2019 G20 Osaka Summit Final Compliance Report

Prepared by
Sofia Lopez and the G20 Research Group
University of Toronto
Toronto
and
Irina Popova and the Center for International Institutions Research
Russian Presidential Academy of National Economy and Public Administration,
Moscow

From 30 June 2019 to 10 October 2020

19 November 2020

"The University of Toronto … produced a detailed analysis to the extent of which each G20 country has met its commitments since the last summit … I think this is important; we come to these summits, we make these commitments, we say we are going to do these things and it is important that there is an organisation that checks up on who has done what."

— *David Cameron, Prime Minister, United Kingdom, at the 2012 Los Cabos Summit*

Munk School of Global Affairs
Trinity College at the University of Toronto
1 Devonshire Place, Room 209N
Toronto, Ontario M5S 3K7
Canada
www.g20.utoronto.ca

G20 RESEARCH GROUP
@G20rg

Centre for International Institutions Research at
the Russian Presidential Academy of National
Economy and Public Administration
11 Prechistenskaya nabarezhnaya
Moscow, Russia 119034
www.ranepa.ru/eng/ciir

Contents

9. Terrorism: Internet Security

"For us all to reap the rewards of digitalisation, we are committed to realising an open, free and secure internet."

G20 2019 Osaka Leaders' Declaration

Assessment

	No Compliance	Partial Compliance	Full Compliance
Argentina		0	
Australia		0	
Brazil		0	
Canada			+1
China		0	
France		0	
Germany		0	
India		0	
Indonesia	−1		
Italy		0	
Japan		0	
Korea			+1
Mexico	−1		
Russia		0	
Saudi Arabia		0	
South Africa		0	
Turkey	−1		
United Kingdom		0	
United States		0	
European Union			+1
Average	0 (50%)		

Background

G20 members are fundamentally united against any form of terrorism or terrorist activity. The leaders believe that a concerted effort is necessary by governments to stop terrorism and terrorist activity. Before the Osaka Summit, the group had specifically dealt with issues concerning illegal financial activities that may support terrorist activities and terrorist financing.

At the first summit in 2008, in Washington DC, the G20 committed to addressing the fight against terrorism and declared that "national and regional authorities should implement national and international measures that protect the global financial system from uncooperative and non-transparent jurisdictions that pose risks of illicit financial activity."[2637]

At the 2009 Pittsburgh Summit, the G20 also expressed its continued support for the Financial Action Task Force (FATF) and its significant work to deter terrorist financing.[2638] The G20 called on the FATF to publish a list of high-risk jurisdictions in the fight against terrorist financing and money

[2637] Declaration of the Summit on Financial Markets and the World Economy, G20 Information Centre (Toronto) 15 November 2008. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2008/2008declaration1115.html.
[2638] G20 Leaders Statement: The Pittsburgh Summit, G20 Information Centre (Toronto) 25 September 2009. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2009/2009communique0925.html

laundering.[2639] The G20 also welcomed the expansion of the Global Forum on Transparency and Exchange of Information.[2640]

At the 2015 Antalya Summit, the G20 reaffirmed its commitment to the fight against terrorism and all its forms, no matter where it occurs.[2641] The leaders also expressed their continued support for the FATF's work in the fight against terrorism.[2642] The G20 committed "to tackling the financing channels of terrorism, particularly by enhanced cooperation on exchange of information, freezing of terrorist assets, criminalization of terrorist financing, robust targeted financial sanctions regimes related to terrorism and terrorist financing, including through swift implementation of Financial Action Task Force (FATF) standards in all jurisdictions."[2643]

At the 2016 Hangzhou Summit, the G20 condemned terrorism in all forms. The leaders committed to "tackle all sources, techniques and channels of terrorist financing, including extortion, taxation, smuggling of natural resources, bank looting, looting of cultural property, external donation, and kidnapping for ransom."[2644]

Commitment Features

This commitment consists primarily of three features: 1) realize an open internet, 2) realize a free internet, and 3) realize a secure internet.

The realization of an open internet refers to actions dedicated to creating an accessible digital world free of illicit terrorist activities.[2645] Fundamentally, the G20 commits to creating a digital sphere where international and national laws are effectively enforced.[2646] In addition, they hope to foster an environment where digital platforms interact with one another and work together to effectively detect and prevent terrorist content from appearing on their sites.[2647]

The realization of a free internet refers to actions that foster a digital domain that reflects human rights, freedom of expression and access to information. In this regard, G20 members "commit to

[2639] G20 Leaders Statement: The Pittsburgh Summit, G20 Information Centre (Toronto) 25 September 2009. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2009/2009communique0925.html
[2640] G20 Leaders Statement: The Pittsburgh Summit, G20 Information Centre (Toronto) 25 September 2009. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2009/2009communique0925.html
[2641] G20 Leaders' Communique Antalya, G20 Information Centre (Toronto) 15 November 2015. Access Date: 22 January 2017. http://www.g20.utoronto.ca/2015/151116-communique.html
[2642] G20 Leaders' Communique Antalya, G20 Information Centre (Toronto) 15 November 2015. Access Date: 22 January 2017. http://www.g20.utoronto.ca/2015/151116-communique.html
[2643] G20 Leaders' Communique Antalya, G20 Information Centre (Toronto) 20 November 2015. Access Date: 22 January 2017. http://www.g20.utoronto.ca/2015/151116-communique.html
[2644] G20 Leaders' Communique Hangzhou, G20 Information Centre (Toronto) 5 September 2016. Access Date: 28 October 2016. http://www.g20.utoronto.ca/2016/160905-communique.html
[2645] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT), G20 Information Centre (Toronto) 29 June 2019. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2019/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf
[2646] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT), G20 Information Centre (Toronto) 29 June 2019. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2019/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf
[2647] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT), G20 Information Centre (Toronto) 29 June 2019. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2019/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf

collaborate with states, international organizations, industry, and civil society in this endeavour" to achieve this goal.[2648]

Furthermore, the G20 intends to urge online platforms to continue to prevent terrorist groups from gaining a presence in the digital world, in particular to prevent terrorist content from "being streamed, uploaded, or re-uploaded."[2649]

The realization of a secure internet refers to actions that helps to locate and prevent terrorist content from appearing on the internet. The G20 views technological innovation as one of the most promising methods to succeed in this endeavour. It also recognizes the significance of the Global Internet Forum to Counter Terrorism (GIFCT) in responding to this issue. Nevertheless, the G20 believes that increased action through collaboration with "industry, media outlets, researchers and civil society" will strengthen the GIFCT's effort and membership in helping to combat this issue. G20 members also commit to sharing domestic experience, while also collaborating on the international stage to effectively combat this issue.[2650]

Thus, to earn a score of full compliance with this commitment, G20 members must take action in all three features: taking action to realize an open, free and secure internet. Partial compliance entails taking action in one or two of these three features. No compliance entails no action taken to realize an open, free or secure internet. Actions that realize an open internet include those that allow diverse groups to access the digital world efficiently and that prevent extremist content from circulating. For instance, policy initiatives that increase government capabilities to enforce digital infringements or that strengthen the ability of a certain demographic to better their access to the internet both count towards this action. Actions that realize a free internet include those that foster relationships between various organizations to promote human rights, freedom of expression and access to information in the digital realm. An example of such an action would involve a state establishing a relationship with leading organizations in the technology industry to increase people's abilities in freely expressing themselves. Actions that realize a secure internet involve those that identify and block terrorist content from appearing on the web through technological innovations and partnerships. For example, policies that increase funding or establish new projects for technological endeavours that reduce the ability of terrorist organizations to spread propaganda would count towards this action.

This assessment covers G20 members' actions taken between 30 June 2019 and 10 October 2020.

[2648] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT), G20 Information Centre (Toronto) 29 June 2019. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2019/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf
[2649] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT), G20 Information Centre (Toronto) 29 June 2019. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2019/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf
[2650] G20 Osaka Leaders' Statement on Preventing Exploitation of the Internet for Terrorism and Violent Extremism Conducive to Terrorism (VECT), G20 Information Centre (Toronto) 29 June 2019. Access Date: 18 November 2019. http://www.g20.utoronto.ca/2019/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf

Scoring Guidelines

−1	G20 member takes no action to realize any of the three features of an open OR free OR secure internet.
0	G20 member takes action to realize one or two of the three features of an open OR free OR secure internet.
+1	G20 member takes action to realize all three commitment features of an open AND free AND secure internet.

Compliance Director: Arshia Hassani
Lead Analyst: Vannie Kopalakrishnan

Argentina: 0

Argentina has partially complied with its commitment to realize an open, free and secure internet.

On 18 July 2019, the Argentine government designated Hezbollah as a terrorist group and the Financial Information Unit of Argentina froze the assets of the group and of its identified members in the country.[2651]

On 19 July 2019, Argentina hosted the Second Hemispheric Ministerial Conference for the Fight Against Terrorism.[2652] The 16 participating countries, including Argentina, "condemned terrorism in all its forms and manifestations" and pledged to increase international cooperation against "terrorists use of new technologies and electronic communication platforms to recruit or radicalize, spread terrorist material, and incite violence, while remaining committed to an open, free and secure internet."[2653]

On 19 July 2019, the Minister of Security of Argentina Patricia Bullrich asserted at the Second Hemispheric Ministerial Conference for the Fight Against Terrorism that the government is aware of the use of the "internet, social networks, the deep web and encrypted messaging" for terrorist purposes.[2654] She also assured that the government is working on the detection of potential terrorist cells in Argentina.[2655]

On 30 July 2019, the Argentina representative at the United Nations identified the several challenges related to the use of communication technologies for criminal purposes and supported the resolution 73/187 entitled "Countering the use of information and communications technologies for criminal purposes" taken by the General Assembly of the United Nations during the same session.[2656]

[2651] Argentina brands Hezbollah terrorist organization, freezes assets, Reuters (London) 18 July 2019. Access Date: 20 March 2020. https://www.reuters.com/article/us-argentina-hezbollah/argentina-brands-hezbollah-terrorist-organization-freezes-assets-idUSKCN1UD1XE
[2652] Joint Communique: Second Hemispheric Ministerial Conference on the Fight Against Terrorism, US Department of State (Washington DC) 19 July 2019. Access Date: 20 March 2020. https://www.state.gov/joint-communique-second-hemispheric-ministerial-conference-on-the-fight-against-terrorism/
[2653] Joint Communique: Second Hemispheric Ministerial Conference on the Fight Against Terrorism, US Department of State (Washington DC) 19 July 2019. Access Date: 20 March 2020. https://www.state.gov/joint-communique-second-hemispheric-ministerial-conference-on-the-fight-against-terrorism/
[2654] Secretary of State Michael R. Pompeo at the Counterterrorism Ministerial Plenary, US Department of State (Washington DC) 19 July 2019. Access Date: 20 March 2020. https://www.state.gov/secretary-of-state-michael-r-pompeo-at-the-counterterrorism-ministerial-plenary/
[2655] Secretary of State Michael R. Pompeo at the Counterterrorism Ministerial Plenary, US Department of State (Washington DC) 19 July 2019. Access Date: 20 March 2020. https://www.state.gov/secretary-of-state-michael-r-pompeo-at-the-counterterrorism-ministerial-plenary/
[2656] Countering the use of information and communications technologies for criminal purposes, United Nations (New York) 30 July 2019. Access Date: 20 March 2020.
https://www.unodc.org/documents/Cybercrime/SG_report/V1908182_E.pdf

On 23 September 2019, Argentina announced its support for the Christchurch Call.[2657] By being a signatory of the agreement, the Argentinian government commits to "redirect users from terrorist and violent extremist content," "accelerate research into and development of technical solutions to prevent the upload of and to detect and immediately remove terrorist and violent extremist content online," "support research and academic efforts to better understand, prevent and counter terrorist and violent extremist content online," "investigating and prosecuting illegal online activity," as well as to implement other measures designed to fight against the use of internet for terrorist purposes.[2658]

On 3 October 2019, the Organization of American States, of which Argentina is a member, launched the Inter-American Network on Counterterrorism in order to enhance international cooperation between Latin American countries in the fight against terrorism on the continent.[2659]

On 22 October 2019, the Argentina National Direction for Personal Data Protection abstained from the resolution on Social Media and Violent Extremist Content Online taken by the 41st International Conference of Data Protection and Privacy Commissioners, which emphasized the role played by social media in recent terrorist attacks and urged social media providers to take action against the use of their platforms for terrorist purposes.[2660]

On 20 January 2020, the 19 participating countries of the Third Hemispheric Ministerial Conference to Combat Terrorism in Bogota, including Argentina, reiterated their pledge to "prevent, combat, counter and suppress Internet use, for terrorist purposes," "while taking measures to maintain an open and free internet and a secure cyberspace, with full respect for privacy and freedom of expression."[2661]

On 21 August 2020, the Argentine government issued a Decree of Necessity and Urgency that underlined the right of internet access as a universal right.[2662] The decree regulates the Information and Communications Technology market in order to guarantee internet access at a fair price.[2663]

On 22 August 2020, it was announced that a Cybercrime Combat Coordination Center will be created and led by the Ministry of Security as part of the Federal Plan for the Prevention of

[2657] Christchurch Call. New Zealand Ministry of Foreign Affairs and Trade (Wellington). Access Date: 20 March 2020. https://www.christchurchcall.com/call.html, https://www.christchurchcall.com/supporters.html
[2658] Christchurch Call. New Zealand Ministry of Foreign Affairs and Trade (Wellington). Access Date: 20 March 2020. https://www.christchurchcall.com/call.html, https://www.christchurchcall.com/supporters.html
[2659] OAS and United States Sign Agreement to Create Inter-American Network on Counterterrorism. U.S. Mission to the Organization of American States (Washington) 3 October 2019. Access Date: 20 March 2020. https://usoas.usmission.gov/oas-and-united-states-sign-agreement-to-create-inter-american-network-on-counterterrorism/
[2660] Resolution on Social Media and Violent Extremist Content Online. 41st International Conference of Data Protection and Privacy Commissioners (Tirana). 22 October 2019. Access Date: 20 March 2020. https://edps.europa.eu/sites/edp/files/publication/draft-resolution-on-social-media-and-extremist-content-online-updated-with-abstentions-1_en.pdf
[2661] Third Hemispheric Ministerial Conference to Combat Terrorism — Joint Communique, Brazilian Ministry of Foreign Affairs (Brasilia) 20 January 2020. Access Date: 20 March 2020. http://www.itamaraty.gov.br/en/press-releases/21235-third-hemispheric-ministerial-conference-to-combat-terrorism-joint-communique
[2662] Decreto 690/2020, Argentina Presidencia (Buenos Aires) 21 August 2020. Access Date: 30 August 2020. https://www.boletinoficial.gob.ar/detalleAviso/primera/233932/20200822
[2663] Decreto 690/2020, Argentina Presidencia (Buenos Aires) 21 August 2020. Access Date: 30 August 2020. https://www.boletinoficial.gob.ar/detalleAviso/primera/233932/20200822

Technological Crimes and Cybercrimes launched in November 2019. This "C4" will fight all types of cybercrime.[2664]

Argentina has partially complied with this commitment by taking action to realise a secure internet such as in being a signatory to the Christchurch Call agreement which emphasizes the prevention of terrorist content from appearing on the internet. However, it has not taken action to realise an open and free internet.

Thus, Argentina receives a score of 0.

Analyst: Xavier Bornert

Australia: 0

Australia has partially complied with its commitment to realizing an open, free and secure internet by taking specific action to realize these commitments.

On 25 August 2019, Australian Prime Minister Scott Morrison announced that the Australian government had accepted some of the recommendations of the Taskforce to Combat Terrorist and Extreme Violent Material Online (the Taskforce). The Taskforce was established in March 2019 following the Christchurch terrorist attack in New Zealand.[2665] The Australian government accepted its recommendation to develop measures to block websites hosting harmful and extreme content.[2666] The Australian eSafety Commissioner will work with industry actors on options for introducing arrangements to quickly and effectively block access to domains hosting material from the Christchurch attack and from future similar events.[2667] The Australian government also accepted the Taskforce's recommendation to establish an updated crisis management framework that includes a protocol for managing terrorist and violent material posted online. The new protocol will include a 24/7 Crisis Coordination Centre to monitor and notify relevant agencies of online crisis events and provide the eSafety Commissioner with the information needed to undertake rapid assessments.[2668]

On 10 December 2019, the fourth Foreign and Defence Ministers' meeting between Korea and Australia was held in Sydney.[2669] The two sides agreed to strengthen cooperation in cybersecurity through the Korea-Australia Cyber Policy Dialogue and to respond to terrorism.[2670]

[2664] El Gobierno pondrá en marcha una organización especial para combatir el ciberdelito, Infobae (Buenos Aires) 22 August 2020. Access Date: 30 August 2020. https://www.infobae.com/politica/2020/08/22/el-gobierno-pondra-en-marcha-una-organizacion-especial-para-combatir-el-ciberdelito/

[2665] Halting the Spread of Terrorism and Extreme Violent Content Online, Prime Minister of Australia, (Canberra) 25 August 2019. Access Date: 15 May 2020. https://www.pm.gov.au/media/halting-spread-terrorism-and-extreme-violent-content-online

[2666] Halting the Spread of Terrorism and Extreme Violent Content Online, Prime Minister of Australia, (Canberra) 25 August 2019. Access Date: 15 May 2020. https://www.pm.gov.au/media/halting-spread-terrorism-and-extreme-violent-content-online

[2667] Govt to Develop Violent Content Blocking Framework, Technology Decisions, (Australia) 27 August 2019. Access Date: 15 May 2020. https://www.technologydecisions.com.au/content/it-management/news/govt-to-develop-violent-content-blocking-framework-795172476

[2668] Govt to Develop Violent Content Blocking Framework, Technology Decisions, (Melbourne) 27 August 2019. Access Date: 15 May 2020. https://www.technologydecisions.com.au/content/it-management/news/govt-to-develop-violent-content-blocking-framework-795172476

[2669] 4th ROK-Australia Foreign and Defense Ministers' 2+2 Meeting Takes Place, Ministry of Foreign Affairs (Seoul) 10 December 2019. Access Date: 19 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320887.

[2670] 4th ROK-Australia Foreign and Defense Ministers' 2+2 Meeting Takes Place, Ministry of Foreign Affairs (Seoul) 10 December 2019. Access Date: 19 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320887.

On 11 December 2019, the Australian Department of Communications (DOC) and the Arts began a consultation on its proposal to create a new Online Safety Act in order to reform and expand its existing patchwork of online safety laws.[2671] The DOC also issued an Online Safety Charter, outlining expectations for industry to protect Australians from harmful online experiences. It is based on the premise that behaviour which would be unacceptable offline should not be tolerated or enabled online, and that internet service providers (ISPs) have a responsibility to respect the rights and dignity of users online and should address and prevent harms being incurred by those using their products or services.[2672]

On 24 March 2020, the Australian Minister for Communications, Cyber Safety and the Arts announced the agreement of a new protocol between ISPs and the eSafety Commissioner, which positions ISPs to block websites hosting graphic material that depicts a terrorist act or violent crime, to stem the risk of its rapid spread as an online crisis event unfolds.[2673]

On 22 April 2020, the Australian Signals Directorate, along with its counterpart in the United States, the National Security Agency, published a set of guidelines to help companies avoid a web shell exploits: a common cyber-attack that gives an attacker remote access to a system and lets them execute functions on a victim's web server.[2674] The guidelines address several layers of defence, and also advises internet users to watch for uncommon activity such as running network enumeration commands that have no place in most legitimate web apps.[2675]

Through a series of policy initiatives that aim to increase the state's technological capabilities of securing the internet while also establishing programs that ensure the protection of one's rights and freedoms online, Australia has partially complied with its commitment to realise an open, free and secure internet. It has not taken action to realise an open internet that increase accessibility to diverse populations.

Thus, Australia receives a score of 0.

Analyst: Dan Poliwoda

Brazil: 0

Brazil has partially complied with its commitment toward an open, free and secure internet.

On 6 January 2020, Artur Coimbra, Broadband Director of Brazil's Ministry of Science, Technology, Innovation and Communication, announced new measures to facilitate private projects in

[2671] Australian Government Opens Consultation on New Online Safety Act, Baker McKenzie, (Melbourne) 7 January 2020. Access Date: 16 May 2020. https://www.bakermckenzie.com/en/insight/publications/2020/01/australia-consultation-new-online-safety-act

[2672] Australian Government Opens Consultation on New Online Safety Act, Baker McKenzie, (Melbourne) 7 January 2020. Access Date: 16 May 2020. https://www.bakermckenzie.com/en/insight/publications/2020/01/australia-consultation-new-online-safety-act

[2673] Government and Internet Providers Finalise Protocol to Block Terrorist and Graphic Violent Content, Minister for Communications, Cyber Safety and the Arts, (Canberra) 24 March 2020. Access Date: 16 May 2020. https://minister.infrastructure.gov.au/fletcher/media-release/government-and-internet-providers-finalise-protocol-block-terrorist-and-graphic-violent-content

[2674] Web Shell Warning Issued by US and Australia, Naked Security, (Abingdon) 27 April 2020. Access Date: 15 May 2020. https://nakedsecurity.sophos.com/2020/04/27/web-shell-warning-issued-by-us-and-australia/

[2675] Web Shell Warning Issued by US and Australia, Naked Security, (Abingdon) 27 April 2020. Access Date: 15 May 2020. https://nakedsecurity.sophos.com/2020/04/27/web-shell-warning-issued-by-us-and-australia/

telecommunications.[2676] He proposed three key policies of reducing bureaucracy and facilitating approbation of projects with support from state company Anatel and supervision from the ministry.[2677]

On 30 June 2020, the Brazilian Law on Freedom, Responsibility and Transparency on the Internet (Bill 2630/2020), also coined the "Fake News" bill, was approved by the Senate.[2678] The bill aims to curb the dissemination of false information by establishing rules regarding the transparency of social networks and private messaging services, the transparency of sponsored content and sanctions for non-compliance with the law.[2679] However, the bill has received criticism for its provisions and penalties, which purportedly threaten freedom of expression and association and the right to privacy under human rights law.[2680]

Brazil has taken action to increase the security of the internet through the approval of certain laws like Bill 2630/2020. However, it has not taken action to realize a free and open internet.

Thus, Brazil receives a score of 0.

Analysts: Raphaël Colombier and Emily Yu

Canada: +1

Canada has fully complied with its commitment to realize an open, free and secure internet.

On 26 June 2019, Public Safety Canada (PSC) announced that it is providing CAD1,000,000 to Tech Against Terrorism which aims to help smaller technology companies in spotting and removing terrorist content when detected.[2681]

On 26 June 2019, PSC announced its commitment to empower young leaders to help shape the internet landscape by collaborating with the Youth Summit on Countering Violent Extremism Online.[2682] This will be done in collaboration with technology companies including Twitter,

[2676] MCTIC propoe menos burocracia e mais fiscalizacao para debentures incentivadas, Telesinte (Brazilia, Brazil) 6 January 2020. Access Date: 24 March 2020. http://www.telesintese.com.br/mctic-propoe-menos-burocracia-e-mais-fiscalizacao-para-debentures-incentivadas/

[2677] MCTIC propoe menos burocracia e mais fiscalizacao para debentures incentivadas, Telesinte (Brazilia, Brazil) 6 January 2020. Access Date: 24 March 2020. http://www.telesintese.com.br/mctic-propoe-menos-burocracia-e-mais-fiscalizacao-para-debentures-incentivadas/

[2678] Projeto de Lei n° 2630, de 2020, Senado Federal (Brazilia), 27 July 2020. Access date: 24 September 2020. https://www25.senado.leg.br/web/atividade/materias/-/materia/141944

[2679] Projeto de Lei n° 2630, de 2020, Senado Federal (Brazilia), 27 July 2020. Access date: 24 September 2020. https://www25.senado.leg.br/web/atividade/materias/-/materia/141944

[2680] Greg Nojeim, Update on Brazil's Fake News Bill: The Draft Approved by the Senate Continues to Jeopardize Users' Rights, Center for Democracy and Technology (Washington, D.C.), 24 July 2020. Access date: 24 September 2020. https://cdt.org/insights/update-on-brazils-fake-news-bill-the-draft-approved-by-the-senate-continues-to-jeopardize-users-rights/

[2681] Government of Canada Announces Initiatives to Address Violent Extremist and Terrorist Content Online, Public Safety Canada (Ottawa) 26 June 2019. Access Date: 1 February 2020. https://www.canada.ca/en/public-safety-canada/news/2019/06/government-of-canada-announces-initiatives-to-address-violent-extremist-and-terrorist-content-online.html

[2682] Government of Canada Announces Initiatives to Address Violent Extremist and Terrorist Content Online, Public Safety Canada (Ottawa) 26 June 2019. Access Date: 1 February 2020. https://www.canada.ca/en/public-safety-canada/news/2019/06/government-of-canada-announces-initiatives-to-address-violent-extremist-and-terrorist-content-online.html

Facebook, Microsoft and Google which allow for cooperation between the government, civil society and private actors.[2683]

On 21 August 2019, PSC announced that it will be investing CAD304,253 over three years to the Centre of Expertise and Training on Religious Fundamentalism, Political Ideologies and Radicalization to research far-right extremism in Quebec.[2684] The main focus will be on media research and interviews with experts and activists.[2685]

On 10 March 2020, PSC published their Departmental Plan for 2020-2021 and reinforced their commitment to the Christchurch call as well as the Global Internet Forum to Counter Terrorism (GIFCT).[2686] These plans are outlined as priorities that the department wishes to accomplish under the broader role of their public safety goals.[2687]

On 13 March 2020, PSC formed the National Expert Committee on Countering Radicalization to Violence.[2688] This committee is made up of experts in the fields of academia, civil society, public policy and extremism experts where their main goal is to oversee and aid in the implementation of the National Strategy on Countering Radicalization to Violence.[2689] The committee's role will be to ensure that the strategy is implemented to meet its three goals of building, sharing and using knowledge to reinforce a free, open and secure internet.[2690]

The Government of Canada has announced policies and funding to meet its prior commitments to both the Christchurch Call and to the GIFCT to help the international push against online extremism. In addition, the government has also engaged with both private and civil society groups to better encompass a diverse group of actors to help in preventing the spread of online extremism. Lastly, the government made progress within its own domestic policy to fight online extremism through the formation of the National Expert Committee that oversees the national strategy.

Thus, Canada receives a score of +1.

Analyst: Khurram Shamim

[2683] Government of Canada Announces Initiatives to Address Violent Extremist and Terrorist Content Online, Public Safety Canada (Ottawa) 26 June 2019. Access Date: 1 February 2020. https://www.canada.ca/en/public-safety-canada/news/2019/06/government-of-canada-announces-initiatives-to-address-violent-extremist-and-terrorist-content-online.html

[2684] Government of Canada Funds Research into Far-Right Extremism in Quebec, Public Safety Canada (Ottawa) 21 August 2019. Access Date: 2 February 2020. https://www.canada.ca/en/public-safety-canada/news/2019/08/government-of-canada-funds-research-into-far-right-extremism-in-quebec.html

[2685] Government of Canada Funds Research into Far-Right Extremism in Quebec, Public Safety Canada (Ottawa) 21 August 2019. Access Date: 2 February 2020. https://www.canada.ca/en/public-safety-canada/news/2019/08/government-of-canada-funds-research-into-far-right-extremism-in-quebec.html

[2686] Departmental Plan 2020-2021: Building a Safe and Reliant Canada, Public Safety Canada (Ottawa) 10 March 2020. Access Date: 15 March 2020. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2020-21/index-en.aspx

[2687] Departmental Plan 2020-2021: Building a Safe and Reliant Canada, Public Safety Canada (Ottawa) 10 March 2020. Access Date: 15 March 2020. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2020-21/index-en.aspx

[2688] National Expert Committee on Countering Radicalization to Violence, Public Safety Canada (Ottawa) 13 March 2020. Access Date: 15 March 2020. https://www.publicsafety.gc.ca/cnt/bt/cc/ntnl-xprt-cmmtt-en.aspx

[2689] National Expert Committee on Countering Radicalization to Violence, Public Safety Canada (Ottawa) 13 March 2020. Access Date: 15 March 2020. https://www.publicsafety.gc.ca/cnt/bt/cc/ntnl-xprt-cmmtt-en.aspx

[2690] National Expert Committee on Countering Radicalization to Violence, Public Safety Canada (Ottawa) 13 March 2020. Access Date: 15 March 2020. https://www.publicsafety.gc.ca/cnt/bt/cc/ntnl-xprt-cmmtt-en.aspx

China: 0

China has partially complied with its commitment to realizing a free, open and secure internet through various policy initiatives.

On 13 June 2019, the new Draft Measures on Security Assessment of the Cross-Border Transfer of Personal Information were issued.[2691] The regulation aims to monitor cross-border transfer that could present a risk to national security, damage public interest or provide inadequate protection for the personal information.[2692]

On 11 July 2019, Vice President of China Academy of Information and Communications Technology Li Yong announced the 2019 China Internet Conference.[2693] The conference promised to offer a bottom-up, participatory, open, transparent and inclusive platform where government, business, tech-community, civil society and all stakeholders.[2694]

On 26 October 2019, the National People's Congress released the Encryption Law of the People's Republic of China to safeguard China's national security and public interests.[2695] The law encourages "technological cooperation on commercial cryptography to be conducted in the course of foreign investment and on the basis of the voluntariness principle and business rules" and exposes activities that "engage in illegal activities such as endangering national security, the societal public interest, or the lawful rights and interests of others."[2696]

On 18 November 2019, the Ministry of Foreign Affairs held the fourth Korea-Japan-China Cyber Policy Consultation in Beijing to discuss and enhance regional cybersecurity cooperation.[2697] There was a shared understanding that discussions regarding cybersecurity norms at the United Nations are essential to creating a safe cyberspace and explored ways to cooperate on joint response to cybercrimes among law enforcement agencies.[2698]

On 28 November 2019, the Cybersecurity Administration of China issued new regulations for online information, specifying requirements for online information producers.[2699] The regulations aim to establish a clean and reliable internet ecosystem, prohibiting illegal activities including terrorism.[2700]

[2691] New Draft Rules on Cross-Border Transfer of Personal Information Out of China. New America (Washington) 13 June 2019. Access Date: 27 January 2020. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/

[2692] New Draft Rules on Cross-Border Transfer of Personal Information Out of China. New America (Washington) 13 June 2019. Access Date: 27 January 2020. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/

[2693] China IGF Initiative Announced during the 2019 China Internet Conference. IGF China (Beijing). 11 July 2019. Access Date: 27 January 2020. http://igfchina.caict.ac.cn/english/global/201908/t20190802_2599878.html.

[2694] China IGF Initiative Announced during the 2019 China Internet Conference. IGF China (Beijing). 11 July 2019. Access Date: 27 January 2020. http://igfchina.caict.ac.cn/english/global/201908/t20190802_2599878.html.

[2695] China's New Draft Encryption Law. 4 September 2019. Access Date: 1 June 2019. https://www.jdsupra.com/legalnews/china-s-new-draft-encryption-law-52672/

[2696] Cryptography Law of the P.R.C. 27 October 2019. Unofficial translation. https://www.chinalawtranslate.com/en/cryptography-law/#_Toc23080195

[2697] 4th ROK-Japan-China Cyber Policy Consultation Held, Ministry of Foreign Affairs (Seoul) 19 November 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320841.

[2698] 4th ROK-Japan-China Cyber Policy Consultation Held, Ministry of Foreign Affairs (Seoul) 19 November 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320841.

[2699] CAC and other ministries provide guidance on illegal collection and use of personal information by Apps. Practical Law China (Toronto). 13 January 2020. Access Date: 27 Jan 2020. https://ca.practicallaw.thomsonreuters.com/w-023-5835?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)

On 12 December 2019, China, as a member of the Shanghai Cooperation Organization (SCO), held a joint drill on combating cyber-terrorism in Xiamen.[2701] During the drill, each SCO member state participated in a online terrorist propaganda exercise, which indicated SCO's "determination to crackdown online terror activities and safeguard regional security and stability."[2702] Liu Yuejin, a senior anti-terrorism official at the Ministry of Public Security, pledged that China would further enhance cooperation with the SCO members to enhance law enforcement and security.[2703]

On 1 January 2020, China adopted a national law on cryptography that aims to secure cyberspace and information regulation, specifying core and common cryptography for encrypted protection and security verification.[2704] The goal is to protect the state security from encrypted information.[2705]

On 27 April 2020, the Cyberspace Administration of China released a final version of the measures on cybersecurity review, regulating the safety of online products and content.[2706] The new regulations "oblige critical information infrastructure operators to carry out a self-assessment of the national security risks in connection with their online products and services, and to report where any risks are identified."[2707] Online operators are required to identify and report any content that poses threat to national security.[2708]

On 30 June 2020, China announced the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region.[2709] For the purpose of preventing terrorist activities, the law includes regulation of public communication through the media and the Internet.[2710]

China has partially complied with this commitment by taking national action and establishing partnerships that aim to realise a free and secure internet. However, it has not taken action to realise an open internet that increases accessibility to diverse populations.

Thus, China receives a score of 0.

[2700] China Cybersecurity and Data Protection: Monthly Update — January 2020 Issue. Herbert Smith Freehills 13 January 2020 (Beijing) 13 Jan 2020. Access Date: 27 Jan 2020. https://sitesherbertsmithfreehills.vuturevx.com/95/21584/compose-email/china-cybersecurity-and-data-protection--monthly-update---january-2020-issue(en).asp#five

[2701] SCO anti-cyber-terrorism drill held in China. Xinhua Net (Beijing) 12 December 2020. Access Date: 5 June 2020. http://www.xinhuanet.com/english/2019-12/12/c_138626263.htm

[2702] SCO carries out online anti-terrorism drill. Global Times (Beijing) 12 December 2020. Access Date: 5 June 2020. https://www.globaltimes.cn/content/1173369.shtml

[2703] SCO carries out online anti-terrorism drill. Global Times (Beijing) 12 December 2020. Access Date: 5 June 2020. https://www.globaltimes.cn/content/1173369.shtml

[2704] China Focus: China adopts law on cryptography. Xinhua Net (Beijing) 26 October 2019. Access Date: 16 January 2020. http://www.xinhuanet.com/english/2019-10/26/c_138505655.html

[2705] China Focus: China adopts law on cryptography. Xinhua Net (Beijing) 26 October 2019. Access Date: 16 January 2020. http://www.xinhuanet.com/english/2019-10/26/c_138505655.html

[2706] Cybersecurity Review. Cyberspace Administration of China (Beijing) 27 April 2020.Access Date: 1 Jun 2020 http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

[2707]China Cybersecurity and Data Protection: Monthly Update — May 2020 Issue. Herbert Smith Freehills LLP (Beijing) 25 May 2020. Access Date: 1 Jun 2020. https://www.lexology.com/library/detail.aspx?g=304cca9e-fdb1-447c-89aa-6ff8f028e1da

[2708] Cybersecurity Review. Cyberspace Administration of China (Beijing) 27 April 2020.Access Date: 1 June 2020 http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm

[2709] English translation of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region. Xinhua (Beijing). 30 June 2020. Access Date: 17 July 2020. http://www.xinhuanet.com/english/2020-07/01/c_139178753.htm

[2710] English translation of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region. Xinhua (Beijing). 30 June 2020. Access Date: 17 July 2020. http://www.xinhuanet.com/english/2020-07/01/c_139178753.htm

Analyst: Scarlett Lin

France: 0

France has partially complied with its commitment to realizing a free, open and secure internet.

On 9 July 2019, the French National Assembly passed the Loi Avia designed to combat hate speech on the internet by identifying and punishing the author and social media companies who do not remove such content from their platforms within 24 hours.[2711]

On 28 February 2020, India hosted the 14th meeting of India-France Joint Working Group on Counter Terrorism.[2712] The Joint Secretary for Counter Terrorism of the Ministry of External Affairs of India and the French delegation "condemned terrorism in all its forms" and committed to "prevent the use of internet for terrorist purposes."[2713]

On 13 May 2020, the National Assembly passed the Loi Avia bill (355 votes for, 150 against, 47 abstaining).[2714] The legislation requires that social media sites operating in France remove offending content within 24 hours of being flagged or face a fine of up to EUR1.25 million.[2715] This period is reduced to one hour for terrorist- or child pornography-related content.[2716]

On 18 June 2020, the Constitutional Council struck down key provisions of the Loi Avia, including clauses requiring platforms to remove illegal hate speech within 24 hours of being notified by users, and child pornography or content promoting terrorism within an hour of being flagged.[2717] All provisions dependent on the aforementioned censored clauses were also subsequently rendered null.[2718] The court stated that the short deadlines created an incentive for platforms to over-censure, which posed a constitutional threat to freedom of speech and expression.[2719]

[2711] PROPOSITION DE LOI visant à lutter contre la haine sur internet, Assemblée Nationale (Paris) 9 July 2019. Access Date: 29 January 2020. http://www.assemblee-nationale.fr/15/propositions/pion1785.asp

[2712] India-France Joint Working Group on Counter Terrorism, French Embassy in New Delhi (New Delhi) 28 February 2020. Access Date: 21 March 2020. https://in.ambafrance.org/India-France-Joint-Working-Group-on-Counter-Terrorism

[2713] India-France Joint Working Group on Counter Terrorism, French Embassy in New Delhi (New Delhi) 28 February 2020. Access Date: 21 March 2020. https://in.ambafrance.org/India-France-Joint-Working-Group-on-Counter-Terrorism

[2714] PPL visant à lutter contre les contenus haineux sur internet : adoption en lecture définitive, Assemblée Nationale (Paris), 13 May 2020. Access date: 24 September 2020. http://www.assemblee-nationale.fr/dyn/actualites-accueil-hub/ppl-visant-a-lutter-contre-les-contenus-haineux-sur-internet-adoption-en-lecture-definitive

[2715] PPL visant à lutter contre les contenus haineux sur internet : adoption en lecture définitive, Assemblée Nationale (Paris), 13 May 2020. Access date: 24 September 2020. http://www.assemblee-nationale.fr/dyn/actualites-accueil-hub/ppl-visant-a-lutter-contre-les-contenus-haineux-sur-internet-adoption-en-lecture-definitive

[2716] PPL visant à lutter contre les contenus haineux sur internet: adoption en lecture définitive, Assemblée Nationale (Paris), 13 May 2020. Access date: 24 September 2020. http://www.assemblee-nationale.fr/dyn/actualites-accueil-hub/ppl-visant-a-lutter-contre-les-contenus-haineux-sur-internet-adoption-en-lecture-definitive

[2717] Nicolas Boring, France: Constitutional Court Strikes Down Key Provisions of Bill on Hate Speech, Library of Congress (Washington, D.C.), 29 June 2020. Access date: 24 September 2020. https://www.loc.gov/law/foreign-news/article/france-constitutional-court-strikes-down-key-provisions-of-bill-on-hate-speech/

[2718] Nicolas Boring, France: Constitutional Court Strikes Down Key Provisions of Bill on Hate Speech, Library of Congress (Washington, D.C.), 29 June 2020. Access date: 24 September 2020. https://www.loc.gov/law/foreign-news/article/france-constitutional-court-strikes-down-key-provisions-of-bill-on-hate-speech/

[2719] Aurelien Breeden, French Court Strikes Down Most of Online Hate Speech Law, *The New York Times* (New York City), 18 June 2020. Access date: 24 September 2020. https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation.html

On 24 June 2020, the Loi Avia was signed into law by President Emmanuel Macron, excluding the provisions struck down by the Constitutional Council.[2720] The most significant contribution of the bill that remained was the authorization to create a specialized court that would adjudicate cases of hate speech.[2721]

France has partially complied with this commitment by realising a free and secure internet. Through the Loi Avia, France is increasing digital security by prohibiting terrorist and extremist content from appearing online, and the law also protects fundamental human rights and freedoms. However, it has not taken action to realise an open internet.

Thus, France receives a score of 0.

Analysts: Raphaël Colombier and Emily Yu

Germany: 0

Germany has partially complied with its commitment to realizing an open, free and secure internet.

On 24 September 2019, Germany announced that it will provide the Office for the Protection of the Constitution with 300 additional jobs in order to combat terrorism.[2722] The 300 additional jobs will entail the identification of terrorist cells and individual perpetrators, with social media platforms and the internet being monitored more closely to identify radicalization of extremists.[2723]

On 17 October 2019, Federal Minister Horst Seehofer announced that the government would be taking "appropriate preventative measures" and plans to tighten laws on hate speech on the internet.[2724] The government plans to work with specialists and representatives of the Jewish community on this initiative.[2725]

On 26 October 2019, Minister Seehofer met with the G7 interior ministers.[2726] He discussed the threat of right-wing extremism and the need of preventive measures to mitigate threats on the internet.[2727]

On 30 October 2019, the German government unveiled new measures to combat right-wing extremism and hate crimes on the internet.[2728] The new measures will oblige online service providers

[2720] Nicolas Boring, France: Constitutional Court Strikes Down Key Provisions of Bill on Hate Speech, Library of Congress (Washington, D.C.), 29 June 2020. Access date: 24 September 2020. https://www.loc.gov/law/foreign-news/article/france-constitutional-court-strikes-down-key-provisions-of-bill-on-hate-speech/

[2721] Nicolas Boring, France: Constitutional Court Strikes Down Key Provisions of Bill on Hate Speech, Library of Congress (Washington, D.C.), 29 June 2020. Access date: 24 September 2020. https://www.loc.gov/law/foreign-news/article/france-constitutional-court-strikes-down-key-provisions-of-bill-on-hate-speech/

[2722] Bundesregierung will Verfassungsschutz massiv aufstocken, Spiegel Online (Cologne) 24 September 2019. Access Date: 19 March 2020. https://www.spiegel.de/politik/deutschland/horst-seehofer-will-verfassungsschutz-massiv-aufstocken-regierungsplaene-a-1288364.html

[2723] Germany to create 300 jobs to combat right-wing extremism, The Local (Berlin) 24 September 2019. Access Date: 19 March 2020. https://www.thelocal.de/20190924/germany-to-create-300-jobs-to-fight-right-wing-extremism .

[2724] Minister calls for better protection of Jewish institutions in Germany, Xinhuanet (Berlin) 17 October 2019. Access Date: 20 March 2020. http://www.xinhuanet.com/english/2019-10/17/c_138480221.htm

[2725] Better protection for Jewish Life in Germany, Federal Ministry of the Interior (Berlin) 17 October 2019. Access Date: 20 March 2020. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2019/10/better-protection-jewish-life.html

[2726] G6 interior ministers meet in Munich, Federal Ministry of the Interior (Munich) 29 October 2019. Access Date: 20 March 2020. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2019/10/g6-innenministertreffen-en.html

[2727] G6 interior ministers meet in Munich, Federal Ministry of the Interior (Munich) 29 October 2019. Access Date: 20 March 2020. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2019/10/g6-innenministertreffen-en.html

such as Facebook, YouTube and Twitter to report hate speech to German authorities and also pass on the IP addresses of conspicuous users.[2729] The new measures will crackdown on illegal content such as death threats or incitement of hatred on their platforms.[2730]

On 1 November 2019, during the fifth German-Indian government consultations in New Delhi, Germany and India announced that they will be strengthening their bilateral and multilateral cooperation to combat terrorism and extremism.[2731] In a joint statement, Prime Minister Modi and Chancellor Angela Merkel emphasized strengthening counter-terrorism cooperation and working towards rooting out terrorist safe havens, infrastructure and disrupting networks and financing channels.[2732]

On 14 November 2019, the German parliament passed a raft of anti-money laundering measures to prevent the illegal financing of terrorist and criminal networks.[2733] The reform packet imposes stricter regulations on real estate agents, notaries, precious metals dealers and auction houses to declare transactions.[2734]

On 1 April 2020, the German government published a new draft bill to amend the German Hate Speech Act (Netzwerkdurchsetzungsgesetz — "NetzDG").[2735] The goal is to prevent the dissemination of offensive and aggressive content falling within the scope of application under the NetzDG bill.[2736] The new amendment obliges social networks to transmit some user data, such as IP addresses or port numbers.[2737]

On 30 April 2020, Minister Seehofer banned all activities by the terrorist organization Hezbollah in Germany.[2738] He stated at a press conference that "The organization is therefore fundamentally

[2728] Germany unveils new measures to combat far-right, Anadolu Agency (Berlin) 30 October 2019. Access Date: 17 March 2020. https://www.aa.com.tr/en/europe/germany-unveils-new-measures-to-combat-far-right/1631080
[2729] Germany announces plans to combat far-right extremism and online hate speech, Deutsche Welle (Berlin) 30 October 2019. Access Date: 17 March 2020. https://www.dw.com/en/germany-announces-plans-to-combat-far-right-extremism-and-online-hate-speech/a-51049129
[2730] Germany to tighten hate speech law to fight far-right violence, Politico (Berlin) 30 October 2019. Access Date: 17 March 2020. https://www.politico.eu/article/germany-to-tighten-hate-speech-law-to-fight-far-right-violence/
[2731] India, Germany to intensify cooperation in combating terror: PM, Rediff.com (New Delhi) 1 November 2019. Access Date: 18 March 2020. https://www.rediff.com/news/report/pix-germanys-angela-merkel-in-india-day-1/20191101.htm
[2732] PM Modi, German Chancellor Angela Merkel vow joint fight against terror, India Today (New Delhi) 2 November 2019. Access Date: 18 March 2020. https://www.indiatoday.in/mail-today/story/pm-modi-german-chancellor-angela-merkel-vow-joint-fight-on-terror-1614965-2019-11-02
[2733] German Parliament passes anti-money-laundering laws, Deutsche Welle (Berlin) 15 November 2019. Access Date: 18 March 2020. https://www.dw.com/en/german-parliament-passes-anti-money-laundering-laws/a-51260043
[2734] German Parliament passes anti-money-laundering laws, Deutsche Welle (Berlin) 15 November 2019. Access Date: 18 March 2020. https://www.dw.com/en/german-parliament-passes-anti-money-laundering-laws/a-51260043
[2735] German government introduces new bill to amend Germany's Hate Speech Act, establishing new requirements for social networks and video-sharing platforms, Technology Law Dispatch (Berlin) 6 April 2020. Access Date: 20 July 2020. https://www.technologylawdispatch.com/2020/04/regulatory/german-government-introduces-new-bill-to-amend-germanys-hate-speech-act-establishing-new-requirements-for-social-networks-and-video-sharing-platforms/
[2736] Germany is amending its online speech act NetzDG… but not only that, Internet Policy Review (Hamburg) 6 April 2020. Access Date: 23 July 2020. https://policyreview.info/articles/news/germany-amending-its-online-speech-act-netzdg-not-only/1464
[2737] German online hate speech reform criticized for allowing 'backdoor' data collection, Euractiv (Berlin) 19 June 2020. Access Date: 20 July 2020. https://www.euractiv.com/section/data-protection/news/german-online-hate-speech-reform-criticised-for-allowing-backdoor-data-collection/
[2738] Ban on activities of terrorist organzation Hezbollah in Germany, the Federal Ministry of the Interior, Building and Community (Berlin) 30 April 2020. Access Date: 20 July 2020. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2020/04/ban-of-hizb-allah-activities.html

against the concept of international understanding regardless of whether it presents itself as a political, social military structure."[2739]

On 19 May 2020, the German Federal Constitutional Court ruled that foreigners also benefit from privacy protections under Germany's constitution.[2740] The powers of Germany's foreign intelligence service to eavesdrop on foreign nationals' internet were deemed unconstitutional.[2741]

On 11 August 2020, the German government announced a federal agency to combat cyberthreats.[2742] The government plans to coordinate innovative research on cybersecurity and help turn it into practicable approaches to mitigate cyberthreats.[2743] The federal agency will receive EUR350 million in funding and will hold headquarters in the city of Halle.[2744]

Through its efforts in legislating measures that prevent terrorist and extremist activity on the internet, and by establishing partnerships with the international community, other G20 members and private technology companies to combat hate speech, Germany has partially complied with this commitment by taking action to realise a free and secure internet. However, it has not taken action to realise an open internet.

Thus, Germany receives a score of 0.

Analyst: Sebastian Vecerina

India: 0

India has partially complied with its commitment to realize an open, free and secure internet.

On 4 August 2019, Indian authorities cut the internet connection in the autonomous region of Kashmir, among other measures designed to regain control of this disputed territory where unrests were likely to break out.[2745] The Indian government shut down the internet 95 times in 2019.[2746]

On 8 August 2019, during an address to the nation, Prime Minister Narendra Modi "appealed to those who are associated with technology to give priority in their policies and their decisions as to

[2739] German government bans Hezbollah – Interior Ministry, Deutsche Welle (Berlin) 30 April 2020. Access Date: 21 21 July 2020. https://www.dw.com/en/german-government-bans-hezbollah-interior-ministry/a-53287126 .
[2740] German intelligence can no longer freely spy on the world's Internet traffic, top court rules, Fortune (Berlin) 19 May 2020. Access Date: 19 July 2020. https://fortune.com/2020/05/19/germany-snowden-spying-bnd-nsa-de-cix/
[2741] Top German court deems spying on foreigners' internet traffic is unconstitutional, Politico (Berlin) 19 May 2020. Access Date: 20 July 2020. https://www.politico.eu/article/top-german-court-deems-spying-on-foreigners-internet-traffic-is-unconstitutional/
[2742] Germany launches national cybersecurity agency to strengthen 'digital sovereignty', The Bharat Express News (Germany) 11 August 2020. Access Date: 23 September 2020. https://www.thebharatexpressnews.com/germany-launches-national-cybersecurity-agency-to-strengthen-digital-sovereignty-tben-11-08-2020/
[2743] Germany launches cybersecurity agency to strengthen 'digital sovereignty', Deutsche Welle (Berlin) 11 August 2020. Access Date: 23 September 23, 2020. https://www.dw.com/en/germany-launches-cybersecurity-agency-to-strengthen-digital-sovereignty/a-54529134
[2744] Germany launches a new agency dedicated to cybersecurity, inside telecom (Berlin) 14 August 2020. Access Date: 23 September 2020. https://www.insidetelecom.com/germany-launches-a-new-agency-dedicated-to-cybersecurity/
[2745] India Revokes Kashmir's Special Status, Raising Fears of Unrest, The New York Times (New York) 5 August 2019. Access Date: 21 March 2020. https://www.nytimes.com/2019/08/05/world/asia/india-pakistan-kashmir-jammu.html
[2746] Why India shuts down the internet more than any other democracy, BBC News (London) 19 December 2019. Access Date: 21 March 2020. https://www.bbc.com/news/world-asia-india-50819905

how to disseminate technology in Jammu and Kashmir."[2747] He stressed the importance of the strengthening of digital communications in these regions.[2748]

On 19 September 2019, the Federal Information and Technology Minister said that the internet "must be safe and secure."[2749] He added that "it must safeguard the privacy rights of the individual and you must make extra efforts that people don't abuse the system."[2750]

On 30 October 2019, the Minister of State for the Development of North Eastern Region said that the internet blackout in Jammu and Kashmir has enabled the elimination of several terrorists and prevented several terror incidents.[2751]

On 30 October 2019, Indian Secretary of External Affairs Vijay Thakur Singh and Russian Deputy Foreign Minister Oleg Syromolotov met for the 11th meeting of the India-Russia joint working group on counter terrorism in New Delhi.[2752] Both sides deliberated upon measures to further strengthen and deepen counterterrorism cooperation and both agreed on united efforts to fight terrorism and terrorism financing at multilateral forums.[2753]

On 1 November 2019, during the fifth German-Indian government consultations in New Delhi, Germany and India announced that they will be strengthening their bilateral and multilateral cooperation to combat terrorism and extremism.[2754] In a joint statement, Prime Minister Modi and Chancellor Angela Merkel emphasized strengthening counter-terrorism cooperation and working towards rooting out terrorist safe havens, infrastructure and disrupting networks and financing channels.[2755]

On 8 November 2019, the Union Minister of State for Home Affairs of India participated in the 2019 "No Money for Terror" Ministerial Conference on Counter-Terrorism Financing.[2756] The 65 delegations of the conference, including India, "reaffirmed support for international efforts to

[2747] PM's address to the Nation, PM India (New Delhi) 8 August 2019. Access Date: 21 March 2020. https://www.pmindia.gov.in/en/news_updates/pms-address-to-the-nation-2/?comment=disable
[2748] PM's address to the Nation, PM India (New Delhi), 8 August 2019. Access Date: 21 March 2020. https://www.pmindia.gov.in/en/news_updates/pms-address-to-the-nation-2/?comment=disable
[2749] India tells tech firms to protect user privacy, prevent abuse, Reuters (New Delhi) 19 September 2019. Access Date: 21 March 2020. https://fr.reuters.com/article/idUSKBN1W41S3
[2750] India tells tech firms to protect user privacy, prevent abuse, Reuters (New Delhi) 19 September 2019. Access Date: 21 March 2020. https://fr.reuters.com/article/idUSKBN1W41S3
[2751] Internet suspension averted major terror attacks in J&K: Union Minister Jitendra Singh, India Today (New Delhi) 30 October 2019. Access Date: 21 March 2020. https://www.indiatoday.in/india/story/internet-suspension-averted-major-terror-incidents-in-j-k-union-minister-jitendra-singh-1613925-2019-10-30
[2752] Joint Press Statement: India-Russia High Level Consultations on Counter Terrorism, Ministry of External Affairs (New Delhi) 30 October 2019. Access Date: 20 March 2020. https://www.mea.gov.in/bilateral-documents.htm?dtl/31986/joint+press+statement+indiarussia+high+level+consultations+on+counter+terrorism
[2753] Press release on the 11th meeting of the India-Russia Joint Working Group on Counter Terrorism, Ministry of Foreign Affairs Russia (New Delhi) 30 October 2019. Access Date: 20 March 2020. https://www.mid.ru/en/web/guest/maps/in/-/asset_publisher/EpJ5G4lcymvb/content/id/3879023
[2754] India, Germany to intensify cooperation in combating terror: PM, Rediff.com (New Delhi) 1 November 2019. Access Date: 18 March 2020. https://www.rediff.com/news/report/pix-germanys-angela-merkel-in-india-day-1/20191101.htm
[2755] PM Modi, German Chancellor Angela Merkel vow joint fight against terror, India Today (New Delhi) 2 November 2019. Access Date: 18 March 2020. https://www.indiatoday.in/mail-today/story/pm-modi-german-chancellor-angela-merkel-vow-joint-fight-on-terror-1614965-2019-11-02
[2756] Chair's Statement, 2019 'No Money for Terror' Ministerial Conference on Counter-Terrorism Financing, Department of Home Affairs of Australia (Canberra) 8 November 2019. Access Date: 21 March 2020. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/crime-prevention/anti-money-laundering-counter-terrorism-financing/ministerial-conference-statement-20191107

prevent terrorist and violent extremist exploitation of the Internet, including through the Christchurch Call to Action,"[2757] and "recognised the need to identify emerging risks from new technology platforms."[2758]

On 12 November 2019, the Foreign Minister of India said at the Paris Peace Forum that India is "concerned about the threats from the cyberspace" and suggested a global regulation of the cyberspace "in order that the cyberspace remains open, safe and secure."[2759] He said that the states are responsible for their national cyber security as well as for the data security of their citizens.[2760]

On 26 November 2019, the Joint Secretary on Counter Terrorism of the Ministry of External Affairs of India reaffirmed the opposition of his country to all forms of terrorism, including against "the online threat of radicalisation," as part of the 13th meeting of the India-UK Joint Working Group on Counter Terrorism in London.[2761]

On 30 November 2019, the Japanese Foreign Minister and the Minister of Defence took part in a ministerial dialogue with India to discuss the threats posed to regional peace by terror networks operating from Pakistan.[2762] The Japanese members, along with their Indian counterparts, called upon Pakistan to "take resolute and irreversible action against [terror networks] and fully comply with international commitments"[2763] including the steps prescribed by the Financial Action Task Force, the global anti-terror watchdog.[2764]

On 21 December 2019, Indian authorities suspended internet and phone services "in areas of New Delhi, in the eastern state of West Bengal, the northern city of Aligarh and the entire state of Assam,"[2765] where protests against a new citizenship law were likely to break out.[2766]

[2757] Chair's Statement, 2019 'No Money for Terror' Ministerial Conference on Counter-Terrorism Financing, Department of Home Affairs of Australia (Canberra) 8 November 2019. Access Date: 21 March 2020. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/crime-prevention/anti-money-laundering-counter-terrorism-financing/ministerial-conference-statement-20191107

[2758] Chair's Statement, 2019 'No Money for Terror' Ministerial Conference on Counter-Terrorism Financing, Department of Home Affairs of Australia (Canberra) 8 November 2019. Access Date: 21 March 2020. https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/crime-prevention/anti-money-laundering-counter-terrorism-financing/ministerial-conference-statement-20191107

[2759] India suggests a global regulation for open, safe and secure cyberspace, The Economic Times (Mumbai) 12 November 2019. Access Date: 21 March 2020. https://economictimes.indiatimes.com/tech/internet/india-suggests-a-global-regulation-for-open-safe-and-secure-cyberspace/articleshow/72027153.cms

[2760] India suggests a global regulation for open, safe and secure cyberspace, The Economic Times (Mumbai) 12 November 2019. Access Date: 21 March 2020. https://economictimes.indiatimes.com/tech/internet/india-suggests-a-global-regulation-for-open-safe-and-secure-cyberspace/articleshow/72027153.cms

[2761] 13th meeting of India-UK Joint Working Group on Counter Terrorism, Ministry of External Affairs of India (New Delhi) 28 November 2019. Access Date: 21 March 2020. https://mea.gov.in/press-releases.htm?dtl/32133/13th+meeting+of+IndiaUK+Joint+Working+Group+on+Counter+Terrorism

[2762] India and Japan ask Pakistan to Take Concrete Action Against Terror Infrastructure, The Economic Times, (Mumbai) 30 November 2019. Access date: 16 May 2020. https://economictimes.indiatimes.com/news/defence/india-and-japan-ask-pakistan-to-take-concrete-action-against-terror-infrastructure/articleshow/72310162.cms?from=mdr

[2763] India and Japan ask Pakistan to Take Concrete Action Against Terror Infrastructure, The Economic Times, (Mumbai) 30 November 2019. Access date: 16 May 2020. https://economictimes.indiatimes.com/news/defence/india-and-japan-ask-pakistan-to-take-concrete-action-against-terror-infrastructure/articleshow/72310162.cms?from=mdr

[2764] India and Japan ask Pakistan to Take Concrete Action Against Terror Infrastructure, The Economic Times, (Mumbai) 30 November 2019. Access date: 16 May 2020. https://economictimes.indiatimes.com/news/defence/india-and-japan-ask-pakistan-to-take-concrete-action-against-terror-infrastructure/articleshow/72310162.cms?from=mdr

[2765] India suspends internet and phone services to quell protests, Associated Press (New Delhi) 21 December 2019. Access Date: 21 March 2020. https://apnews.com/643423717f6494718e449dac441c3db9

On 14 February 2020, India's government restored slow-speed internet (2G connection) in the regions of Kashmir and Jammu only for government-approved websites.[2767] Social media platforms remain blocked.[2768]

On 28 February 2020, India hosted the 14th Meeting of India-France Joint Working Group on Counter Terrorism.[2769] The Joint Secretary for Counter Terrorism of the Ministry of External Affairs of India and the French delegation "condemned terrorism in all its forms" and committed to "prevent the use of internet for terrorist purposes."[2770]

On 29 June 2020, the Ministry of Electronics and Information Technology banned 59 Chinese mobile apps which are claimed to be "prejudicial to sovereignty and integrity of India."[2771] This ban includes worldwide popular apps such as TikTok, Shein or CleanMaster and is a "targeted move to ensure safety and sovereignty of Indian cyberspace."[2772]

India has partially complied with this commitment by taking action to realise a secure internet through their bilateral agreement with Germany. However, India has not taken action to realise an open and free internet.

Thus, India receives a score of 0.

Analyst: Xavier Bornert

Indonesia: −1

Indonesia has not complied with its commitment to unite against all forms of terrorism and terrorist activity.

On 12 November 2019, Deputy Secretary General of the European External Action Service Jean-Christophe Belliard and Ambassador of Indonesia to the European Union Yuri Thamrin discussed a shared view on strengthening international rules-based orders and reiterated their commitment to multilateralism.[2773]

[2766] India suspends internet and phone services to quell protests, Associated Press (New Delhi) 21 December 2019. Access Date: 21 March 2020. https://apnews.com/643423717f6494718e449dac441c3db9
[2767] India keeps lid on Kashmir's internet 6 months into lockdown, Associated Press (New Delhi), 14 February 2020. Access Date: 21 March 2020. https://apnews.com/6c9f105f899cadee6c22e567057a4fd4.
[2768] India keeps lid on Kashmir's internet 6 months into lockdown, Associated Press (New Delhi), 14 February 2020. Access Date: 21 March 2020. https://apnews.com/6c9f105f899cadee6c22e567057a4fd4.
[2769] India-France Joint Working Group on Counter Terrorism, French Embassy in New Delhi (New Delhi), 28 February 2020. Access Date: 21 March 2020. https://in.ambafrance.org/India-France-Joint-Working-Group-on-Counter-Terrorism
[2770] India-France Joint Working Group on Counter Terrorism, French Embassy in New Delhi (New Delhi) 28 February 2020. Access Date: 21 March 2020. https://in.ambafrance.org/India-France-Joint-Working-Group-on-Counter-Terrorism
[2771] Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order, Press Information Bureau Government of India (New Delhi) 29 June 2020. Access Date: 30 August 2020. https://pib.gov.in/PressReleseDetail.aspx?PRID=1635206
[2772] Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order, Press Information Bureau Government of India (New Delhi) 29 June 2020. Access Date: 30 August 2020. https://pib.gov.in/PressReleseDetail.aspx?PRID=1635206
[2773] European Union and Indonesia hold their fourth Political Dialogue, European Union External Action (Brussels) 13 November 2019. Access Date: 5 June 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/70369/european-union-and-indonesia-hold-their-fourth-political-dialogue_en

On 22 May 2020, Indonesia co-sponsored the Arria-Formula Meeting of the United Nations Security Council.[2774] The purpose of this meeting was to discuss the global efforts made in strengthening cyber stability as well as preventing cyber threats.[2775]

While Indonesia has participated in discussions relating to this commitment, it has not taken action to realise an open, free and secure internet.

Thus, Indonesia receives a score of −1.

Analyst: Vannie Kopalakrishnan

Italy: 0

Italy has partially complied with its commitment to realize an open, free and secure internet.

On 22 September 2019, Decree Law No. 105 entered into force with the goal of increasing national cybersecurity in Italy.[2776] The law includes policies that increase internet security and so, reduce the capabilities of cyber threats.[2777] The law also includes punitive measures for organizations who fail to take relevant action in accordance with this new law.[2778] Additionally, it directs the government to hire a maximum of 77 new staff members for the implementation of the necessary policies.[2779]

On 28 May 2020, SIA, a tech company that provides information technology (IT) services and infrastructure especially in the financial sector, signed an extension to its agreement with the Italian State Police to continue strengthening cybersecurity in the country.[2780] Past directives from Italy's Ministry of the Interior aimed to prevent cybercrime through greater cooperation with IT operators, making this agreement a continuation of the collaboration between the public and private sectors in Italy.[2781]

On 7 July 2020, the Italian National Postal and Communication Police Unit, in collaboration with the Romanian National Police, Europol and Eurojust dismantled a criminal group responsible for fraud,

[2774] Indonesia Voices Cyber Stability in the UN, Ministry of Foreign Affairs of the Republic of Indonesia (New York) 23 May 2020. Access Date: 5 June 2020. https://kemlu.go.id/portal/en/read/1327/berita/indonesia-voices-cyber-stability-in-the-un

[2775] Indonesia Voices Cyber Stability in the UN, Ministry of Foreign Affairs of the Republic of Indonesia (New York) 23 May 2020. Access Date: 5 June 2020. https://kemlu.go.id/portal/en/read/1327/berita/indonesia-voices-cyber-stability-in-the-un

[2776] Italy: New Provisions on National Cybersecurity Enter into Force, Library of Congress (Italy) 16 October 2019. Access Date: 15 June 2020. https://www.loc.gov/law/foreign-news/article/italy-new-provisions-on-national-cybersecurity-enter-into-force/

[2777] Italy: New Provisions on National Cybersecurity Enter into Force, Library of Congress (Italy) 16 October 2019. Access Date: 15 June 2020. https://www.loc.gov/law/foreign-news/article/italy-new-provisions-on-national-cybersecurity-enter-into-force/

[2778] Italy: New Provisions on National Cybersecurity Enter into Force, Library of Congress (Italy) 16 October 2019. Access Date: 15 June 2020. https://www.loc.gov/law/foreign-news/article/italy-new-provisions-on-national-cybersecurity-enter-into-force/

[2779] Italy: New Provisions on National Cybersecurity Enter into Force, Library of Congress (Italy) 16 October 2019. Access Date: 15 June 2020. https://www.loc.gov/law/foreign-news/article/italy-new-provisions-on-national-cybersecurity-enter-into-force/

[2780]Italian State Police and SIA renew the agreement on prevention and the fight against cybercrime, SIA (Rome) 28 May 2020. Access Date: 28 August 2020. https://www.sia.eu/en/media-events/news-press-releases/italian-state-police-and-sia-renew-the-agreement-on-prevention-and-the-fight-against-cybercrime

[2781] Italian State Police and SIA renew the agreement on prevention and the fight against cybercrime, SIA (Rome) 28 May 2020. Access Date: 28 August 2020. https://www.sia.eu/en/media-events/news-press-releases/italian-state-police-and-sia-renew-the-agreement-on-prevention-and-the-fight-against-cybercrime

money laundering and other cybercrime activity.[2782] Eight were arrested in Italy, and the group's assets were seized, with their crimes estimated to have caused EUR20 million losses for victims across Europe annually.[2783]

Italy has partially complied with this commitment. Though it has enacted a law that aims to increase the country's digital security capabilities, it has not taken action to create an open and free internet.

Thus, Italy receives a score of 0.

Analysts: Arshia Hassani and Jonathan Ku

Japan: 0

Japan has partially complied with its commitment to realizing an open, free and secure internet.

On 18 November 2019, the Ministry of Foreign Affairs held the fourth Korea-Japan-China Cyber Policy Consultation in Beijing to discuss and enhance regional cybersecurity cooperation.[2784] There was a shared understanding that discussions regarding cybersecurity norms at the UN are essential to creating a safe cyberspace and explored ways to cooperate on joint response to cybercrimes among law enforcement agencies.[2785]

On 30 November 2019, the Japanese Foreign Minister and the Minister of Defence took part in a ministerial dialogue with India to discuss the threats posed to regional peace by terror networks operating from Pakistan.[2786] The Japanese members, along with their Indian counterparts, called upon Pakistan to "take resolute and irreversible action against [terror networks] and fully comply with international commitments"[2787] including the steps prescribed by the Financial Action Task Force, the global anti-terror watchdog.[2788]

On 6 April 2020, the Japanese Ministry of Defense (MOD) confirmed that it would invest approximately USD237.12 million to develop AI-based security tools to defend against cyberattacks.[2789] The MOD also invested approximately USD277,711 to: build a Cyber Information Gathering System, which gathers information on the tactics, techniques and procedures of

[2782] Italy and Romania take down cyber fraud ring generating €20 million per year in criminal profits, EUROPOL (The Hague) 7 July 2020. Access Date: 28 August 2020. https://www.europol.europa.eu/newsroom/news/italy-and-romania-take-down-cyber-fraud-ring-generating-%E2%82%AC20-million-year-in-criminal-profits

[2783] Italy and Romania take down cyber fraud ring generating €20 million per year in criminal profits, EUROPOL (The Hague) 7 July 2020. Access Date: 28 August 2020. https://www.europol.europa.eu/newsroom/news/italy-and-romania-take-down-cyber-fraud-ring-generating-%E2%82%AC20-million-year-in-criminal-profits

[2784] 4th ROK-Japan-China Cyber Policy Consultation Held, Ministry of Foreign Affairs (Seoul) 19 November 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320841.

[2785] 4th ROK-Japan-China Cyber Policy Consultation Held, Ministry of Foreign Affairs (Seoul) 19 November 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320841.

[2786] India and Japan ask Pakistan to Take Concrete Action Against Terror Infrastructure, The Economic Times (Mumbai) 30 November 2019. Access date: 16 May 2020. https://economictimes.indiatimes.com/news/defence/india-and-japan-ask-pakistan-to-take-concrete-action-against-terror-infrastructure/articleshow/72310162.cms?from=mdr

[2787] India and Japan ask Pakistan to Take Concrete Action Against Terror Infrastructure, The Economic Times, (Mumbai) 30 November 2019. Access Date: 16 May 2020. https://economictimes.indiatimes.com/news/defence/india-and-japan-ask-pakistan-to-take-concrete-action-against-terror-infrastructure/articleshow/72310162.cms?from=mdr

[2788] India and Japan ask Pakistan to Take Concrete Action Against Terror Infrastructure, The Economic Times, (Mumbai) 30 November 2019. Access Date: 16 May 2020. https://economictimes.indiatimes.com/news/defence/india-and-japan-ask-pakistan-to-take-concrete-action-against-terror-infrastructure/articleshow/72310162.cms?from=mdr

[2789] Japan Embraces AI Tools to Fight Cyberattacks with US$237 Million Investment, Cybersecurity Magazine, (Albuquerque) 6 April 2020. Access Date: 16 May 2020. https://www.cisomag.com/japan-embraces-ai-tools-to-fight-cyberattacks-with-us237-mn-investment/

cyberattacks on government and private entities; expand the Cyber Defense Group from 220 to 290 personnel; and perform research on cybersecurity measures for network devices used by the Japanese military.[2790]

Japan has partially complied with its commitment to realising an open, free and secure internet. It has established policies that aim to identify mitigate the presence of violent content in the digital world, thus realising a secure internet, however, it has not taken action to realise an open and free internet.

Thus, Japan receives a score of 0.

Analyst: Dan Poliwoda

Korea: +1

Korea has fully complied with its commitment to realize an open, free and secure internet.

On 28 June 2019, the Ministry of Foreign Affairs held the fifth Korea-European Union Cyber Policy Consultation and the second meeting of the Korea-European Union Specialised Working Group on Counter-Terrorism in Brussels, in which the two sides discussed cybersecurity and counter-terrorism strategies and reaffirmed their commitment in cooperating for an open and safe cyberspace.[2791]

On 2 August 2019, Minister of Foreign Affairs Kang Kyung-wha attended the 26th ASEAN Regional Forum in Bangkok to exchange views with other members of the Association of South East Asian Nations (ASEAN) on regional and international issues, including the cybersecurity and security threats rising from tension over protectionism.[2792] An aim to prevent and mitigate terrorism and violent extremism was also adopted at the forum.[2793]

On 1 October 2019, the Ministry of Science and ICT (MSIT) hosted the fourth annual meeting of the Cybersecurity Alliance for Mutual Progress (CAMP) in Seoul to foster international cooperation and trust to respond to cyber threats, discussing the alliance's progress and future activities.[2794] As the Korea Internet and Security Agency has renewed their tenure for CAMP operations, Korea will continue its commitment to a secure internet by playing a leading role in international cooperation for cybersecurity.[2795]

On 2 October 2019, the Ministry of National Defence announced that Vice Minister of Korea Park Jae-min and Vice Minister of United Arab Emirates (UAE) Matar Salem Al-Dhaheri agreed to

[2790] Japan Embraces AI Tools to Fight Cyberattacks with US$237 Million Investment, Cybersecurity Magazine, (Albuquerque) 6 April 2020. Access Date: 16 May 2020. https://www.cisomag.com/japan-embraces-ai-tools-to-fight-cyberattacks-with-us237-mn-investment/

[2791] 5th ROK-EU Cyber Policy Consultation and 2nd Meeting of ROK-EU Specialised Working Group on Counter-Terrorism Take Place, Ministry of Foreign Affairs (Seoul) 1 July 2019. Access Date: 19 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320587

[2792] Outcome of 26th ASEAN Regional Forum, Ministry of Foreign Affairs (Seoul) 2 August 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320631

[2793] Outcome of 26th ASEAN Regional Forum, Ministry of Foreign Affairs (Seoul) 2 August 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320631

[2794] The Fourth Annual Meeting of CAMP (Oct 11), Ministry of Science and ICT (Sejong) 27 November 2019. Access Date: 27 January 2020. https://english.msit.go.kr/english/msipContents/contentsView.do?cateId=tst56&artId=2339767

[2795] The Fourth Annual Meeting of CAMP (Oct 11), Ministry of Science and ICT (Sejong) 27 November 2019. Access Date: 27 January 2020. https://english.msit.go.kr/english/msipContents/contentsView.do?cateId=tst56&artId=2339767

strengthen cooperation in establishing international peace, including furthering the expansion of bilateral cooperation in the information and cybersecurity realms.[2796]

On 8 October 2019, Korea co-hosted the Warsaw Process Working Group on Cybersecurity in Seoul with the United States and Poland.[2797] The meeting was attended by 50 countries and worked towards creating a secure and peaceful cyberspace by sharing each country's cybersecurity policy and best practices, thus enhancing cooperation in responding to cyber threats.[2798] The Korea National Policy Agency also presented about collaboration in countering cybercrime.[2799]

On 13 October 2019, MSIT began hosting the 2019 Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group in Seoul.[2800] The MSIT explored cooperation with APEC members by sharing policies, including information security.[2801]

On 18 November 2019, Minister of National Defence Jeong Kyeong-doo called for the international community to come together to cope with new security threats and issues at the sixth ASEAN Defence Ministers' Meeting-Plus in Bangkok by introducing methods to be led by ASEAN countries.[2802] These methods include: "establishing principles and codes in every country to respect international laws and individual country's rights and interests,"[2803] "boosting consultative groups to promote multilateral security cooperation"[2804] and "increasing mutual trust among regional countries and strengthening partnerships."[2805] Jeong pointed to the developments of advanced science and

[2796] Republic of Korea, UAE agree to strengthen cooperation in establishing international peace, Ministry of National Defense (Seoul) 16 October 2019. Access Date: 7 February 2020. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_47261&boardSeq=O_226723&titleId=null&siteId=mndEN&id=mndEN_020100000000

[2797] Warsaw Process Working Group on Cybersecurity Convened in Seoul, Ministry of Foreign Affairs (Seoul) 8 October 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320733

[2798] Warsaw Process Working Group on Cybersecurity Convened in Seoul, Ministry of Foreign Affairs (Seoul) 8 October 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320733

[2799] Warsaw Process Working Group on Cybersecurity Convened in Seoul, Ministry of Foreign Affairs (Seoul) 8 October 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320733

[2800] 2019 APEC TEL Meeting is Held (Oct 14), Ministry of Science and ICT (Sejong) 27 November 2019. Access Date: 27 January 2020. https://english.msit.go.kr/english/msipContents/contentsView.do?cateId=tst56&artId=2339769

[2801] 2019 APEC TEL Meeting is Held (Oct 14), Ministry of Science and ICT (Sejong) 27 November 2019. Access Date: 27 January 2020. https://english.msit.go.kr/english/msipContents/contentsView.do?cateId=tst56&artId=2339769

[2802] Republic of Korea Defense Minister calls for close cooperation to cope with new security threats, Ministry of National Defense (Seoul) 27 November 2019. Access Date: 7 February 2020. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_47261&boardSeq=O_230312&titleId=null&siteId=mndEN&id=mndEN_020100000000

[2803] Republic of Korea Defense Minister calls for close cooperation to cope with new security threats, Ministry of National Defense (Seoul) 27 November 2019. Access Date: 7 February 2020. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_47261&boardSeq=O_230312&titleId=null&siteId=mndEN&id=mndEN_020100000000.

[2804] Republic of Korea Defense Minister calls for close cooperation to cope with new security threats, Ministry of National Defense (Seoul) 27 November 2019. Access Date: 7 February 2020. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_47261&boardSeq=O_230312&titleId=null&siteId=mndEN&id=mndEN_020100000000.

[2805] Republic of Korea Defense Minister calls for close cooperation to cope with new security threats, Ministry of National Defense (Seoul) 27 November 2019. Access Date: 7 February 2020. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_47261&boardSeq=O_230312&titleId=null&siteId=mndEN&id=mndEN_020100000000.

technology in the Fourth Industrial Revolution as a means for humans to create security threats in cyberspace.[2806]

On 18 November 2019, the Ministry of Foreign Affairs held the fourth Korea-Japan-China Cyber Policy Consultation in Beijing to discuss and enhance regional cybersecurity cooperation.[2807] There was a shared understanding that discussions regarding cybersecurity norms at the United Nations are essential to creating a safe cyberspace and explored ways to cooperate on joint response to cybercrimes among law enforcement agencies.[2808]

On 23 November 2019, President of the Korea Internet and Security Kim Seok-hwan and Chief Executive of the Cyber Security Agency of Singapore signed a memorandum of understanding (MOU) to enhance cooperation and sharing information on cybersecurity issues.[2809]

On 24 November 2019, Minister of the Interior and Safety Chin Young signed an MOU to continue to support Brunei's e-government establishment project until 2024.[2810] The MOU allows Korea and Brunei to share data opening policies and experiences for allowing public data to be used by the private sector.[2811]

On 2 December 2019, the Ministry of Foreign Affairs and Institute for National Security Strategy co-hosted the 2019 International Conference on Emerging Security Threats to discuss best practices in responding to emerging security threats and international cooperation, including cybersecurity and terrorist use of technologies.[2812]

On 10 December 2019, the fourth Foreign and Defence Ministers' meeting between Korea and Australia was held in Sydney.[2813] The two sides agreed to strengthen cooperation in cybersecurity through the Korea-Australia Cyber Policy Dialogue and to respond to terrorism.[2814]

On 16 December 2019, the Minister of National Defence Jeong Kyeong-doo and his counterpart Mohammed Ahmed Al Bowardi of the UAE agreed to further enhance cooperation in areas of

[2806] Republic of Korea Defense Minister calls for close cooperation to cope with new security threats, Ministry of National Defense (Seoul) 27 November 2019. Access Date: 7 February 2020. http://www.mnd.go.kr/user/boardList.action?command=view&page=1&boardId=O_47261&boardSeq=O_230312&titleId=null&siteId=mndEN&id=mndEN_020100000000.
[2807] 4th ROK-Japan-China Cyber Policy Consultation Held, Ministry of Foreign Affairs (Seoul) 19 November 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320841.
[2808] 4th ROK-Japan-China Cyber Policy Consultation Held, Ministry of Foreign Affairs (Seoul) 19 November 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320841.
[2809] Singapore Signs MOU With S. Korea on Cybersecurity Cooperation, Bloomberg (Singapore) 23 November 2019. Access Date: 7 February 2020. https://www.bloomberg.com/news/articles/2019-11-23/singapore-signs-mou-with-s-korea-on-cybersecurity-cooperation
[2810] MOIS to extend support for Brunei's e-government establishment project by 2024, Ministry of the Interior and Safety (Sejong) 18 December 2019. Access Date: 23 January 2020. https://www.mois.go.kr/eng/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000019&nttId=74806.
[2811] MOIS to extend support for Brunei's e-government establishment project by 2024, Ministry of the Interior and Safety (Sejong) 18 December 2019. Access Date: 23 January 2020. https://www.mois.go.kr/eng/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000019&nttId=74806
[2812] Ministry of Foreign Affairs and Institute for National Security Strategy to Co-host "2019 International Conference on Emerging Security Threats", Ministry of Foreign Affairs (Seoul) 29 November 2019. Access Date: 19 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320863
[2813] 4th ROK-Australia Foreign and Defense Ministers' 2+2 Meeting Takes Place, Ministry of Foreign Affairs (Seoul) 10 December 2019. Access Date: 19 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320887
[2814] 4th ROK-Australia Foreign and Defense Ministers' 2+2 Meeting Takes Place, Ministry of Foreign Affairs (Seoul) 10 December 2019. Access Date: 19 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320887

intelligence, cybersecurity and munitions at the seventh Korea-UAE defence ministers' talks, meant to further strengthen their cooperation to establish permanent peace in the region.[2815]

On 29 January 2020, the second Korea-United Kingdom Cyber Dialogue was held in Seoul.[2816] Both Korea and UK shared experiences and expertise in the increasing challenge of cyber threats by sharing information and agreeing to work more closely on responses to cyber incidents and cybercrime investigations.[2817]

On 14 February 2020, Minister Kang Kyung-wha and Minister of Foreign Affairs of Lithuania Linas Linkevicius held a bilateral meeting at the 56th Munich Security Conference in which the two ministers discussed methods of promoting cooperation in various industries, including cybersecurity and information technology.[2818]

On 30 April 2020, Minister Choi Ki-young participated in the Extraordinary G20 Digital Economy Ministerial Meeting and discussed methods to strengthen technologies for the COVID-19 response, such as creating a secure internet by counteracting cyber activities that threaten the security of the digital economy.[2819]

On 20 May 2020, the 20th National Assembly approved a bill to prevent online sex crimes following the "Nth Room" case in which a Telegram chat room operator coerced over 100 people into performing sexual acts and shared their photos.[2820] The bill aims to remove and prevent the circulation of illegal pornography and block its access.[2821]

On 14 July 2020, the Korean government announced the Digital New Deal, which comprises 12 goals, including the establishment of a strong cybersecurity system to deal with online threats, establish digital education infrastructure in schools, improve online education and support small businesses online.[2822]

[2815] Republic of Korea, UAE discuss approaches to cooperation in national defense and the defense industry, Ministry of National Defense (Seoul) 6 January 2020. Access Date: 8 February 2020. http://www.mnd.go.kr/user/boardList.action?boardId=O_47317&siteId=mndEN&page=1&search=&column=&boardType=02&listType=&parent=&boardSeq=O_233642&command=albumView&chkBoxSeq=&chkBoxId=&chkBoxPos=&chkBoxDepth=&chkBoxFamSeq=&warningYn=N&categoryId=&categoryDepth=&id=mndEN_020200000000

[2816] The 2nd ROK-UK Cyber Dialogue Held, Ministry of Foreign Affairs (Seoul) 29 January 2020. Access Date: 20 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320935

[2817] The 2nd ROK-UK Cyber Dialogue Held, Ministry of Foreign Affairs (Seoul) 29 January 2020. Access Date: 20 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320935

[2818] Outcome of Bilateral Meetings between Minister of Foreign Affairs and her Lithuanian, Finnish and Norwegian Counterparts Held on Occasion of 56th Munich Security Conference, Ministry of Foreign Affairs (Seoul) 15 February 2020. Access Date: 20 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320961

[2819] Minister Choi Shared Korea's COVID-19 Response Experience at Extraordinary G20 Digital Economy Ministerial Meeting. (May 1), Ministry of Science and ICT (Seoul) 1 May 2020. Access Date: 19 July 2020. https://english.msit.go.kr/english/msipContents/contentsView.do?cateId=tst56&artId=2939696

[2820] Assembly rushes through over 100 bills, The Korea Herald (Seoul) 20 May 2020. Access Date: 24 July 2020. http://www.koreaherald.com/view.php?ud=20200520000721

[2821] Assembly rushes through over 100 bills, The Korea Herald (Seoul) 20 May 2020. Access Date: 24 July 2020. http://www.koreaherald.com/view.php?ud=20200520000721

[2822] The Digital New Deal Is to Lead Digital Transition in the World After COVID-19 (July 15), Ministry of Science and ICT (Seoul) 27 August 2020. Access Date: 25 September 2020. https://english.msit.go.kr/english/msipContents/contentsView.do?cateId=tst56&artId=3057114

On 15 July 2020, the Korea Communications Commission fined TikTok, a Chinese video app, KRW186 million for collecting user data, including the data of those under aged 14 without parental consent, and sharing it to overseas servers, which violated local telecommunication laws in Korea.[2823]

On 13 September 2020, the Ministry of Foreign Affairs announced that they would be investing in their own video conference platform to strengthen security and minimise the possibility of hacking.[2824]

On 24 September 2020, the Korea Communications Standards Commission blocked public access to a website which disclosed personal information of alleged sex offenders and pedophiles due to the possibility of false accusations.[2825]

Korea has taken actions in creating an open, free and secure internet by cooperating with the international community to share experiences, information and by agreeing to cooperate with other countries to work more closely to respond to cybersecurity issues through bilateral and multilateral conferences, meetings, and memorandums of understanding. Korea has also launched investigations into private companies regarding personal data breaches.

Thus, Korea receives a score of +1.

Analyst: Ingrid Wong

Mexico: −1

Mexico has not yet complied in its efforts into ensuring a free, secure and open internet.

On 19 December 2019, the Federal Institute of Telecommunications proposed to repeal net neutrality in Mexico.[2826] The net neutrality ensured equal access to content from any service providers, thus supporting an open and free internet.[2827]

Mexico has not complied with its commitment to realise an open, free and secure internet.

Thus, Mexico receives a score of −1.

Analyst: Raphaël Colombier

Russia: 0

Russia has partially complied with its commitment to realize an open, free and secure internet.

[2823] Korea punishes TikTok for data mishandling, The Korea Times (Seoul) 15 July 2020. Access Date: 23 July 2020. https://www.koreatimes.co.kr/www/tech/2020/07/133_292855.html

[2824] Foreign ministry to set up own videoconferencing system for better security, The Korea Herald (Seoul) 13 September 2020. Access Date: 25 September 2020. http://www.koreaherald.com/view.php?ud=20200913000060

[2825] S. Korea blocks access to 'Digital Prison' website, The Korea Herald (Seoul) 24 September 2020. Access Date: 25 September 2020. http://www.koreaherald.com/view.php?ud=20200924001041.

[2826] Anteproyecto De Lineamientos Para La Gestión De Tráfico Y Administración De Red A Que Deberán Sujetarse Los Concesionarios Y Autorizados Que Presten El Servicio De Acceso A Internet, Instituto Federal de Telecomunicaciones (Mexico City), December 19, 2020, access date 01/02/2020. http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/13791/documentos/1documentoenconsultapublicaanteproyectodelineamientos.pdf

[2827] Anteproyecto De Lineamientos Para La Gestión De Tráfico Y Administración De Red A Que Deberán Sujetarse Los Concesionarios Y Autorizados Que Presten El Servicio De Acceso A Internet, Instituto Federal de Telecomunicaciones (Mexico City), December 19, 2020, access date 01/02/2020. http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/13791/documentos/1documentoenconsultapublicaanteproyectodelineamientos.pdf

On 9 September 2019, Russian Deputy Foreign Minister Oleg Syromolotov met with U.S. Deputy Secretary of State John Sullivan to hold another round of consultations on the fight against terrorism.[2828] Syromolotov and Sullivan discussed topics of the state and prospects for bilateral cooperation on countering terrorist threats.[2829]

On 12 October 2019, Chair of the State Duma Vyacheslav Volodin took part in the third Conference of Speakers of Parliaments on Countering Terrorism and Strengthening Regional Connectivity in Istanbul.[2830] Chair Volodin and his counterparts agreed to 20 commitments with an emphasis on peace and security as well as counter terrorism measures.[2831]

On 21 October 2019, Russia held the 33rd session of the Foreign Investment Advisory Council.[2832] Proposals for initiatives included improving laws and regulations to counter money laundering and the financing of terrorism.[2833]

On 30 October 2019, Deputy Minister Syromolotov, and Indian Secretary of External Affairs Vijay Thakur Singh met for the 11th meeting of the India-Russia joint working group on counter terrorism in New Delhi.[2834] Both sides deliberated upon measures to further strengthen and deepen counterterrorism cooperation and both agreed on united efforts to fight terrorism and terrorism financing at multilateral forums.[2835]

On 1 November 2019, the Russian federal law on "sovereign internet" was enacted to ensure the safe and stable functioning of the internet on Russian territory.[2836] The federal law will tighten state control over the global network, routing Russian web traffic and data through points controlled by

[2828] U.S., Russian Officials Discuss Fight Against Terror in Vienna, RadioFreeEurope RadioLiberty (Russia) 10 September 2019. Access Date: 19 March 2020. https://www.rferl.org/a/u-s-russian-officials-discuss-fight-against-terror-in-vienna/30156111.html

[2829] Press Release on Deputy Foreign Minister Oleg Syromolotov's meeting with United States Deputy Secretary of State John J. Sullivan and Russia-US High-Level Counterterrorism Dialogue, Ministry of Foreign Affairs Russia (Moscow) 9 September 2019. Access Date: 20 March 2020. https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3780958

[2830] Chairman of the State Duma of Russia Viacheslav Volodin visited Turkey, Embassy of the Russian Federation in the Republic of Turkey (Istanbul) 11 October 2019. Access Date: 20 March 2020. https://turkey.mid.ru/en/press_center/news/chairman_of_the_state_duma_of_russia_viacheslav_volodin_visited_turkey/

[2831] Joint Declaration of the "Third Conference of Speakers of Parliaments on Countering Terrorism and Strengthening Regional Connectivity", The State Duma (Istanbul) 12 October 2019. Access Date: 19 March 2020. http://duma.gov.ru/en/news/46594/

[2832] Communique of the 33rd Session of the Foreign Investment Advisory Council in Russia (Moscow, 21 October 2019, The Russian Government (Moscow) 21 October 2019. Access Date: 19 March 2020. http://government.ru/en/news/38156/

[2833] Communique of the 33rd Session of the Foreign Investment Advisory Council in Russia (Moscow, 21 October 2019, The Russian Government (Moscow) 21 October 2019. Access Date: 19 March 2020. http://government.ru/en/news/38156/

[2834] Joint Press Statement: India-Russia High Level Consultations on Counter Terrorism, Ministry of External Affairs (New Delhi) 30 October 2019. Access Date: 20 March 2020. https://www.mea.gov.in/bilateral-documents.htm?dtl/31986/joint+press+statement+indiarussia+high+level+consultations+on+counter+terrorism

[2835] Press release on the 11th meeting of the India-Russia Joint Working Group on Counter Terrorism, Ministry of Foreign Affairs Russia (New Delhi) 30 October 2019. Access Date: 20 March 2020. https://www.mid.ru/en/web/guest/maps/in/-/asset_publisher/EpJ5G4lcymvb/content/id/3879023

[2836] In Russia, the law on "sovereign RuNEt" entered into force, The State Duma (Moscow) 1 November 2019. Access Date: 19 March 2020. http://duma.gov.ru/news/46811/

state authorities and to build a national domain to allow the internet to continue working should Russia get cut off from foreign infrastructure.[2837]

On 23 December 2019, Minister of Internal Affairs Vladimir Kolokoltsev met with Internal Affairs minister of the Republic of Ingushetia to discuss improvement for the fight against terrorism and extremism, the fight against drug crime, and control of migration processes.[2838]

On 26 December 2019, Russia began testing for a national internet system that would operate as an alternative to the global network.[2839] The national internet system, RuNet was successfully tested against different scenarios that included cyber attacks.[2840] RuNet makes internet freely and easily accessible regardless of external or internal conditions.[2841]

On 19 February 2020, Minister Kolokoltsev and Swedish Minister of Home Affairs Mikael Damberg held a meeting discussing pressing issues regarding combating organized crime, illegal migration, drug trafficking and anti-terrorism activities.[2842]

On 28 May 2020, the Commission of the State Duma on the Investigation of Foreign Interference in Russia's Internal Affairs proposed amendments that will restrict access to information containing justification for extremist or terrorist activities.[2843]

On 17 June 2020, Russian foreign minister Sergey Lavrov held a videoconference with the foreign ministers of the Association of Southeast Asian Nations (ASEAN) member states discussing Russian-ASEAN cooperation plans for combatting terrorism and promoting education.[2844]

On 18 June 2020, Minister Lavrov and Serbian Deputy Prime Minister and Minister of the Interior Nebojsa Stefanovic signed an intergovernmental agreement on cooperation in combatting terrorism.[2845]

[2837] Russia enacts 'sovereign internet' law, free speech activists cry foul, Reuters (Moscow) 1 November 2019. Access Date: 19 March 2020. https://uk.reuters.com/article/uk-russia-internet-bill/russia-enacts-sovereign-internet-law-free-speech-activists-cry-foul-idUKKBN1XB4U7

[2838] Working visit of Vladimir Kolokoltsev to Republic of Ingushetia, Ministry of Internal Affairs of the Russian Federation (Magas) 23 December 2019. Access Date: 20 March 2020. https://en.mvd.ru/news/item/19185848

[2839] Russia starts testing its own internal internet, Techcrunch 26 December 2019. Access Date: 20 March 2020. https://techcrunch.com/2019/12/26/russia-starts-testing-its-own-internal-internet/

[2840] Russia successfully disconnected from the internet, ZDNet 23 December 2019. Access Date: 28 October 2020. https://www.zdnet.com/article/russia-successfully-disconnected-from-the-internet/

[2841] How will the sovereign internet law operate?, the State Duma (Moscow) 1 November 2019. Access Date: 20 March 2020. http://duma.gov.ru/news/46774/

[2842] Vladimir Kolokoltsev and Mikael Damberg discussed pressing issues of interaction of Russia and Sweden in law enforcement, Ministry of Internal Affairs of the Russian Federation (Stockholm) 19 February 2020. Access Date: 20 March 2020. https://en.mvd.ru/news/item/19587281

[2843] State Duma prepared bills to counter interference in the Russian internal affairs, The State Duma (Moscow) 28 May 2020. Access Date: 18 July 2020. http://duma.gov.ru/en/news/48683/

[2844] Remarks and replies by Foreign Minister Sergey Lavrov at the news conference following the Russia-ASEAN Foreign Ministers' Meeting on Coronavirus Disease 2019 via videoconference, The Ministry of Foreign Affairs of the Russian Federation (Moscow) 17 June 2020. Access Date: 19 July 2020. https://www.mid.ru/en/web/guest/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/4168016

[2845] Foreign Minister Sergey Lavrov's opening remarks at talks with Serbian Deputy Prime Minister and Minister of the Interior Nebojsa Stefanovic, The Ministry of Foreign Affairs of the Russian Federation (Belgrade) 18 June 2020. Access Date: 21 July 2020. https://www.mid.ru/en/web/guest/meropriyatiya_s_uchastiem_ministra/-/asset_publisher/xK1BhB2bUjd3/content/id/4169208.

On 13 October 2020, the State Duma adopted a new bill which fines website owners for refusing to delete extremist and harmful material such as child pornography, and the development, manufacturing and use of drugs.[2846] Fines can reach up to RUB15 million; the amounts increasing based on the offender (citizens, officials and legal entities) and whether it is a repeat offense.[2847] This law obliges hosting providers and site owners to remove prohibited content, but has no compliance measures yet.[2848]

Russia has taken measures to cooperate with international organizations and internet service providers to fulfill a secure internet as demonstrated by the development of RuNet. Russia has collaborated with organizations to discuss digital innovation and solutions to threats from criminal activity on the internet. Although Russia has made efforts to ensure a secure and safe internet, the commitment to a free internet was not fulfilled.

Thus, Russia receives a score of 0.

Analyst: Sebastian Vecerina

Saudi Arabia: 0

Saudi Arabia has partially complied with its commitment to realze an open, free and secure internet.

On 23 December 2019, the Computer Emergency Response Team (CERT) joined the international Forum of Incident Response and Security Teams.[2849] CERT is working to enhance the Kingdom's efforts in raising the awareness maturity of Saudi Arabia and to collaborate with international CERT teams.[2850] Saudi CERT has three main functions: increasing the level of knowledge and awareness regarding cybersecurity, disseminate information about vulnerabilities, and to campaign and cooperate with other response teams.[2851] CERTs can include detecting terrorist threats.

On 20 January 2020, a delegation of members from 15 states of the Arab Diplomatic Corps met in Riyadh, Saudi Arabia to discuss enhanced mutual cooperation between the Global Center for Combatting Extremist Ideology and their states.[2852] These discussions were focused on eliminating the rise of extremism in youth and on the Global Center's research on social media's role in radicalization.[2853]

On 4 February 2020, a memorandum of understanding was signed between the National Cybersecurity Authority and the Global Resilience Federation aimed at enabling better knowledge

[2846] The State Duma introduces fines of up to 15 million rubles for refusing to remove prohibited information from sites, TASS (Moscow) 13 October 2020. Access Date: 19 October 2020. https://tass.ru/ekonomika/9704661
[2847] The State Duma introduces fines of up to 15 million rubles for refusing to remove prohibited information from sites, TASS (Moscow) 13 October 2020. Access Date: 19 October 2020. https://tass.ru/ekonomika/9704661
[2848] The State Duma introduces fines of up to 15 million rubles for refusing to remove prohibited information from sites, TASS (Moscow) 13 October 2020. Access Date: 19 October 2020. https://tass.ru/ekonomika/9704661
[2849] Saudi CERT, FIRST (North Carolina) 23 December 2019. Access Date: 26 August 2020. https://www.first.org/members/teams/saudi_cert.
[2850] Saudi CERT, FIRST (North Carolina) 23 December 2019. Access Date: 26 August 2020. https://www.first.org/members/teams/saudi_cert.
[2851] Saudi CERT, FIRST (North Carolina) 23 December 2019. Access Date: 26 August 2020. https://www.first.org/members/teams/saudi_cert.
[2852]Ambassadors Of 15 Countries Discuss With Etidal Ways To Combat Extremism, Global Center for Combating Extremist Ideology (Riyadh) 20 January 2020. Access Date: 3 February 2020. https://etidal.org/en/ambassadors-of-15-countries-discuss-with-etidal-ways-to-combat-extremism/
[2853] Ambassadors Of 15 Countries Discuss With Etidal Ways To Combat Extremism, Global Center for Combating Extremist Ideology (Riyadh) 20 January 2020. Access Date: 3 February 2020. https://etidal.org/en/ambassadors-of-15-countries-discuss-with-etidal-ways-to-combat-extremism/.

sharing and developing information sharing and analysis capabilities.[2854] In addition, the partnership will provide extensive training to more than 500 cyber specialists.[2855]

On 5 February 2020, the Riyadh Declaration on Cybersecurity was adopted based on the discussions throughout the sessions of the Global Cybersecurity Forum.[2856] The Riyadh Declaration calls for joint efforts to build a better cyber world for all, focusing on: fostering a thriving industry, building a capable workforce, creating cyber-aware communities, enhancing global cybersecurity resilience, and advancing inclusive cybersecurity capacity building.[2857] It included a statement to "enable the role of women in cyber."

On 5 February 2020, two initiatives were adopted by Crown Prince Mohammed Bin Salman to serve global cybersecurity.[2858] The first initiative is meant to protect children in the cyber world by launching projects that lead efforts aiming to strengthen the protection mechanisms designed to advance the safety of children in relation to the digital sphere.[2859] The second initiative empowers women in cybersecurity by encouraging them to actively participate in this industry.[2860] It also promotes the professional development of women and increases human capital within cybersecurity.[2861]

On 15 September 2020, Cabinet approved the National Cybersecurity Strategy which aims to safeguard Saudi Arabia's infrastructure, priority sectors, and government services and activities.[2862] The project will integrate the country's cybersecurity governance as well as strengthen national technical capacity in defense against cyber threats and risks.[2863]

On 27 September 2020, the Board of Directors of the Saudi Authority for Data and Artificial Intelligence, "Sadaya", approved new national data governance policies concerning data

[2854] Saudi Arabia's National Cybersecurity Authority launches today the Global Cybersecurity Forum in Riyadh, the Middle East largest to date cybersecurity event, Global Cybersecurity Forum (Riyadh) 4 February 2020. Access Date: 26 August 2020. https://nca.gov.sa/en/pages/news/news27.html
[2855] Saudi Arabia's National Cybersecurity Authority launches today the Global Cybersecurity Forum in Riyadh, the Middle East largest to date cybersecurity event, Global Cybersecurity Forum (Riyadh) 4 February 2020. Access Date: 26 August 2020. https://nca.gov.sa/en/pages/news/news27.html
[2856] Riyadh Declaration for Cybersecurity, Global Cybersecurity Forum (Riyadh) 5 February 2020. Access Date: 26 August 2020. https://globalcybersecurityforum.com/declaration.
[2857] Riyadh Declaration for Cybersecurity, Global Cybersecurity Forum (Riyadh) 5 February 2020. Access Date: 26 August 2020. https://globalcybersecurityforum.com/declaration.
[2858] The Crown Prince Mohammed Bin Salman Initiative for Enable Women in Cyber, Global Cybersecurity Forum (Riyadh) 5 February 2020. Access Date: 26 August 2020. https://globalcybersecurityforum.com/initiative.
[2859] The Crown Prince Mohammed Bin Salman Initiative for Enable Women in Cyber, Global Cybersecurity Forum (Riyadh) 5 February 2020. Access Date: 26 August 2020. https://globalcybersecurityforum.com/initiative.
[2860] The Crown Prince Mohammed Bin Salman Initiative for Enable Women in Cyber, Global Cybersecurity Forum (Riyadh) 5 February 2020. Access Date: 26 August 2020. https://globalcybersecurityforum.com/initiative.
[2861] The Crown Prince Mohammed Bin Salman Initiative for Enable Women in Cyber, Global Cybersecurity Forum (Riyadh) 5 February 2020. Access Date: 26 August 2020. https://globalcybersecurityforum.com/initiative.
[2862] His Excellency Dr. Musaed Al-Aiban Expresses Gratitude and Appreciation to The Leadership Following The Cabinet's Approval of The National Cybersecurity Strategy A Resilient secure and trusted Saudi cyberspace that enables growth and prosperity, National Cybersecurity Authority (Riyadh) 15 September 2020. Access Date: 18 November 2020. https://nca.gov.sa/en/pages/news/news36.html
[2863] His Excellency Dr. Musaed Al-Aiban Expresses Gratitude and Appreciation to The Leadership Following The Cabinet's Approval of The National Cybersecurity Strategy A Resilient secure and trusted Saudi cyberspace that enables growth and prosperity, National Cybersecurity Authority (Riyadh) 15 September 2020. Access Date: 18 November 2020. https://nca.gov.sa/en/pages/news/news36.html

protection.[2864] The policies include: (1) a data protection policy which preserves the privacy of data owners; (2) a freedom of information policy which aims to enhance integration between government agenices; and (3) an open data policy which aims to make information accessible to entrepreneurs, researchers and academics among others.[2865]

Saudi Arabia has partially complied with its commitment to realize an open, free and secure internet. Through actions such as international collaboration with CERT teams and efforts to protect children in the cyberspace as well as make the industry more accessible to women, Saudi Arabia has taken action to realize an open internet and secure internet. It has not taken action to realize a free internet.

Thus, Saudi Arabia receives a score of 0.

Analyst: Khurram Shamim

South Africa: 0

South Africa has partially complied with its commitment to realise an open, free and secure internet.

On 25 June 2019, the Independent Communications Authority of South Africa issued the Spectrum Usage and Availability Q1 2019.[2866] This process will include measures to promote competition, transformation, inclusive growth and universal access of the communications sector.[2867]

On 26 July 2019, Communications and Digital Technologies Minister Stella Ndabeni-Abrahams issued the Government Gazette 42597 that provided policy direction for the licensing of high-demand spectrum.[2868] The gazette specifies the wholesale open access network licensing process, which enables the "allocation of 4G spectrum in order to provide faster and more widespread high-speed data services."[2869]

On 19 September 2019, Parliament enacted the Firms and Publications Amendment Act. The Act regulates the online distribution of films and games. In the Act 18H and 24G, the act prohibits the distribution of terrorism-related content, including propaganda for war, incitement of imminent violence and advocacy of hatred.[2870]

On 13 February 2020, President Cyril Ramaphosa announced during the State of the Nation Address about a joint effort with mobile operators to enact price deduction for data usage and the issuance of

[2864] General / Board of Directors of the Data and Artificial Intelligence Authority adopts (5) special policies for national data governance, Saudi Press Agency (Riyadh) 27 September 2020. Access Date: 18 November 2020. https://www.spa.gov.sa/2138798

[2865] General / Board of Directors of the Data and Artificial Intelligence Authority adopts (5) special policies for national data governance, Saudi Press Agency (Riyadh) 27 September 2020. Access Date: 18 November 2020. https://www.spa.gov.sa/2138798

[2866] Spectrum Licensing. Independent Communications Authority of South Africa (Pretoria) 25 June 2019. Access Date: 20 May 2020. https://www.icasa.org.za/pages/spectrum-licensing

[2867] Spectrum Licensing. Independent Communications Authority of South Africa (Pretoria) 25 June 2019. Access Date: 20 May 2020. https://www.icasa.org.za/pages/spectrum-licensing

[2868] Government Gazette Vol.649. Minister of Communications (Pretoria) 26 July 2019. Access Date: 20 May 2020. https://www.itweb.co.za/static/misc/pdf/Gazette-2019.pdf

[2869] Ndabeni-Abrahams issues policy direction on spectrum. IT Web (Johannesburg) 26 July 2019. Access Date: 20 May 2020. https://www.itweb.co.za/content/VgZey7JAgoVvdjX9

[2870] Films and Publications Amendment Act 11 of 2019 (English / Afrikaans). South African Government(Pretoria) 19 September 2019. Access Date: 16 March 2020 https://www.gov.za/documents/films-and-publications-amendment-act-11-2019-3-oct-2019-0000

Wireless Open Access Network.[2871] The proposal will facilitate the open access of internet and online resources.

On 10 March 2020, the Ministry of Communications and Digital Technologies and the Independent Communications Authority of South Africa announced the agreement reached between the competition commission and Vodacom. The undertaking will reduce data prices, thereby opening internet access to more South Africans.

On 17 May 2020, Minister of Communications and Digital Technologies, Jackson Mthembu, joined World Telecommunication and Information Society Day.[2872] The day fosters awareness on the use of the internet and other information and communication technologies, as well as of ways to bridge digital divide.[2873]

On 2 July 2020, the National Council of Provinces passed the Cybercrimes and Cybersecurity Bill.[2874] The objective of the bill is to regulate cybercrime and impose obligations on both electronic communications service providers and financial institutions for a safe cyber environment.[2875]

South Africa has partially complied with its commitment to realising an open, secure and free internet. Through various policy initiatives, it has increased access to the digital world for its citizens, but it has not taken action to realise a free and secure internet.

Thus, South Africa receives a score of 0.

Analyst: Scarlett Lin

Turkey: −1

Turkey has not complied with its commitment to realize an open, free and secure internet.

On 1 August 2019, the Turkish Radio and Television Supreme Council was granted the authority to regulate and monitor broadcasts shared on the internet, including movies and television series on streaming and social media platforms.[2876] This is part of a new regulation, the "Presentation of Radio, Television and Optional Broadcasts on the Internet."[2877] The aim is to provide measures "to ensure

[2871] South Africans may get free data every day, and surf sites like Wikipedia for free, if Ramaphosa gets his way. Business Insider South Africa (Cape Town) Feb 14, 2020. Access Date: 20 March 2020 https://www.gov.za/speeches/president-cyril-ramaphosa-2020-state-nation-address-13-feb-2020-0000

[2872] Government joins the world in observing World Telecommunication and Information Society Day. Ministry of Communications and Digital Technologies (Pretoria) 17 May, 2020. Access Date: 29 May 2020. https://www.doc.gov.za/newsroom/media-releases/government-joins-world-observing-world-telecommunication-and-information

[2873] Government joins the world in observing World Telecommunication and Information Society Day. Ministry of Communications and Digital Technologies (Pretoria) 17 May, 2020. Access Date: 29 May 2020. https://www.doc.gov.za/newsroom/media-releases/government-joins-world-observing-world-telecommunication-and-information

[2874] South Africa: NCOP Approves Cybercrimes Bill, Two Amendment Bills, AllAfrica (Tshwane) 2 July 2020. Access Date: 17 July 2020. https://allafrica.com/stories/202007020392.html

[2875] South Africa: NCOP Approves Cybercrimes Bill, Two Amendment Bills, AllAfrica (Tshwane) 2 July 2020. Access Date: 17 July 2020. https://allafrica.com/stories/202007020392.html

[2876] Internet radio-TV broadcasts are now under the control of RTÜK, Hürriyet Daily News (Ankara) 2 August 2019. Access Date: 4 February 2020. https://www.hurriyetdailynews.com/internet-radio-tv-broadcasts-are-now-under-the-control-of-rtuk-145464

[2877] Internet radio-TV broadcasts are now under the control of RTÜK, Hürriyet Daily News (Ankara) 2 August 2019. Access Date: 4 February 2020. https://www.hurriyetdailynews.com/internet-radio-tv-broadcasts-are-now-under-the-control-of-rtuk-145464

parental control of media content that could harm the physical, mental and moral development of children and young people."[2878] Moreover, the Turkish regulation will also apply to foreign service providers and operators and will require overseas companies intending to broadcast in Turkey to obtain a license.[2879]

On 20 November 2019, President of Defence Industries Ismail Demir highlighted the emergence of crime due to developments in cybersecurity at the International Cyber Warfare and Security Conference.[2880] He stated that cybersecurity is a field for cooperation to ensure the safety of communities and governments should therefore work together on the matter.[2881]

On 13 April 2020, President Recep Tayyip Erdogan announced the areas of development to prioritize during the COVID-19 pandemic, including the strengthening of communication infrastructure in cybersecurity.[2882]

On 30 April 2020, the Minister of Industry and Technology Mustafa Varank attended the Extraordinary G20 Digital Economy Ministerial Meeting and discussed methods of effective digital economy policies during the COVID-19 pandemic, including increasing internet connectivity and providing data safety.[2883]

On 23 July 2020, the Turkish Parliament passed a social media regulation bill which aims to define who is allowed to create, monitor or share online content while also having social media providers store data on its users in Turkey.[2884]

While Turkey has passed a regulation to monitor broadcasts on the internet, this action is not directed to internet security. Turkey has not taken action to fulfill its commitment to realise an open, free and secure internet.

Thus, Turkey receives a score of −1.

Analyst: Ingrid Wong

United Kingdom: 0

The United Kingdom has partially complied with its commitment to realizing an open, free and secure internet.

[2878] Internet radio-TV broadcasts are now under the control of RTÜK, Hürriyet Daily News (Ankara) 2 August 2019. Access Date: 4 February 2020. https://www.hurriyetdailynews.com/internet-radio-tv-broadcasts-are-now-under-the-control-of-rtuk-145464.

[2879] Internet radio-TV broadcasts are now under the control of RTÜK, Hürriyet Daily News (Ankara) 2 August 2019. Access Date: 4 February 2020. https://www.hurriyetdailynews.com/internet-radio-tv-broadcasts-are-now-under-the-control-of-rtuk-145464.

[2880] World needs international cooperation on cybersecurity, Anadolu Agency (Ankara) 20 November 2019. Access Date: 8 February 2020. https://www.aa.com.tr/en/science-technology/world-needs-international-cooperation-on-cybersecurity/1651291.

[2881] World needs international cooperation on cybersecurity, Anadolu Agency (Ankara) 20 November 2019. Access Date: 8 February 2020. https://www.aa.com.tr/en/science-technology/world-needs-international-cooperation-on-cybersecurity/1651291.

[2882] Turkey prioritizes biosafety, cybersecurity, food security amid COVID-19 pandemic, Daily Sabah (Istanbul) 14 April 2020. Access Date: 24 July 2020. https://www.dailysabah.com/politics/legislation/turkey-prioritizes-biosafety-cybersecurity-food-security-amid-covid-19-pandemic

[2883] G20 should design int'l accountability mechanism: Minister, Hürriyet Daily News (Ankara) 1 May 2020. Access Date: 24 July 2020. https://www.hurriyetdailynews.com/g20-should-design-intl-accountability-mechanism-minister-154369

[2884] Social media regulation bill passed in parliament committee, Hürriyet Daily News (Ankara) 24 July 2020. Access Date: 24 July 2020. https://www.hurriyetdailynews.com/parliament-commission-passes-social-media-bill-156819

On 3 October 2019, the United Kingdom and Singapore signed the Internet of Things security pledge that aims to allow the countries to work together on "improving the security of internet connected devices."[2885] The two countries intend to collaborate on ensuring that devices capable of connecting to the internet are secure from various cyber threats.[2886]

On 29 January 2020, the second Korea-United Kingdom Cyber Dialogue was held in Seoul.[2887] Both the UK and Korea shared experiences and expertise in the increasing challenge of cyber threats by sharing information and agreeing to work more closely on responses to cyber incidents and cybercrime investigations.[2888]

On 18 February 2020, the National Cyber Security Centre (NCSC) announced that it will be working with its Northern Ireland counterparts to help increase the region's "digital strength" for its businesses, citizens and charities.[2889] The two bodies intend to provide guidance for such groups to be able to easily and securely access the digital world while also collaborating to increase cybersecurity within Northern Ireland.[2890]

On 20 May 2020, the NCSC announced that it will be helping small businesses move their activities from the physical sphere to the digital sphere.[2891] The strategy hopes to allow small businesses to be able to securely and reliably conduct their work online.[2892]

On 24 June 2020, the UK in conjunction with the Welsh government announced greater funding for internet access in the form of broadband vouchers for an estimated 50,000 eligible rural homes and businesses in Wales.[2893]

On 13 July 2020, the NCSC released the "Home and Remote Working" Exercise as part of its Exercise-in-a-Box toolkit, which is an online service intended to help small and medium businesses strengthen their cyber-security.[2894] Focusing on remote work and video-conference security, the

[2885] Secure by Design — UK-Singapore IoT Statement, British High Commission Singapore (London) 3 October 2019. Access Date: 15 June 2020. https://www.gov.uk/government/news/secure-by-design-uk-singapore-iot-statement
[2886] Secure by Design — UK-Singapore IoT Statement, British High Commission Singapore (Singapore) 3 October 2019. Access Date: 15 June 2020. https://www.gov.uk/government/news/secure-by-design-uk-singapore-iot-statement
[2887] The 2nd ROK-UK Cyber Dialogue Held, Ministry of Foreign Affairs (Seoul) 29 January 2020. Access Date: 20 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320935
[2888] The 2nd ROK-UK Cyber Dialogue Held, Ministry of Foreign Affairs (Seoul) 29 January 2020. Access Date: 20 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320935
[2889]NCSC supports Northern Ireland's push to strengthen cyber security capabilities, National Cyber Security Centre (London) 18 February 2020. Access Date: 15 June 2020. https://www.ncsc.gov.uk/news/northern-ireland-cyber-security-centre
[2890] NCSC supports Northern Ireland's push to strengthen cyber security capabilities, National Cyber Security Centre (London) 18 February 2020. Access Date: 15 June 2020. https://www.ncsc.gov.uk/news/northern-ireland-cyber-security-centre
[2891] NCSC helps small businesses move from physical to digital, National Cyber Security Centre (London) 20 May 2020. Access Date: 15 June 2020. https://www.ncsc.gov.uk/news/ncsc-helps-small-businesses-move-from-physical-to-digital
[2892] NCSC helps small businesses move from physical to digital, National Cyber Security Centre (London) 20 May 2020. Access Date: 15 June 2020. https://www.ncsc.gov.uk/news/ncsc-helps-small-businesses-move-from-physical-to-digital
[2893] UK and Welsh governments team up on big broadband boost for rural Wales, Department for Digital, Culture, Media & Sport (London) 24 June 2020. Access Date: 21 September 2020. https://www.gov.uk/government/news/uk-and-welsh-governments-team-up-on-big-broadband-boost-for-rural-wales
[2894] Businesses helped to keep home workers secure with NCSC cyber exercise, National Cyber Security Centre (London) 13 July 2020. Access Date: 17 August 2020. https://www.ncsc.gov.uk/news/businesses-helped-keep-home-workers-secure-with-cyber-exercise

exercise aims to improve the safety of employees working from home and make businesses more resilient to hacking.[2895]

On 1 September 2020, the NCSC released an advisory to assist organizations in defending against cybercrime.[2896] The advisory was published in conjunction with American, Australian, Canadian and New Zealand cybersecurity agencies and contains technical guidance on how businesses, organizations and the wider public can protect themselves from malicious cyber actors.[2897]

On 12 September 2020, the United Kingdom increased funding for its Gigabit Broadband Voucher Scheme by GBP22 million.[2898] The additional funding provides subsidies for the creation of high-speed internet connections for an estimated 250,000 eligible businesses and homes in rural areas of the country.[2899]

On 17 September 2020, the NCSC issued an alert to the country's academia and education sector, following a rise in cyber-attacks against schools, colleges, and universities in August.[2900] The alert outlined ways academic institutions can prepare for such attacks and stay safe from threats, specifically ransomware.[2901]

The United Kingdom has partially complied with its commitment to realising an open, secure and free internet. Through various policy initiatives, the government has increased the accessibility of the internet for various populations while also improving upon security capabilities so to reduce a range of cyber threats. While it has taken action to realise an open and secure internet, it has not taken action to realise a free one.

Thus, the United Kingdom receives a score of 0.

Analysts: Arshia Hassani and Jonathan Ku

United States: 0

The United States has partially complied with its commitment to realize an open, free and secure internet.

[2895] Businesses helped to keep home workers secure with NCSC cyber exercise, National Cyber Security Centre (London) 13 July 2020. Access Date: 17 August 2020. https://www.ncsc.gov.uk/news/businesses-helped-keep-home-workers-secure-with-cyber-exercise

[2896] UK joins international allies in issuing cyber defence advice for organisations , National Cyber Security Centre (London) 1 September 2020. Access Date 21 September 2020. https://www.ncsc.gov.uk/news/uk-joins-international-allies-in-issuing-cyber-defence-advice-for-organisations

[2897] UK joins international allies in issuing cyber defence advice for organisations , National Cyber Security Centre (London) 1 September 2020. Access Date 21 September 2020. https://www.ncsc.gov.uk/news/uk-joins-international-allies-in-issuing-cyber-defence-advice-for-organisations

[2898] Big broadband boost for rural English shires and counties, Department for Digital, Culture, Media & Sport (London) 12 September 2020. Access Date: 21 September 2020. https://www.gov.uk/government/news/big-broadband-boost-for-rural-english-shires-and-counties

[2899] Big broadband boost for rural English shires and counties, Department for Digital, Culture, Media & Sport (London) 12 September 2020. Access Date: 21 September 2020. https://www.gov.uk/government/news/big-broadband-boost-for-rural-english-shires-and-counties

[2900] Cyber security alert issued following rising attacks on UK academia, National Cyber Security Centre (London) 17 September 2020. Access Date: 21 September 2020. https://www.ncsc.gov.uk/news/alert-issued-following-rising-attacks-on-uk-academia

[2901] Cyber security alert issued following rising attacks on UK academia, National Cyber Security Centre (London) 17 September 2020. Access Date: 21 September 2020. https://www.ncsc.gov.uk/news/alert-issued-following-rising-attacks-on-uk-academia

On September 2019, the Department for Homeland Security (DHS) released a Strategic Framework for Countering Terrorism and Targeted Violence.[2902] This framework includes a section on Counter Terrorists and Violent Extremists Influence Online, which aims to engage and work with partners in the private sector and civil society to prevent the spread of violent extremist content.[2903]

On 9 September 2019, U.S. Deputy Secretary of State John Sullivan met with Russian Deputy Foreign Minister Oleg Syromolotov to hold another round of consultations on the fight against terrorism.[2904] Sullivan and Syromolotov discussed topics of the state and prospects for bilateral cooperation on countering terrorist threats.[2905]

On 11 September 2019, the DHS Office for Targeted Violence and Terrorism Prevention (TVTP), along with the Carnegie Mellon University, the University of Pittsburgh and Tech Against Terrorism collaborated through the fourth Digital Forum on Terrorism Prevention in Pittsburgh.[2906] The goal of the meeting was to discuss innovations and objectives that will help in building the ability of local and non-government voices to challenge terrorism and violence.[2907]

On 8 October 2019, the United States co-hosted the Warsaw Process Working Group on Cybersecurity in Seoul with Korea and Poland.[2908] The meeting was attended by 50 countries and worked towards creating a secure and peaceful cyberspace by sharing each country's cybersecurity policy and best practices, thus enhancing cooperation in responding to cyber threats.[2909]

On 22 October 2019, the National Commission on Online Platforms and Homeland Security Act was introduced in the House of Representatives of the United States of America.[2910] This bill aims to create a commission that will monitor and examine the ways that online platforms are or could be

[2902] Strategic Framework for Countering Terrorism and Targeted Violence, Department of Homeland Security (DHS). United States September 2019. Access Date: 4 February 2019. https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.
[2903] Strategic Framework for Countering Terrorism and Targeted Violence, Department of Homeland Security (DHS). United States September 2019. Access Date: 4 February 2019. https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.
[2904] U.S., Russian Officials Discuss Fight Against Terror in Vienna, RadioFreeEurope RadioLiberty (Russia) 10 September 2019. Access Date: 19 March 2020. https://www.rferl.org/a/u-s-russian-officials-discuss-fight-against-terror-in-vienna/30156111.html
[2905] Press Release on Deputy Foreign Minister Oleg Syromolotov's meeting with United States Deputy Secretary of State John J. Sullivan and Russia-US High-Level Counterterrorism Dialogue, Ministry of Foreign Affairs Russia (Moscow) 9 September 2019. Access Date: 20 March 2020. https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/3780958
[2906] Pittsburgh Hosts the 4th Digital Forum on Terrorism Pervention, Department of Homeland Security (DHS), United States 11 September 2019. Access Date: 17 March 2020. https://www.dhs.gov/blog/2019/10/30/pittsburgh-hosts-4th-digital-forum-terrorism-prevention
[2907] Pittsburgh Hosts the 4th Digital Forum on Terrorism Pervention, Department of Homeland Security (DHS), United States 11 September 2019. Access Date: 17 March 2020. https://www.dhs.gov/blog/2019/10/30/pittsburgh-hosts-4th-digital-forum-terrorism-prevention
[2908] Warsaw Process Working Group on Cybersecurity Convened in Seoul, Ministry of Foreign Affairs (Seoul) 8 October 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320733
[2909] Warsaw Process Working Group on Cybersecurity Convened in Seoul, Ministry of Foreign Affairs (Seoul) 8 October 2019. Access Date: 10 March 2020. http://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320733
[2910] National Commission on Online Platforms and Homeland Security Act, House of Representatives, 116th Congress of the United States (Washington DC) 22 October 2019. Access Date: 17 March 2020. https://www.congress.gov/bill/116th-congress/house-bill/4782/text

used in acts of targeted violence and extremism while examining the impact on civil liberties as a result of increased restrictions to prevent online extremism.[2911]

On 15 January 2020, the United States House of Representatives Committee on Financial Services held a hearing for the examination of the Financing of Domestic Terrorism and Extremism.[2912] This examination focused on countering the use of financial services of financial institutions to fund terrorism which includes online transactions that can be used to fund domestic terrorism.[2913] The committee pushed for a greater recognition of these transactions and of their regulation to prevent further use.[2914]

On 10 February 2020, the White House released the budget for the fiscal year of 2020-2021 where the Department of Homeland Security was given USD800 million to Combat Violence and Extremism through community-based initiatives and to provide support services to de-escalate individuals who are becoming radicalized.[2915] This funding is targeted at ensuring that individuals can be pulled away from the sources that are causing their radicalization.[2916]

On 11 March 2020, Congress granted the Targeted Violence and Terrorism Prevention Grant Program USD10 million to provide funding for state, local, non-profits and higher education institutions to help establish or improve the capabilities of preventing targeted violence and extremism.[2917]

On 16 September 2020, DHS awarded USD10 million to 29 select programs nationwide to support the development of the TVTP framework.[2918] The money will be used to fund programs that will help build relevant resilience, intervention, prevention and reintegration programs at a local level.[2919]

[2911] National Commission on Online Platforms and Homeland Security Act, House of Representatives, 116th Congress of the United States (Washington DC) 22 October 2019. Access Date: 17 March 2020. https://www.congress.gov/bill/116th-congress/house-bill/4782/text

[2912] A Persistent and Evolving Threat: An Examination of the Financing of Domestic Terrorism and Extremism, US House Committee on Financial Services (Washington DC) 15 January 2020. Access Date: 4 February 2020. https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=406018

[2913] A Persistent and Evolving Threat: An Examination of the Financing of Domestic Terrorism and Extremism, US House Committee on Financial Services (Washington DC) 15 January 2020. Access Date: 4 February 2020. https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=406018

[2914] A Persistent and Evolving Threat: An Examination of the Financing of Domestic Terrorism and Extremism, US House Committee on Financial Services (Washington DC) 15 January 2020. Access Date: 4 February 2020. https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=406018

[2915] A Budget for America's Future: 2020-2021, The White House (Washington DC) 10 February 2020. Access Date: 19 March 2020. https://www.whitehouse.gov/wp-content/uploads/2020/02/budget_fy21.pdf

[2916] A Budget for America's Future: 2020-2021, The White House (Washington DC) 10 February 2020. Access Date: 19 March 2020. https://www.whitehouse.gov/wp-content/uploads/2020/02/budget_fy21.pdf

[2917] Targeted Violence and Terrorism Prevention Grant Program, Department of Homeland Security () 11 March 2020. Access Date: 19 March 2020. https://www.dhs.gov/tvtpgrants

[2918] DHS Provides $10 Million to Local Communities to Prevent Targeted Violence and Terrorism, Department of Homeland Security (Washington D.C) 16 September 2020. Access Date: 17 September 2020. https://www.dhs.gov/news/2020/09/16/dhs-provides-10-million-local-communities-prevent-targeted-violence-and-terrorism.

[2919] DHS Provides $10 Million to Local Communities to Prevent Targeted Violence and Terrorism, Department of Homeland Security (Washington D.C) 16 September 2020. Access Date: 17 September 2020. https://www.dhs.gov/news/2020/09/16/dhs-provides-10-million-local-communities-prevent-targeted-violence-and-terrorism.

The projects that were selected directly support the objectives within the DHS's 2019 Strategic Framework for Countering Terrorism and Targeted Violence.[2920]

The United States has partially complied its commitment to realising an open, free and secure internet. It has announced policies that focus on a free and secure internet such as in the Targeted Violence and Terrorism Prevention Grant Program grant program, the House of Representatives bill and the DHS Strategic Framework. However, it has not taken action to realize an open internet.

Thus, the United States receives a score of 0.

Analyst: Khurram Shamim

European Union: +1

The European Union has fully complied with its commitment to realize an open, free and secure internet.

On 1 October 2019, the European Union launched the European Cybersecurity Month to promote cybersecurity practices among individuals and businesses.[2921] The campaign hopes to educate such groups about appropriate practices in maintaining and increasing a secure cyber environment.[2922]

On 7 October 2019, the EU Internet Forum Ministerial Meeting took place where the members committed to an EU-wide crisis protocol that allows governments and internet platforms to respond rapidly and in a coordinated fashion in pursuit of disseminating online terrorist content.[2923] The meeting ultimately aimed to strengthen cooperation between law enforcement and online platforms within the EU Internet Forum framework.[2924]

On 9 December 2019, the European Commission tasked the European Union Agency for Cybersecurity with preparing a "cybersecurity certification candidate scheme for cloud services."[2925] The project aims to increase trust in a secure cloud infrastructure so that data mobility can become

[2920] DHS Provides $10 Million to Local Communities to Prevent Targeted Violence and Terrorism, Department of Homeland Security (Washington D.C) 16 September 2020. Access Date: 17 September 2020. https://www.dhs.gov/news/2020/09/16/dhs-provides-10-million-local-communities-prevent-targeted-violence-and-terrorism.

[2921] European Cybersecurity Month: EU promotes security culture among citizens, European Commission (Brussels) 30 September 2019. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/european-cybersecurity-month-eu-promotes-security-culture-among-citizens

[2922] European Cybersecurity Month: EU promotes security culture among citizens, European Commission (Brussels) 30 September 2019. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/european-cybersecurity-month-eu-promotes-security-culture-among-citizens

[2923] Fighting Terrorism Online: EU Internet Forum committed to an EU-wide Crisis Protocol, European Commission (Brussels) 7 October 2019. Access Date: 26 August 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6009.

[2924] Fighting Terrorism Online: EU Internet Forum committed to an EU-wide Crisis Protocol, European Commission (Brussels) 7 October 2019. Access Date: 26 August 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6009.

[2925] Towards a more secure and trusted cloud in Europe, European Commission (Brussels) 9 December 2019. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

viable in Europe.[2926] It will ultimately make businesses, public administrations and individuals more confident that their data will be secure.[2927]

On 20 May 2020, the EU announced that it will grant EUR49 million for projects that increase the ability to counter cyber threats and the privacy of organizations and individuals within the digital sphere.[2928]

On 20 May 2020, the European Union announced that it will grant EUR41 million to develop innovative projects on improving digital security.[2929] The funding is aimed at developing new ways to increase digital security while also improving privacy and data protection.[2930]

On 15 June 2020, the European Union announced that it will grant EUR30 million to protect public infrastructure from cyber threats.[2931] The policy aims to reduce the capabilities of certain groups from using the internet as a means to generate harm in the physical and digital world.[2932] The grant is expected to cover 100 per cent of the costs to achieve this goal and the projects will take place over a two-year period.[2933]

On 2 July 2020, the European Commission adopted guidelines to further assist member states to enact the 2018 Audiovisual Media Services Directive, which aims to promote the cultural diversity of European media and protect users from hate speech and other harmful content.[2934] The newly released guidelines are meant to streamline and harmonize the Directive's implementation, which includes a minimum 30 per cent share of European content in on-demand media catalogues, and requires online platforms to take action against inappropriate content targeted at children as well as content which incites hatred, violence and terrorism.[2935]

[2926] Towards a more secure and trusted cloud in Europe, European Commission (Brussels) 9 December 2019. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

[2927] Towards a more secure and trusted cloud in Europe, European Commission (Brussels) 9 December 2019. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/towards-more-secure-and-trusted-cloud-europe

[2928] EU grants nearly €49 million to boost innovation in cybersecurity and privacy systems, European Commission (Brussels) 20 May 2020. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/eu-grants-nearly-eu49-million-boost-innovation-cybersecurity-and-privacy-systems

[2929] EU to dedicate nearly EUR 41 million to innovative projects on digital security, European Commission (Brussels) 20 May 2020. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/eu-dedicate-nearly-eur-41-million-innovative-projects-digital-security

[2930] EU to dedicate nearly EUR 41 million to innovative projects on digital security, European Commission (Brussels) 20 May 2020. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/eu-dedicate-nearly-eur-41-million-innovative-projects-digital-security

[2931] EU grants €38 million for protection of critical infrastructure against cyber threats, European Commission (Brussels) 15 June 2020. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/eu-grants-eu38-million-protection-critical-infrastructure-against-cyber-threats

[2932] EU grants €38 million for protection of critical infrastructure against cyber threats, European Commission (Brussels) 15 June 2020. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/eu-grants-eu38-million-protection-critical-infrastructure-against-cyber-threats

[2933] EU grants €38 million for protection of critical infrastructure against cyber threats, European Commission (Brussels) 15 June 2020. Access Date: 15 June 2020. https://ec.europa.eu/digital-single-market/en/news/eu-grants-eu38-million-protection-critical-infrastructure-against-cyber-threats

[2934] Commission takes further steps to promote European audiovisual works and protect vulnerable viewers, European Commission (Brussels) 2 July 2020. Access Date: 15 June 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1209

[2935] Commission takes further steps to promote European audiovisual works and protect vulnerable viewers, European Commission (Brussels) 2 July 2020. Access Date: 15 June 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1209

On 30 July 2020, the Council of the European Union decided to impose sanctions, for the first time, against six individuals and three entities all involved in cyberattacks.[2936] The measures include banning travel, freezing assets and forbidding the provision of funds.[2937]

On 4 August 2020, the European Commission approved a EUR200 million voucher scheme for distribution to low-income families in Italy to help them in purchasing broadband access of at least 30 Megabits per second, as well as necessary devices and equipment.[2938] The announcement, which made reference to the increased need for digital access after the COVID pandemic, aims to enable eligible recipients to telework, access online education and seek other public services. The aid scheme is part of broader EU plans to improve social and territorial cohesion and increase economic growth through greater internet access, in order to heal the "digital divide."[2939]

The European Union has fully complied with its commitment to realizing a free, secure and open internet. Through various policy initiatives, the EU has embarked on projects to increase cybersecurity and reduce the possibility of threats from arising, thus realising a secure internet. It has also engaged in activities that make the internet more open to diverse populations. Finally, by releasing guidelines to advance the Audiovisual Media Services Directive, the EU has taken action to realize a free internet that promotes human rights.

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

Analysts: Arshia Hassani and Jonathan Ku

[2936] State aid: Commission approves €200 million voucher scheme to support access to broadband services by low-income families in Italy, European Commission (Brussels) 4 August 2020. Access Date: 26 August 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1445

[2937] EU imposes the first ever sanctions against cyber-attacks, Council of the EU (Brussels) 30 July 2020. Access Date: 17 August 2020. https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

[2938] State aid: Commission approves €200 million voucher scheme to support access to broadband services by low-income families in Italy, European Commission (Brussels) 4 August 2020. Access Date: 26 August 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1445

[2939] State aid: Commission approves €200 million voucher scheme to support access to broadband services by low-income families in Italy, European Commission (Brussels) 4 August 2020. Access Date: 26 August 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1445