt/cnslttns/cnsltng-cnd-pprch-cbr-scrt/index-en.aspx

Canadian systems; (2) an innovative and adaptive cyber ecosystem; and (3) effective leadership, governance and collaboration.

On 3 August 2022, the Canadian Centre for Cyber Security (CCCS) released guidelines in response to the threat posed by quantum computers to network accessible data confidentiality.[1806] Information with a long lifespan in transit could be "collected, stored, then read" in the future by quantum computers immune to current methods of cryptography. The CCCS recommends organizations evaluate information lifespan and sensitivity, review IT lifecycle management plans and budget for updates and determine when and how to incorporate quantum-safe cryptography in said plan.

On 19 September 2022, Statistics Canada completed a study on the use of blockchain (distributed leger technology) to authenticate data from the Statistics Canada Website.[1807] The study aimed to identify the feasibility and benefit of this method for Canadians, as well as its environmental impact, public perception and lack of regulations. The study urges the undertaking of a pilot project allowing both online and offline users to authenticate their data.

On 26 October 2022, Minister of Rural Economic Development Gudie Hutchings and Ontario's Parliamentary Assistant to the Minister of Infrastructure Amarjot Sandhu announced several high-speed internet projects funded by both levels of government and delivered by Bell Canada and Cogeco Connexion Inc.[1808] The two levels of government expect to provide high-speed internet access to more than 16,000 homes in rural eastern Ontario by investing over CAD56 million into the projects.

On 4 November 2022, the Department of National Defense and the Canadian Armed Forces offered a research grant of up to CAD1.5 million over three years to stimulate the application of advances in 5G technologies to defence and security problems.[1809] Led by Canadian universities, innovators would assemble a multidisciplinary group of researchers to collaborate on research within the 5G domain with applications relevant to cyber security.

On 7 November 2022, Minister of Innovation, Science and Industry François-Philippe Champagne launched phase two of the Accessible Technology Program (ATP) alongside a CAD5.8 million investment into the program.[1810] The ATP seeks projects that are aiming to develop assistive and adaptive digital technologies that can improve accessibility to the digital economy for Canadians with disabilities.

On 2 December 2022, Shared Services Canada (SSC) announced the successful administration of Canada's first digital census.[1811] This project included powering over 700 servers to support census collection, data processing and dissemination; equipping 22 virtual offices for census staff; and establishing six virtual call centres. In

[1806] Research Security Information Update – July 2022, Public Safety Canada (Ottawa) n.d. Access Date: 6 November 2022. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2022-06-rsiu/index-en.aspx

[1807] Investigating the Use of Blockchain to Authenticate Data from the Statistics Canada Website, Statistics Canada (Ottawa) 19 September 2022. Access Date: 6 November 2022. https://www150.statcan.gc.ca/n1/pub/11-633-x/11-633-x2022007-eng.htm

[1808] Governments of Canada and Ontario invest over $56 million to bring high-speed Internet access to over 16,000 rural homes in eastern Ontario, Innovation, Science and Economic Development Canada (Ottawa) n.d. Access Date: 6 January 2023. https://www.canada.ca/en/innovation-science-economic-development/news/2022/10/governments-of-canada-and-ontario-invest-over-56-million-to-bring-high-speed-internet-access-to-over-16000-rural-homes-in-eastern-ontario.html

[1809] Faster, Stronger, More Secure: Advancing 5G capabilities and concepts for defense and security, Government of Canada (Ottawa) n.d. Access Date: 6 November 2022. https://www.canada.ca/en/department-national-defence/programs/defence-ideas/element/innovation-networks/challenge/advancing-5g-capabilities.html

[1810] Making digital technologies more accessible to Canadians with disabilities, Innovation, Science and Economic Development Canada (Ottawa) 7 November 2022. Access Date: 6 January 2023. https://www.canada.ca/en/innovation-science-economic-development/news/2022/11/making-digital-technologies-more-accessible-to-canadians-with-disabilities.html

[1811] 2021-22 Departmental Results Report, Shared Services Canada (Ottawa) n.d. Access Date: 28 December 2022. https://www.canada.ca/en/shared-services/corporate/publications/departmental-results-report-2021-22.html

collaboration with Statistics Canada and the Canadian Centre for Cyber Security, the SSC ensured the reliability and security of the census infrastructure in order to protect against cyber threats.

On 2 December 2022, the SSC announced the successful establishment of secure "cloud to ground connectivity" for 18 partners in the interest of safeguarding Canadian data.[1812] As the government hosts increasing amounts of data in the cloud, securing cloud connectivity becomes a necessary step in ensuring cyber security.

On 19 December 2022, Minister of Immigration, Refugees and Citizenship Sean Fraser announced funding of up to CAD31 million through the Universal Broadband Fund to the municipality of Pictou County.[1813] The funding aims to provide high-speed internet access to more than 4,700 homes in the rural communities of Nova Scotia. This investment is in line with the government's goal of ensuring that 98 per cent of Canadians have access to high-speed internet by 2026 and 100 per cent by 2030.

Canada has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely. Canada has taken action to identify areas of concern within the realm of cyber security, open internet and digital infrastructure. It has also taken steps to ensure accessibility and safety for vulnerable groups.

Thus, Canada receives a score of +1.

Analyst: Mary Ditta

France: +1

France has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely.

On 13 September 2022, Minister of Economy and Finance Bruno Le Maire and Minister Delegate for Digital Transition and Telecommunications Jean-Noël Barrot renewed their "digital ambition" and support for the "cloud ecosystem," citing its importance as a major pillar of France's digital sovereignty.[1814] Ministers Le Maire and Barrot urged the European Commission to validate the Important Project of Common European Interest cloud, a EUR5 billion project supporting the invention of an upgraded cloud in Europe — the "cloud of tomorrow."

On 4 October 2022, Secretary of State to the Prime Minister Charlotte Caubel and Minister of National Education and Youth Pap Ndiaye launched a campaign to promote free crisis response lines to children and teenagers at risk.[1815] The phone number 30 18 seeks to support young victims or witnesses of cyberbullying, such as webcam blackmail, identity theft or exposure to violent content.

[1812] 2021-22 Departmental Results Report, Shared Services Canada (Ottawa) n.d. Access Date: 28 December 2022. https://www.canada.ca/en/shared-services/corporate/publications/departmental-results-report-2021-22.html

[1813] Government of Canada invests up to $31 million to bring high-speed Internet access to over 4,700 households in Nova Scotia, Innovation, Science and Economic Development Canada (Ottawa) 19 December 2022. Access Date: 6 January 2023. https://www.canada.ca/en/innovation-science-economic-development/news/2022/12/government-of-canada-invests-up-to-31-million-to-bring-high-speed-internet-access-to-over-4700households-in-nova-scotia0.html

[1814] De nouveaux dispositifs en faveur de la stratégie nationale pour le cloud, Government of France (Paris) 13 September 2022. Translation provided by Google Translate. Access Date: 6 November 2022. https://www.gouvernement.fr/actualite/de-nouveaux-dispositifs-en-faveur-de-la-strategie-nationale-pour-le-cloud

[1815] Harcèlement, agressions, violences : trois numéros pour aider les enfants en danger, Government of France (Paris) 4 October 2022. Translation provided by Google Translate. Access Date: 6 November 2022. https://www.gouvernement.fr/actualite/harcelement-agressions-violences-trois-numeros-pour-aider-les-enfants-en-danger

On 28 October 2022, Minister Barrot announced the support of 17 projects through the "national acceleration strategy for cyber security."[1816] The government will allocate EUR39 million to the projects to develop innovative cyber security solutions.

France has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely. The country has taken action to support the goals of developing and ensuring cyber safety and supporting projects dedicated to improving cyber security.

Thus, France receives a score of +1.

Analyst: Mary Ditta

Germany: +1

Germany has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely.

On 13 July 2022, Minister of Digital Affairs and Transport Volker Wissing announced the Gigabit Strategy, which aims to achieve widespread coverage of fiber optic networks and the latest mobile communications standard where people work, live and travel by 2030.[1817] The government plans to triple fiber optic connections by the end of 2025.

On 27 July 2022, the Federal Cabinet adopted the first comprehensive start-up-strategy, which prioritizes giving start-ups access to funding and financing without "unnecessary bureaucracy" to promote young and innovative companies.[1818] A component of the start-up-strategy enables the possibility to set up companies entirely digitally within 24 hours.

On 31 August 2022, the government approved its new Digital Strategy to advance digitalization in Germany.[1819] With this plan, the government seeks to focus on promoting a connected digital sovereign society, an innovative economy and a learning digital government while ensuring secure data exchanges and confidential communication.

On 5 September 2022, the Ministry of Digital Affairs and Transport made funding of up to EUR300 million available until 2024 to promote innovative technologies in the mobile communications sector.[1820] The funding particularly aims to assist innovative SMEs in developing a more diverse range of mobile communications services through accelerated network rollouts and increased competition.

On 30 November 2022, Minister Wissing appointed 19 representatives from industry, academia and the public to the Digital Strategy Germany Advisory Board.[1821] The goal of the advisory board is to support ministries in

---

[1816] France 2030 soutient 17 projets pour la cybersécurité, Government of France (Paris) 4 November 2022. Translation provided by Google Translate. Access Date: 6 November 2022. https://www.gouvernement.fr/actualite/france-2030-soutient-17-projets-pour-la-cybersecurite

[1817] Gigabitstrategie der Bundesregierung, The Federal Government (Berlin) 13 July 2022. Access Date: 5 November 2022. https://www.bundesregierung.de/breg-de/themen/digitaler-aufbruch/gigabitstrategie-2017464

[1818] Facilitating company foundations, strengthening funding, The Federal Government (Berlin) 27 July 2022. Access Date: 5 November 2022. https://www.bundesregierung.de/breg-en/search/start-up-strategy-2066026

[1819] The Federal Government's new Digital Strategy, Federal Foreign Office (Meseberg) 13 September 2022. Access Date: 11 January 2023. https://www.auswaertiges-amt.de/en/aussenpolitik/digital-strategy/2551972

[1820] 300 million euros for innovations in mobile communications, Federal Ministry for Digital and Transport (Berlin) 5 September 2022. Access Date: 6 January 2023. https://bmdv.bund.de/SharedDocs/EN/PressRelease/2022/060-300-million-euros-mobile-communications.html

[1821] Wissing: Making Germany fit for the digital future, Federal Ministry for Digital and Transport (Berlin) 30 November 2022. Access Date: 6 January 2023. https://bmdv.bund.de/SharedDocs/EN/PressRelease/2022/089-wissing-digital-future.html

their implementation of the government's Digital Strategy, particularly by analyzing its results, identifying any obstacles and ensuring its transparency.

On 20 December 2022, the Ministry of Digital Affairs and Transport and the Federal Network Agency launched a new Gigabit Register as part of the Gigabit Strategy.[1822] The purpose of this register is to establish a digital data hub that offers a comprehensive and user-friendly overview of the gigabit network rollout status, which plays a role in accelerating the implementation of fiber optic and 5G networks.

Germany has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely. The government has established initiatives such as the Gigabit Register to help citizens and new businesses access and use the internet safely. It has also taken measures to ensure the safety and security of digital technologies through initiatives like the Digital Strategy.

Thus, Germany receives a score of +1.

Analyst: Michael Lecchino

Italy: 0

Italy has partially complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely.

On 19 December 2022, the Government of Italy launched a new cyber security campaign, which, among other things, promotes the value of personal data, recognizes the risks of social networks and notes the dangers to user privacy during use of new digital technologies.[1823] The campaign seeks to promote digital literacy and increase users' awareness of legislation that protects their rights concerning their personal data online.

Italy has partially complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely. The country has taken strong action to empower vulnerable groups in using digital technologies safely. However, it has not taken strong action to ensure the safety and security of the internet and digital technologies.

Thus, Italy receives a score of 0.

Analyst: Pengyu Chen

Japan: 0

Japan has partially complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely.

On 5 July 2022, the Ministry of Economy, Trade and Industry announced plans to investigate and conduct trials on methods of constructing and expanding "Web 3.0 creator economies."[1824] The ministry acknowledged that the current legal framework on this increasingly prevalent digital sphere is vague and that they must identify any obstacles that ordinary users may face while accessing the sphere.

[1822] Wissing: New Gigabit Register for Germany, Federal Ministry for Digital and Transport (Berlin) 20 December 2022. Access Date: 6 January 2023. https://bmdv.bund.de/SharedDocs/EN/PressRelease/2022/096-wissing-new-gigabit-register-for-germany.html
[1823] Communication campaign "Privacy by your side," Italian Government (Rome) 19 December 2022. Access Date: 6 January 2023. https://www.governo.it/en/node/21341
[1824] Research Project on Constructing Web-3.0-Era Creator Economies to Be Launched, Ministry of Economy, Trade and Industry (Tokyo) 5 July 2022. Access Date: 6 January 2023. https://www.meti.go.jp/english/press/2022/0705_002.html

On 15 July 2022, the Ministry of Economy, Trade and Industry set up the Web 3.0 Policy Office.[1825] The office will collect information from relevant business entities and work with the Digital Agency to establish projects related to Web 3.0.

On 21 September 2022, the Government of Japan announced that it plans to strengthen cyber security standards for defense contractors.[1826] The government based the new standards on the cyber security guidelines adopted by the US National Institute of Standards and Technology.

On 30 October 2022, the Defense Ministry announced plans to boost its cyber defense personnel up to 5,000 by 2027 to address cyberattacks targeting Japanese institutions.[1827] This move is in response to China's increasing efforts to bolster "cyberwarfare capabilities."

On 31 October 2022, the Government of Japan signed a memorandum of cooperation with the UK to deepen ties on digital government transformation and digital service promotion.[1828] The memorandum brings together Japan's Digital Agency with the UK's Government Digital Service.

Japan has partially complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely. The country has taken strong action to ensure the safety and security of the internet and digital technologies. However, it has not taken strong action to empower vulnerable groups in using digital technologies safely.

Thus, Japan receives a score of 0.

Analyst: Daanish Bhatti

United Kingdom: +1

The United Kingdom has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely.

On 27 July 2022, Deputy Commander Strategic Command Lieutenant General Tom Copinger-Symes and Germany's Chief of Cyber and Information Domain Service Vice Admiral Thomas Daum signed a bilateral agreement on cyber cooperation.[1829] The aim of this agreement is to enhance cyber capacities and safety, share information and experiences and learn from each other's strengths.

On 29 September 2022, the Government of the United Kingdom released GBP200,000 for organizations to bid to research and assess the cyber resilience of popular smart devices used by the country's businesses.[1830] The successful bidder organization will assess the strength of existing cyber security measures and guidance for smart device cyber threats.

[1825] Web 3.0 Policy Office Established in the Minister's Secretariat as a Cross-Departmental Internal Organization, Ministry of Economy, Trade, and Industry (Tokyo) 15 July 2022. Access Date: 9 November 2022. https://www.meti.go.jp/english/press/2022/0715_002.html

[1826] Japan to boost cybersecurity for defense contractors, Nikkei Asia (Tokyo) 21 September 2022. Access Date: 9 November 2022. https://asia.nikkei.com/Business/Aerospace-Defense/Japan-to-boost-cybersecurity-for-defense-contractors

[1827] Japan plans to boost cyberdefense personnel to 5,000 by fiscal 2027, The Japan Times (Tokyo) 30 October 2022. Access Date: 9 November 2022. https://www.japantimes.co.jp/news/2022/10/30/national/japan-cyber-defense/

[1828] UK and Japan strengthen cooperation in the area of digital government, Government Digital Service (London) 31 October 2022. Access Date: 9 November 2022. https://www.gov.uk/government/news/uk-and-japan-strengthen-cooperation-in-the-area-of-digital-government

[1829] Cyber Co-operation with Germany Strengthens, Ministry of Defence (London) 27 July 2022. Access Date: 30 October 2022. https://www.gov.uk/government/news/cyber-co-operation-with-germany-strengthens

[1830] Up to £200,000 available to test security of smart devices used by nearly all UK businesses, Department for Digital, Culture, Media & Sport (London) 29 September 2022. Access Date: 20 December 2022. https://www.gov.uk/government/news/up-to-200000-available-to-test-security-of-smart-devices-used-by-nearly-all-uk-businesses

On 20 October 2022, the Ministry of Defence's Strategic Command began work with the US Cyber Command and other partners on a cooperative initiative to "improve interoperability and strengthen cyber resilience."[1831] The initiative aims to strengthen the capacity to detect threats that could endanger internal cyber systems of all parties.

On 31 October 2022, the UK Government signed a memorandum of cooperation with Japan to deepen ties on digital government transformation.[1832] The memorandum brings together the Government Digital Service with Japan's Digital Agency.

On 1 November 2022, the UK Government provided a GBP6.35 million support package to improve Ukraine's cyber defences from malicious cyber-attacks that target its national infrastructure.[1833] The funding, among other things, allows Ukrainian citizens to access vital information and prevents malicious actors from accessing certain information.

On 8 November 2022, the UK Government and industry senior leaders chaired a new National Cyber Advisory Board and discussed the ways in which they will protect and promote the country's interests in cyberspace.[1834] The board aims to ensure that senior leaders "challenge, support and inform the UK's strategic approach" to issues in the cyberspace, including the protection of the public from cybercrime such as fraud.

On 30 November 2022, the UK Government announced plans to update its cyber laws to improve resilience against cyber-attacks.[1835] Specifically, the government confirmed the strengthening of the Network and Information Systems Regulations to protect the country's everyday service infrastructure, such as computing, from cyber-attacks. This legislative change is a part of the government's GBP2.6 billion National Cyber Strategy, an initiative that aims to improve cyber resilience for at-risk businesses and to secure the UK's digital economy.

On 9 December 2022, the UK Government announced plans to work with app store operators and developers over a nine-month period to develop new privacy and security rules for app stores to protect consumers from malicious apps that can steal data and funds.[1836] This measure sets a new code of practice for developers, establishes a process in which security experts can report software vulnerabilities and ensures that security and privacy information is available to users in an easy-to-understand way.

On 6 January 2023, the UK Government amended Building Regulations 2010 statute to ensure that newly constructed homes in England are connected to the infrastructure necessary to receive gigabit broadband

---

[1831] Collaborating with U.S. on Cyber, Ministry of Defence (London) 20 October 2022. Access Date: 30 October 2022. https://www.gov.uk/government/news/collaborating-with-us-on-cyber

[1832] UK and Japan strengthen cooperation in the area of digital government, Government Digital Service (London) 31 October 2022. Access Date: 9 November 2022. https://www.gov.uk/government/news/uk-and-japan-strengthen-cooperation-in-the-area-of-digital-government

[1833] UK boosts Ukraine's cyber defences with £6 million support package, Foreign, Commonwealth & Development Office (London) 1 November 2022. Access Date: 2 November 2022. https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package

[1834] New National Cyber Advisory Board meets to protect UK's interests, Cabinet Office (London) 9 November 2022. Access Date: 20 December 2022. https://www.gov.uk/government/news/new-national-cyber-advisory-board-meets-to-protect-uks-interests

[1835] Cyber laws updated to boost UK's resilience against online attacks, Department for Digital, Culture, Media & Sport (London) 30 November 2022. Access Date: 20 December 2022. https://www.gov.uk/government/news/cyber-laws-updated-to-boost-uks-resilience-against-online-attacks

[1836] New rules for apps to boost consumer security and privacy, Department for Digital, Culture, Media & Sport (London) 9 December 2022. Access Date: 20 December 2022. https://www.gov.uk/government/news/new-rules-for-apps-to-boost-consumer-security-and-privacy

internet access.[1837] This amendment seeks to prevent the need for expensive and disruptive installation of the necessary infrastructure for people moving into new homes.

The United Kingdom has fully complied with its commitment to empower citizens through the digital economy. The government has improved internet safety and security by signing bilateral treaties with Germany and the United States to enhance its cyber security capacities. The government has also invested GBP6.5 million to support the UK-Ukraine cyber security programme against cyber threats.

Thus, the United Kingdom receives a score of +1.

Analyst: Pengyu Chen

United States: +1

The United States has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely.

On 12 July 2022, the Department of the Treasury released a notice requesting public comment on the risks and opportunities for developments in the digital assets space.[1838] This constitutes a part of its work under President Joe Biden's digital assets Executive Order 14067 that seeks to ensure the "responsible development of digital assets."

On 9 August 2022, President Biden signed the CHIPS [Creating Helpful Incentives to Produce Semiconductors] and Science Act into law.[1839] The Act is designed to boost US competitiveness and international security. It allows for development in leading edge technologies like quantum computing, artificial intelligence and nanotechnology, all uniquely important to the advancement of the digital economy.[1840]

On 14 September 2022, the Office of Management and Budget issued guidance to ensure that government agencies are using digital technologies that are in line with common cyber security practices.[1841] This guidance is built on President Biden's executive order on "Improving the Nation's Cybersecurity" and seeks to protect the security and reliability of the government's digital services so that Americans can safely access them.

On 20 September 2022, the Department of the Treasury published its Action Plan to Address Illicit Financing Risks of Digital Assets.[1842] The Department announced seven areas of focus to enhance regulatory compliance in the digital assets space: monitoring emerging risks, improving global regulation and enforcement, updating regulations on anti-money laundering and the combating of the financing of terrorism, strengthening supervision of virtual asset activities, holding illicit actors accountable for misconduct, engaging with the private sector and supporting US leadership in financial technology.

[1837] Millions of homeowners and tenants to get better access to faster broadband, Department for Digital, Culture, Media & Sport (London) 6 January 2023. Access Date: 6 January 2023. https://www.gov.uk/government/news/millions-of-homeowners-and-tenants-to-get-better-access-to-faster-broadband
[1838] Treasury Releases Request for Comment on Risks and Opportunities and Presented by Digital Assets, U.S. Department of the Treasury (Washington D.C.) 12 July 2022. Access Date: 9 November 2022. https://home.treasury.gov/news/press-releases/jy0861
[1839] FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China, The White House (Washington D.C.) 9 August 2022. Access Date: 9 November 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/
[1840] The CHIPS and Science Act: Here's what's in it, McKinsey & Company (New York City) 4 October 2022 Access Date: 9 November 2022. https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-chips-and-science-act-heres-whats-in-it
[1841] Enhancing the Security of the Software Supply Chain to Deliver a Secure Government Experience, The White House (Washington D.C.) 14 September 2022. Access Date: 6 January 2023. https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/
[1842] Fact Sheet: Action Plan to Address Illicit Financing Risks of Digital Assets, U.S. Department of the Treasury (Washington D.C.) 20 September 2022. Access Date: 9 November 2022. https://home.treasury.gov/system/files/136/Fact-Sheet-Action-Plan-to-Address-Illicit-Financing-Risks-of-Digital-Assets.pdf

On 22 September 2022, the US Department of Agriculture announced it is awarding USD502 million in loans and grants to provide high-speed internet access to residents and businesses in rural areas in 20 states.[1843] The department plans to make additional investments in the near future with some of the funds coming from President Biden's Bipartisan Infrastructure Law.

On 3 October 2022, the Financial Stability Oversight Council released the Report on Digital Asset Financial Stability Risks and Regulation in response to President Biden's Executive Order 14067.[1844] The report reviews the financial stability risks and regulatory gaps related to several digital assets and provides recommendations for how to address these risks.

On 14 December 2022, at the US-Africa Business Forum, President Biden announced the launch of the Digital Transformation with Africa (DTA) initiative, which seeks to expand digital literacy and access as well as strengthen the digital ecosystem across Africa.[1845] The DTA initiative intends to invest over USD350 million and facilitate over USD450 million in financing for Africa.

The United States has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely. Agencies have committed to plans that advance legal and economic reforms to advance the digital assets space. Government monetary and infrastructure contributions have also expanded access to the internet both domestically and abroad. Policies are on the way to protect citizens' data.

Thus, the United States receives a score of +1.

Analyst: Daanish Bhatti

European Union: +1

The European Union has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely.

On 29 June 2022, the European Council created the European Single Access Point (ESAP).[1846] The ESAP is a digital hub that provides free and user-friendly access to financial and sustainability related information by European companies that can help facilitate the decision-making process for investors. By increasing the digital use of this information, the ESAP also takes steps in meeting the objectives of the Digital Finance Strategy.

On 30 June 2022, the European Council and the European Parliament reached an agreement on the "markets in crypto-assets" (MiCA) proposal, a regulatory framework for crypto-assets, crypto-asset issuers and crypto-asset service providers.[1847] The MiCA proposal aims to protect consumers from the risks associated with investing in crypto-assets, such as fraudulent schemes.

[1843] Biden-Harris Administration Announces $502 Million for High-Speed Internet in Rural Communities, U.S. Department of Agriculture (Washington D.C.) 22 September 2022. Access Date: 9 November 2022. https://www.usda.gov/media/press-releases/2022/09/22/biden-harris-administration-announces-502-million-high-speed
[1844] PRESS RELEASE: Financial Stability Oversight Council Releases Report on Digital Asset Financial Stability Risks and Regulation, U.S. Department of the Treasury (Washington D.C.) 3 October 2022. Access Date: 9 November 2022. https://home.treasury.gov/news/press-releases/jy0986
[1845] FACT SHEET: New Initiative on Digital Transformation with Africa (DTA), The White House (Washington D.C.) 14 December 2022. Access Date: 6 January 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta/
[1846] Easy access to corporate information for investors: Council agrees its position on the European Single Access Point (ESAP), European Council (Brussels) 29 June 2022. Access Date: 6 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/easier-access-to-corporate-information-for-investors-council-agrees-its-position-on-a-single-access-platform/
[1847] Digital finance: agreement reached on European crypto-assets regulation (MiCA), European Council (Brussels) 30 June 2022. Access Date: 6 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/

On 14 July 2022, the European Council and the European Parliament reached a provisional agreement on the 2030 policy programme "Path to the Digital Decade."[1848] The programme outlines digital targets in the areas of digital literacy, secure and sustainable digital infrastructure and goals of digitalizing public services that the EU aims to meet by 2030.

On 18 July 2022, the European Council announced its final approval on new rules through the Digital Markets Act (DMA), which ensures a fair and competitive digital sector.[1849] The DMA's goal is to ensure a "level playing field" in the digital sphere by regulating large online platforms to protect both companies and consumers.

On 4 October 2022, the European Council approved the Digital Services Act (DSA).[1850] The goal of the DSA is to protect the digital sphere from the dissemination of illegal content while protecting users' rights online. To do this, the DSA, among other things, prohibits targeted advertising based on minors' personal data, bans misleading interfaces and counters illegal content.

On 28 November 2022, the European Council adopted the Digital Operational Resilience Act (DORA).[1851] The adoption of DORA seeks to mitigate cyber threats and strengthen IT security for financial entities such as banks by setting standards for network security and stability to keep financial services resilient through service disruptions.

On 28 November 2022, the European Council adopted legislation for a "high common level of cybersecurity" across the EU with the "NIS2" directive.[1852] The legislation aims to improve cyber resilience in both the public and private sector across the EU by setting standards for cyber security measures and a regulatory framework that ensures effective cooperation among the relevant authorities.

On 30 November 2022, the European Data Protection Supervisor and the EU Agency for Cybersecurity signed a memorandum of understanding to establish a cooperative framework between the two bodies.[1853] They agreed to design, develop and deliver capacity building and awareness-raising activities concerning cyber security and data protection efforts.

On 15 December 2022, the European Council, the European Parliament and the European Commission signed the "European declaration on digital rights and principles for the digital decade."[1854] The declaration aims to

---

[1848] Policy Programme "Path to the Digital Decade": The Council and the European Parliament reach a provisional agreement, European Council (Brussels) 14 July 2022. Access Date: 6 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/07/14/policy-programme-path-to-the-digital-decade-the-council-and-the-european-parliament-reach-a-provisional-agreement/
[1849] DMA: Council gives final approval to new rules for fair competition online, European Council (Brussels) 18 July 2022. Access Date: 6 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/07/18/dma-council-gives-final-approval-to-new-rules-for-fair-competition-online/
[1850] DSA: Council gives final approval to the protection of users' rights online, Council of the European Union and the European Council (Brussels) 4 October 2022. Access Date: 6 January 2023. https://www.consilium.europa.eu/en/press-releases/2022/10/04/dsa-council-gives-final-approval-to-the-protection-of-users-rights-online/
[1851] Digital finance: Council adopts Digital Operational Resilience Act, European Council (Brussels) 28 November 2022. Access Date: 6 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/
[1852] EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation, European Council (Brussels) 28 November 2022. Access Date: 7 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/
[1853] Pairing up Cybersecurity and Data Protection efforts: EDPS and ENISA sign Memorandum of Understanding, European Data Protection Supervisor (Brussels) 30 November 2022. Access Date: 7 January 2023. https://edps.europa.eu/press-publications/press-news/press-releases/2022/pairing-cybersecurity-and-data-protection-efforts-edps-and-enisa-sign-memorandum-understanding_en
[1854] Declaration on digital rights and principles: EU values and citizens at the centre of digital transformation, European Council (Brussels) 15 December 2022. Access Date: 7 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/12/15/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation/

put "people at the centre of digital transformation" by ensuring connectivity, digital literacy and increasing cyber safety and security.[1855]

The European Union has fully complied with its commitment to empower citizens, especially vulnerable groups to use the Internet and digital technologies safely and securely. The EU has played an important role in successfully creating legislation to protect and empower citizens in the digital economy. The EU is also taking a proactive approach to the digital transition by creating policies and programmes to ensure that digital technologies can be used safely and securely.

Thus, the European Union receives a score of +1.

Analyst: Michael Lecchino

[1855] Declaration on digital rights and principles: EU values and citizens at the centre of digital transformation, European Council (Brussels) 15 December 2022. Access Date: 7 January 2023. https://www.consilium.europa.eu/en/press/press-releases/2022/12/15/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation/