G7 RESEARCH GROUP

www.g7.utoronto.ca

2023 G7 Hiroshima Summit Interim Compliance Report

22 May 2023 to 3 December 2023

Prepared by
Samraggi Hazra and Ambra Bisagni
and the G7 Research Group
19 February 2024
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

16. Digital Economy: Digital Ecosystem with Trust

"We seek to increase trust across our digital ecosystem and to counter the influence of authoritarian approaches."

G7 Hiroshima Leaders' Communiqué

Assessment

	No Compliance	Partial Compliance	Full Compliance
Canada			+1
France			+1
Germany			+1
Italy		0	
Japan			+1
United Kingdom			+1
United States			+1
European Union			+1
Average	+0.88 (94%)		

Background

The G7 recognizes the role that digitalization has in economic growth and social well-being.[2187] As such, G7 members stress the importance of developing and implementing frameworks that focus on data privacy, intellectual property rights protection, and the strengthening of democratic principles to combat authoritarian practices such as mass surveillance and network restrictions. At the same time, G7 members remain committed to improving internet governance to ensure that cyberspaces remain free, secure, and global. The G7 also calls for the responsible use of new technologies including artificial intelligence (AI) and endorses international cooperation to regulate its use with policies that are centred on human rights and democratic values. Although the topic of the digital economy is relatively new, the rise of new technologies and the concern for users' security and privacy has become increasingly relevant. Thus, discussions on tackling computer and telecommunications crimes, protecting personal data, and countering interference in information and communication technologies by state and non-state actors have been recurring themes on the G7's agenda.

At the 1997 Denver Summit, G8 leaders committed to investigate, prosecute, and punish technology criminals who interfere with computers and telecommunications technology regardless of their location.[2188]

At the 2000 Okinawa Summit, G8 leaders reaffirmed their concern for cyber-crime and welcomed the results provided by the Government/Industry Dialogue on Safety and Confidence in Cyberspace in Paris.[2189]

At the 2001 Genoa Summit, G8 leaders committed to keep fighting against transnational organized crime, including cyber-crime and online child pornography.[2190]

At the 2011 Deauville Summit, G8 leaders called partners to fight against the use of the internet for purposes of child trafficking and their sexual exploitation.[2191] Leaders also committed to guarantee effective actions

[2187] Ministerial Declaration: The G7 Digital and Tech Ministers' Meeting, G7 Information Centre (Toronto) 30 April 2023. Access Date: 05 October 2023. http://www.g7.utoronto.ca/ict/2023-declaration.html

[2188] Denver Summit of the Eight Communiqué, G7 Information Centre (Toronto) 22 June 1997. Access Date: 27 September 2023. http://www.g7.utoronto.ca/summit/1997denver/g8final.htm

[2189] G8 Communiqué Okinawa 2000, G7 Information Centre (Toronto) 23 July 2000. Access Date: 27 September 2023. http://www.g7.utoronto.ca/summit/2000okinawa/finalcom.htm

[2190] Communiqué, G7 Information Centre (Toronto) 22 July 2001. Access Date: 27 September 2023. http://www.g7.utoronto.ca/summit/2001genoa/finalcommunique.html

[2191] G8 Declaration: Renewed Commitment for Freedom and Democracy, G7 Information Centre (Toronto) 27 May 2011. Access Date: 27 September 2023. http://www.g7.utoronto.ca/summit/2011deauville/2011-declaration-en.html#internet against intellectual property rights violations in the digital realm. Leaders recognized that effective protection of personal data and privacy on the Internet is key to ensure users' trust. Leaders called for cooperation between governments, regional and international organizations, the private sector, civil society and the G8 to fight against the use of information and communications technologies (ICTs) for terrorism and criminal activities. Finally, leaders also encouraged international action to reinforce patent quality and improve the distribution of patent information while calling for transparency in technology markets.

At the 2015 Elmau Summit, G7 leaders recognized the importance of implementing mechanisms to detect and prevent terrorism and violent extremism, as well as the increase of hatred and intolerance including through the internet.[2192] Leaders also committed to ensure the protection of intellectual property rights.

At the 2016 Ise-Shima Summit, G7 leaders committed to support accessible, reliable, and secure cyberspaces to promote economic growth and prosperity.[2193] Leaders also committed to implement mechanisms to combat the malicious use of cyberspace by state and non-state actors. Leaders stated that no country should conduct or support theft of intellectual property facilitated by ICTs with the aim of increasing their companies competitive advantages. Leaders reaffirmed their support for the free flow of information to ensure transparency and internet freedom, while promoting privacy, data protection, and cyber security. Finally, leaders also committed to protect and promote human rights online, emphasizing the importance of full and active participation of governments, the private sector, civil society, the technical community, and international organizations in Internet governance.

At the 2018 Charlevoix Summit, G7 leaders committed to cooperate in enforcing new and already existing international rules to tackle the inadequate protection of intellectual property rights, including forced technology transfer and cyber-enabled theft.[2194] Leaders also committed to address the use of the internet for terrorism, including as a tool for recruitment, training, propaganda and financing. At the same time, leaders called for cooperation with the Global Internet Forum to Counter Terrorism.

At the 2019 Biarritz Summit, G7 leaders addressed the importance of reinforcing democracies against malicious behaviors and foreign hostile intervention by state and non-state actors.[2195] Leaders thereby committed to undertake threats to cybersecurity, strategic communications and counter-intelligence. Leaders also noted the efforts made towards ensuring an open, free and secure internet, while working to tackle terrorist propaganda. Leaders recognized the need for action against threats fostered by security vulnerabilities in 5G networks and supply chains. Finally, leaders acknowledged the importance of supporting the responsible development of AI.

At the 2021 Cornwall Summit, G7 leaders committed to maintain an open, interoperable, reliable and secure internet.[2196] Leaders also affirmed their disapproval of measures that weaken the G7's shared democratic values, namely government-imposed internet shutdowns and network restrictions. Finally, leaders endorsed the use of the Digital Ministers' Internet Safety Principles to improve online safety, including tackling hate speech and protecting human rights and freedom of expression.

[2192] Leaders' Declaration: G7 Summit, G7 Information Centre (Toronto) 08 June 2015. Access Date: 27 September 2023. http://www.g7.utoronto.ca/summit/2015elmau/2015-G7-declaration-en.html

[2193] G7 Ise-Shima Leaders' Declaration, G7 Information Centre (Toronto) 27 May 2016. Access Date: 27 September 2023. http://www.g7.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html

[2194] The Charlevoix G7 Summit Communiqué, G7 Information Centre (Toronto) 09 June 2018. Access Date: 28 September 2023. http://www.g7.utoronto.ca/summit/2018charlevoix/communique.html

[2195] Biarritz Strategy for an Open, Free and Secure Digital Transformation, G7 Information Centre (Toronto) 26 August 2019. Access Date: 28 September 2023. http://www.g7.utoronto.ca/summit/2019biarritz/biarritz-strategy-for-digital-transformation.html

[2196] Carbis Bay G7 Summit Communiqué: Our Shared Agenda for Global Action to Build Back Better, G7 Information Centre (Toronto) 13 June 2021. Access Date: 28 September 2023. http://www.g7.utoronto.ca/summit/2021cornwall/210613-communique.html

At the 2022 Elmau Summit, G7 leaders committed to create an inclusive and global digital ecosystem that promotes an open, free and secure Internet, protecting privacy and personal data.[2197] Leaders also welcomed the Declaration for the Future of the Internet, calling for partners to fight against digital authoritarianism. Finally, leaders affirmed their efforts towards the strengthening of cyber defenses, cooperating to improve cyberspace security against malicious uses from state and non-state actors.

Commitment Features

At the 2023 Hiroshima Summit, leaders committed to "seek to increase trust across our digital ecosystem and to counter the influence of authoritarian approaches."[2198] This commitment has two main components for assessment to first improve confidence in digital technology, such as by addressing cyber-crimes and the protection of personal data. The second component is to fight against limitations and restrictions against transparency and Internet freedoms, such as internet shutdowns, censorship, and mass-surveillance.

"Increase" is understood to mean furthering the efforts to a previous commitment.[2199] The interpretation does not include new and unique efforts and initiatives.

"Trust" is understood to mean the sense that another person or institution is secure, dependable and accurate.[2200] In the context of the commitment, it refers to the belief that the use of digital technology will reasonably not lead to any harm or attacks, nor will it be restricted and factually false.

"Digital ecosystem" is understood to mean the network of digital platforms and users that interact through the Internet through the exchange of services, communication and content.[2201] Examples include e-commerce and social media.

"Influence" is understood to mean the ability or impact to affect and change individuals, decisions, or outcomes.[2202]

"Counter" is understood to mean to respond to something in the converse direction, with aims of clashing, differing, and contrasting.[2203] In the context of the commitment, it refers to responding to authoritarian controls on the digital ecosystem.

"Authoritarian approaches" is understood to mean the restriction of freedoms on the Internet, such as the limitation of privacy and accurate information.[2204] Examples of digital authoritarian tools include censorship, surveillance, misinformation, internet shutdowns, biometric tracking tools, as well as arresting protestors.

Full compliance, or a score of +1, will be given to G7 members who demonstrate strong action in both dimensions of the commitment. Actions in both elements of the commitment can include both domestic and international actions.

[2197] G7 Leaders' Communiqué, G7 Information Centre (Toronto) 28 June 2022. Access Date: 28 September 2023. http://www.g7.utoronto.ca/summit/2022elmau/220628-communique.html

[2198] G7 Leaders' Communiqué, G7 Information Centre (Toronto) 20 May 2023. Access Date: 29 September 2023. http://www.g7.utoronto.ca/summit/2023hiroshima/230520-communique.html

[2199] Compliance Coding Manual for International Institutional Commitments, Global Governance Program (Toronto) 12 November 2020. Access Date: 6 October 2023. https://www.g7.utoronto.ca/compliance/Compliance_Coding_Manual_2020.pdf

[2200] Trust, Cambridge Dictionary (Cambridge) n.d. Access Date: 29 September 2023. https://dictionary.cambridge.org/dictionary/english/trust

[2201] Digital Platforms and Global Value Chains, World Trade Organization (Geneva) 2021. Access Date: 29 September 2023. https://www.wto.org/english/res_e/booksp_e/09_gvc_ch6_dev_report_2021_e.pdf

[2202] Influence, Cambridge Dictionary (Cambridge) n.d. Access Date: 8 October 2023. https://dictionary.cambridge.org/dictionary/english/influence

[2203] Counter, Cambridge Dictionary (Cambridge) n.d. Access Date: 29 September 2023. https://dictionary.cambridge.org/dictionary/english/counter

[2204] 8. Case study; Digital Citizenship or Digital Authoritarianism, OECD iLibrary (Paris, France) 2021. Access Date: 6 October 2023. https://www.oecd-ilibrary.org/sites/1b3dc767-en/index.html?itemId=/content/component/1b3dc767-en

Examples of strong actions to increase trust domestically include but are not limited to: enforcing policies to penalize digital actors infringing democratic guidelines and cracking down on malicious or criminal behaviour digitally. International examples of strong actions include initiating education for individuals on data protection and cybersecurity; leading discussions on data protection issues through meetings and international organizations; advancing international initiatives to clamp down on international cyber-crime; and through partnering with countries to research and improve regulation as new technology emerges.

For the second pillar of countering authoritarian influences domestically, examples of strong actions include but are not limited to increasing funding to improve individuals' access to free and fair information, protecting access to services within the digital ecosystem, and increasing regulation of privacy infringement. International actions may include actively identifying countries that fail to comply with democratic principles around technology and sanctioning these countries to disincentivize authoritarian approaches.

Partial compliance, or a score of 0, will be assigned to G7 members who demonstrate strong action in one of the target dimensions while demonstrating weak or no action in the other dimension or some action in both areas. Weak actions can include both domestic and international actions. Examples of weak actions include but are not limited to attending meetings on addressing cybercrime or insufficient data protection; verbally condemning actors that have committed cybercrime, data privacy infringements, or digital authoritarianism; and verbally committing towards increasing trust in the digital ecosystem.

Non-compliance, or a score of −1, will be assigned if the G7 member demonstrates weak action in one dimensions, fails to demonstrate an action in either dimension, or takes action that is directly antithetical to the commitment.

Scoring Guidelines

−1	The G7 member has not taken any action to increase trust across digital ecosystems or counter the influence of authoritarian approaches.
0	The G7 member has taken strong action either to increase trust across digital ecosystems or to counter the influence of authoritarian approaches or has taken weak action in both increasing trust across digital ecosystems and countering the influence of authoritarians approaches
+1	The G7 member has taken strong action to increase trust across digital ecosystems and to counter the influence of authoritarian approaches.

Compliance Director: Eliza Yip
Lead Analyst: Anali Arambula Galindo

Canada: +1

Canada has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches.

On 31 May 2023, Government of Canada announced the Canadian Program for Cyber Security Certification for cyber security certification that will result in mandatory certification requirements in select federal defense contracts.[2205] The primary objective of the Canadian Program for Cyber Security Certification is to safeguard the Government of Canada's unclassified contractual information held on defense suppliers' networks, systems, and applications against cyber threats and to reinforce the goals of Canada's National Cyber Security Action Plan and National Cyber Security Strategy. It is set to take effect in 2024.

On 22 June 2023, Government of Canada implemented Bill-C18, also known as the Online News Act.[2206] The Act presents a framework requiring social media platforms to develop agreements with Canadian news sites to

[2205] Government of Canada helping defence industry protect itself from cyber security threats, the Government of Canada (Ottawa) 31 May 2023. Access Date: 03 November 2023. https://www.canada.ca/en/public-services-procurement/news/2023/05/government-of-canada-helping-defence-industry-protect-itself-from-cyber-security-threats.html

[2206] Building a bargaining framework for the Online News Act, the Government of Canada (Ottawa) 22 June 2023. Access Date: 30 October 2023. https://crtc.gc.ca/eng/industr/info.html provide them with compensation for sharing their journalistic content that appears on their platforms; while the Act emphasizes protecting the revenue of national and local Canadian news agencies, it also stated its intent to promote news content of "public interest."[2207]

On 22 September 2023, Canadian delegates met with representatives from the North Atlantic Treaty Organization.[2208] A joint statement was released following the meeting that encouraged continued cooperation in the cyber domain, especially regarding building cyber capabilities.

On 27 September 2023, Minister of Innovation, Science and Industry François-Philippe Champagne announced the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems, effective immediately.[2209] The managers and developers choosing to uphold the code commit to achieving outcomes of accountability, safety, fairness and equity, transparency, human oversight and monitoring, and validity and robustness for advanced generative systems.

On 1 October 2023, the Government of Canada announced its annual Cyber Security Awareness Month, also known as Cyber Month.[2210] Cyber Month is a part of Canada's larger Get Cyber Safe national public awareness campaign created to inform Canadians about cyber security and protection measures individuals can implement.

On 27 November 2023, the Treasury Board of Canadian Secretariat published the Government of Canada Cyber Security Event Management Plan.[2211] This plan is an operational framework for the management of cyber security events, including cyber threats, vulnerabilities, or security incidents, that impact or threaten to impact the government's ability to deliver programs and services to Canadians.

Canada has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches. Canada has demonstrated active willingness to increase national cybersecurity awareness, thus decreasing the likelihood of cyber threats, and to invest in investigating new digital technologies. Canada has also taken actions to ensure transparency, safety, equity, fairness, and accountability to protect citizens and democratic norms.

Thus, Canada receives a score of +1.

Analyst: Anna Lysenko

France: +1

France has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches.

On 16 June 2023, the Ministry of the Economy, Finance, and of Digital and Industrial Sovereignty, as part of the strategy for cyber security under the international investment France 2030 plan, renewed a third cycle of

[2207] Bill C-18, Parliament of Canada (Ottawa) 22 June 2023. Access Date: 30 October 2023. https://www.parl.ca/DocumentViewer/en/44-1/bill/C-18/royal-assent

[2208] The European Union and NATO intensify cooperation on addressing cyber threats, the European Commission (Brussels) 22 September 2023. Access Date: 03 November 2023. https://digital-strategy.ec.europa.eu/en/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats

[2209] Minister Champagne Launches Voluntary Code of Conduct Relating to Advanced Generative AI Systems, the Government of Canada (Ottawa) 27 September 2023. Access Date: 31 October 2023. https://www.canada.ca/en/innovation-science-economic-development/news/2023/09/minister-champagne-launches-voluntary-code-of-conduct-relating-to-advanced-generative-ai-systems.html

[2210] October Is Cyber Security Awareness Month in Canada, the Government of Canada (Ottawa) 20 July 2023. Access Date: 02 November 2023. https://www.getcybersafe.gc.ca/en/cyber-security-awareness-month

[2211] Government of Canada Cyber Security Event Management Plan (GC CSEMP), the Government of Canada (Ottawa) 27 November 2023. Access Date: 2 December 2023. https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html calls for project proposals.[2212] This initiative supports the development of crucial and innovative technological building blocks.

On 11 July 2023, Minister of Higher Education and Research Sylvie Retailleau and Minister Barrot launched the Networks of the Future research program, and the France 6G campaign.[2213] The research program will be supported by EUR65 million in funding from the France 2030 investment plan.

On 25 August 2023, the French Presidency of the Council of the European Union adopted the Digital Services Act.[2214] The Act will promote the safety of European internet users from illegal, dangerous, and harmful content by regulating the activities of major platforms, such as Amazon, Google, Instagram, and LinkedIn.

On 22 September 2023, French delegates met with representatives from the North Atlantic Treaty Organization.[2215] A joint statement was released following the meeting that encouraged continued cooperation in the cyber domain, especially regarding building cyber capabilities.

On 4 October 2023, the eNSEMBLE (Future of Digital Collaboration) was unveiled as part of the Priority Research Program and Equipment.[2216] The program will be funded as part of the France 2030 investment plan to reduce digital divides, increase innovation and accessibility, and integrate artificial intelligence to advance daily activities. The program also has EUR38.25 million distributed across more than 60 labs and participating teams.

France has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches. On both fronts, France has taken strong actions in increasing trust, as seen in its initiatives that are researching and preparing for 6G technology, researching cybersecurity, reducing inequality, increasing accessibility and advancing technology for everyday life. As well, its commitment to countering the influence of disinformation and campaigns of the like, is seen through the Digital Services Act.

Thus, France receives a score of +1.

Analyst: Lesley Isaro

Germany: +1

Germany has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches.

On 4 August 2023, the Federal Ministry for Digital and Transport published the draft of the "Digitale Dienste Gesetz (DDG)," a supplement to the EU's Digital Services Act (DSA), and welcomed comments and feedback

[2212] Cybersécurité : un appel à projets pour soutenir le développement de briques technologiques critiques, Ministère de l'Économie des Finances et de la Souveraineté industrielle et numérique (Paris) 16 June 2023. Translation provided by Google Translate. Access Date: 28 October 2023. https://www.economie.gouv.fr/cybersecurite-appel-projets-soutien_developpement-briques-technologiques-critiques

[2213] Numérique: lancement du programme de recherche «Réseaux du futur» et de la plateforme «France 6G», Ministère de l'Économie des Finances et de la Souveraineté industrielle et numérique (Paris) 11 July 2023. Translation provided by Google Translate. Access Date: 28 October 2023. https://www.economie.gouv.fr/numerique-lancement-programme-recherche-reseaux-futur-plateforme-france-6g

[2214] Numérique: le règlement sur les services numériques entre en vigueur, Ministère de l'Économie des Finances et de la Souveraineté industrielle et numérique (Paris) 28 August 2023. Translation provided by Google Translate. Access Date: 28 October 2023. https://www.economie.gouv.fr/numerique-dsa-entre-en-vigueur

[2215] The European Union and NATO intensify cooperation on addressing cyber threats, the European Commission (Brussels) 22 September 2023. Access Date: 03 November 2023. https://digital-strategy.ec.europa.eu/en/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats

[2216] eNSEMBLE, le PEPR qui dessine le futur de la collaboration numérique, Ministère de l'Enseignement supérieur et de la Recherche (Paris) 4 October 2023. Translation provided by Google Translate. Access Date: 28 October 2023. https://www.enseignementsup-recherche.gouv.fr/fr/pepr-ensemble-le-futur-de-la-collaboration-numerique from the public.[2217] The draft outlines fines and penalties regarding violations of the EU's DSA, and requires services providers to take precaution against illegal content. According to the draft proposal, the Federal Network Agency will act as a central coordinator.

On 31 August 2023, the Federal Ministry for Digital and Transport and the Indonesian Ministry of Communication and Information Technology jointly hosted the Indonesian-German Digital Dialogue.[2218] The countries discussed their national digital strategies. The aim of these dialogues is to foster digital and connected societies, and to engage in best-practices sharing to tackle issues regarding data protection. Following, on 26 September 2023, both countries jointly hosted a virtual event with relevant stakeholders to exchange data protection policies.[2219]

On 22 September 2023, German delegates met with representatives from the North Atlantic Treaty Organization.[2220] A joint statement was released following the meeting that encouraged continued cooperation in the cyber domain, especially regarding building cyber capabilities.

On 8 October 2023, the Federal Foreign Office and the Federal Ministry for Digital and Transport attended the Internet Governance Forum (IGF) in Kyoto, Japan, under the theme: "Internet We Want – Empowering All People."[2221] This year's IGF featured eight pillars, including artificial intelligence and emerging technologies, avoiding internet fragmentation, cybersecurity, cybercrime and online safety, data governance and trust, digital divides and inclusion, and global digital governance and cooperation.

On 10 October 2023, the Federal Cartel Office, the Bundeskartellamt, ruled that Google's parent company, Alphabet, must provide service users the option to decide how their personal data is collected and utilized across its various digital services.[2222] Specifically, it ruled that Google must "provide its users with the possibility to give free, specific, informed and unambiguous consent to the processing of their data across services." This decision aligns Germany with the European Union's Digital Markets Act.

Germany has fully complied with the commitment to increase trust across our digital ecosystem and to counter the influence of authoritarian approaches. Germany has taken action to formalize and align its legislation with wider EU-regulations and laws. Germany has also participated in multilateral workshops to share best practices regarding data security in order to increase trust in the digital ecosystem.

Thus, Germany receives a score of +1.

Analyst: Grace Ho Lan Chong

[2217] BMDV legt Entwurf für ein Digitale-Dienste-Gesetz vor, Bundesministerium für Digitales und Verkehr (Berlin) 04 August 2023. Access Date: 30 October 2023. https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2023/079-wissing-digitale-dienste-gesetz.html https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2023/079-wissing-digitale-dienste-gesetz.html

[2218] Exchange on national digital strategies of Indonesia and Germany, International Digital Dialogues of the German Federal Ministry for Digital and Transport (Berlin) 06 September 2023. Access Date: 01 November 2023. https://digital-dialogues.net/en/news-details/exchange-on-national-digital-strategies-of-indonesia-and-germany

[2219] Exchange on data protection policies of Indonesia and Germany, International Digital Dialogues of the German Federal Ministry for Digital and Transport (Berlin) 26 September 2023. Access Date: 05 November 2023. https://digital-dialogues.net/en/events/details/exchange-on-data-protection-policies-of-indonesia-and-germany

[2220] The European Union and NATO intensify cooperation on addressing cyber threats, the European Commission (Brussels) 22 September 2023. Access Date: 03 November 2023. https://digital-strategy.ec.europa.eu/en/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats

[2221] 18th annual meeting, Internet Governance Forum (Geneva). 12 October, 2023. Access Date: 02 November, 2023. https://www.intgovforum.org/en/content/igf-2023

[2222] Bundeskartellamt gives users of Google services better control over their data, Bundeskartellamt (Bonn) 05 October 2023. Access Date: 03 November 2023. https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/05_10_2023_Google_Data.html

Italy: 0

Italy has partially complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches.

On 14 July 2023, Undersecretary to the Presidency of the Council of Ministers Alessio Butti committed to the "Together for digital transformation" initiative.[2223] In partnership with Italy's regions and autonomous provinces, the partnership is focusing on integrating digitization with the development of the regions by 2026. More specifically, this agreement includes sharing knowledge, collaborating on digital strategies, standardizing technology and modernizing government infrastructure.

On 24 July 2023, the Department for Digital Transformation of the Presidency of the Council committed EUR5 million to the "Digital Twin for Innovative Air Service" initiative, in partnership with the National Civil Aviation Board.[2224] This initiative will use technology to research the safety and possibilities of automated aviation in urban and rural environments.

On 27 July 2023, Undersecretary Butti met with the President of the Italian Football Federation, Gabriele Gravina to discuss the integration of artificial intelligence to achieve readily accessible and secure health documents.[2225]

On 22 September 2023, the Department for Digital Transformation established a memorandum of understanding (MoU) with telecom industry partners, as part of the "Ultrafast and 5GNetworks" of the National Recovery and Resilience Plan.[2226] The MoU prioritizes greater collaboration between the government and industry, ensures a timely and standardized implementation of 5G and increases connectivity throughout the country by 2026.

On 22 September 2023, Italian delegates met with representatives from the North Atlantic Treaty Organization.[2227] A joint statement was released following the meeting that encouraged continued cooperation in the cyber domain, especially regarding building cyber capabilities.

On 13 October 2023, Italy successfully campaigned for Luca Tagliaretti to become the first Executive Director of the European Competence Center on Cyber-security as part of Italy's priority to be a leader in cyber-security.[2228]

[2223] Governo e Conferenza delle Regioni e delle Province autonome insieme per la trasformazione digitale, Dipartimento per la trasformazione digitale (Rome) 14 July 2023. Translation provided by Google Translate. Access Date: 16 November 2023. https://innovazione.gov.it/notizie/comunicati-stampa/governo-e-conferenza-delle-regioni-e-delle-province-autonome-insieme-per-la-trasf/

[2224] Al via il progetto del Dipartimento ed ENAC per la mobilità aerea avanzata, Dipartimento per la trasformazione digitale (Rome) 24 July 2023. Translation provided by Google Translate. Access Date: 16 November 2023. https://innovazione.gov.it/notizie/comunicati-stampa/al-via-il-progetto-del-dipartimento-ed-enac-per-la-mobilita-aerea-avanzata/

[2225] Il Sottosegretario Butti incontra il Presidente FIGC Gravina, Dipartimento per la trasformazione digitale (Rome) 27 July 2023. Translation provided by Google Translate. Access Date: 16 November 2023. https://innovazione.gov.it/notizie/comunicati-stampa/il-sottosegretario-butti-incontra-il-presidente-figc-gravina/

[2226] Reti ultraveloci e 5G, intesa con ANCI e operatori Tlc per rafforzare la connettività, Dipartimento per la trasformazione digitale (Rome) 22 September 2023. Translation provided by Google Translate. Access Date: 16 November 2023. https://innovazione.gov.it/notizie/comunicati-stampa/reti-ultraveloci-e-5g-intesa-con-anci-e-operatori-tlc-per-rafforzare-la-connettiv/

[2227] The European Union and NATO intensify cooperation on addressing cyber threats, the European Commission (Brussels) 22 September 2023. Access Date: 03 November 2023. https://digital-strategy.ec.europa.eu/en/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats

[2228] Nomina del Dott. Luca Tagliaretti a Direttore Esecutivo del Centro europeo di competenza sulla cyber-sicurezza, Ministero degli Affari Esteri e della Cooperazione Internazionale (Rome) 13 October 2023. Translation provided by Google Translate. Access Date: 16 November 2023. https://www.esteri.it/it/sala_stampa/archivionotizie/comunicati/2023/10/nomina-del-dott-luca-tagliaretti-a-direttore-esecutivo-del-centro-europeo-di-competenza-sulla-cyber-sicurezza/

On 20 October 2023, Deputy Minister for Development Cooperation Edmondo Cirielli affirmed Italy's commitment towards collaborating with African countries on developing strong digital ecosystems in his keynote address.[2229]

On 28 November 2023, Prime Minister Giorgia Meloni chaired a meeting for the Inter-ministerial Committee for Cybersecurity.[2230] The Committee focused on the increase in cyberattacks, particularly on institutional websites, following the geopolitical conflicts in Ukraine and the Middle East.

On 30 November 2023, the Department for Digital Transformation and the Union of Provinces of Italy signed a memorandum of understanding to provide further guidelines on how the government would implement further development of digital skills in the economy.[2231]

Italy has partially complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches. Italy has taken strong action in increasing trust across the digital ecosystem, ranging from actions in increasing research on the safety of automated aviation, developing accessible and secure health records, taking a regional leadership role and standardizing the roll-out of 5G networks. That being said, Italy has not taken action in combating authoritarianism.

Thus, Italy receives a score of 0.

Analyst: Zekai Zhu

Japan: +1

Japan has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches.

On 29 May 2023, the Personal Information Protection Commission (PPC) of Japan hosted its annual Privacy Awareness Week.[2232] This is an initiative started by the Asia Pacific Privacy Authorities (APPA) in 2006, and aims to raise awareness on the importance of digital privacy and protecting personal data. As a member of the APPA since 2016, the theme of Japan's Privacy Awareness Week this year was "Back to Basics – Privacy Foundations," and featured awareness campaigns for businesses, families, and individuals on privacy protection.

On 3 July 2023, the Japan-EU Digital Partnership Council held its first meeting in Tokyo.[2233] Minister for Digital Transformation Taro Kono, Minister for Internal Affairs and Communications Takeaki Matsumoto, and State Minister of Economy, Trade and Industry Fusae Ota represented Japan on the Council. They discussed the development of 6G technology, expansion of generative AI, and cross-border data and protection. Both parties committed to establishing a permanent communication channel to provide regular

[2229] Il Vice Ministro degli Esteri On.Cirielli apre il seminario "Rafforzare gli Ecosistemi Digitali Locali in Africa," Ministero degli Affari Esteri e della Cooperazione Internazionale (Rome) 22 October 2023. Translation provided by Google Translate. Access Date: 16 November 2023. https://www.esteri.it/it/sala_stampa/archivionotizie/comunicati/2023/10/il-vice-ministro-degli-esteri-on-cirielli-apre-il-seminario-rafforzare-gli-ecosistemi-digitali-locali-in-africa/

[2230] Meeting of the Interministerial Committee for Cybersecurity, Presidency of the Council of Ministers (Rome) 28 November 2023. Access Date: 22 December 2023. https://www.governo.it/en/articolo/meeting-interministerial-committee-cybersecurity/24456

[2231] Governo e Province, firmato l'accordo per la trasformazione digitale del Paese, Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri (Rome) 30 November 2023. Translation provided by Google Translate. Access Date: 01 December 2023. https://innovazione.gov.it/notizie/articoli/governo-e-province-firmato-l-accordo-per-la-trasformazione-digitale-del-paese/

[2232] Privacy Awareness Week 2023 (29th May-4th June), Personal Information Protection Commission Japan (PPC) (Tokyo) 29 May 2023. Access Date: 25 October, 2023. https://www.ppc.go.jp/en/aboutus/roles/international/conferences/PAW2023e/

[2233] Japan – EU Joint Statement of the first meeting of the Japan – EU Digital Partnership Council, Ministry of Economy, Trade, and Industry (Tokyo) 03 July 3 2023. Access Date: 30 October 2023. https://www.meti.go.jp/press/2023/07/20230703003/20230703003-4.pdf updates on legislative and non-legislative frameworks with regards to AI, and reaffirmed the importance of the strong data protection rules. They both demonstrated their support for the establishment of an Institutional Arrangement for a Partnership (IAP) to operationalize DFFT.

On 10 August 2023, Japan became the second state to ratify the Second Additional Protocol to the Cybercrime Convention.[2234] The treaty aims to provide more effective steps for international cooperation and evidence sharing across borders regarding cybercrime.

On 14 September 2023, Ambassador Hideo Ishizuki, Ambassador in charge of Cyber Policy and Deputy Director General of Foreign Policy Bureau, and Ministry of Foreign Affairs of Japan, led the Japanese delegation for the Fifth Japan-India Cyber Dialogue.[2235] Both parties discussed national cyber policies and security strategies, along with 5G and Open Radio Access Network (RAN) technology developments. Both sides also explored opportunities for bilateral cooperation in capacity building, particularly under the United Nations and the Quadrilateral meeting of Japan, Australia, India and the US.

On 3 October 2023, the Cabinet Secretariat, the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry hosted the 16th meeting of the Association of Southeast Asian Nations and Japan on cyber security policy.[2236] At this year's meeting, parties exchanged practices regarding cybersecurity policies, and reaffirmed collaboration activities for the upcoming year. These practices include joint awareness raising, multi-stakeholder partnerships, and cyber-exercises.

On 8 October 2023, Japan hosted the Internet Governance Forum (IGF) under the theme of "Internet We Want – Empowering All People." This year's IGF featured eight pillars, including AI and emerging technologies, avoiding internet fragmentation, cybersecurity, cybercrime and online safety, data governance and trust, digital divides and inclusion, and global digital governance and cooperation.

On 9 October 2023, Japan co-hosted the Japan-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region.[2237] This week-long training session featured hands-on training with industry experts in AI and cybersecurity, and seminars on four key topics: awareness of issues and initiatives by government officials in each region; standardization; incident response; and supply chain risk management.

On 2 November 2023, the National Diet established a supra-partisan group to develop and propose policies regarding the protection of freedom of speech on the internet whilst ensuring people's privacy.[2238]

On 6 November 2023, Japan, South Korea, and the US announced that they would establish a high-level consultative group to address North Korean cyberattacks, and other cyber and emerging technology issues.[2239] The trilateral group had previously agreed to set up a group after an August summit at Camp David in the United States.

[2234] Japan becomes 2nd state to ratify the Second Additional Protocol to the Convention on Cybercrime, Council of Europe (Strasbourg) 10 August 2023. Access Date: 31 October 2023. https://www.coe.int/en/web/cybercrime/-/japan-becomes-2nd-state-to-ratify-the-second-additional-protocol-to-the-convention-on-cybercrime

[2235] Fifth Japan-India Cyber Dialogue, Ministry of Foreign Affairs Japan (Tokyo) 15 September 2023. Access Date: 01 November 2023. https://www.mofa.go.jp/press/release/press4e_003297.html

[2236] Outcomes of the 16th ASEAN-Japan Cybersecurity Policy Meeting, Ministry of Economy, Trade and Industry (Tokyo). 06 October 2023. Access Date: 03 November 2023. https://www.meti.go.jp/english/press/2022/1006_002.html

[2237] Japan-US-EU Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region, European Commission (Brussels) 15 October 2023. Access Date: 03 November 2023. https://digital-strategy.ec.europa.eu/en/library/japan-us-eu-industrial-control-systems-cybersecurity-week-indo-pacific-region#

[2238] Japan Diet Members Launch Group to Consider Internet Privacy Policy, the Japan News (Tokyo). 03 November, 2023. Access Date: 02 December, 2023. https://www.de.digital/DIGITAL/Redaktion/EN/Dossier/digital-summit.html

[2239] US, South Korea, Japan to launch consultative group on North's cyber threats, Reuters (Seoul). 06 November, 2023. Access Date: 01 December, 2023. https://www.reuters.com/technology/us-south-korea-japan-launch-consultative-group-norths-cyber-threats-2023-11-06/

On 14 November 2023, Japan and the US held the second ministerial meeting of the Japan-US Economic Policy Consultative Committee.[2240] One of the key pillars of this continued bilateral diplomacy is personal data protection and privacy. Both parties expressed continued commitment towards facilitating cross-border data flows and effective data and privacy protections globally. To demonstrate this commitment, both parties expressed their interest in the expansion and promotion of the Global Cross-Border Privacy Rules Forum and Global Privacy Recognition for Processors Systems. Japan and the US also stated plans to uphold and promote the Organisation for Co-operation and Economic Development's Declaration on Government Access to Personal Data Held by Private Sector Entities.[2241]

On 21 November 2023, the first Cyber Dialogue between Japan and the North Atlantic Treaty Organization took place in Brussels, Belgium. Both parties committed to strong working relations in the field of digital technology.[2242]

Japan has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches. Japan has taken action to improve confidence in digital technology by hosting awareness campaigns and taking steps to implement the DFFT. Japan has also increased bilateral and multilateral collaborations to exchange cyber-exercises, hands-on training and discussions on the latest technology like Open RAN and 6G. As for countering authoritarian influences, Japan has taken strong action to support international cooperation, information sharing, the free flow of data and data protection.

Thus, Japan receives a score of +1.

Analyst: Grace Ho Lan Chong

United Kingdom: +1

The United Kingdom has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches.

On 28 June 2023, the United Kingdom and Singapore signed a joint agreement on boosting the technology for trade and security.[2243] Deputy Prime Minister Oliver Dowden signed the agreement, containing clauses with the goals of discussing data regulation, protection, and the international transfer of data. Additionally, the two nations agreed to share best practices on data management in the government.

On 7 September 2023, the United Kingdom, in a joint operation with the United States, sanctioned 11 members of a cyber-criminal gang found responsible for a chain of ransomware attacks.[2244] The goal of the sanctions is to disrupt ransomware attacks and expose the people implementing them.

On 22 September 2023, delegates from the United Kingdom met with representatives from the North Atlantic Treaty Organization.[2245] A joint statement was released following the meeting that encouraged continued cooperation in the cyber domain, especially regarding building cyber capabilities.

[2240] Joint Statement of the Japan-U.S. Economic Policy Consultative Committee, US Department of Commerce (Washington, D.C). 14 November, 2023. Access Date: 01 December, 2023. https://www.commerce.gov/news/press-releases/2023/11/joint-statement-japan-us-economic-policy-consultative-committee

[2241] Joint Statement of the Japan-U.S. Economic Policy Consultative Committee, US Department of Commerce (Washington, D.C). 14 November, 2023. Access Date: 01 December, 2023. https://www.commerce.gov/news/press-releases/2023/11/joint-statement-japan-us-economic-policy-consultative-committee

[2242] The First Japan - NATO Cyber Dialogue, Ministry of Foreign Affairs (Tokyo). 24 November, 2023. Access Date: 01 December, 2023. https://www.mofa.go.jp/press/release/press4e_003343.html

[2243] UK-Singapore data and tech agreements to boost trade and security, Department for Science, Innovation, and Technology (London) 28 June 2023. Access Date: 01 November 2023. https://www.gov.uk/government/news/uk-singapore-data-and-tech-agreements-to-boost-trade-and-security

[2244] UK sanctions members of Russian cybercrime gang, National Crime Agency (London) 07 September 2023. Access date: 01 November 2023. https://www.gov.uk/government/news/uk-sanctions-members-of-russian-cybercrime-gang

[2245] The European Union and NATO intensify cooperation on addressing cyber threats, the European Commission (Brussels) 22 September 2023. Access Date: 03 November 2023. https://digital-strategy.ec.europa.eu/en/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats

On 5 October 2023, the Competition and Markets Authority launched an investigation into the supply of public cloud infrastructure services in the United Kingdom.[2246] After a recommendation by the Office of Communications, the Competition and Markets Authority began to investigate whether various factors within the market, including but not limited to egress fees, discounts, and technical barriers were likely to lead to a monopoly or oligopoly within the cloud infrastructure market.

On 25 October 2023, the Prime Minister, Rishi Sunak, announced details regarding a future speech on artificial intelligence (AI) safety and how to better harness the future benefits of AI.[2247] Additionally, the government of the United Kingdom has published a paper detailing the risks and capabilities of frontier AI, as well as how to manage those risks.

On 2 November 2023, the Counter Ransomware Initiative (CRI) signed a joint statement denouncing ransomware and payments being made to cyber criminals.[2248] Members of the CRI, including the UK and other international partners, are committed to disrupting organized crime and developing robust and effective policies and practices to enhance the global response to ransomware members. The statement is the first international statement to strongly oppose paying ransom attackers with relevant funds from central governments.

On 21 November, the UK signed an Accord with the Republic of Korea to further enforce sanctions against North Korea.[2249] As part of the Accord, both parties will commit to cooperating on security and defence issues, including the signing of a Strategic Cyber Partnership to tackle cyber threats.

On 2 December 2023, Defence Secretary Grant Shapps, Australian Deputy Prime Minister Richard Marles and the US Secretary of Defense Lloyd Aust strengthened their security partnership.[2250] Together they seek to advance new programmes on threat detection, strengthening the cyber capabilities across the three to protect critical communications and operations systems.

The United Kingdom has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches. It has taken strong action in increasing trust across digital ecosystems by identifying risks to data protection in the cloud industry alongside sanctioning cyber-crime. As well, the United Kingdom has taken strong action in combating authoritarian influences through international agreements sharing best practices, ensuring data protection, and addressing the flow of data.

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

Analyst: Zekai Zhu

United States: +1

The United States has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches.

[2246] CMA launches market investigation into cloud services, Competition and Markets Authority (London) 05 October 2023. Access Date: 01 November 2023. https://www.gov.uk/government/news/cma-launches-market-investigation-into-cloud-services

[2247] Prime Minister calls for global responsibility to take AI risks seriously and seize its opportunities, Prime Minister's Office (London) 25 October 2023. Access Date: 01 December 2023. https://www.gov.uk/government/news/prime-minister-calls-for-global-responsibility-to-take-ai-risks-seriously-and-seize-its-opportunities

[2248] UK and Singapore secure agreement against ransomware payments, National Cyber Security Centre (London) 2 November 2023. Access Date: 23 December 2023. https://www.gov.uk/government/news/uk-and-singapore-secure-agreement-against-ransomware-payments

[2249] UK and Republic of Korea to enforce sanctions against North Korea through joint sea patrols, Ministry of Defence (London) 21 November 2023. Access Date: 22 December 2023. https://www.gov.uk/government/news/uk-and-republic-of-korea-to-enforce-sanctions-against-north-korea-through-joint-sea-patrols

[2250] UK powers up partnership with US and Australia to strengthen security, Ministry of Defence (London) 2 December 2023. Access Date: 22 December 2023. https://www.gov.uk/government/news/uk-powers-up-partnership-with-us-and-australia-to-strengthen-security

In May 2023, the National Science and Technology Council together with a select committee on artificial intelligence (AI) authored a report on the National Artificial Intelligence Research and Development Strategy Plan 2023 Update.[2251] The report detailed proposals for long-term investments in fundamental and responsible AI research. The report went on to cite the importance of exploring pathways for human-AI collaboration, in addition to discussing environments for AI training and testing including the use of public datasets.

In May 2023, the Office of Educational Technology published its insights and recommendations for educators and other similarly interested parties on Artificial Intelligence and the Future of Teaching and Learning.[2252] While also raising important concerns regarding the ethics of AI model training and the need to safeguard human cognitive autonomy and upholding equity among students.

On 23 May 2023, the Office of Science and Technology Policy put out a call for public comments and information on National Priorities for Artificial Intelligence.[2253] This knowledge will serve to inform future work on this subject and promote an inclusive decision-making process ahead of further AI regulation and policy developments.

On 31 May 2023, the United States and the EU reiterated their partnership in matters of AI development, 6G exploration, and digital identity among other key focus areas in a joint statement from the fourth Ministerial meeting of the Trade and Technology Council.[2254] This statement expressed a particular emphasis on coordinated responses to confront foreign information manipulation and interference and disinformation campaigns. The partnership intends to explore the opportunities and risks involved in generative AI. In particular, as the matter relates to the Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management. Three expert groups have been appointed to support this work, focusing on: AI terminology and taxonomy; cooperation on AI standards and tools for trustworthy AI and risk management; and monitoring and measuring existing and emerging AI risks.

On 22 June 2023, the Secretary of Commerce, Gina Raimondo, announced the inauguration of a public working group on AI led by the National Institute of Standards and Technology.[2255] The group's focus will remain on the opportunities presented in generative AI development in order to address broader technical issues that may arise from AI content generation. The public working group will primarily consist of experts from both the public and private sectors.

On 21 July 2023, the Biden-Harris administration presented voluntary commitments made by seven leading AI companies including: Amazon, Google, Meta, and OpenAI.[2256] The agreement serves to sustain the

[2251] Artificial Intelligence and the Future of Teaching and Learning, Department of Education: Office of Education Technology (Washington D.C.) May 2023. Access Date: 1 November 2023. https://www2.ed.gov/documents/ai-report/ai-report.pdf

[2252] National Artificial Intelligence Research and Development Strategic Plan 2023 Update, Executive Office of the President of the United States (Washington D.C.) May 2023. Access Date:1 November 2023. https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf

[2253] Request for information: National Priorities for Artificial Intelligence, Office of Science and Technology (Washington D.C.) 23 May 2023. Access Date: 1 November 2023. https://www.whitehouse.gov/wp-content/uploads/2023/05/OSTP-Request-for-Information-National-Priorities-for-Artificial-Intelligence.pdf

[2254] U.S.-EU Joint Statement of the Trade and Technology Council, The White House (Washington D.C.) 31 May 2023. Access Date: 1 November 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/

[2255] Biden-Harris Administration Announces New NIST Public Working Group on AI, Department of Commerce (Washington D.C.) 22 June 2023. Access Date: 1 November 2023. https://www.commerce.gov/news/press-releases/2023/06/biden-harris-administration-announces-new-nist-public-working-group-ai

[2256] FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI, The White House (Washington D.C.) 21 July 2023. Access Date: 01 November 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/) (https://www.whitehouse.gov/wp-content/uploads/2023/07/Ensuring-Safe-Secure-and-Trustworthy-AI.pdf administration's commitment to a future with AI that includes safety, security, and trust. Continuing the work toward a future with responsible AI.

On 22 September 2023, American delegates met with representatives from the North Atlantic Treaty Organization.[2257] A joint statement was released following the meeting that encouraged continued cooperation in the cyber domain, especially regarding building cyber capabilities.

On 30 October 2023, President Joe Biden signed a landmark Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[2258] The order calls for new standards for AI safety and security, the protection of civil privacy, support of workers, advocating on behalf of consumers, patients, and students among other objectives.

On 1 November 2023, the Office of the Management and Budget released a draft policy on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.[2259] So as to establish AI regulatory frameworks for federal agencies, promote responsible AI innovation, increase transparency, protect federal employees, and mitigate the risks of government AI use.

On 13 November 2023, the Biden-Harris administration released the National Spectrum Strategy, in a move to bolster American innovation, competition, and security in advanced wireless technologies.[2260] This effort speaks directly to America's commitment to strengthening trust across digital ecosystems. Longer term objectives for this policy will support the expansion of 5G networks; the development of precision agriculture; and remote aerial vehicles for the purpose of space exploration.

The United States has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches. The United States has taken strong actions in increasing trust by researching AI, protecting students from AI harms, testing AI, training AI, addressing AI ethics, incorporating public opinions on AI, and ensuring responsible use of AI. As well, it has taken strong action in combating authoritarian approaches by supporting cooperation in the face of foreign manipulation and interference, disinformation, creating standards and examining risks for AI, and ensuring protected rights against AI.

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

Analyst: Lesley Isaro

European Union: +1

The European Union has fully complied with its commitment to increase trust across the digital ecosystem and to counter the influence of authoritarian approaches.

[2257] The European Union and NATO intensify cooperation on addressing cyber threats, the European Commission (Brussels) 22 September 2023. Access Date: 03 November 2023. https://digital-strategy.ec.europa.eu/en/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats

[2258] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, The White House (Washington D.C.) 30 October 2023. Access Date: 01 November 2023. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[2259] Draft For Public Review: Proposed Memorandum for the Heads of Executive Departments and Agencies, Office of Management and Budget (Washington D.C.) 01 November 2023. Access Date: 02 November 2023. https://www.whitehouse.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-draft-for-public-review.pdf

[2260] FACT SHEET: Biden-Harris Administration Issues Landmark Blueprint to Advance American Innovation, Competition and Security in Wireless Technologies (Washington, D.C.) 13 November 2023. Access Date: 7 November 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/13/fact-sheet-biden-harris-administration-issues-landmark-blueprint-to-advance-american-innovation-competition-and-security-in-wireless-technologies/

On 17 May 2023, the European Union approved the Markets in Cryptoassets regulation.[2261] These are the world's first guidelines designed to broadly regulate the cryptocurrency market against malicious activity.[2262] Chief amongst them was one that undermines cryptocurrencies' anonymous nature, with a need to "collect and make accessible certain information about the sender and beneficiary of the transfers of crypto assets." The regulation is set to take effect in June 2024.

On 20 June 2023, the European Commission and the High Representative published a Joint Communication on a European Economic Security Strategy.[2263] The Joint Communication focuses on minimising risks arising from certain economic flows in the context of increased geopolitical tensions and accelerated technological shifts while preserving maximum levels of economic openness and dynamism.

On 10 July 2023, the European Commission adopted the EU-US Data Privacy Framework.[2264] The EU-US Data Privacy Framework aims to ensure safe, encrypted data flows to and from Europe and ensure legal compliance and transparency for companies on both sides of the Atlantic.

On 11 July 2023, the European Commission's POTENTIAL Consortium was launched in Paris by the French Ministry of the Interior and Overseas and the National Agency for Secure Documents.[2265] POTENTIAL will test a digital wallet for European citizens in order to prevent identity theft.

On 19 July 2023, the European Council introduced a draft regulation of mandatory cybersecurity requirements.[2266] The draft proposes new processes for the design, development, production and making available on the market of hardware and software products to avoid overlapping requirements stemming from different pieces of legislation in EU member states.

On 18 September 2023, the European Union released the Commission Guidelines discussing the relationship between the Network and Information Security Directive Version 2 (NIS 2 Directive) and the Digital Operational Resilience Act (DORA).[2267] The NIS 2 Directive is an expansion of EU-wide security requirements to improve the security of supply chains, simplify reporting obligations, and enforce more stringent measures throughout Europe; it went into effect on 16 January, 2023.[2268] The DORA extends operational resilience requirements that were established by EU financial services regulatory bodies to include oversight of digital information and communications technology; it is set to take effect in 2025.[2269]

[2261] REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, the European Commission (Brussels) 31 May 2023. Access Date: 27 October 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114

[2262] Markets in crypto-assets (MiCA), the European Parliament (Brussels) 29 September 2023. Access Date: 28 October 2023. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)739221

[2263] An EU approach to enhance economic security, the European Commission (Brussels) 20 June 2023. Access Date: 29 October 2023. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3358

[2264] Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows, the European Commission (Brussels) 10 July 2023. Access Date: 30 October 2023. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721

[2265] Lancement du consortium européen POTENTIAL pour l'identité numérique, Ministére de l'Intérieur et des Outre-Mer (Paris) 10 July 2023. Access Date: 15 January 2024. https://www.interieur.gouv.fr/actualites/communiques-de-presse/lancement-du-consortium-europeen-potential-pour-lidentite

[2266] Cyber resilience act: member states agree common position on security requirements for digital products, the European Council (Brussels) 19 July 2023. Access Date: 31 October 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/

[2267] The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554, the European Union (Horgen) 18 September 2023. Access Date: 01 November 2023. https://www.digital-operational-resilience-act.com

[2268] Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), the European Commission (Brussels) 14 September 2023. Access Date: 02 November 2023. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[2269] The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554, the European Union (Horgen) 18 September 2023. Access Date: 01 November 2023. https://www.digital-operational-resilience-act.com

On 22 September 2023, senior officials from the European Union met with senior officials from North Atlantic Treaty Organization (NATO).[2270] A joint statement was released following the meeting that encouraged continued cooperation in the cyber domain, especially regarding building cyber capabilities.

On 3 October 2023, the European Commission established an assessment into four key technologies that may pose a risk to the bloc's economic security, specifically artificial intelligence (AI), advanced semiconductors, quantum computing and biotechnology.[2271] Results from the assessment will determine whether the European Union will impose export controls on them.

On 13 November 2023, the European Union Agency for Cybersecurity formalized a Working Arrangement with Ukrainian counterparts focused on improving cybersecurity capacity-building, best practices exchange and boosting situational awareness.[2272]

On 30 November 2023, the Council of the European Union reached a provisional agreement introducing EU-wide cybersecurity requirements for products with digital elements.[2273] The law ensures that products such as connected home cameras, fridges, televisions and toys are safe for users before they are placed on the market. It aims to streamline regulation and avoid overlapping requirements stemming from different pieces of legislation in EU member states.

The European Union has fully complied with its commitment to empower citizens to use the Internet and digital technologies safely and securely. The European Union has taken strong actions to increase trust in digital ecosystems by regulating cryptocurrency, establishing a data privacy and data flow framework, ensuring citizens are protected from cyberattacks that undermine device functionality, assessing risks and raising privacy concerns. The European Union has also taken strong action in countering authoritarian influences by introducing long-term regulations that aim to address rising technologies, such as AI and quantum computing. As well, the EU has strongly supported bilateral and multilateral cooperation, secure data flows, standardization, and addressing cyber risks.

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

Analyst: Anna Lysenko

[2270] The European Union and NATO intensify cooperation on addressing cyber threats, the European Commission (Brussels) 22 September 2023. Access Date: 03 November 2023. https://digital-strategy.ec.europa.eu/en/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats

[2271] ANNEX to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, the European Commission (Strasbourg) 03 October 2023. Access Date: 30 October 2023. https://defence-industry-space.ec.europa.eu/system/files/2023-10/C_2023_6689_1_EN_annexe_acte_autonome_part1_v9.pdf

[2272] Enhanced EU-Ukraine cooperation in Cybersecurity, European Union Agency for Cybersecurity (Brussels) 13 November 2023. Access Date: 30 November 2023. https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity

[2273] Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products, the European Council of the European Union (Brussels) 30 November 2023. Access Date: 02 December 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products