UNIVERSITY OF TORONTO

G7 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 Final Compliance Report

27 August 2019 — 1 November 2020

Prepared by
Meagan Byrd
and the G7 Research Group

14 December 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

www.g7.utoronto.ca
munkschool.utoronto.ca

At Trinity College
1 Devonshire Place
Toronto, ON
Canada M5S 3K7
T: 416.946.8900 F: 416.946.8915

At the Observatory
315 Bloor Street West
Toronto, ON
Canada M5S 0A7
T: 416.946.8929 F: 416.946.8877

At the Canadiana Gallery
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079

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			+1
France			+1
Germany			+1
Italy			+1
Japan			+1
United Kingdom			+1
United States			+1
European Union			+1
Average		+1.00 (100%)	

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.[92]

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."[93] Further commitments include both national and international cooperation to maintain the security and resilience of cyberspace.[94]

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*.[95] Part of this commitment emphasized increased engagement with civil society, youth and others at risk of radicalization.[96]

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

[92] G8 Open Data Charter, G7 Information Centre (Toronto) 18 June 2013. Access Date: 12 October 2019. http://www.g8.utoronto.ca/summit/2013lougherne/lough-erne-open-data.html.

[93] G7 Principles and Actions on Cyber, G7 Information Centre (Toronto) 27 May 2016. Access Date: 12 October 2019. http://www.g7.utoronto.ca/summit/2016shima/cyber.html.

[94] G7 Principles and Actions on Cyber, G7 Information Centre (Toronto) 27 May 2016. Access Date: 12 October 2019. http://www.g7.utoronto.ca/summit/2016shima/cyber.html.

[95] G7 Taormina Statement on the Fight Against Terrorism and Violent Extremism, G7 Information Centre (Toronto) 26 May 2017. Access Date: 12 October 2019. http://www.g8.utoronto.ca/summit/2017taormina/statement-on-terrorism-and-extremism.html.

[96] G7 Taormina Statement on the Fight Against Terrorism and Violent Extremism, G7 Information Centre (Toronto) 26 May 2017. Access Date: 12 October 2019. http://www.g8.utoronto.ca/summit/2017taormina/statement-on-terrorism-and-extremism.html.

undermining the democratic processes and the national interests of a G7 state.[97] 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.[98]

The 2019 Biarritz summit outlined its commitments on digital democracy in the wide-ranging *Biarritz Strategy for an Open, Free and Secure Digital Transformation*.[99] 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.[100] The document also takes note of the work done by the G7 Rapid Response Mechanism established at the 2018 Charlevoix summit.[101]

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 vs. 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.

[97] Charlevoix Commitment on Defending Democracy from Foreign Threats, G7 Information Centre (Toronto) 9 June 2018. Access Date: 12 October 2019. http://www.g7.utoronto.ca/summit/2018charlevoix/democracy-commitment.html.

[98] Charlevoix Commitment on Defending Democracy from Foreign Threats, G7 Information Centre (Toronto) 9 June 2018. Access Date: 12 October 2019. http://www.g7.utoronto.ca/summit/2018charlevoix/democracy-commitment.html.

[99] Biarritz Strategy for an Open, Free and Secure Digital Transformation, G7 Information Centre (Toronto) 26 August 2019. Access Date: 12 October 2019. http://www.g7.utoronto.ca/summit/2019biarritz/biarritz-strategy-for-digital-transformation.html.

[100] Biarritz Strategy for an Open, Free and Secure Digital Transformation, G7 Information Centre (Toronto) 26 August 2019. Access Date: 12 October 2019. http://www.g7.utoronto.ca/summit/2019biarritz/biarritz-strategy-for-digital-transformation.html.

[101] Biarritz Strategy for an Open, Free and Secure Digital Transformation, G7 Information Centre (Toronto) 26 August 2019. Access Date: 12 October 2019. http://www.g7.utoronto.ca/summit/2019biarritz/biarritz-strategy-for-digital-transformation.html.

Thus, to receive a score of full compliance, G7 members must take substantial action in three or 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 two 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 one 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 ONE 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 TWO 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 THREE OR 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: +1

Canada 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."

Throughout September 2019, the Government of Canada launched programs as part of Canadian Heritage's Digital Citizen Initiative.[102] The Government of Canada has invested almost CAD7 million in programs teaching citizens to think critically and recognize fake news.[103] This initiative protects citizens from being susceptible to disinformation.[104]

On 26 September 2019, the Government of Canada announced the Joint Initiative for Digital Citizen Research.[105] 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

[102] 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.

[103] 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.

[104] 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.

[105] 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.

disinformation and finding the most effective programs and policies to counter online disinformation.[106]

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.[107] The goal of this meeting was to discuss how to collaboratively regulate the spread of disinformation on social media platforms.[108]

On 12 March 2020, the National Security and Intelligence Committee of Parliamentarians (NSICP) Annual Report 2019 was tabled.[109] This report examined threats posed by state and non-state actors against Canada's democracy, and proposed recommendations to reduce threats. [110] These recommendations included "develop[ing] practical, whole-of-government operational and policy mechanisms to identify and respond to the activities of hostile states" and "updat[ing] existing legislation, such as the Security of Information Act or the Canadian Security Intelligence Service Act."[111] The NSICP suggested using a sustained central leadership and coordination to implement these changes.[112]

Canada has taken both domestic and international actions towards reinforcing democratic institutions. Canada has acted to reinforce democratic institutions against state and non-state actors. These actions fulfil all four components of the commitment.

Thus, Canada receives a score of +1.

Analyst: Isabelle Buchanan

France: +1

France 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." It has exemplified progress in three of the four dimensions, only failing to act in a multilateral fashion against state actors specifically.

[106] 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.

[107] 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/.

[108] 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/.

[109] National Security and Intelligence Committee of Parliamentarians Annual Report 2019, National Security and Intelligence Committee of Parliamentarians (Ottawa) 12 March 2010. Access Date: 5 April 2020. https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf.

[110] National Security and Intelligence Committee of Parliamentarians Annual Report 2019, National Security and Intelligence Committee of Parliamentarians (Ottawa) 12 March 2010. Access Date: 5 April 2020. https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf.

[111] National Security and Intelligence Committee of Parliamentarians Annual Report 2019, National Security and Intelligence Committee of Parliamentarians (Ottawa) 12 March 2010. Access Date: 5 April 2020. https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf.

[112] National Security and Intelligence Committee of Parliamentarians Annual Report 2019, National Security and Intelligence Committee of Parliamentarians (Ottawa) 12 March 2010. Access Date: 5 April 2020. https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf.

On 31 August 2019, the Government of France officially accepted French translations of terms such as "data privacy" and "cyber espionage" for use in government and legislative contexts.[113]

On 28 November 2019, President Emmanuel Macron, speaking alongside NATO Secretary General Jens Stoltenberg, said he "requested [France's government] services to work on [cybersecurity]" though never pointing out a particular operator or a particular actor to defend against.[114]

On 3 December 2019, the Government of France put out a news release regarding President Emmanuel Macron's agenda at the NATO summit.[115]. Within the second priority issue, regarding a "common enemy," France called on members to address "new security challenges, such as cybersecurity."'[116]

On 22 January 2020, the French Government's Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) published its strategic direction "manifesto" for the next ten years, which places emphasis on national cybersecurity partnerships as well as strengthening its European commitments.[117]

On 29 January 2020, France developed a "5G Toolbox" following discussions with the European Commission and the European Agency for Cybersecurity. A "5G Toolbox" identifies strategic measures to enhance cybersecurity including by diversifying network supply needs across multiple providers, and conducting risk assessments of such suppliers.[118]

On 29 January 2020, the ANSSI published a report on the subject of ransomware, which consists of malware attacks in which files or system access can be held hostage by an intervening third party.[119] Ransomware is considered "the most serious current IT threat for businesses and institutions."[120] The report examined techniques of the perpetrators alongside costs of the victims, to provide more information about the threat and prevention efforts.[121]

[113] Vocabulaire du droit (liste de termes, expressions et définitions adoptés), Government of France (Paris) 31 August 2019. Access date: 16 December 2019. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000039002295&categorieLien=id.

[114] 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.

[115] NATO Summit, Government of France (Paris) 3 December 2019. Access date: 16 December 2019. https://www.gouvernement.fr/en/nato-summit.

[116] NATO Summit, Government of France (Paris) 3 December 2019. Access date: 16 December 2019. https://www.gouvernement.fr/en/nato-summit.

[117] l'ANSSI Dévoile ses Nouvelles Orientations Stratégiques pour les Années à Venir, Agence Nationale de la Sécurité des systèmes d'information (Paris) 22 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/lanssi-devoile-ses-nouvelles-orientations-strategiques-pour-les-annees-a-venir/.

[118] La France Accueille Favorablement La Publication de la « Boîte à outils 5G », Agence Nationale de la Sécurité des Systèmes d'Information (Paris) 29 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/la-france-accueille-favorablement-la-publication-de-la-boite-a-outils-5g/.

[119] Rançongiciels - L'ANSSI Livre Son Analyse de la Menace pour les Entreprises et les Institutions, Agence Nationale de la Sécurité des Systèmes d'Information (Paris) 29 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/rancongiciels-lanssi-livre-son-analyse-de-la-menace-pour-les-entreprises-et-les-institutions/.

[120] Rançongiciels - L'ANSSI Livre Son Analyse de la Menace pour les Entreprises et les Institutions, Agence Nationale de la Sécurité des Systèmes d'Information (Paris) 29 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/rancongiciels-lanssi-livre-son-analyse-de-la-menace-pour-les-entreprises-et-les-institutions/.

[121] Rançongiciels - L'ANSSI Livre Son Analyse de la Menace pour les Entreprises et les Institutions, Agence Nationale de la Sécurité des Systèmes d'Information (Paris) 29 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/rancongiciels-lanssi-livre-son-analyse-de-la-menace-pour-les-entreprises-et-les-institutions/.

On 29 January 2020, ANSSI participated in the 12th Forum International de la Cybersécurité (FIC).[122]It used such a forum to call on the European Union (EU) to develop sovereignty in matters of "autonomy and leadership in cybersecurity" and to support European citizens and institutions in threat prevention.[123] For ANSSI, this "European sovereignty" will require "renewed efforts in terms of capacity developments, regulations, industrial policy, as well as governance adapted to the challenges."[124] At the FIC, ANSSI expressed its interest in "cooperation with its European partners" and wants to "make this common set of rules operational" throughout the EU.[125]

France has taken both domestic and international actions towards reinforcing democratic institutions. France has acted to reinforce democratic institutions against non-state actors. These actions fulfil three of the four components of the commitment.

Thus, France receives a score of +1.

Analyst: Alex Erickson

Germany: +1

Germany 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 12 September 2019, German lawmakers introduced a new cloud-computing project, Gaia-X.[126] The cloud-computing platform was designed for European companies to store, process, exchange data, and cooperate on developing products.[127] The idea of the project came over fears of heavy reliance of foreign-owned cloud platforms which have been known for data interference practices.[128] German lawmakers claim that Gaia-X will not cut the country off from the global-supply chain or end divisions of labour, but instead will enable Germany's "digital infrastructures to run independently if they were ever to be cut off from foreign cloud providers."[129]

On 18 November 2019, the Bundestag Budget Committee approved 67 new posts to the Federal Commissioner for Data Protection and Freedom Information.[130] The federal body plans to push General

[122] FIC 2020: L'ANSSI Plaide pour une Souveraineté Européenne en Matière de Cybersécurité, Agence Nationale de la Securite des systemes d'information, (Paris) 29 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/fic-2020-lanssi-plaide-pour-une-souverainete-europeenne-en-matiere-de-cybersecurite/.

[123] FIC 2020: L'ANSSI Plaide pour une Souveraineté Européenne en Matière de Cybersécurité, Agence Nationale de la Securite des systemes d'information, (Paris) 29 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/fic-2020-lanssi-plaide-pour-une-souverainete-europeenne-en-matiere-de-cybersecurite/.

[124] FIC 2020: L'ANSSI Plaide pour une Souveraineté Européenne en Matière de Cybersécurité, Agence Nationale de la Securite des systemes d'information, (Paris) 29 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/fic-2020-lanssi-plaide-pour-une-souverainete-europeenne-en-matiere-de-cybersecurite/.

[125] FIC 2020: L'ANSSI Plaide pour une Souveraineté Européenne en Matière de Cybersécurité, Agence Nationale de la Securite des systemes d'information, (Paris) 29 January 2020. Access date: 10 April 2020. https://www.ssi.gouv.fr/actualite/fic-2020-lanssi-plaide-pour-une-souverainete-europeenne-en-matiere-de-cybersecurite/.

[126] 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/.

[127] 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/.

[128] 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/.

[129] 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/.

[130] 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.

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.[131]

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 (GDPR).[132] The fines are classified as minor, moderate, severe, and very severe.[133] Following the announcement of the new enforcement procedures on online platforms, Berlin issued a EUR14.5 million fine against a real estate agency for unjustified retention of customer data.[134]

Germany took actions to strengthen cybersecurity through domestic policy changes, thus fulfilling the domestic dimension. Germany 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, Germany receives a score of +1.

Analyst: Yousef Choudhri

Italy: +1

Italy 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 21 September 2019, the Italian Government adopted the Law Decree n. 105 as part of the implementation of a comprehensive national cybersecurity framework.[135] The decree requires that individuals in the public and private sectors, who serve functions that are key components 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.[136]

On 22 December 2019, Industry Minister Stefano Patuanelli announced that Chinese telecommunication firm Huawei, should be allowed to participate in the development of Italy's future 5G network.[137] The announcement was released after the parliamentary security committee,

[131] 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.

[132] 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.

[133] 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.

[134] 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.

[135] 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.

[136] 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.

[137] 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.

Copasir, stated that the government should consider preventing Huawei from participating in the development of a future 5G network.[138]

Italy has taken domestic actions towards reinforcing democratic institutions. Italy has acted to reinforce democratic institutions against state and non-state actors. These actions fulfil three of the four components of the commitment.

Thus, Italy receives a score of +1.

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 UN Open-ended Working Group (OEWG) on Cybersecurity held in New York.[139] 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."[140] 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.[141]

On 9 to 12 September 2019, Japan's Ministry of Economy, Trade and Industry (METI) and the Industrial Cyber Security Center of Excellence (ICSCoE) under the information-technology Promotion Agency (IPA), hosted the Japan-US Industrial Control Systems Cybersecurity Training in Tokyo.[142] American and Japanese experts delivered lectures on the security of control systems of critical infrastructure.[143] Attendees were from 14 countries and regions in the Indo-Pacific region. [144]

[138] 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.

[139] 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.

[140] 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.

[141] 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.

[142] 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.

[143] 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.

[144] 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.

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.[145] Officials compared notes on current efforts in strengthening cyber defence.[146] They also affirmed commitment in "[supporting] a norms-based, predictable, and secure cyberspace."[147] Japanese Director of Strategic Planning Division at the Ministry of Defence Kyosuke Matsumoto, said Japan gave priority to "strengthening our cyber defence capability" and Japan valued "effectively cooperate with other like-minded countries to take prompt and appropriate actions against cyberattacks."[148]

On 11 October 2019, Japan hosted the 7th US-Japan Cyber Dialogue in Tokyo.[149] 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."[150]

On 18 October 2019, the Japanese government increased the budget for cybersecurity from JPY71.29 billion to JPY88.11 billion.[151] The new budget distributed more fundings for unauthorized communication monitoring, operation cost of the Cyber Security Council, cyber security awareness-raising projects, and international collaboration.[152]

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 awareness."[153]

On 4 November 2019, Japan and ASEAN issued the Joint Statement of the 22nd ASEAN-Japan Summit on connectivity.[154] These countries declared to "[enhance] cybersecurity capacity building for

[145] 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.

[146] 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.

[147] 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.

[148] 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.

[149] 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.

[150] 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.

[151] 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.

[152] 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.

[153] Results of the Japan-ASEAN Cybersecurity Policy Conference, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 19 November 2019. Access Date: 15 December 2019. https://www.nisc.go.jp/press/pdf/aseanj_meeting20191119.pdf.

[154] 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/.

ASEAN through the ASEAN-Japan Cybersecurity Capacity Building Centre and the ASEAN-Singapore Cybersecurity Centre of Excellence."[155]

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.[156] They discussed the current environment in the field of cyber affairs, each country's policies on cyber issues, and future cooperation on cyber issues.[157]

On 18 November 2019, the Cabinet Secretariat Cyber Security Center Tomoo Yamauchi issued a document on 2020 Cyber Security Month.[158] The government planned to raise public awareness on 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.[159]

On 19 November 2019, Minister for Foreign Affairs Motegi Toshimitsu met with the Chairman of Rasmussen Global Anders Fogh Rasmussen.[160] Rasmussen acknowledged Japan as "an important partner for Europe in a global battle for freedom and democracy."[161] He also invited Japan to attend a democracy summit meeting next June in Copenhagen.[162]

On 20 November 2019, Japan hosted the 4th Japan-Russia Cyber Security Consultation in Tokyo.[163] The representatives discussed the current landscape in cyberspace, and strategies and policies each country's strategies and policies on cyber issues.[164] They also discussed the issues of cybersecurity in multilateral and regional context and security of critical information infrastructure. [165]

[155] 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/.

[156] 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.

[157] 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.

[158] 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.

[159] 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.

[160] 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.

[161] 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.

[162] 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.

[163] 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.

[164] 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.

[165] 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.

On 16 January 2020, Japan, represented by Yamaguchi Isamu, the director of Emerging Security Challenges Division, Ministry of Foreign Affairs, co-chaired the fifth open-ended study group of Asean Regional Forum (ARF) Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ICT) on Confidence Building Measures, with Malaysia and Singapore.[166] The participating experts discussed proposals on a whole range of ICT security issues, including confidence building measures.[167]

On 21 January 2020, the Management Committee of ICT Information Sharing and Analysis Centre (ICT-ISAC), headed by Management Committee Chair Satoru Koyama, discussed information sharing initiatives, including collaborations with domestic and international working groups.[168] The committee also discussed the private sector's expectation and issues regarding public-private information sharing.[169]

On 23 January 2020, the Cabinet Cyber Security Center collaborated with "Sword Art Online Alicization War of Underworld" (SAO-O) Project to create a tie-up poster and a web banner using characters from the aforementioned animation, to disseminate knowledge and raise awareness about cyber security, especially toward the younger demographic.[170]

On 27 January 2020, Japan Internet Providers Association and Japan Network Information Center organized a brief session for the Internet Governance Forum (IGF) 2019 report, "Is One World, One Net, One Vision Possible?."[171] The event planned to discuss "the main agenda items at IGF2019" and the development of Internet governance in Japan.[172]

On 29 January 2020, the Cabinet Cyber Security Center issued a quarterly situation analysis of critical infrastructure.[173] The report acknowledged the importance of exchanging values and sharing information regarding critical infrastructure and analysis of cybersecurity incidents with stakeholders.[174] The report also suggested cybersecurity policies, such as implementing multifaceted defence, designing countermeasures based on thorough understanding of current attacks, using external services if necessary, and reviewing supply chain risks.[175]

[166] ARF-ISM on ICTs Security 5th SG, Ministry of Foreign Affairs of Japan (Tokyo) 16 January 2020. Access Date: 23 March 2020. https://www.mofa.go.jp/press/release/press4e_002757.html.

[167] ARF-ISM on ICTs Security 5th SG, Ministry of Foreign Affairs of Japan (Tokyo) 16 January 2020. Access Date: 23 March 2020. https://www.mofa.go.jp/press/release/press4e_002757.html.

[168] ICT-ISAC Initiatives, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 23 January 2020. Access Date: 1 April 2020. https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou04.pdf.

[169] ICT-ISAC Initiatives, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 23 January 2020. Access Date: 1 April 2020. https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou04.pdf.

[170] Tie-up with Sword Art Online Alicization War of the Underworld. National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 23 January 2020. Access Date: 1 April 2020. https://www.nisc.go.jp/security-site/month/sao.html.

[171] Announcement of IGE2019 Report Session-Is One World, One Net, One Vision Possible? Access Date: March 2020. https://japanigf.jp/topics/igf2019_readout.

[172] Announcement of IGE2019 Report Session-Is One World, One Net, One Vision Possible? Access Date: March 2020. https://japanigf.jp/topics/igf2019_readout.

[173] Situation surrounding critical infrastructure. National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 29 January 2020. Access Date: 1 April 2020. https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou05.pdf.

[174] Situation surrounding critical infrastructure. National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 29 January 2020. Access Date: 1 April 2020. https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou05.pdf.

[175] Situation surrounding critical infrastructure. National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 29 January 2020. Access Date: 1 April 2020. https://www.nisc.go.jp/conference/cs/ciip/dai21/pdf/21shiryou05.pdf.

On 30 January 2020, the Secretariat of Cabinet Cyber Security Center (NISC) Tomoo Yamauchi discussed the formulation of the 2020 cyber security annual plan.[176] The Center asked for the public's input on necessary measures for cyber security.[177]

On 31 January 2020, the Fifth Japan-UK Bilateral Consultation on Cyberspace, chaired by Ambassador Akahori Takeshi and Dr. Alexandre Evans, took place in Tokyo.[178] At this meeting, the participants discussed "the latest cybersecurity strategy and efforts," bilateral cooperation on capacity building, and multilateral cooperation in the United Nations.[179]

On 7 February 2020, the 13th meeting of the Cyber Security Strategy Division Research and Development Strategy Expert Committee took place in Tokyo.[180] The participants discussed initiatives of ministries and agencies based on "Cyber Security Research and Technology Development Policy" and community formation through industry-academia-government collaboration.[181]

On 10 February 2020, the Japan-Estonia Summit Meeting took place in Tokyo.[182] Prime Minister Shinzo Abe mentioned a previous collaboration with Estonia regarding ICT.[183] He also discussed Japanese participation in NATO cyber defence exercises, and the NATO Cooperative Cyber Defence Centre of Excellence hosted by Estonia.[184]

On 2 March 2020, the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) released a Cyber Security Law Q and A Handbook, aimed at informing businesses on "legal issues concerning information handling" and laws "related to cyber security measures and response to incidents."[185]

On 2 March 2020, the 12th meeting of the Cyber Security Strategy Headquarters Awareness Promotion/Human Resource Development Special Investigation Committee took place in Tokyo.[186]

[176] Call for opinions on measures to be implemented in 2020 based on the Cyber Security Strategy (closed), National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 30 January 2020. Access Date: 11 April 2020. https://www.nisc.go.jp/active/kihon/cyber-security2020.html.

[177] Call for opinions on measures to be implemented in 2020 based on the Cyber Security Strategy (closed), National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 30 January 2020. Access Date: 11 April 2020. https://www.nisc.go.jp/active/kihon/cyber-security2020.html.

[178] The 5th Japan-UK Consultations on Cyberspace, Ministry of Foreign Affairs of Japan (Tokyo) 31 January 2020. Access Date: 11 April 2020. https://www.mofa.go.jp/press/release/press4e_002766.html.

[179] The 5th Japan-UK Consultations on Cyberspace, Ministry of Foreign Affairs of Japan (Tokyo) 31 January 2020. Access Date: 11 April 2020. https://www.mofa.go.jp/press/release/press4e_002766.html.

[180] Cyber Security Strategy Division Research and Development Strategy Expert Committee, the 13th Meeting Agenda, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 7 February 2020. Access Date: 11 April 2020. https://www.nisc.go.jp/conference/cs/kenkyu/dai13/pdf/13gijishidai.pdf.

[181] Cyber Security Strategy Division Research and Development Strategy Expert Committee, the 13th Meeting Agenda, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 7 February 2020. Access Date: 11 April 2020. https://www.nisc.go.jp/conference/cs/kenkyu/dai13/pdf/13gijishidai.pdf.

[182] Japan-Estonia Summit Meeting, Ministry of Foreign Affairs of Japan (Tokyo) 10 February 2020. Access Date: 18 April 2020. https://www.mofa.go.jp/erp/we/ee/page4e_001177.html.

[183] Japan-Estonia Summit Meeting, Ministry of Foreign Affairs of Japan (Tokyo) 10 February 2020. Access Date: 18 April 2020. https://www.mofa.go.jp/erp/we/ee/page4e_001177.html.

[184] Japan-Estonia Summit Meeting, Ministry of Foreign Affairs of Japan (Tokyo) 10 February 2020. Access Date: 18 April 2020. https://www.mofa.go.jp/erp/we/ee/page4e_001177.html.

[185] About "Cyber Security Law Q & A Handbook," National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 2 March 2020. Access Date: 11 April 2020. https://www.nisc.go.jp/security-site/law_handbook/index.html.

[186] Cyber Security Strategy Headquarters Awareness Promotion / Human Resource Development Special Investigation Committee, the 12th meeting agenda, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 2 March 2020. Access Date: 11 April 2020. https://www.nisc.go.jp/conference/cs/jinzai/dai12/pdf/12gijishidai.pdf.

The participants discussed the approaches of the Cyber Security Awareness and Action Enhancement Program, the overview of development of strategic management, the cyber security laws and regulations sub-workings, and to report on group study results.[187]

Japan has taken both domestic and international actions towards reinforcing democratic institutions. Japan has acted to reinforce democratic institutions against state and non-state actors. These actions fulfil all four components of the commitment.

Thus, Japan receives a score of +1.

Analyst: Zihan (Alison) Pang

United Kingdom: +1

The United Kingdom has fully complied with its commitment to "work collaboratively to reinforce G7 democracies against illicit and malign behavior and foreign hostile interference by state and non-state actors."

From 3 September 2019 to 17 March 2020, the Democracy and Digital Technologies Committee convened 16 times to converse with witnesses about the reconciliation of democracy and digital technologies.[188] Ranging from government officials to industry experts, these witnesses answered various inquiries that the committee may have about misinformation, cybersecurity, digital campaigning, etc.[189]

On 18 October 2019, Business Secretary Andrea Leadsom announced that the UK government will be partnering with technology firm ARM, by providing GBP36 million towards a new project to develop computer hardware that is more resistant to cyber attacks.[190] This is the next phase of the UK government's Digital Security by Design initiative.[191]

In November 2019, Politico reported that the UK's electoral laws were insufficient in addressing "clandestine digital political interference."[192] 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."[193]

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

[187] Cyber Security Strategy Headquarters Awareness Promotion / Human Resource Development Special Investigation Committee, the 12th meeting agenda, National Centre of Incident Readiness and Strategy for Cybersecurity (Tokyo) 2 March 2020. Access Date: 11 April 2020. https://www.nisc.go.jp/conference/cs/jinzai/dai12/pdf/12gijishidai.pdf.

[188] All events, UK Parliament Democracy and Digital Technologies Committee (London) 17 March 2020. Access Date: 4 April 2020. https://committees.parliament.uk/work/5/democracy-and-digital-technologies/events/all/?SessionId=0&SortBy=StartDateAscending.

[189] Committee news, UK Parliament Democracy and Digital Technologies Committee (London) 17 March 2020. Access Date: 4 April 2020. https://committees.parliament.uk/committee/407/democracy-and-digital-technologies-committee/news/.

[190] 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.

[191] 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.

[192] 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/.

[193] 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/.

cybersecurity measures.[194] Minister Warman stated that overcoming barriers to improving cybersecurity "can help make the UK the safest place to live and do business online."[195]

On 5 November 2019, Minister for the Cabinet Office Oliver Dowden updated Parliament on numerous actions that the government took "to tackle intimidation" online, especially in relation to electoral matters.[196] In this update, the Minister spoke about the Online Harms White Paper, intended to make online platforms responsible for their user's illegal activities; to illegalize "undue influence of" a voter during elections; to "introduce a digital imprints regime"; and to introduce the Defending Democracy Programme, which aims to "protect…UK democratic processes…from interference, including from cyber…threats."[197]

On 25 November 2019, the Ministry of Justice announced that it was inviting bids for the creation of a centralized cybersecurity log collection and aggregation platform.[198] 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."[199]

On 16 December 2019, Prime Minister Boris Johnson announced that his government will release an Intelligence and Security Committee of Parliament (ISC) report on Russian interference during the 2016 UK European Union membership referendum in 2020.[200]

On 15 January 2020, then Secretary of State for Digital, Culture, Media and Sport Baroness Nicky Morgan revealed that the government had invested "1.9 billion pounds to protect the nation online" through the National Cyber Security Strategy.[201]

On 3 February 2020, Baroness Nicky Morgan disclosed that the government committed GBP 2 million "for the pilot of the Future News Fund"[202]. According to the innovation charity Nesta, who

[194] 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.

[195] 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.

[196] Update on tackling intimidation in public life, Government of the United Kingdom (London) 5 November 2019. Access Date: 9 April 2020. https://www.gov.uk/government/speeches/update-on-tackling-intimidation-in-public-life.

[197] Update on tackling intimidation in public life, Government of the United Kingdom (London) 5 November 2019. Access Date: 9 April 2020. https://www.gov.uk/government/speeches/update-on-tackling-intimidation-in-public-life.

[198] 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/.

[199] 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/.

[200] 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.

[201] Baroness Morgan speaking on how we can make technology work for everyone, Government of the United Kingdom (London) 15 January 2020. Access Date: 12 April 2020. https://www.gov.uk/government/speeches/baroness-morgan-speaking-on-how-we-can-make-technology-work-for-everyone.

[202] Letter from Secretary of State for Digital, Culture, Media and Sport, Rt Hon Baroness Morgan of Cotes to the Chair, UK Parliament Democracy and Digital Technologies Committee (London) 11 March 2020. Access Date: 12 April 2020. https://committees.parliament.uk/committee/407/democracy-and-digital-technologies-committee/publications/3/correspondence/.

is responsible for the pilot, the project gives "communities in England…access to reliable…news" to protect the UK's democracy.[203]

On 12 February 2020, the Department for Digital, Culture, Media & Sport revised the Online Harms White Paper[204] This report addresses the "real danger that hostile actors" online can have on the UK's "democratic values and principles" and outlines the UK government's intention to establish a "duty of care to make companies…tackle harm caused by content or activity on their services," invest in new technologies in the field of cybersecurity, and inform citizens about online safety.[205]

The UK has taken domestic actions towards reinforcing democratic institutions. The UK has acted to reinforce democratic institutions against state and non-state actors. These actions fulfil three of the four components of the commitment.

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

Analyst: Kevin Zuo

United States: +1

The United States has fully complied with its commitment to reinforce democratic institutions against illicit and malign behaviour and foreign hostile interference by state and non-state actors.

On 4 September 2019, US 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.[206] 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.[207] 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."[208]

From 9 to 13 September 2019, the United States hosted the first meeting of the UN 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.[209] He has also stated that one of the key goals of this initiative is to ensure that the US and

[203] Government-backed pilot fund to innovate public interest news to protect democracy, Nesta (London) 4 November 2019. Access Date: 12 April 2020. https://www.nesta.org.uk/news/government-backed-pilot-fund-innovate-public-interest-news-protect-democracy/

[204] Online Harms White Paper, Government of the United Kingdom (London) 12 February 2020. Access Date: 9 April 2020. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

[205] Online Harms White Paper, Government of the United Kingdom (London) 12 February 2020. Access Date: 9 April 2020. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

[206] 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.

[207] 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.

[208] 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.

[209] 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/.

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.[210]

On 24 September 2019, the Cybersecurity and Infrastructure Security Agency released an updated National Emergency Communications Plan aimed at improving the US emergency communications capabilities at all levels of government.[211] 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.[212] This public safety development will prevent the exacerbation of internal emergencies within the United States due to malign interference in the communications system.[213]

On 30 September 2019, the United States imposed sanctions on four entities and seven individuals associated with the Russian Internet Research Agency and its financier, Yevgeniy Prigozhin.[214] The government of the United States promised to ensure that people who "carry out destabilizing activities that threaten the interests of the United States and its allies and partners" are subject to sanctions.[215] Michael R. Pompeo, Secretary of State, also stated that the US will continue fighting against malign actors who seek to subvert American democratic processes and will impose further punishment on Russian Federation for "its destabilizing and unacceptable activities" because the US will not tolerate foreign interference in its elections.[216]

On 3 October 2019, an inaugural US-ASEAN Cyber Policy Dialogue was held in Singapore. The Statement of the Co-chairs – the US and Laos – 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.[217] 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."[218]

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

[210] 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/.

[211] 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.

[212] 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.

[213] 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.

[214] U.S. Targets Russian Actors Involved in Efforts to Influence U.S. Elections, U.S. Department of State (Washington) 30 September 2019. Access Date: 6 December 2019. https://www.state.gov/u-s-targets-russian-actors-involved-in-efforts-to-influence-u-s-elections/.

[215] U.S. Targets Russian Actors Involved in Efforts to Influence U.S. Elections, U.S. Department of State (Washington) 30 September 2019. Access Date: 6 December 2019. https://www.state.gov/u-s-targets-russian-actors-involved-in-efforts-to-influence-u-s-elections/.

[216] U.S. Targets Russian Actors Involved in Efforts to Influence U.S. Elections, U.S. Department of State (Washington) 30 September 2019. Access Date: 6 December 2019. https://www.state.gov/u-s-targets-russian-actors-involved-in-efforts-to-influence-u-s-elections/.

[217] 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.

[218] 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.

region.[219] As part of the Asia Reassurance Initiative Act of 2018, the US 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."[220]

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.[221] 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.[222]

On 5 November 2019, Cybersecurity and Infrastructure Security Agency (CISA) released a joint statement from a number of US government agencies concerning the 2020 election security.[223] It stated that the federal government prioritizes the sharing of threat intelligence and providing services that improve the security of election infrastructure.[224] The US government is cooperating with all 50 states to identify threats, safely share information, and protect the democratic process.[225] The statement also assures that, despite the current absence of threats to the US 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.[226]

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.[227] This

[219] 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/.

[220] 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/.

[221] 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/.

[222] 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/.

[223] 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.

[224] 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.

[225] 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.

[226] 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.

[227] 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/.

innovative workshop, organized by the US, was the first such event in the region and designed to enhance local cybersecurity and combat cybercrime.[228]

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.[229] 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.[230] The TOC Rewards Program is one of the tools used by US authorities to bring major cybercriminals like Yakubets, who pose a national security threat, to justice.[231]

On 16 January 2020, bill S.3207, titled Cybersecurity State Coordinator Act of 2020, was introduced to the US Senate.[232] This bill would obligate the Department of Homeland Security to appoint a Cybersecurity State Coordinator in each state, who would be responsible for advising on the development of secure infrastructure, serving as the main federal cybersecurity risk advisor, and facilitating the transmission of cyberthreat information between federal and non-federal entities.[233]

On 29 January 2020, bill H.R.5680, titled the Cybersecurity Vulnerability Identification and Notification Act of 2020, passed the House Committee on Homeland Security.[234] This bill proposes to amend the Homeland Security Act of 2002 by granting the CISA subpoena authority to compel internet service providers to disclose the identity of owners of critical infrastructure whose devices the agency cannot identify otherwise.[235] This information would be used to notify critical infrastructure entities of vulnerabilities in their systems.[236]

On 30 January 2020, the US expressed its support for a Toolbox developed by the European Union Network Information Security Cooperation Group.[237] This Toolbox includes an acknowledgment of

[228] 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/.

[229] 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/.

[230] 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/.

[231] 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/.

[232] S. 3207 - Cybersecurity State Coordinator Act of 2020, Congress.gov (Washington) 11 March 2020. Access Date: 10 April 2020. https://www.congress.gov/bill/116th-congress/senate-bill/3207.

[233] S. 3207 - Cybersecurity State Coordinator Act of 2020, Congress.gov (Washington) 11 March 2020. Access Date: 10 April 2020. https://www.congress.gov/bill/116th-congress/senate-bill/3207.

[234] H.R.5680 - Cybersecurity Vulnerability Identification and Notification Act of 2020, Congress.gov (Washington) 29 January 2020. Access Date: 9 April 2020. https://www.congress.gov/bill/116th-congress/house-bill/5680/text?q=%7B%22search%22%3A%5B%22HR+1%22%5D%7D&r=17&s=1.

[235] H.R.5680 - Cybersecurity Vulnerability Identification and Notification Act of 2020, Congress.gov (Washington) 29 January 2020. Access Date: 9 April 2020. https://www.congress.gov/bill/116th-congress/house-bill/5680/text?q=%7B%22search%22%3A%5B%22HR+1%22%5D%7D&r=17&s=1.

[236] H.R.5680 - Cybersecurity Vulnerability Identification and Notification Act of 2020, Congress.gov (Washington) 29 January 2020. Access Date: 9 April 2020. https://www.congress.gov/bill/116th-congress/house-bill/5680/text?q=%7B%22search%22%3A%5B%22HR+1%22%5D%7D&r=17&s=1.

[237] United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers, U.S. Department of State (Washington) 30 January 2020. Access Date: 10 April 2020. https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/.

risks posed by 5G suppliers based in authoritarian countries with previous history of malign cyber behaviour and a recommendation for EU members to exclude such companies from critical parts of their 5G networks.[238] The US welcomed this action by the EU; however, it added that all parts of 5G networks must be viewed as "critical infrastructure" that every country should take steps to protect.[239] The US called upon its European allies to implement EU recommendations, referencing its own measures taken to secure American 5G networks, mainly prohibiting "untrusted suppliers" such as Huawei and ZTE.[240]

On 10 February 2020, the National Counterintelligence and Security Center (NCSC) released a report, concluding that the US is facing espionage threats from state adversaries, namely China, Russia, Iran, North Korea, Cuba, the Lebanese Hizballah, ISIS, and al-Qaeda.[241] This report, titled the National Counterintelligence Strategy for 2020-2022, warns against artificial intelligence, advanced encryption, and the Internet, as the aforementioned adversaries are increasingly using emerging technologies to attack the US private sector and democratic institutions.[242] The objectives outlined in this document include "countering cyber and other technological espionage" as well as defending the democratic tradition from covert media campaigns designed to sway Americans' public opinion against the US government and towards foreign agendas.[243]

On 10 February 2020, the Department of Justice issued charges against four members of China's People's Liberation Army who stole personal data of millions of American citizens from the US credit agency, Equifax, in 2017.[244] Their action was labelled as a "counterintelligence attack" on the US.[245] During a subsequent briefing for reporters, NCSC Director William Evanina stated that the diversity and intensity of cyber attacks against the US are increasing, so any individuals involved in them will face severe legal consequences.[246]

On 11 February 2020, Republican Senators rejected three election-security bills.[247] The first one was the Defending Elections from Threats by Establishing Redlines (DETER) Act designed to disincentivize Russia from interfering in the US elections via sanctions.[248] The second one was the

[238] United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers, U.S. Department of State (Washington) 30 January 2020. Access Date: 10 April 2020. https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/.

[239] United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers, U.S. Department of State (Washington) 30 January 2020. Access Date: 10 April 2020. https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/.

[240] United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers, U.S. Department of State (Washington) 30 January 2020. Access Date: 10 April 2020. https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/.

[241] U.S. Counterintelligence Chief Warns of Broadening Spy Threat, CBS News (New York City) 10 February 2020. Access Date: 10 April 2020. https://www.cbsnews.com/news/u-s-counterintelligence-chief-warns-of-broadening-spy-threat/.

[242] U.S. Counterintelligence Chief Warns of Broadening Spy Threat, CBS News (New York City) 10 February 2020. Access Date: 10 April 2020. https://www.cbsnews.com/news/u-s-counterintelligence-chief-warns-of-broadening-spy-threat/.

[243] U.S. Counterintelligence Chief Warns of Broadening Spy Threat, CBS News (New York City) 10 February 2020. Access Date: 10 April 2020. https://www.cbsnews.com/news/u-s-counterintelligence-chief-warns-of-broadening-spy-threat/.

[244] U.S. Counterintelligence Chief Warns of Broadening Spy Threat, CBS News (New York City) 10 February 2020. Access Date: 10 April 2020. https://www.cbsnews.com/news/u-s-counterintelligence-chief-warns-of-broadening-spy-threat/.

[245] U.S. Counterintelligence Chief Warns of Broadening Spy Threat, CBS News (New York City) 10 February 2020. Access Date: 10 April 2020. https://www.cbsnews.com/news/u-s-counterintelligence-chief-warns-of-broadening-spy-threat/.

[246] U.S. Counterintelligence Chief Warns of Broadening Spy Threat, CBS News (New York City) 10 February 2020. Access Date: 10 April 2020. https://www.cbsnews.com/news/u-s-counterintelligence-chief-warns-of-broadening-spy-threat/.

[247] Senate GOP Rejects Election-Security Measures (Yes, Again), MSNBC (New York City) 11 February 2020. Access Date: 11 April, 2020. https://www.msnbc.com/rachel-maddow-show/senate-gop-rejects-election-security-measures-yes-again-n1135221.

[248] Senate GOP Rejects Election-Security Measures (Yes, Again), MSNBC (New York City) 11 February 2020. Access Date: 11 April, 2020. https://www.msnbc.com/rachel-maddow-show/senate-gop-rejects-election-security-measures-yes-again-n1135221.

Securing America's Federal Elections (SAFE) Act that required voting systems to use backup paper ballots and technological safeguards.[249] The last one was the Stopping Harmful Interference in Elections for a Lasting Democracy (SHIELD) Act mandating candidates to inform law enforcement officials about a foreign power's offer of campaign assistance.[250] The rejection of these bills blocks US efforts to strengthen cybersecurity in the upcoming presidential elections.[251]

On 20 February 2020, the US government condemned a cyber attack against the country of Georgia. This attack was carried out by Russian General Staff Main Intelligence Directorate and disrupted the operation of several thousand Georgian government and private websites as well as interrupting the broadcasts of two television stations.[252] The US called on Russia to discontinue its behaviour in Georgia as it undermines democratic institutions and creates uncertainty.[253] The US Secretary of State Michael R. Pompeo reiterated that responsible behaviour of countries is key to stable international cyberspace, which the US will continue to uphold.[254] Furthermore, the US pledged to support Georgia in improving their cybersecurity by providing technical assistance to strengthen the country's public institutions.[255]

On 11 March 2020, the Cyberspace Solarium Commission (CSC) published a report that presented a strategic approach to protecting the security of American cyberspace against cyber attacks.[256] The CSC proposed "a strategy of layered cyber deterrence," which consisted of more than 80 recommendations.[257] These recommendations include reforming the federal government's structure and organization for cyberspace, strengthening non-military cyber tools, promoting national resilience, and enhancing cybersecurity cooperation with the private sector.[258]

The US has taken domestic and international actions towards reinforcing democratic institutions. The US has acted to reinforce democratic institutions against state and non-state actors. These actions fulfil all four components of the commitment.

Thus, the US receives a score of +1.

Analyst: Nadiya Kovalenko

[249] Senate GOP Rejects Election-Security Measures (Yes, Again), MSNBC (New York City) 11 February 2020. Access Date: 11 April, 2020. https://www.msnbc.com/rachel-maddow-show/senate-gop-rejects-election-security-measures-yes-again-n1135221.

[250] Senate GOP Rejects Election-Security Measures (Yes, Again), MSNBC (New York City) 11 February 2020. Access Date: 11 April, 2020. https://www.msnbc.com/rachel-maddow-show/senate-gop-rejects-election-security-measures-yes-again-n1135221.

[251] Senate GOP Rejects Election-Security Measures (Yes, Again), MSNBC (New York City) 11 February 2020. Access Date: 11 April, 2020. https://www.msnbc.com/rachel-maddow-show/senate-gop-rejects-election-security-measures-yes-again-n1135221.

[252] The United States Condemns Russian Cyber Attack Against the Country of Georgia, U.S. Department of State (Washington) 20 February 2020. Access Date: 10 April 2020. https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

[253] The United States Condemns Russian Cyber Attack Against the Country of Georgia, U.S. Department of State (Washington) 20 February 2020. Access Date: 10 April 2020. https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

[254] The United States Condemns Russian Cyber Attack Against the Country of Georgia, U.S. Department of State (Washington) 20 February 2020. Access Date: 10 April 2020. https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

[255] The United States Condemns Russian Cyber Attack Against the Country of Georgia, U.S. Department of State (Washington) 20 February 2020. Access Date: 10 April 2020. https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

[256] CSC Executive Summary, United States of America Cyberspace Solarium Commission (Washington) 11 March 2020. Access Date: 11 April 2020. https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view.

[257] CSC Executive Summary, United States of America Cyberspace Solarium Commission (Washington) 11 March 2020. Access Date: 11 April 2020. https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view.

[258] CSC Executive Summary, United States of America Cyberspace Solarium Commission (Washington) 11 March 2020. Access Date: 11 April 2020. https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view.

European Union: +1

The European Union 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 19 February 2020, the EU Commission released a white paper regarding artificial intelligence (AI).[259] The white paper aims to support Europe's core values of openness, diversity and democracy.[260] President of the EU Commission Ursula von der Leyen outlined the intentions of the white paper, which cover areas including cybersecurity, critical digital infrastructure, democracy and media.[261]

On 19 February 2020, Politico published an article stating that the EU Commission intends on delivering a concrete data strategy framework by the end of 2020.[262] The framework would be applied towards "common European data spaces" which could be implemented as early as 2022.[263] The report also mentions the Commission's goal to implement the Data Act by 2021.[264] This new policy would seek to remove existing barriers and introduce rules for business-to-business as well as business-to-government data sharing.[265]

The EU has taken domestic actions towards reinforcing democratic institutions. The EU has acted to reinforce democratic institutions against state and non-state actors. These actions fulfil three of the four components of the commitment.

Thus, The European Union has received a score of +1.

Analyst: Yousef Choudhri

[259] The European Commission has Released their White Paper on Artificial Intelligence today as Promise, Patently Apple (Brussels) 19 February 2020. Access Date: 13 April 2020. https://www.patentlyapple.com/patently-apple/2020/02/the-european-commission-has-released-their-white-paper-on-artificial-intelligence-today-as-promised.html.

[260] The European Commission has Released their White Paper on Artificial Intelligence today as Promise, Patently Apple (Brussels) 19 February 2020. Access Date: 13 April 2020. https://www.patentlyapple.com/patently-apple/2020/02/the-european-commission-has-released-their-white-paper-on-artificial-intelligence-today-as-promised.html.

[261] The European Commission has Released their White Paper on Artificial Intelligence today as Promise, Patently Apple (Brussels) 19 February 2020. Access Date: 13 April 2020. https://www.patentlyapple.com/patently-apple/2020/02/the-european-commission-has-released-their-white-paper-on-artificial-intelligence-today-as-promised.html.

[262] Europe's digital vision, explain, Politico (Arlington) 19 February 2020. Access Date: 13 April 2020. https://www.politico.eu/article/europes-digital-vision-explained/.

[263] Europe's digital vision, explain, Politico (Arlington) 19 February 2020. Access Date: 13 April 2020. https://www.politico.eu/article/europes-digital-vision-explained/.

[264] Europe's digital vision, explain, Politico (Arlington) 19 February 2020. Access Date: 13 April 2020. https://www.politico.eu/article/europes-digital-vision-explained/.

[265] Europe's digital vision, explain, Politico (Arlington) 19 February 2020. Access Date: 13 April 2020. https://www.politico.eu/article/europes-digital-vision-explained/.