UNIVERSITY OF TORONTO

G20 RESEARCH GROUP | munk school OF GLOBAL AFFAIRS & PUBLIC POLICY

The
G7 Research Group
at the Munk School of Global Affairs and Public Policy at Trinity College
in the University of Toronto presents the

2019 G7 Biarritz Summit Interim Report

27 August 2019 — 20 December 2019

Prepared by
Meagan Byrd and Ivan Hsieh
and the G7 Research Group

15 March 2020

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

2. Digital Economy: Digital Democracy

"We are determined to work collaboratively to reinforce our democracies against illicit and malign behavior and foreign hostile interference by state and non-state actors."

Biarritz Strategy for an Open, Free and Secure Digital Transformation

Assessment

	Lack of Compliance	Work in Progress	Full Compliance
Canada		0	
France	−1		
Germany		0	
Italy		0	
Japan			+1
United Kingdom		0	
United States			+1
European Union		0	
Average	+0.13 (56%)		

Background

The relatively recent introduction of digital issues into the G7 agenda began with a variety of commitments that sought to harness the power of the digital transformation to improve governance and accountability, most notably in the *G8 Open Data Charter* adopted at the 2013 Lough Erne summit.

The first discussion of the problems that the digital transformation posed for democratic institutions was introduced with the *G7 Principles and Actions on Cyber* adopted the 2016 Ise-Shima summit, which included a pledge to "take decisive and robust measures in close cooperation against malicious use of cyberspace both by states and non-state actors, including terrorists." Further commitments include both national and international cooperation to maintain the security and resilience of cyberspace.

At the 2017 Taormina summit, the G7 committed to combatting the "misuse of the Internet by terrorists" in the *G7 Taormina Statement on the Fight Against Terrorism and Violent Extremism*. Part of this commitment emphasized increased engagement with civil society, youth and others at risk of radicalization.

The 2018 Charlevoix summit addressed the issues of this commitment feature in its *Charlevoix Commitment on Defending Democracy from Foreign Threats*, which committed to "strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state. A key commitment in that document was the establishment of a G7 Rapid Response Mechanism to increase international coordination in the face of threats to democracy.

The 2019 Biarritz summit outlined its commitments on digital democracy in the wide-ranging *Biarritz Strategy for an Open, Free and Secure Digital Transformation*. The commitments in that document include upholding freedom of opinion and expression, the privacy and data protection issues raised by the digital transformation, and the potential of AI to generate innovation and growth. The document also takes note of the work done by the G7 Rapid Response Mechanism established at the 2018 Charlevoix summit.

Commitment Features

At the 2019 Biarritz summit the G7 members committed to "work collaboratively to reinforce our democracies against illicit and malign behavior and foreign hostile interference by state and non-state

actors." This commitment should be interpreted as having two dimensions required for compliance: domestic versus international actions, and reinforcing against hostile interference by state versus non-state actors.

A domestic action is an action that a G7 member undertakes to reinforce their own institutions against illicit and malign behavior and foreign hostile interference while respecting the rights of freedom of opinion and expression. Relevant actions can include the promotion of positive narratives surrounding institutions and democracy. An international action is an action that a G7 member undertakes to reinforce global institutions or the institutions of their global partners against illicit and malign behavior and foreign hostile interference while respecting relevant international law and the laws of other jurisdictions.

Reinforcing against hostile interference by state actors involves the use of diplomacy, stronger security measures, and potentially sanctions against other states whose actions are undermining democratic institutions. Such actions could include the deliberate spread of misinformation, the infiltration of political institutions (including political parties), and attempts to use state resources to influence the outcomes of decision-making processes. Reinforcing against hostile interference by non-state actors includes the strengthening of anti-terrorism measures, the promotion of positive narratives surrounding democratic institutions, and cooperation with other states who are facing threats from similar or identical non-state actors.

As examples, an action taken by a country to regulate political advertising on social media during election campaigns would count as a domestic action that reinforces against non-state actors, whereas an action taken to create a multilateral protocol to respond to attempted state-based interference in democratic institutions would count as an international action that reinforces against state actors.

Thus, to receive a score of full compliance, G7 members must take substantial action in all four dimensions, including multiple actions in at least two dimensions to reinforce democracies against illicit and malign behaviour, as well as foreign hostile interference by state and non-state actors.

If action is only taken in three dimensions to reinforce our democracies against illicit and malign behaviour, as well as foreign and hostile interferences by state and non-state actors, a score of partial compliance, or 0 will be assigned.

A score of −1, or no compliance, will be assigned if the G7 member exemplifies demonstrable action in two or fewer dimensions to reinforce our democracies against illicit and malign behaviour, and foreign hostile interference by state and non-state actors.

Scoring Guidelines

−1	Members take action in TWO or fewer dimensions to reinforce our democracies against illicit and malign behavior, and foreign hostile interference by state and non-state actors.
0	Members take action in at least THREE dimensions to reinforce our democracies against illicit and malign behavior, and foreign hostile interference by state and non-state actors.
+1	Members take substantial action in all four dimensions, including multiple action in at least two dimensions to reinforce our democracies against illicit and malign behavior, and foreign hostile interference by state and non-state actors.

Compliance Director: Christopher Sims
Lead Analyst: Emily Eng

Canada: 0

Canada has partially complied with its commitment to "work collaboratively to reinforce our democracies against illicit and malign behaviour and foreign hostile interference by state and non-state actors."

Throughout September 2019, the Government of Canada launched programs as part of Canadian Heritage's Digital Citizen Initiative.[69] The Government of Canada has invested almost CAD 7 million in programs teaching citizens to think critically and recognize fake news.[70] This initiative protects citizens from being susceptible to disinformation.[71]

On 26 September 2019, the Government of Canada announced the Joint Initiative for Digital Citizen Research.[72] Canadian Heritage will partner with and provide funding to the Social Sciences and Humanities Research Council, with the goal of better understanding the effects of online disinformation and finding the most effective programs and policies to counter online disinformation.[73]

From 6 November to 9 November 2019, Canadian law makers represented Canada at the third meeting of the International Grand Committee on Disinformation and "Fake News" in Dublin, Ireland.[74] The goal of this meeting was to discuss how to collaboratively regulate the spread of disinformation on social media platforms.[75]

Canada took actions to strengthen cybersecurity through domestic policy changes, and bilateral and multilateral collaboration, thus fulfilling both the domestic and international dimensions. Canada took actions to reinforce democratic institutions against non-state actors but took no actions to reinforce democratic institutions against state actors. These actions fulfil three of the four dimensions of the commitment.

Thus, Canada receives a score of 0.

Analyst: Isabelle Buchanan

[69] Backgrounder – Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation, Government of Canada (Ottawa) 21 August 2019. Access Date: 4 December 2019. https://www.canada.ca/en/canadian-heritage/news/2019/07/backgrounder--helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html.

[70] Backgrounder – Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation, Government of Canada (Ottawa) 21 August 2019. Access Date: 4 December 2019. https://www.canada.ca/en/canadian-heritage/news/2019/07/backgrounder--helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html.

[71] Backgrounder – Helping Citizens Critically Assess and Become Resilient Against Harmful Online Disinformation, Government of Canada (Ottawa) 21 August 2019. Access Date: 4 December 2019. https://www.canada.ca/en/canadian-heritage/news/2019/07/backgrounder--helping-citizens-critically-assess-and-become-resilient-against-harmful-online-disinformation.html.

[72] Joint Initiative for Digital Citizen Research, Government of Canada (Ottawa) 26 September 2019. Access Date: 4 December 2019. https://www.canada.ca/en/canadian-heritage/services/online-disinformation/joint-initiative-digital-citizen-research.html.

[73] Joint Initiative for Digital Citizen Research, Government of Canada (Ottawa) 26 September 2019. Access Date: 4 December 2019. https://www.canada.ca/en/canadian-heritage/services/online-disinformation/joint-initiative-digital-citizen-research.html.

[74] Update: International Grand Committee on Disinformation and 'Fake News' Dublin, Ireland – Wednesday 6 and Thursday 7 November 2019, Houses of the Oireachtas (Dublin) 6 November 2019. Access Date: 19 December 2019. https://www.oireachtas.ie/en/press-centre/press-releases/20191106-update-international-grand-committee-on-disinformation-and-fake-news-dublin-ireland-wednesday-6-and-thursday-7-november-2019/.

[75] Update: International Grand Committee on Disinformation and 'Fake News' Dublin, Ireland – Wednesday 6 and Thursday 7 November 2019, Houses of the Oireachtas (Dublin) 6 November 2019. Access Date: 19 December 2019. https://www.oireachtas.ie/en/press-centre/press-releases/20191106-update-international-grand-committee-on-disinformation-and-fake-news-dublin-ireland-wednesday-6-and-thursday-7-november-2019/.

France: −1

France has failed to comply with its commitment to "work collaboratively to reinforce our democracies against illicit and malign behaviour and foreign hostile interference by state and non-state actors."

On 28 November 2019, President Emmanuel Macron, speaking alongside North Atlantic Treaty Organization (NATO) Secretary General Jens Stoltenberg, said he had "requested [French government] services to work on [cybersecurity, though] never pointing out a particular operator or a particular country" in terms of focus.[76]

On 3 December 2019, the Government of France published a news release regarding President Macron's agenda at the NATO summit.[77] Within the second priority issue, regarding a "common enemy," France called on members to address "new security challenges, such as cybersecurity."[78]

France has not taken any relevant actions within the compliance period.[79]

Thus, France receives a score of −1.

Analyst: Alex Erickson

Germany: 0

Germany has partially complied with its commitment to "work collaboratively to reinforce our democracies against illicit and malign behaviour and foreign hostile interference by state and non-state actors."

On 12 September 2019, German lawmakers introduced a new cloud-computing project, Gaia-X.[80] The cloud-computing platform was designed for European companies to store, process, exchange data, and cooperate on developing products.[81] The idea of the project came over fears of heavy reliance of foreign-owned cloud platforms which have been known for data interference practices.[82]

On 18 November 2019, the Bundestag Budget Committee approved 67 new posts to the Federal Commissioner for Data Protection and Freedom Information.[83] The federal body plans to push

[76] Joint press point with NATO Secretary General Jens Stoltenberg and the President of France Emmanuel Macron, NATO (Paris) 28 November 2019. Access Date: 14 December 2019. https://www.nato.int/cps/en/natohq/opinions_170790.htm?selectedLocale=en.
[77] NATO Summit, Government of France (Paris) 3 December 2019. Access Date: 16 December 2019. https://www.gouvernement.fr/en/nato-summit.
[78] NATO Summit, Government of France (Paris) 3 December 2019. Access Date: 16 December 2019. https://www.gouvernement.fr/en/nato-summit.
[79] This non-compliance was determined after a deep search of the following websites: https://www.allianceofdemocracies.org/transatlantic-commission-on-election-integrity/; https://www.igf2019.berlin/IGF/Navigation/DE/Home/home.html; https://icspa.org; https://dig.watch/sites/default/files/2019-12/IGF2019Report.pdf; http://www.macronometre.fr; https://pariscall.international; https://legifrance.gouv.fr; https://gouvernement.fr; https://diplomatie.gouv.fr; https://nytimes.com and https://bbc.com.
[80] Germany's Plan to Control its own Data, Politico (Berlin) 12 September 2019. Access Date: 17 December 2019.https://www.politico.eu/article/germanys-plan-to-control-its-own-data-digital-infrastructure/.
[81] Germany's Plan to Control its own Data, Politico (Berlin) 12 September 2019. Access Date: 17 December 2019. https://www.politico.eu/article/germanys-plan-to-control-its-own-data-digital-infrastructure/.
[82] Germany's Plan to Control its own Data, Politico (Berlin) 12 September 2019. Access Date: 17 December 2019. https://www.politico.eu/article/germanys-plan-to-control-its-own-data-digital-infrastructure/.
[83] The Bundestag strengthens the data protection supervisory authority, Federal Commissioner for Data Protection and Freedom of Information (Berlin) 18 November 2019. Access Date: 17 December 2019. https://www.bfdi.bund.de/EN/Home/Press_Release/2019/28_Budget-BfDI.html.

General Data Protection Regulation under the EU by imposing new regulations which will limit and block tracking across all devices and platforms, and curtailing insufficient technical protection of data.[84]

On 8 November 2019, German Data Protection Authorities released new guidelines for fining companies violating the regulations set out by the General Data Protection Regulation.[85] The fines are classified as minor, moderate, severe, and very severe.[86]

Germany took actions to strengthen cybersecurity through domestic policy changes, thus fulfilling both the domestic dimension. Germany took actions to reinforce democratic institutions against both state and non-state actors. These actions fulfil three of the four dimensions of the commitment.

Thus, Germany receives a score of 0.

Analyst: Yousef Choudhri

Italy: 0

Italy has partially complied with its commitment to "work collaboratively to reinforce our democracies against illicit and malign behaviour and foreign hostile interference by state and non-state actors."

On 21 September 2019, the Italian Government adopted the Law Decree n. 105 as part of the implementation of a comprehensive national cybersecurity framework.[87] The decree requires that individuals in the public and private sectors who serve functions that are key component of the national security system disclose relevant information to the Council of Ministers and the Minister of Economic Development and comply with measures aimed at upholding a high level of national security.[88]

On 22 December 2019, Industry Minister Stefano Patuanelli announced that Chinese telecom firm Huawei should be allowed to participate in the development of Italy's future 5G network.[89] The announcement comes after the parliamentary security committee Copasir stated that the government should consider preventing Huawei from participating in the development of a future 5G network.

Italy took actions to strengthen cybersecurity through domestic policy changes, thus fulfilling both the domestic and international dimensions. Japan took actions to reinforce democratic institutions against both state and non-state actors. These actions fulfill three of the four dimensions of the commitment.

---

[84] The Bundestag strengthens the data protection supervisory authority, Federal Commissioner for Data Protection and Freedom of Information (Berlin) 18 November 2019. Access Date: 17 December 2019.https://www.bfdi.bund.de/EN/Home/Press_Release/2019/28_Budget-BfDI.html.

[85] How are German Data Protection Authorities going to determine a fine? /EUR 14.5 million fine imposed by Berlin DPA, Baker Mckenzie (Berlin) November 2019. Access Date: 17 December 2019.https://www.bakermckenzie.com//-/media/files/insight/publications/2019/11/client-alert-dpa-concept-for-fines-final.pdf.

[86] How are German Data Protection Authorities going to determine a fine? /EUR 14.5 million fine imposed by Berlin DPA, Baker Mckenzie (Berlin) November 2019. Access Date: 17 December 2019.https://www.bakermckenzie.com//-/media/files/insight/publications/2019/11/client-alert-dpa-concept-for-fines-final.pdf.

[87] Italy towards an effective National Cyber Security Strategy, Lexology (Rome) 26 September 2019. Access Date: 3 January 2020. https://www.lexology.com/library/detail.aspx?g=bfe7f1d9-d5ea-4126-adf6-e74a58096249.

[88] Italy towards an effective National Cyber Security Strategy, Lexology (Rome) 26 September 2019. Access Date: 3 January 2020. https://www.lexology.com/library/detail.aspx?g=bfe7f1d9-d5ea-4126-adf6-e74a58096249.

[89] Huawei should be allowed 5G role in Italy: Industry minister, Reuters (Rome) 22 December 2019. Access Date: 3 January 2020. https://www.reuters.com/article/us-italy-5g-security-patuanelli/huawei-should-be-allowed-5g-role-in-italy-industry-minister-idUSKBN1YQ0D7.

Thus, Italy receives a score of 0.

Analyst: Eunice Yong

Japan: +1

Japan has fully complied with its commitment to "work collaboratively to reinforce our democracies against illicit and malign behaviour and foreign hostile interference by state and non-state actors."

On 9 to 13 September 2019, a Japanese delegation, which included Japanese Deputy Assistant Minister Satoshi Akahori, Foreign Policy Bureau, attended the first meeting of the United Nations Open-ended Working Group on Cybersecurity held in New York.[90] On 9 September 2019, Akahori stated that Japan increased its international collaboration in three areas: "promotion of the rule of law, confidence-building measures, and capacity-building."[91] He reaffirmed Japan's position that "existing international law applies in cyberspace" and expressed Japanese support for the upcoming Group of Governmental Experts on cybersecurity.[92]

On 9 to 12 September 2019, Japan's Ministry of Economy, Trade and Industry and the Industrial Cyber Security Center of Excellence under the information-technology Promotion Agency, hosted the Japan-US Industrial Control Systems Cybersecurity Training in Tokyo.[93] American and Japanese experts delivered lectures on the security of control systems of critical infrastructure.[94] Attendees were from 14 countries and regions in the Indo-Pacific region.[95]

On 9 October 2019, Japan and the North Atlantic Trade Organization (NATO), held defence staff talks on cybersecurity to assess current cyber threats and policies.[96] Officials compared notes on current efforts in strengthening cyber defence.[97] They also affirmed commitment in "[supporting] a norms-based, predictable, and secure cyberspace."[98] Japanese Director of Strategic Planning Division at the Ministry of Defence Kyosuke Matsumoto, said Japan gave priority to "strengthening our cyber

[90] The UN Open-ended Working Group (OEWG) on Cybersecurity 1st Meeting, Ministry of Foreign Affairs of Japan (Tokyo) 10 September 2019. Access Date: 2 December 2019. https://www.mofa.go.jp/press/release/press4e_002616.html.
[91] Statement by H.E. Mr. Takeshi Akahori, Ambassador in charge of Cyber Policy, Deputy Assistant Minister, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan, At the Open Ended Working Group on Information and Communications, Ministry of Foreign Affairs of Japan (Tokyo) 9 September 2019. Access Date: 18 December 2019. https://www.mofa.go.jp/files/000515730.pdf.
[92] Statement by H.E. Mr. Takeshi Akahori, Ambassador in charge of Cyber Policy, Deputy Assistant Minister, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan, At the Open Ended Working Group on Information and Communications, Ministry of Foreign Affairs of Japan (Tokyo) 9 September 2019. Access Date: 18 December 2019. https://www.mofa.go.jp/files/000515730.pdf.
[93] Japan - US Industrial Control Systems Cybersecurity Training for Indo-Pacific Region Held, Ministry of Economy, Trade, and Industry (Tokyo) 12 September 2019. Access Date: 2 December 2019. https://www.meti.go.jp/english/press/2019/0912_002.html.
[94] Japan - US Industrial Control Systems Cybersecurity Training for Indo-Pacific Region Held, Ministry of Economy, Trade, and Industry (Tokyo) 12 September 2019. Access Date: 2 December 2019. https://www.meti.go.jp/english/press/2019/0912_002.html.
[95] Japan - US Industrial Control Systems Cybersecurity Training for Indo-Pacific Region Held, Ministry of Economy, Trade, and Industry (Tokyo) 12 September 2019. Access Date: 2 December 2019. https://www.meti.go.jp/english/press/2019/0912_002.html.
[96] NATO and Japan Intensify Dialogue on Cyber Defence, North Atlantic Treaty Organization (Brussels) 9 October 2019. Access Date: 2 December 2019. https://www.nato.int/cps/en/natohq/news_169493.htm?selectedLocale=en.
[97] NATO and Japan Intensify Dialogue on Cyber Defence, North Atlantic Treaty Organization (Brussels) 9 October 2019. Access Date: 2 December 2019. https://www.nato.int/cps/en/natohq/news_169493.htm?selectedLocale=en.
[98] NATO and Japan Intensify Dialogue on Cyber Defence, North Atlantic Treaty Organization (Brussels) 9 October 2019. Access Date: 2 December 2019. https://www.nato.int/cps/en/natohq/news_169493.htm?selectedLocale=en.

defence capability" and Japan valued "effectively cooperate with other like-minded countries to take prompt and appropriate actions against cyberattacks."[99]

On 11 October 2019, Japan hosted the 7th US-Japan Cyber Dialogue in Tokyo.[100] Representatives of both countries reaffirmed their commitment in confronting emerging cyber challenges, including "shared commitment to deter cyber adversaries and malicious cyber activities, to protect the cybersecurity of critical infrastructure, to enhance information sharing, to improve military-to-military cyber cooperation, and to address international security issues in cyberspace."[101]

On 18 October 2019, the Japanese government increased the budget for cybersecurity from JPY 71.29 billion to JPY 88.11 billion.[102]

On 29 October 2019, Japan and the Association of Southeast Asian Nations (ASEAN) held the 12th Policy Conference on Cyber Security. These countries affirmed commitments on "strengthening information sharing systems and response systems in the event of cyber incidents, promoting initiatives related to protection of critical infrastructure, and [promoting cooperation] in capacity building and awareness."[103]

On 4 November 2019, Japan and ASEAN issued the Joint Statement of the 22nd ASEAN-Japan Summit on connectivity.[104] These countries declared to "[enhance] cybersecurity capacity building for ASEAN through the ASEAN-Japan Cybersecurity Capacity Building Centre and the ASEAN-Singapore Cybersecurity Centre of Excellence."[105]

On 18 November 2019, Ambassador in Charge of Cyber Security Akahori Takeshi attended the 4th Trilateral Cyber Policy Consultation between Japan, the People's Republic of China and South Korea.[106] They discussed the current environment in the field of cyber affairs, each country's policies on cyber issues, and future cooperation on cyber issues.[107]

On 18 November 2019, the Cabinet Secretariat Cyber Security Center Tomoo Yamauchi issued a document on 2020 Cyber Security Month.[108] The government planned to raise public awareness on

[99] NATO and Japan Intensify Dialogue on Cyber Defence, North Atlantic Treaty Organization (Brussels) 9 October 2019. Access Date: 2 December 2019. https://www.nato.int/cps/en/natohq/news_169493.htm?selectedLocale=en.
[100] The 7th Japan-US Cyber Dialogue, Ministry of Foreign Affairs of Japan (Tokyo) 10 October 2019. Access Date: 26 November 2019. https://www.mofa.go.jp/press/release/press4e_002646.html.
[101] The 7th Japan-US Cyber Dialogue, Ministry of Foreign Affairs of Japan (Tokyo) 10 October 2019. Access Date: 26 November 2019. https://www.mofa.go.jp/press/release/press4e_002646.html.
[102] Government Cybersecurity Budget, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 18 October 2019. Access Date: 18 December 2019. https://www.nisc.go.jp/active/kihon/pdf/yosan2020.pdf.
[103] Results of the Japan-ASEAN Cybersecurity Policy Conference, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 19 Nivember 2019. Access Date: 15 December 2019. https://www.nisc.go.jp/press/pdf/aseanj_meeting20191119.pdf.
[104] Joint Statement of the 22nd ASEAN-Japan Summit on Connectivity, ASEAN Thailand 2019 (Bangkok) 4 November 2019. Access Date: 18 December 2019. https://www.asean2019.go.th/en/news/joint-statement-of-the-22nd-asean-japan-summit-on-connectivity-2/.
[105] Joint Statement of the 22 nd ASEAN-Japan Summit on Connectivity, ASEAN Thailand 2019 (Bangkok) 4 November 2019. Access Date: 18 December 2019. https://www.asean2019.go.th/en/news/joint-statement-of-the-22nd-asean-japan-summit-on-connectivity-2/.
[106] The 4th Trilateral Cyber Policy Consultation, Ministry of Foreign Affairs of Japan (Tokyo) 18 November 2019. Access Date: 18 November 2019. https://www.mofa.go.jp/press/release/press4e_002682.html.
[107] The 4th Trilateral Cyber Policy Consultation, Ministry of Foreign Affairs of Japan (Tokyo) 18 November 2019. Access Date: 18 November 2019. https://www.mofa.go.jp/press/release/press4e_002682.html.
[108] With the implementation of Cybersecurity Month 2020 Recruitment of related events, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 18 November 2019. Access Date: 30 December 2019. https://www.nisc.go.jp/active/kihon/pdf/csm2020kanren.pdf.

cybersecurity through various public activities during the Cyber Security Month (1 February 2020 to 18 March 2020). Governmental agencies will collaborate with awareness-raising organizations for this event.[109]

On 19 November 2019, Minister for Foreign Affairs Motegi Toshimitsu met with the Chair of Rasmussen Global Anders Fogh Rasmussen.[110] Rasmussen acknowledged Japan as "an important partner for Europe in a global battle for freedom and democracy."[111] He also invited Japan to attend a democracy summit meeting next June in Copenhagen.[112]

On 20 November 2019, Japan hosted the 4th Japan-Russia Cyber Security Consultation in Tokyo.[113] The representatives discussed the current landscape in cyberspace, and strategies and policies each country's strategies and policies on cyber issues.[114] They also discussed the issues of cybersecurity in multilateral and regional context and security of critical information infrastructure.[115]

Japan took actions to strengthen cybersecurity through domestic policy changes, and bilateral and multilateral collaboration, thus fulfilling both the domestic and international dimensions. Japan took actions to reinforce democratic institutions against both state and non-state actors. These actions fulfill all four dimensions of the commitment.

Thus, Japan receives a score of +1.

Analyst: Zihan (Alison) Pang

United Kingdom: 0

The United Kingdom has partially complied with its commitment to "work collaboratively to reinforce our democracies against illicit and malign behaviour and foreign hostile interference by state and non-state actors."

On 18 October 2019, Business Secretary Andrea Leadsom announced that the UK government be partnering with technology firm ARM in a new project to develop computer hardware that is more

[109] With the implementation of Cybersecurity Month 2020 Recruitment of related events, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 18 November 2019. Access Date: 30 December 2019. https://www.nisc.go.jp/active/kihon/pdf/csm2020kanren.pdf.
[110] Meeting between Foreign Minister Motegi and Mr. Rasmussen Chairman of Rasmussen Global (former Secretary General of the North Atlantic Treaty Organization (NATO), former Prime Minister of Denmark), Ministry of Foreign Affairs of Japan (Tokyo) 19 November 2019. Access Date: 17 December 2019. https://www.mofa.go.jp/press/release/press4e_002688.html.
[111] Meeting between Foreign Minister Motegi and Mr. Rasmussen Chairman of Rasmussen Global (former Secretary General of the North Atlantic Treaty Organization (NATO), former Prime Minister of Denmark), Ministry of Foreign Affairs of Japan (Tokyo) 19 November 2019. Access Date: 17 December 2019. https://www.mofa.go.jp/press/release/press4e_002688.html.
[112] Meeting between Foreign Minister Motegi and Mr. Rasmussen Chairman of Rasmussen Global (former Secretary General of the North Atlantic Treaty Organization (NATO), former Prime Minister of Denmark), Ministry of Foreign Affairs of Japan (Tokyo) 19 November 2019. Access Date: 17 December 2019. https://www.mofa.go.jp/press/release/press4e_002688.html.
[113] The 3rd Japan-Russia Cyber Policy Consultation, Ministry of Foreign Affairs of Japan (Tokyo) 20 November 2019. Access Date: 26 November 2019. https://www.mofa.go.jp/press/release/press4e_002687.html.
[114] The 3rd Japan-Russia Cyber Policy Consultation, Ministry of Foreign Affairs of Japan (Tokyo) 20 November 2019. Access Date: 26 November 2019. https://www.mofa.go.jp/press/release/press4e_002687.html.
[115] The 3rd Japan-Russia Cyber Policy Consultation, Ministry of Foreign Affairs of Japan (Tokyo) 20 November 2019. Access Date: 26 November 2019. https://www.mofa.go.jp/press/release/press4e_002687.html.

resistant to cyber-attacks, with the government providing GBP36 million towards the scheme.[116] This is the next phase of the UK government's Digital Security by Design initiative.[117]

In November 2019, Politico reported that the UK's electoral laws were insufficient in addressing "clandestine digital political interference."[118] In the article, Politico quotes special advisor to the UK House of Lords committee on democracy and digital technologies Kate Dommett, who expressed that existing laws have loopholes regarding the verification of "online campaign material," and that "voters are … at risk" of manipulation and can expect "limited, if any, responses from both regulators and politicians to protect them."[119]

On 4 November 2019, Digital Minister Matt Warman launched a "call for evidence" to seek views from across the digital sector on how the government can help organizations improve their cybersecurity measures.[120, 121] Minister Warman stated that overcoming barriers to improving cybersecurity "can help make the UK the safest place to live and do business online."[122]

On 25 November 2019, the Ministry of Justice announced that it is inviting bids for the creation of a centralized cybersecurity log collection and aggregation platform.[123] A spokesperson for the Ministry of Justice stated that the objective of the project is to resolve the Ministry's inability to "understand the cybersecurity posture of its current estates due to security logs being held in multiple systems."[124]

On 16 December 2019, Prime Minister Boris Johnson announced that his government will release an Intelligence and Security Committee of Parliament report on Russian interference during the 2016 UK European Union membership referendum in 2020.[125]

The UK took actions to strengthen cybersecurity through domestic policy changes, thus fulfilling the domestic dimension. The UK took actions to reinforce democratic institutions against both state and non-state actors. These actions fulfil three of the four dimensions of the commitment.

Thus, the United Kingdom receives a score of 0.

---

[116] Confronting cyber threats to businesses and personal data, Government of the UK (London) 18 October 2019. Access Date: 3 January 2020. https://www.gov.uk/government/news/confronting-cyber-threats-to-businesses-and-personal-data.
[117] Confronting cyber threats to businesses and personal data, Government of the UK (London) 18 October 2019. Access Date: 3 January 2020. https://www.gov.uk/government/news/confronting-cyber-threats-to-businesses-and-personal-data.
[118] UK ignores warnings of digital election interference, Politico (Brussels) 5 November 2019. Access Date: 11 December 2019. https://www.politico.eu/article/uk-general-election-facebook-misinformation-boris-johnson-interference-russia/.
[119] UK ignores warnings of digital election interference, Politico (Brussels) 5 November 2019. Access Date: 11 December 2019. https://www.politico.eu/article/uk-general-election-facebook-misinformation-boris-johnson-interference-russia/.
[120] Call for evidence launched on improving cyber security across the UK economy, Government of the United Kingdom (London) 4 November 2019. Access Date: 3 January 2020. https://www.gov.uk/government/news/call-for-evidence-launched-on-improving-cyber-security-across-the-uk-economy.
[121] Call for evidence launched on improving cyber security across the UK economy, Government of the United Kingdom (London) 4 November 2019. Access Date: 3 January 2020. https://www.gov.uk/government/news/call-for-evidence-launched-on-improving-cyber-security-across-the-uk-economy.
[122] Call for evidence launched on improving cyber security across the UK economy, Government of the United Kingdom (London) 4 November 2019. Access Date: 3 January 2020. https://www.gov.uk/government/news/call-for-evidence-launched-on-improving-cyber-security-across-the-uk-economy.
[123] UK Government Invites Bids for New Cybersecurity Platform, Infosecurity Magazine (London) 25 November 2019. Access Date: 3 January 2020. https://www.infosecurity-magazine.com/news/uk-invites-bids-for-cybersecurity/.
[124] UK Government Invites Bids for New Cybersecurity Platform, Infosecurity Magazine (London) 25 November 2019. Access Date: 3 January 2020. https://www.infosecurity-magazine.com/news/uk-invites-bids-for-cybersecurity/.
[125] Boris Johnson approves release of Russian interference report following election win, Independent (London) 17 December 2019. Access Date: 19 December 2019. https://www.independent.co.uk/news/uk/politics/boris-johnson-russia-report-brexit-interference-general-election-release-a9248446.html.

Analyst: Kevin Zuo

United States: +1

The United States has fully complied with its commitment to "work collaboratively to reinforce our democracies against illicit and malign behaviour and foreign hostile interference by state and non-state actors."

On 4 September 2019, U.S. government officials met with representatives of major American technological companies, such as Microsoft, Facebook, Google and Twitter, to discuss strategies for securing the upcoming American election from the kind of foreign interference associated with the 2016 election.[126] The discussion revolved around potential threats and threat detection, effective information sharing methods, as well as prevention of disinformation and foreign interference via social media.[127] An FBI official stated that the agency, along with the Office of the Director of National Intelligence and the Department of Homeland Security, attended this meeting to explore ways of "protecting democracy and securing the 2020 U.S. state, federal and presidential elections."[128]

From 9 to 13 September 2019, the United States hosted the first meeting of the United Nations Open-Ended Working Group on Cybersecurity in New York City. Principal Deputy Assistant Secretary of the Bureau of East Asian and Pacific Affairs Ambassador Atul Keshap promised to continue offering cybersecurity, digital economy, and cybercrime workshops for the benefit of many Indo-Pacific nations.[129] He also stated that one of the key goals of this initiative is to ensure that the US and its partners maintain secure networks as well as information and communications technology (ICT) supply chains to reduce the risk of unauthorized access and malicious cyber activity.[130]

On 24 September 2019, the Cybersecurity and Infrastructure Security Agency (CISA) released an updated National Emergency Communications Plan aimed at improving the U.S. emergency communications capabilities at all levels of government.[131] The update includes the addition of a cybersecurity goal and a focus on integrating new technologies which would improve the U.S. first responders' ability to effectively communicate in real time.[132] This public safety development will

[126] Big Tech Companies Meeting With U.S. Officials on 2020 Election Security, The New York Times (New York City) 4 September 2019. Access Date: 16 December 2019. https://www.nytimes.com/2019/09/04/technology/2020-election-facebook-google.html.
[127] Big Tech Companies Meeting With U.S. Officials on 2020 Election Security, The New York Times (New York City) 4 September 2019. Access Date: 16 December 2019. https://www.nytimes.com/2019/09/04/technology/2020-election-facebook-google.html.
[128] Big Tech Companies Meeting With U.S. Officials on 2020 Election Security, The New York Times (New York City) 4 September 2019. Access Date: 16 December 2019. https://www.nytimes.com/2019/09/04/technology/2020-election-facebook-google.html.
[129] Industrial Control Systems Cybersecurity Training, U.S. Department of State (Washington) 11 September 2019. Access Date: 6 December 2019. https://www.state.gov/industrial-control-systems-cybersecurity-training/.
[130] Industrial Control Systems Cybersecurity Training, U.S. Department of State (Washington) 11 September 2019. Access Date: 6 December 2019. https://www.state.gov/industrial-control-systems-cybersecurity-training/.
[131] CISA Releases the Updated National Emergency Communications Plan, CISA (Washington) 25 September 2019. Access Date: 10 December 2019. https://www.cisa.gov/cisa/news/2019/09/24/cisa-releases-updated-national-emergency-communications-plan.
[132] CISA Releases the Updated National Emergency Communications Plan, CISA (Washington) 25 September 2019. Access Date: 10 December 2019. https://www.cisa.gov/cisa/news/2019/09/24/cisa-releases-updated-national-emergency-communications-plan.

prevent the exacerbation of internal emergencies within the United States due to malign interference in the communications system.[133]

On 3 October 2019, an inaugural U.S.-ASEAN Cyber Policy Dialogue was held in Singapore. The Statement of the Co-chairs – the United States and Laos, which held the presidency of the Association of South East Asian Nations (ASEAN) – supported the 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and telecommunications in the Context of International Security and emphasized the recommended voluntary norms of behaviour in cyberspace.[134] Participating delegations, including that of the US, highlighted the importance of capacity building as well as initiatives and programmes related to "the protection of the critical infrastructure, combating cybercrime and terrorist use of ICT."[135]

On 16 October 2019, Assistant Secretary of State for the Bureau of East Asian and Pacific Affairs David R. Stilwell appeared before the American Senate to discuss the US policy in the Indo-Pacific region.[136] As part of the Asia Reassurance Initiative Act of 2018, the United States is providing increased support to its Indo-Pacific partners to help defend their networks from cyber threats, improve the resilience of critical infrastructure, and "counter malicious cyber activities by North Korea, China, cyber criminals, and other state and non-state cyber actors that seek to steal ... sensitive information."[137]

On 28 October 2019, the United States formalized a contribution of USD639,015 to the Organization of American States (OAS) Cybercrime Program, which is a training and technical assistance program to train judges, law enforcement, and prosecutors "the admissibility of electronic and digital evidence," among other purposes.[138] Since 2015, this is the third such contribution made by the government of the United States to support the work of the OAS as a shared regional commitment to protect individuals and businesses across the Western Hemisphere from cybercrime and transnational crime.[139]

On 5 November 2019, CISA released a joint statement from a number of U.S. government agencies concerning the 2020 election security.[140] It stated that the federal government prioritizes the sharing

[133] CISA Releases the Updated National Emergency Communications Plan, CISA (Washington) 25 September 2019. Access Date: 10 December 2019. https://www.cisa.gov/cisa/news/2019/09/24/cisa-releases-updated-national-emergency-communications-plan.
[134] ASEAN-US Cyber Policy Dialogue Initiated, GIP Digital Watch Observatory (Geneva) 3 October 2019. Access Date: 7 December 2019. https://dig.watch/updates/asean-us-cyber-policy-dialogue-initiated.
[135] ASEAN-US Cyber Policy Dialogue Initiated, GIP Digital Watch Observatory (Geneva) 3 October 2019. Access Date: 7 December 2019. https://dig.watch/updates/asean-us-cyber-policy-dialogue-initiated.
[136] Statement Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, U.S. Department of State (Washington) 16 October 2019. Access Date: 6 December 2019. https://www.state.gov/statement-before-the-senate-foreign-relations-committee-subcommittee-on-east-asia-the-pacific-and-international-cybersecurity-policy/.
[137] Statement Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, U.S. Department of State (Washington) 16 October 2019. Access Date: 6 December 2019. https://www.state.gov/statement-before-the-senate-foreign-relations-committee-subcommittee-on-east-asia-the-pacific-and-international-cybersecurity-policy/.
[138] United States Fights Cybercrime With Contribution to Organization of American States Program, U.S. Department of State (Washington) 29 October 2019. Access Date: 6 December 2019. https://www.state.gov/united-states-fights-cybercrime-with-contribution-to-organization-of-american-states-program/.
[139] United States Fights Cybercrime With Contribution to Organization of American States Program, U.S. Department of State (Washington) 29 October 2019. Access Date: 6 December 2019. https://www.state.gov/united-states-fights-cybercrime-with-contribution-to-organization-of-american-states-program/.
[140] Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, AND CISA on Ensuring Security of 2020 Elections, CISA (Washington) 5 November 2019. Access Date: 17 December 2019. https://www.cisa.gov/cisa/news/2019/11/05/joint-statement-doj-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020.

of threat intelligence and providing services that improve the security of election infrastructure.[141] The U.S. government is cooperating with all 50 states to identify threats, safely share information, and protect the democratic process.[142] The statement also assures that, despite the current absence of threats to the U.S. elections, the FBI, Department of Homeland Security and other agencies are monitoring cyberspace for suspicious social media campaigns, disinformation operations, or disruptive and/or destructive cyber-attacks on state and local infrastructure.[143]

On 5 December 2019, the United States and co-host Jamaica completed a three-day cyber capacity development workshop which included 12 Caribbean and Latin American countries. This innovative workshop, organized by the US, was the first such event in the region and designed to enhance local cybersecurity and combat cybercrime.[144]

On 5 December 2019, the US Department of State's Transnational Organized Crime (TOC) Rewards Program announced a USD5 million reward offer for information that could lead to the arrest and/or conviction of Russian cybercriminal Maksim Yakubets, following the Department of Justice's issue of federal indictments against him.[145] Yakubets was involved with several computer malware conspiracies that caused significant damage to the US as well as international financial institutions in both North America and Europe.[146] The TOC Rewards Program is one of the tools used by US authorities to bring major cybercriminals such as Yakubets, who pose a national security threat, to justice.[147]

The United States took steps to strengthen cybersecurity through domestic policy changes, and bilateral and multilateral collaboration, thus fulfilling both the domestic and international dimensions. The U.S. took actions to reinforce democratic institutions against both state and non-state actors. These actions fulfill all four dimensions of the commitment.

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

Analyst: Nadiya Kovalenko

[141] Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, AND CISA on Ensuring Security of 2020 Elections, CISA (Washington) 5 November 2019. Access Date: 17 December 2019. https://www.cisa.gov/cisa/news/2019/11/05/joint-statement-doj-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020.
[142] Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, AND CISA on Ensuring Security of 2020 Elections, CISA (Washington) 5 November 2019. Access Date: 17 December 2019. https://www.cisa.gov/cisa/news/2019/11/05/joint-statement-doj-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020.
[143] Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, AND CISA on Ensuring Security of 2020 Elections, CISA (Washington) 5 November 2019. Access Date: 17 December 2019. https://www.cisa.gov/cisa/news/2019/11/05/joint-statement-doj-dod-dhs-dni-fbi-nsa-and-cisa-ensuring-security-2020.
[144] The United States Holds Inaugural Cyber Capacity Building Workshop for the Caribbean and Latin America, U.S. Department of State (Washington) 5 December 2019. Access Date: 17 December 2019. https://www.state.gov/the-united-states-holds-inaugural-cyber-capacity-building-workshop-for-the-caribbean-and-latin-america/.
[145] Reward Offer for Information on Russian Cybercriminal Maksim Yakubets, U.S. Department of State (Washington) 5 December 2019. Access Date: 15 December 2019. https://www.state.gov/reward-offer-for-information-on-russian-cybercriminal-maksim-yakubets/.
[146] Reward Offer for Information on Russian Cybercriminal Maksim Yakubets, U.S. Department of State (Washington) 5 December 2019. Access Date: 15 December 2019. https://www.state.gov/reward-offer-for-information-on-russian-cybercriminal-maksim-yakubets/.
[147] Reward Offer for Information on Russian Cybercriminal Maksim Yakubets, U.S. Department of State (Washington) 5 December 2019. Access Date: 15 December 2019. https://www.state.gov/reward-offer-for-information-on-russian-cybercriminal-maksim-yakubets/.

European Union: 0

The European Union has partially complied with its commitment to "work collaboratively to reinforce our democracies against illicit and malign behaviour and foreign hostile interference by state and non-state actors."

On 13 September 2019, EU Competition Commissioner Margrethe Vestager lobbied for new rules against companies that use and collect data.[148] These new regulations ensure that insecure data collection will not interfere with democratic governance.[149] Vestagar hinted that the new regulations would be incorporated into the new Digital Services Act to upgrade liability and safety for digital platforms.[150] This new legislation would be applied across the EU and would target hate speech and increasing regulation in political advertising.[151]

On 10 October 2019, the European Union released a 5G risk assessment report that stated that members can exclude companies from their networks for security reasons while declining to mention any specific companies.[152] The report identified "stated-backed" actions from "non-EU states" as the greatest threats to the cybersecurity of future 5G networks.[153]

On 3 December 2019, the incoming von der Leyen Commission announced its working methods for the upcoming term, emphasizing transparency and efficiency.[154] The report established a new group, the Group for External Coordination, to discuss current international issues and coordinate positions for summits.[155] The Commission had begun to hold paperless meetings under its goal to respect data protection and security requirements as it strives to become increasingly digital.[156]

[148] Europe's New Digital Chief Wants to Protect Democracy From Big Tech, Fortune (New York City) 13 September 2019. Access Date: 17 December 2019. https://fortune.com/2019/09/13/vestager-big-tech-democracy-cambridge-analytica/.
[149] Europe's New Digital Chief Wants to Protect Democracy From Big Tech, Fortune (New York City) 13 September 2019. Access Date: 17 December 2019. https://fortune.com/2019/09/13/vestager-big-tech-democracy-cambridge-analytica/.
[150] Europe's New Digital Chief Wants to Protect Democracy From Big Tech, Fortune (New York City) 13 September 2019. Access Date: 17 December 2019. https://fortune.com/2019/09/13/vestager-big-tech-democracy-cambridge-analytica/.
[151] Europe's New Digital Chief Wants to Protect Democracy From Big Tech, Fortune (New York City) 13 September 2019. Access Date: 17 December 2019. https://fortune.com/2019/09/13/vestager-big-tech-democracy-cambridge-analytica/.
[152] EU cybersecurity report says members can ban firms from 5G networks - but declines to name China or Huawei, South China Morning Post (Hong Kong) 10 October 2019. Access Date: 3 January 2020. https://www.scmp.com/news/china/diplomacy/article/3032232/eu-cybersecurity-report-says-members-can-ban-firms-5g-networks.
[153] EU cybersecurity report says members can ban firms from 5G networks - but declines to name China or Huawei, South China Morning Post (Hong Kong) 10 October 2019. Access Date: 3 January 2020. https://www.scmp.com/news/china/diplomacy/article/3032232/eu-cybersecurity-report-says-members-can-ban-firms-5g-networks.
[154] The Working Methods of the von der Leyen Commission: Striving for more at home and in the world, The European Commission (Brussels) 3 December 2019. Access Date: 17 December 2019. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6657.
[155] The Working Methods of the von der Leyen Commission: Striving for more at home and in the world, The European Commission (Brussels) 3 December 2019. Access Date: 17 December 2019. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6657.
[156] The Working Methods of the von der Leyen Commission: Striving for more at home and in the world, The European Commission (Brussels) 3 December 2019. Access Date: 17 December 2019. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6657.

On 19 December 2019, the European Commission began a public consultation on improving resilience against cyberattacks in the financial services sector.[157] The consultation aims at gathering stakeholder views on the necessary legislative improvements to support cybersecurity measures for financial institutions.[158]

The European Union took actions to strengthen cybersecurity through domestic policy changes, thus fulfilling both the domestic dimension. The European Union took actions to reinforce democratic institutions against both state and non-state actors. These actions fulfill three of the four dimensions of the commitment.

Thus, the European Union receives a score of 0.

Analyst: Yousef Choudhri

[157] Financial services - improving resilience against cyberattacks, European Commission (Brussels) 19 December 2019. Access Date: 3 January 2020. https://ec.europa.eu/info/law/better-regulation/initiatives/financial-services-digital-resilience-2019/public-consultation_en.

[158] Financial services - improving resilience against cyberattacks, European Commission (Brussels) 19 December 2019. Access Date: 3 January 2020. https://ec.europa.eu/info/law/better-regulation/initiatives/financial-services-digital-resilience-2019/public-consultation_en.