January 15, 2020

Recommendations for AICHR

This document has been prepared following the Regional Forum on Freedom of Expression, Opinion and Information in ASEAN, organized by the ASEAN Intergovernmental Commission on Human Rights (AICHR) on 8 to 10 December 2019. It is divided into three parts which recommends AICHR and the Secretariat of Association of Southeast Asian Nations (ASEAN) to (1) look at the emerging threats on human rights, especially on freedom of expression and freedom on information, among ASEAN Member States (AMS) from the use and application of technology; (2) implement new mechanisms to safeguard freedom of expression, freedom of information, and the right to privacy in AMS; and (3) review the ASEAN policies, initiatives, frameworks and mechanisms in response to the threats over freedom of expression, freedom of information, and the right to privacy. These recommendations generally point to the need for AICHR to better understand the situation of freedom of expression and freedom of information and related-human rights issues with the increasing ubiquity of digital technology in order to make more appropriate and effective recommendations and responses toward the implementation of Article 23 of the ASEAN Human Rights Declaration (AHRD).

[1] Looking at New Threats Enabled by Technology

The narratives on the threats against freedom of expression and freedom of information have changed drastically in recent years because of the impact of digital technology. In this regard, there are six trends which bear further examination: (1.1) weaponizing personal data and the rising tendency towards surveillance states, (1.2) controlling freedom of expression and information with disinformation, (1.3) the role of international technology companies (Big Tech), (1.4) internet shutdowns, (1.5) cyberattacks, and (1.6) cyber-army and internet trolls. The Article 23 of the AHRD is a useful standard by which to evaluate these new threats on freedom of expression and freedom of information in the context of the changing communication and information landscape. It is important to look at the impact of technology on freedom of expression and opinion to better understand these threats and seek viable solutions, including preventative methods.

1.1 Weaponizing Personal Data and Possibility of Surveillance State

There has been a trend of states attempting to weaponize personal data and privacy of political dissidents in their exercise of the rights to freedom of expression. The last quarter of 2019 saw a period of crackdown of activists associated with the now-defunct Cambodia National Rescue Party (CNRP). Some activists were surprised that authorities

had a record of their private conversations using their phones[1]. The government of Cambodia later admitted to monitoring these conversations[2]. The Thailand government, meanwhile, citing a provision in the Computer Crime Act, asked café and restaurants owners to collect internet traffic data,[3] including personal information such as visited websites, information exchanged during the connection, and IP addresses. The sudden announcement raised concerns over the actual reason behind the order given that the provision has not been used since the law was adopted in 2007. The country's Cybersecurity Law of 2019 has also raised concerns over violations of personal data and privacy as it gives authorities the power to access computer data and networks, make copies of information, and seize any electronic device "in cases of emergency", which is not clearly defined in the law[4]. Vietnam's Cybersecurity Law also demands Big Tech, including Facebook and Google, to set up offices in the country and store the data locally which would make it easier for the state to access the companies' customers data[5].

With the European Union's (EU) introduction of its General Data Protection Regulations (GDPR), some AMS have paid greater attention to the importance of personal data and privacy protection, as the regulations required compliance from websites accessible from within the EU. In response, Thailand and Indonesia have initiated data protection laws in 2019, while Singapore has tightened the use of its Personal Data Protection Act which has been in place since 2012. Despite these positive developments, the laws are seemingly unable to protect the rights to privacy and personal data of citizens from being exploited. This is because these personal data protection laws in Singapore, Malaysia, and Thailand exclude compliance by state agencies, which can collect and misuse personal data or threaten privacy of citizens especially if it is done in the name of national security and public safety.

New technology has provided AMS the means to turn into a surveillance state. Given the advance of data technology and the onset of the Fourth Industrial Revolution, governments in the region are moving towards new technologies such as automation, robotics, artificial intelligence, and the Internet of Things (IoT). Similarly, fifth generation (5G) digital wireless networks will speed up the adoption of these technologies which require ever-faster transmission speeds because of increasing amounts of data being collected. The IoT—which refers to common tools and appliances using the internet—can be of particular concern since the technology will enable electronic devices to connect with each other and exchange data. The IoT has drawn the

---

[1] Nachemson, A. and Meta, K. (2019, October 19). Cambodia's Digital Surveillance Serves to Silence the Opposition and Suppress Criticism of the Government. Retrieved from https://www.scmp.com/magazines/post-magazine/long-reads/article/3033508/cambodias-digital-surveillance-serves-silence

[2] Vicheika, K. (2019, October 29). Government Admits to Monitoring Opposition Officials Ahead of Sam Rainsy's Return. Retrieved from https://www.voacambodia.com/a/government-admits-to-monitoring-opposition-officials-ahead-of-sam-rainsy-return/5144005.html

[3] Rojanaphruk, P. (2019, October 8) Minister Orders Cafes, Restuarants to Collect Customers' WIFI Data. Retrieved from http://www.khaosodenglish.com/politics/2019/10/08/digital-minister-orders-cafes-restaurants-to-collect-customers-wifi-data/

[4] Tanakasempipat, P. (2019, February 28). Thailand Passes Internet Security Law Decried as 'Cyber Martial Law'. Retrieved from https://www.reuters.com/article/us-thailand-cyber/thailand-passes-internet-security-law-decried-as-cyber-martial-law-idUSKCN1QH1OB

[5] Vu, K. (2019, January 9). Vietnam Says Facebook Violated Controversial Cybersecurity Law. Retrieved from https://www.reuters.com/article/us-vietnam-facebook/vietnam-says-facebook-violated-controversial-cybersecurity-law-idUSKCN1P30AJ

interest of governments in the region due its potential to spur investments and growth[6], but seemingly without concern for data privacy and security concerns associated with it[7], and instead focusing on the conveniences technology provides. The problem is—due to the in-built capacity to collect and use data—IoT technology can also be used for national security by enhancing the surveillance capabilities of repressive states. These IoT technologies, including automation, robotics, and artificial intelligence, are often in line with smart cities programs to which many AMS are moving toward.

Singapore recently announced that all immigration checkpoints will be fully automated with fingerprint, facial and iris scans by 2025[8]. The country, in 2018, also installed facial recognition technology into its network of CCTV cameras on lamp posts around the island[9]. The facial recognition technology in the country has also rapidly expanded into many industries[10], raising concerns over the possibility of it being misused. Since Singapore is considered as an authoritarian state where freedom of expression is tightly controlled, political dissidents can possibly be surveilled at every step of their daily routine.

Chinese surveillance technology has potential to play a crucial role in AMS. These have acquired a reputation from its use in crackdowns on ethnic minorities including the Uighurs and Tibetans, and in which Chinese tech companies like Tencent[11] and Huawei have been allegedly playing a role. This technology can be used to target political dissidents among AMS, especially those under repressive regimes. For example, Cambodia in 2019 is first in the region to test the 5G technology of Huawei, a leading 5G technology provider[12]. Other countries in the region are aiming for 5G adoption as well. Moreover, Chinese companies such as ZTE, Dahua and China Telecom are among those that are proposing new international standards at the International Telecommunication Union (ITU), particularly to create universally consistent technology for facial recognition, video monitoring, city and vehicle surveillance[13]. It is reported that these Chinese tech companies supply surveillance technology in 63 countries globally[14]. The concern is that standards ratified in the ITU influence how technology is developed and used, and are commonly adopted as policy by nations around the world including Africa,

---

[6] Lim, C. (2018, Jan 24). The Potential of the Internet of Things for ASEAN. Retrieved from https://theaseanpost.com/article/potential-internet-things-asean-1
[7] Marcus, A. (2015, Dec 2). Data and the Fourth Industrial Revolution. Retrieved from https://www.weforum.org/agenda/2015/12/data-and-the-fourth-industrial-revolution/
[8] Yee, Y.W. (2019, November 14). All Checkpoints to Have Facial, Iris Scans by 2025. Retrieved from https://www.straitstimes.com/tech/all-checkpoints-to-have-facial-iris-scans-by-2025
[9] Aravindan, A. and Geddie, J. (2018, April 13). Singapore to Test Facial Recognition on Lampposts, Stoking Privacy Fears. Retrieved from https://www.reuters.com/article/us-singapore-surveillance/singapore-to-test-facial-recognition-on-lampposts-stoking-privacy-fears-idUSKBN1HK0RV
[10] Yee, Y.W. (2019, November 11). Facial Recognition in Singapore Growing in Use beyond Security Purposes. Retrieved from https://www.straitstimes.com/tech/facial-recognition-growing-in-use-beyond-security-purposes
[11] Cockerell, I. (2019, September 5). Inside China's Massive Surveillance Operation. Retrieved from https://www.wired.com/story/inside-chinas-massive-surveillance-operation/
[12] Turton, S. and Onishi, T. (2019, September 5). Cambodia 5G Set to Leapfrog ASEAN Rivals with Huawei and ZTE. Retrieved from https://asia.nikkei.com/Spotlight/5G-networks/Cambodia-5G-set-to-leapfrog-ASEAN-rivals-with-Huawei-and-ZTE
[13] Gross, A. and Murgia, M. (2019, December 1). Chinese Tech Groups Shaping UN Facial Recognition Standards. Retrieved from https://www.ft.com/content/c3555a3c-0d3e-11ea-b2d6-9bf4d1957a67
[14] Feldstein, S. (2019, September 17). The Global Expansion of AI Surveillance. Retrieved from https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847

the Middle East, and Asia, including AMS. ITU standards usually take approximately two years to be drafted and adopted. Drafts are put forward by companies and governments and are later discussed at meetings with representatives from member states before the final approval. China's attempt to set up the standards have raised concerns among human rights advocates because human rights including on data privacy protection are non-existent in the drafts, and there are no experts on human rights, consumer protection, or data protection in ITU standards meetings. Thus, potentially harmful standards on technologies that can threaten privacy and freedom of expression can remain unchallenged.

1.2 Controlling Freedom of Expression and Information with "Disinformation"

Disinformation means "false information deliberately and often covertly spread in order to influence public opinion or obscure the truth." Disinformation has been in the spotlight in the recent years due to the impact of its use on major global events such as the 2016 U.S. Presidential Election and Brexit. Taking notice, some AMS, including Malaysia and Singapore, have issued laws to tackle disinformation. Vietnam is also planning to enact a similar one. However, these laws have raised concerns[15] [16] due to their repressive characteristics, particularly since state executive authorities solely decide which content maybe considered as "false".

Malaysia recently repealed the Anti-Fake News Act (AFNA)[17] which shows that a change might be possible under a changed political environment. However, the governments of Singapore and Vietnam are doing the opposite. Singapore adopted the Protection from Online Falsehoods Manipulation Act (POFMA), nicknamed "fake news law", in October 2019. In November the same year, Vietnam announced that it will have a new law targeting "fake news" and "toxic information" online following the Cybersecurity Law in the country came into effect January 2019[18].

As a new method of flagging content as misinformation or disinformation, this development signals a shift from the traditional narrative of government's removal or censoring content considered as criticism. Both AFNA and POFMA give state executives exclusive power to decide which content is seen as false, fake, or misleading, without judicial oversight. Since POFMA came into effect in October 2019, an opposition

---

[15] The Straits Times. (2018, April 11). Malaysia's Anti-fake News Legislation Becomes Law, Is Now Enforceable. Retrieved from https://www.straitstimes.com/asia/se-asia/malaysias-anti-fake-news-legislation-becomes-law-is-now-enforceable

[16] Jaipragas, B. (2019, December 21). Singapore's Fake News Law: Protecting the Truth, or Restricting Free Debate? https://www.scmp.com/week-asia/politics/article/3043034/singapores-fake-news-law-protecting-truth-or-restricting-free

[17] Aljazeera. (2019, October 10). Malaysia Parliament Scraps Law Criminalizing Fake News. Retrieved from https://www.aljazeera.com/news/2019/10/malaysia-parliament-scraps-law-criminalising-fake-news-191010024414267.html

[18] Thu, H. et al. (2019, November 8). Vietnam Plans Laws against Fake News. Retrieved from https://e.vnexpress.net/news/news/vietnam-plans-laws-against-fake-news-4009344.html

politician[19], opposition political parties[20], and an independent news outlet[21] have had their posts been flagged under the law as misinformation and disinformation. The content flagged all shared the same character of being critical of the government and the ruling People's Action Party (PAP). When it was criticized, the government of Singapore claimed it is mere "coincidence" that the law seemed to target opposition parties and government critics[22].

1.3 The Role of Big Tech Companies

Social media—mainly Facebook, Twitter, and Google (YouTube)—have been important platforms for political dissidents to criticize state authorities, conduct political debate, and organize peaceful assemblies. Because of this, there have been demands from state actors to ask big tech companies to comply with their domestic laws to control expression and access to information on the platforms.

Under the Vietnam's Cybersecurity Law, Facebook and Google are required to set up offices in in the country[23]. Apart from demanding these companies to hand over personal information of users to the government, the law also demands the companies to remove content that are considered as anti-government. At the beginning of 2019, Vietnamese authorities alleged that Facebook violated the Cybersecurity Law for failing to remove such content[24]. In December 2018, the Vietnamese government claimed that Google is "studying steps" to open a representative office in the country, while Google said it has nothing to announce[25]." Both Facebook and Google have urged Vietnam not to make them store data in-country[26].

---

[19] Channel News Asia. (2019, November 25). POFMA Office Directs Brad Bowyer to Correct Facebook Post in First Use of 'Fake News' Law. Retrieved from https://www.channelnewsasia.com/news/singapore/brad-bowyer-facebook-post-falsehood-pofma-fake-news-12122952

[20] Channel News Asia. (2019, December 15) SDP Complies with POFMA Order but Will Apply to Cancel Correction Directions. Retrieved from https://www.channelnewsasia.com/news/singapore/sdp-mom-pofma-online-falsehoods-law-facebook-12185584

[21] Channel News Asia. (2019, November 28) States Times Review Directed to Correct Facebook Post under Online Falsehoods Law. Retrieved from https://www.channelnewsasia.com/news/singapore/states-times-review-pofma-facebook-post-fake-news-shanmugam-12133420

[22] Reuters. (2020, Jan 6). Coincidence That Fake News Law Applied to Politicians Singapore Minister Says. Retrieved from https://www.nytimes.com/reuters/2020/01/06/technology/06reuters-singapore-fake-news.html?searchResultPosition=8

[23] McLaughlin, T. (2019, March 17.) Under Vietnam's New Cybersecurity Law, U.S. Tech Giants Face Stricter Censorship. Retrieved from https://www.washingtonpost.com/world/asia_pacific/under-vietnams-new-cybersecurity-law-us-tech-giants-face-stricter-censorship/2019/03/16/8259cfae-3c24-11e9-a06c-3ec8ed509d15_story.html

[24] Reuters. (2019, January 9). Vietnam Says Facebook Violated Controversial Cybersecurity Law. Retrieved from https://www.reuters.com/article/vietnam-facebook/vietnam-says-facebook-violated-controversial-cybersecurity-law-idUSL3N1Z91P0

[25] Nguyen, M. (2018, December 12.) Google Studies Step to Open Representative Office in Vietnam, Government Says. Retrieved from https://www.reuters.com/article/us-google-vietnam/google-studies-steps-to-open-representative-office-in-vietnam-government-says-idUSKBN1OB061

[26]Financial Times. (2018, December 12). Google and Facebook Push Back on Vietnam's Sweeping Cyber Law. Retrieved from https://www.ft.com/content/2c1e4640-fe78-11e8-aebf-99e208d3e521

Before the Cybersecurity Law came into force, Vietnam also made numerous requests for Google to remove videos that are considered as anti-state on YouTube. Among the AMS, Vietnam and Thailand have made the most number of demands to take down content on Google platforms. According to the Google Transparency Report, Vietnam has requested a total of 9,073 items for removal from 2009 until the first half of 2019. Out of this number, 9,066 total items were named for removal between January 1, 2017 and June 30, 2019[27]; with 8,919 items on YouTube, and 6,316 requested because they are considered as "government criticism". All 9,066 items are requests from the executive branch of the government not the judicial branch. The situation in Thailand is also similar. Google states in its Transparency Report that Thailand named 25,995 items named for removal during the same period. The Report shows that out of the total, 25,093 requests occurred between the second half of 2015 until the first half of 2019. Over this period, 24,779 items are on YouTube, and 24,768 items are because these are "government criticism". In that period, 22,469 items named for removal are requested by the executive branch[28], with the rest from the judiciary. The statistics from these two countries show their attempts for Google to comply with their laws. Google needs to respond based on international human rights principles, otherwise it may be seen as taking part in the governments' efforts to restrict freedom of expression and freedom of information.

Facebook has also been asked to comply with the Singapore's POFMA by posting a 'correction notion' on flagged posts on its platform. Unlike the requests for in-country data storage made by Vietnam, Facebook chose to comply with Singapore authorities by putting such a correction notion on a post made by a news outlet, the States Times Review[29]. The notice reads, "Facebook is legally required to tell you that the Singapore government says this post has false information" and is only visible to audiences in Singapore. In an email statement, Facebook admitted that such labels were posted "As required by Singapore law".[30] Facebook's action raises concerns about whether the company's stance was influenced by the fact that it has an office in Singapore. If the company issued the correction notice because it is instructed by the government not because the post fails to meet with its own internal "Community Standards", Facebook may be seen as becoming part of the government's attempt to crackdown on free speech and freedom of information.

Facebook, Twitter, and Google also have an important role during elections in the AMS due to disinformation being distributed on their platforms. Facebook announced that it

---

[27] Google's Transparency Report. Government Requests to Remove Content. Retrieved from https://transparencyreport.google.com/government-removals/by-country/VN

[28] Google's Transparency Report. Government Requests to Remove Content. Retrieved from https://transparencyreport.google.com/government-removals/by-country/TH

[29] Channel News Asia. (2019, November 29). Facebook Instructed by POFMA Office to Publish Correction Notice on States Times Review's Post. Retrieved from https://www.channelnewsasia.com/news/singapore/states-times-review-fake-news-pofma-facebook-correction-12136996

[30] Heijmans, P. (2019, November 29) Facebook Adds Disclaimer to Post That Singapore Deems False. Retrieved from https://www.bloomberg.com/news/articles/2019-11-29/singapore-orders-facebook-to-correct-blog-s-false-statements

will not fact check any political ads in the upcoming 2020 U.S. presidential election[31], while Twitter[32] and Google[33] said it will ban and restrict political ads, respectively. Banning all ads can prevent alternative political voices from exercising their right to freedom of expression, since digital campaigns can reach more audiences with less resources compared with traditional political and media campaigning. On the other hand, not fact-checking political ads can allow disinformation on the platform which can mislead audiences.

These Big tech policy pronouncements are worth observing as these can set examples for political events in AMS, such as the elections in Myanmar and Singapore in 2020. Regarding Singapore, POFMA is likely to be used in suppressing content critical of the government and the ruling party during the campaign period. Google has announced already that it would ban all ads ahead of the Singapore election, causing an outcry from the opposition political parties[34] that had planned to campaign on the Google platform YouTube. In Myanmar's ethnic conflict-ridden political environment, disinformation has been used in 2018 to influence or manipulate people concerning the Rohingya. Facebook admitted to failing to tackle hate speech against the Rohingya, which led to incitement of violence[35]. This confirms how social media companies can play a great role in such events since disinformation and misinformation may influence people's thoughts and actions.

1.4 Internet Shutdown and Disruptions

Access Now, an international digital rights organization, defines an Internet shutdown as a situation where the internet-based communications are "intentionally turned off, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information"[36]. As an important means of communication, ASEAN cannot deny that as Internet shutdown is a new threat for freedom of expression and information. Internet shutdowns, which have been rising globally, usually occur during political-related events such as protests, elections, and political unrest. It is also easier to turn off the Internet in an area where the government does not have to worry much about its impacts on the economy. In 2019, two major internet shutdowns happened in Myanmar and Indonesia, in the conflict-affected areas of Rakhine state and Papua province, respectively.

Rakhine State is known as a battleground of the ethnic conflict. The shutdown occurred as a result of the fighting between Burmese military forces (Tatmadaw) and the ethnic

---

[31] Gilbert, B. (2019, December 14). Facebook Refuses to Fact-Check Political Ads, And It's Infuriating Employees and Lawmakers. Here's Why the Issue Continues to Dog the Company. Retrieved from https://www.businessinsider.com/facebook-political-ads-fact-check-policy-explained-2019-11
[32] BBC. (2019, October 31). Twitter to Ban All Political Advertising. Retrieved from https://www.bbc.com/news/world-us-canada-50243306
[33] Lee, D. (2019, November 21). Google to Restrict Political Adverts Worldwide. Retrieved from https://www.bbc.com/news/technology-50498166
[34] Reuters. (2019, December 4). Google Halts Political Ads in Singapore as Election Looms: Documents. Retrieved from https://www.reuters.com/article/us-google-singapore-election/google-halts-political-ads-in-singapore-as-election-looms-documents-idUSKBN1Y80JM
[35] Stevenson, A. (2018, November 6). Facebook Admits It Was Used to Incite Violence in Myanmar. Retrieved from https://www.nytimes.com/2018/11/06/technology/myanmar-facebook.html
[36] Access Now. What Is an Internet Shutdown? Retrieved from https://www.accessnow.org/keepiton/

Arakan Army (AA). Government ordered four telecom operators to suspend internet services on June 20, 2019 in eight townships in Rakhine and one township in neighboring Chin State. The government order was reported as due to "disturbances of peace and use of internet activities to coordinate illegal activities.[37]" As of December 2019, four townships in Rakhine which are Ponnagyun, Mrauk-U, Kyauktaw, and Minbya are still without Internet access[38].

Two months after the situation in Myanmar, Papua experienced a similar situation following the protests in relation to the mistreatment by police and racial slurring on Papuan students in Surabaya[39]. While the political conflict between Papua and Indonesia has existed for decades, the protests triggered the shutdown to curb "distributing and transmitting electronic information that is still in doubt or that is indicated by hoax or incitement that can cause hatred and animosity[40]."

Apart from these two total internet blackouts, in May 2019, Indonesia restricted the use for three days of Twitter, WhatsApp, Telegram, Facebook, and Instagram following a violent post-election riot in Jakarta [41]. The Minister of Communications and Information Technology claimed that the authorities had to "manage the use of social media and instant messaging due to a lot of 'fake news' given videos and pictures being circulated on the platforms." During the restriction, people could still communicate with text over Twitter and WhatsApp but they could not send pictures and videos over the apps to each other[42]. People also had difficulties posting on Facebook and Instagram[43]. Telegram was completely blocked during the incident, and, in fact, the messaging application was blocked previously in 2017 due to its widespread use among Islamic State sympathizers[44].

Internet shutdown and disruptions are not necessary despite the governments' claims, since it is not an effective method to respond to political situations. Internet shutdown and disruptions threatens freedom of expression and freedom of information in three ways as follows:

---

[37] Telenor Group. (2019, June 21). Network shutdown in Myanmar, 21 June 2019. Retrieved from https://www.telenor.com/network-shutdown-in-myanmar-21-june-2019/

[38] Liu, J. (2019, December 21). Internet Shutdown Has Been Imposed on Rakhine for Six Months. Retrieved from https://www.mmtimes.com/news/internet-shutdown-has-been-imposed-rakhine-six-months.html

[39] Firdaus, F. (2019, August 21). Indonesia Deploys Troops to West Papua as Protests Spread. https://www.aljazeera.com/news/2019/08/indonesia-deploys-troops-west-papua-region-protests-spread-190820230710563.html

[40] Ganguly, S. (2019, August 26.) Internet Suspended in Indonesia's Papua Region for 'Security And Order' Amid Protests. Retrieved from https://www.medianama.com/2019/08/223-internet-shutdown-papua-indonesia/

[41] Jalan, T. (2019, May 27). Indonesia Lifts Social Media Restriction After 3 Days. Retrieved from https://www.medianama.com/2019/05/223-indonesia-restricts-social-media/

[42] Deutsche Welle. (2019, May 24). Internet Blocking Social Media to 'Maintain Democracy'. Retrieved from https://www.dw.com/en/indonesia-blocking-social-media-to-maintain-democracy/a-48858283

[43] Singh, M. and Russell, J. (2019, May 22). Indonesia Restricts WhatsApp, Facebook and Instagram Usage Following Deadly Riots. Retrieved from https://techcrunch.com/2019/05/22/indonesia-restricts-whatsapp-and-instagram/

[44] Reuters. (2017, July 14). Indonesia Blocks Telegram Messaging Service over Security Concerns. Retrieved from https://www.reuters.com/article/us-indonesia-security-apps-idUSKBN19Z1Q2

- **The shutdown can cut down communications.** The internet is a crucial medium for political gatherings during situations of political turmoil. People rely on the internet to communicate with each other, whether it is to organize or stage a protest or to keep informed and updated on each other's whereabouts. The shutdown is a way to cut off these online communication channels and prevent protestors from communicating with each other.

- **The shutdown allows authorities to monopolize information.** In repressive regimes, the government usually controls the media and the information flow. State-controlled media channels can be full of propaganda that distort the truth. People often turn to social media to express their voices or upload their photos or videos that reveal the actual situation. When more and more people share more information on such situations, it can counter state propaganda. Internet shutdowns prevent people from countering state-controlled accounts, and one-sided misleading information and disinformation can spread. During the Rakhine internet shutdown, journalists in Myanmar confirmed having difficulties to verify information released by the government. Fact-checkers in Indonesia also reportedly said that their work has become more challenging since the shutdown in Papua. Due to the shutdown, they could not contact sources in Papua to verify the information which needed to be verified[45].

- **The shutdown can cover up human rights violations**. In case the situation worsens, and result in clashes or violent crackdown, an internet shutdown can stop people from sharing information on these incidents. Video footage taken during a clash can be used as a strong evidence to document the ensuing violence, establish a timeline of events, or identify the key perpetrators and victims. It can help counter disinformation, if there are enough videos or photos that corroborate the account of what truly happened during the same event. In Papua, when at least six protestors and one soldier were reportedly killed during a protest in Deiyai regency on August 28, 2019[46], journalists had difficulties to "coordinate, to find news, to send articles, and verify any news from the ground[47]."

1.5 Cyberattacks against Civil Society

Another threat against freedom of expression and information using technology is cyberattacks. In AMS, there have been numerous reports about this growing threat that use technological methods to put freedom of expression and information at risk.

---

[45] Tardáguila, C. (2019, August 30). Indonesia Faces Two Waves of Misinformation And an Internet Shutdown at the Same Time. Retrieved from https://www.poynter.org/fact-checking/2019/indonesia-faces-two-waves-of-misinformation-and-an-internet-shutdown-at-the-same-time/

[46] Firdaus, F. (2019, August 28). West Papuan Protesters Killed by Indonesian Police: Witnesses. Retrieved from https://www.aljazeera.com/news/2019/08/west-papuan-protesters-killed-indonesian-police-witnesses-190828103919896.html

[47] Firdaus, F. (2019, August 22). Indonesia Blocks Internet in West Papua as Protest Rages. Retrieved from https://www.aljazeera.com/news/2019/08/indonesia-blocks-internet-west-papua-protest-rages-190822022809234.html

In late 2018, distributed denial-of-service (DDoS) attacks targeted several alternative media sites in the Philippines. A DDoS attack is a malicious attempt to disable access to a website or service by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. Alternative media websites targeted during the 2018 DDoS attacks include Altermidya, Bulatlat, Kodao Productions, and Pinoy Weekly[48]. The website owners accuse the administration of Rodrigo Duterte as perpetrators of the attacks[49], leading to a worsening situation regarding press freedom and freedom of information in the Philippines.

Apart from the DDoS attacks in the Philippines, a spyware called FinSpy or FinFisher has also been reported as a tool used by AMS to protect "national security". A Singapore company with a close ties to the government in allegedly bought the tool in 2019[50]. It was also discovered in Myanmar in the same year[51]. Its use was first discovered in the region in 2013 as a government tool to spy on Vietnam dissidents[52]; and then was reported used in 2016 with links to the Indonesian government, which makes the country one of the largest customers of FinSpy[53]. FinSpy, sold by companies based in the UK and Germany, is able to steal everything from text messages to emails, photos, and geolocation. It also targets secure and encrypted messengers including Line, Signal, WhatsApp, and Telegram. The use of spyware in AMS is a concern because it is increasingly used by authoritarian governments globally to suppress dissidents and political opponents. The company that owns FinSpy, Gamma Group, came to prominence after it was discovered to be providing spyware to authoritarian governments in the Middle East during the Arab Spring in 2011.

Another malicious software that is of a global concern is a mobile phone spyware called Pegasus which is developed and sold by the Israel-based company, NSO Group or Q Cyber Technologies to government clients around the world. Pegasus is considered as one of most sophisticated spyware[54], reportedly used to target civil society in over 100 cases around the world[55]. To activate, a target has to click on an exploit link containing the spyware, after which Pegasus will be installed on the target's phone without their knowledge or permission. When infected, Pegasus can access the target's phone

---

[48] Geronimo, Y. J. and Barreiro Jr., V. (2019, March 29). Alternative Media Groups File Civil Case Amid Cyberattacks. Retrieved from https://www.rappler.com/technology/news/226968-alternative-media-groups-file-civil-case-cyberattacks-march-2019

[49] Rappler. (2019, February 8). Altermidya 'Strongly Condemns' DDoS Attacks Against Member Sites. Retrieved from https://www.rappler.com/technology/news/223007-altermidya-statement-ddos-attacks-against-member-sites

[50] F.K. (2019, July 12). Upgraded German Surveillance Malware FinSpy Purchased by Singapore Company Closely Linked with Govt. Retrieved from https://www.theonlinecitizen.com/2019/07/12/upgraded-german-surveillance-malware-finspy-purchased-by-singapore-company-closely-linked-with-govt/

[51] Cimpanu, C. (2019, July 10). New Versions of FinFisher Mobile Spyware Discovered in Myanmar. Retrieved from https://www.zdnet.com/article/new-versions-of-finfisher-mobile-spyware-discovered-in-myanmar/

[52] Marquis-Boire, M. et al. (2013, March 13). You Only Click Twice: FinFisher's Global Proliferation. Retrieved from https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

[53] Barbaschow, A. (2016, January 27). FinFisher Spyware Linked to Indonesian Government Found in Sydney: Report. Retrieved from https://www.zdnet.com/article/finfisher-spyware-linked-to-indonesian-government-found-in-sydney-report/

[54] It has been found in a high-profile case of Jamal Khashoggi, a former Saudi Arabian columnist for the Washington Post who was murdered at the Saudi consulate in Istanbul.

[55] The Citizen Lab. (2019, October 29). NSO Group/ Q Cyber Technologies: Over One Hundred New Abuse Cases. Retrieved from https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

functions like camera and microphone as well as collect private data including passwords, contact lists, calendar events, text messages, and live voice calls from mobile messaging apps. Users of WhatsApp, the most used messaging application in the world, became infected with with Pegasus in October 2019 due to a security flaw that enabled Pegasus to be installed on target phones simply by calling them on the app[56]. In 2018, mobile phones in 45 countries[57], including Thailand and Singapore, were found to be likely infected with Pegasus.

With the ubiquity of smartphones, cyberattack is an increasing threat to freedom of expression and freedom of information. Civil society will increasingly find itself a target such sophisticated cyberattacks, with the impact becoming worse if they are not aware of the threat and how to mitigate it. In ASEAN member states, the shortage of capability, and expertise on cybersecurity needs to be addressed in order for the situation to improve.[58] However recent initiatives to enact laws on cybersecurity, such as in Thailand and Vietnam, have only reinforced repression because laws aimed to crack down and surveil government critics rather than strengthen cybersecurity of citizens.

1.6 Cyber-army and Internet Trolls

The spread of social media use has given rise to a new threat to freedom of expression in AMS in the form of cyber-armies and internet trolls. These are a group of social media users/accounts, whether organized or supported by the state or acting independently, who attack people or entities exercising their rights to freedom of expression. Often hiding fictitious names and accounts, trolls use hate speech and disinformation to incite chaos or even violence.

Troll operations can either be state-sponsored or a group of people who share a common belief or liking. Such operations may be (1) a business or a troll farm hired for a specific purpose; (2) a group of people with shared belief or political view, with or without an influencer that persuades them to 'troll'; and (3) a state-run organized group, usually known as 'cyber-army'. Trolling is an effective method to trigger reactions from millions of people by using information designed to provoke intense feelings. A piece of information, usually on politics and /or religion, might be used by an influencer to trigger or manipulate the group with misleading, false, or fake information often being added. They can create a popular hashtag on social media platforms like Twitter to mobilize or persuade larger crowds in a troll-operated campaign.

Maria Ressa, the editor-in-chief of Rappler, an online news media outlet in Philippines, has been the target of repeated internet troll operations for her outlet's work which is critical to the campaigns of the President of the Philippines, Rodrigo Duterte. Since coming to power of Duterte in 2016, internet trolls have played an important role in

---

[56] Srivastava, M. (2019, May 14). WhatsApp Voice Calls Used to Inject Israeli Spyware on Phones. Retrieved from https://www.ft.com/content/4da1117e-756c-11e9-be7d-6d846537acab?segmentid=acee4131-99c2-09d3-a635-873e61754ec6

[57] At least six countries with significant Pegasus operations have previously been linked to abusive use of spyware to target civil society, including Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates.

[58] Dobberstein, N. et al. Cybersecurity in ASEAN: AN Urgent Call to Action. Retrieved from https://www.southeast-asia.atkearney.com/web/southeast-asia/article?/a/cybersecurity-in-asean-an-urgent-call-to-action

harassing Duterte critics and creating disinformation. Online intimidation is common, and is worse when the target is a woman. Female targets receive rape threats or even doctored pornographic photos. For her work as a journalist, Ressa is often called a different animals and also receives rape and death threats. Trolls have attacked her with hashtag campaigns such as #ArrestMariaRessa and #BringHerToTheSenate[59]. Meanwhile, opposition Senator Leila de Lima,was also the target of attacks by online trolls on YouTube and websites, spreading false information such as a purchase of a $6 million mansion in New York using government funds, and making false headlines about her on YouTube with different video content[60].

There have been reports of troll farms in the Philippines where people can be hired to help create disinformation and harass people[61]. Another trolling tactic is through persuasion of celebrities who identify themselves as Duterte Diehard Supporters (DDS). These bloggers, including Sass Sasot, Mocha Uson, and RJ Nieto (or "Thinking Pinoy"), usually have thousands or millions of followers on their online accounts, which are used to encourage followers to harass Duterte critics with mocking, insulting, and threatening comments. Those who campaign against these online celebrities are themselves also harassed online[62]. In 2019, Facebook removed 200 pages, groups and accounts, including 25 Instagram accounts[63], linked to a network allegedly organized by Duterte's former social media handler. It is reported that one page had around 3.6 million followers, while over 1.8 million accounts joined one group.

The Philippines is not the only country with such internet trolls in the region. In Myanmar, trolls, including operations by members of the military, have been particularly targeting Muslims to spread disinformation about the Rohingya people and attack critics[64]. Lawyers and activists including Ko Ni, Wai Wai Nu, Robert San Aung, and Harry Myo Lin have been attacked by internet trolls[65]. Ko Ni, a Muslim lawyer who was known for his advocacy for constitutional reform, was reported to have received death threats regularly, as well as being the target of internet campaigns on his work and his Muslim background before he was assassinated in 2017. Wai Wai Nu, a Rohingya activist and a lawyer, said that online harassment for her happens regularly. Harassment has included sending her pornographic images and doctored photos that

---

[59] Prosetti, J. (2017). Fighting Back Against Prolific Online Harassment: Maria Ressa. https://unesdoc.unesco.org/ark:/48223/pf0000259399

[60] Alba, D. (2018, September 4). How Duterte Used Facebook to Fuel the Philippine Drug War. Retrieved from https://www.buzzfeednews.com/article/daveyalba/facebook-philippines-dutertes-drug-war

[61] Mahtani, S. and Cabato, R. (2019, July 26). Why Crafty Internet Trolls in the Philippines May Be Coming to a Website Near You. Retrieved from https://www.washingtonpost.com/world/asia_pacific/why-crafty-internet-trolls-in-the-philippines-may-be-coming-to-a-website-near-you/2019/07/25/c5d42ee2-5c53-11e9-98d4-844088d135f2_story.html

[62] Cepeda, M. (2018, April 07). Youth Leaders Harassed Online After Seeking Mocha Uson's Dismissal. Retrieved from https://www.rappler.com/nation/199754-akbayan-youth-harassment-online-mocha-uson-complaint

[63] Dancel, R. (2019, March 29). Facebook Shutters Pages, Groups and Accounts Linked to Duterte's Ex-Social Media Handler. Retrieved from https://www.straitstimes.com/asia/se-asia/facebook-shutters-pages-groups-and-accounts-linked-to-dutertes-ex-social-media-handler

[64] Mozur, P. (2018, October 15). A Genocide Incite on Facebook, With Posts from Myanmar's Military. Retrieved from https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

[65] Rajagopalan, M. (2017, March 18). Internet Trolls Are Using Facebook to Target Myanmar's Muslims. Retrieved from https://www.buzzfeednews.com/article/meghara/how-fake-news-and-online-hate-are-making-life-hell-for

made her appear as carrying banners with separatist slogans. The trolls are also reported to harass some members of parliament she hoped to work with, causing cooperation plans to be scuttled. Robert San Aung, a Muslim human rights lawyer, said that he also receives threats both online and via text messages. Harry Myo Lin, a Muslim activist who runs a nonprofit advocating for religious tolerance, had to deactivate his Facebook account after harassing comments from trolls using one of the photos of him and a Buddhist woman on Facebook. The photo went viral and was shared thousands of times. The caption stated that he, as a Muslim, was trying to convert the Buddhist woman, an issue that is considered to be sensitive in Myanmar. Threatening SMS messages from different numbers were also sent to him.

In Indonesia, where Muslims comprise a majority of the population, trolls' actions are also often related to religion. Trolls in the country are referred to as "buzzers"[66]. They also create political propaganda to influence elections, and were found to be active as early as 2014. The case of a former Jakarta Governor, Basuki Tjahaja Purnama, or "Ahok", is an important example where trolls played an influential role in Ahok's conviction on blasphemy against Islam due to a campaign speech[67]. The footages of the speech by Ahok, who is of Christian Chinese descent, were edited to provoke controversy before it went viral and caused anger among Muslims[68]. There is also a group called Muslim Cyber Army (MCA) that viciously targets people who criticize Islam, and who are reportedly intimidated and forced to record video apologies. The group is said to circulate among its members a list of people to target for attack, including their personal information such as names, addresses, and identities of family members [69].

A cyber-army in Vietnam has also been reported; and is state-sponsored. In 2017, government announced a cyber-warfare unit called Force 47 with a purpose to counter content that is offensive to the state. The unit is reportedly comprised of 10,000 military officers[70]. There is not much documented information on the activities of Force 47 after it was announced, but it is widely believed that the unit is associated with incidents of increasing requests for Google to remove YouTube videos critical of the state mentioned earlier in the previous section, as well as arrests of Vietnamese activists who are critical of the government.

[2] Implementation of New Mechanisms

---

[66] Perper, R. (2018, August 28). Social Media 'Buzzers' Are Being Paid by Indonesian Political Parties to Spread Propaganda Ahead of Local Elections. Retrieved from https://www.businessinsider.com/indonesia-election-buzzers-election-propaganda-2018-8

[67] Lamb, K. (2017, May 9). Jakarta Governor Ahok Sentenced to Two Years in Prison for Blasphemy. Retrieved from https://www.theguardian.com/world/2017/may/09/jakarta-governor-ahok-found-guilty-of-blasphemy-jailed-for-two-years

[68] Holmes, O. (2016, November 25). Jakarta's Violent Identity Crisis: Behind the Vilification of Chinese-Indonesians. Retrieved from https://www.theguardian.com/cities/2016/nov/25/jakarta-chinese-indonesians-governor-ahok

[69] Lamb, K. (2018, March 13). Muslim Cyber Army: A 'Fake News' Operation Designed to Derail Indonesia's Leader. Retrieved from https://www.theguardian.com/world/2018/mar/13/muslim-cyber-army-a-fake-news-operation-designed-to-bring-down-indonesias-leader

[70] Reuters. (2017, December 26). Vietnam Unveils 10,000-Strong Cyber Unit to Combat 'Wrong Views'. Retrieved from https://www.reuters.com/article/us-vietnam-security-cyber/vietnam-unveils-10000-strong-cyber-unit-to-combat-wrong-views-idUSKBN1EK0XN

New mechanisms need to be drawn up in order effectively respond to threats to freedom of expression and access to information with the rise of information technology. Even though the Article 23 of the ASEAN Declaration for Human Rights is in place and endorsed by the ASEAN member states, the article needs to be interpreted to suit the changed digital communication landscape. Even with more traditional applications of the rights under article 23, the political environment in the majority of countries in ASEAN—repressive political regimes—already posed a difficult challenge in repealing or amending repressive laws. This is due to the fact that policy makers themselves also benefit from these laws to preserve their power.

As illustrated in previous sections, current threats against freedom of expression and freedom of information go beyond law and policy. Technology enables new threats that need to be better understood and monitored to develop the best possible solutions, including addressing threats that are coming from outside the region. It is recommended that a long overdue proposal to implement a regional human rights court, comprised of experts who are independent of the government, has to move forward. Such a court with functions similar to the European Court of Human Rights can rule on cases against freedom of expression and freedom of information to set examples among AMS, and create pressure on authoritarian regimes.

Because of new threats that use technology, it is necessary to involve more stakeholders, particularly from the private sector which has played a greater role in this landscape. The protection of freedom of expression and freedom of information has moved beyond being a matter between state actors and citizens. Also, as the technology involved uses a global infrastructure, it also means that threats against freedom of expression and information can come from outside of the region, as well as being exported from AMS to countries outside the region. A monitoring mechanism in this case is therefore critical to watch and report on these new threats, and it should include stakeholders, especially civil society who are among the most vulnerable groups.

[3] Review of ASEAN Policies, Framework, Initiatives, and Mechanisms

The existing ASEAN policies, framework, initiatives, and mechanisms—including those on trade and development—lack elements of human rights protection from emerging threats that come with technology. It is therefore important to review these existing ASEAN policies, framework, initiatives, and mechanisms for loopholes that may threaten human rights, including for preventative methods.

First and foremost, the ASEAN Human Rights Declaration (AHRD) needs to be reviewed. AHRD, as the overarching human rights document of the region, has been criticized specifically because of Articles 6, 7, and 8, which limit how the human rights can be effectively implemented. In the light of the concerns raised previously in this document, subjecting human rights to local concerns will severely affect human rights promotion and protection, particularly the common practice of invoking the 'necessities' of national security and public morals. It is a common concern because the political environment in the majority of AMS is repressive.

Although revising the AHRD can be extremely challenging given the repressive nature of most AMS, this issue must be addressed for the protection of freedom of expression and

information in the region. Similarly, there is a need to for effective mechanisms in order to implement the AHRD for protection and promotion of human rights. The lack of such mechanisms has prevented the enforcement for AMS to respect human rights. The new mechanisms mentioned in the previous section as well as review of the existing mechanisms is therefore necessary.

In the recent years, ASEAN has also made other instruments related to digital technology. These are, for example, the ASEAN ICT Masterplan 2020[71], ASEAN Digital Integration Framework[72], ASEAN Framework on Personal Data Protection[73], and ASEAN Framework on Digital Data Governance[74].Interestingly in 2018, AMS developed a framework and joint declaration to minimize the harmful effects of fake news during the 14th Conference of the ASEAN Ministers Responsible for Information (AMRI)[75]. Unfortunately, the joint declaration seems approach the situation related to disinformation in a manner contrary to the principles of the right to freedom of opinion, expression and access to information.

These instruments generally frame the direction for AMS to follow in the Fourth Industrial Revolution by ensuring that new technology plays an important role in regional development. Smart cities, cross-border data flows, and use of emerging technologies are some of the elements in these instruments. These instruments also mention future initiatives, for example, the ASEAN Framework on Digital Data Governance will bring about the ASEAN Data Classification Framework, ASEAN Cross Border Data Flows Mechanism, and ASEAN Data Protection and Privacy Forum. It is recommended that AICHR examine these instruments and initiatives, and also investigate related issues looking into the types of data, cross-border data flow mechanisms, and its potential effects of human rights.

It is interesting to note that the ASEAN Framework on Digital Data Governance as well as the ASEAN Framework on Personal Data Protection do not mention principles relating to national sovereignty, national security, and public safety which are often found in documents on cross-border issues.

Relatedly, ASEAN Smart Cities Network (ASCN)[76] which was established at the 32nd ASEAN Summit on April 28, 2018, can be another area of inquiry in the area of digital technology and human rights. The ASCN targets 26 cities from all 10 AMS to become

---

[71] ASEAN. The ASEAN ICT Masterplan 2020. Retrieved from https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf

[72] ASEAN. ASEAN Digital Integration Framework. Retrieved from https://asean.org/storage/2019/01/ASEAN-Digital-Integration-Framework.pdf

[73] ASEAN. ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) Framework on Personal Data Protection. Retrieved from https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf

[74] ASEAN. ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN) Framework on Digital Data Governance. Retrieved from https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf

[75] ASEAN. 14th Conference of the ASEAN Ministers Responsible for Information (AMRI) Framework and Joint Declaration to Minimize the Harmful Effects of Fake News. Retrieved from https://asean.org/storage/2012/05/Annex-5-Framework-Declr-Fake-News.pdf

[76] ASEAN. ASEAN Smart Cities Network. Retrieved from https://asean.org/asean/asean-smart-cities-network/

pilot areas for smart city development. The initiative, involving state officials and the private sector, has put forward Smart City Action Plans (SCAPs) and ASEAN Smart Cities Framework (ASCF). However, it does not seem to include discussions on human rights since there is no mention of human rights experts' presence or input at the meetings. Similar to initiatives on cross-border data flows, development of smart cities need checks in terms of human rights impact, particularly on privacy and data ownership: the purpose, kinds, methods and processes of data being collected, and who has rights to access the data.

In 2018, during the 3rd ASEAN Ministerial Conference on Cybersecurity (AMCC), all 10 AMS planned to establish a framework for cybersecurity collaboration[77], with a draft mechanism paper put forward during the succeeding 4th AMCC in 2019[78]. It is likely that the cybersecurity initiative will focus on concerns related to economic development and national security rather than on protecting individual rights. Thus, it is recommended that this framework be examined to see how it can affect human security and human rights, consistent with the international norms, particularly Human Rights Council resolutions 20/8 and 26/13, and on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression[79].

A final area of inquiry by the AICHR can be on dual-use items (DUI), which are goods, materials, technology, and software that can be used for commercial purposes but may also have military applications. In this case, human rights concerns are related to the importation of surveillance technology as well as the use of malicious software, especially spyware like FinSpy and Pegasus. In June 2019, the United Nations Special Rapporteur on Freedom of Expression, David Kaye called for a global moratorium on the sale, transfer and use of surveillance tools[80], while the European Union have attempted for the stricter trade controls of DUI. In AMS, Malaysia and Singapore are the only two nations that have regulations on DUI, while Thailand has recently announced the regulation on DUI which is expected to be adopted in 2020[81]. There is a need to review existing regulations at the national level and provide recommendations for region-wide norms, including mechanisms and instruments to safeguard human rights and human security which are at risk from surveillance technology and malicious software.

---

[77] Baharudin, H. (2018, September 20). Singapore to Draw Up Formal ASEAN Mechanism for Cyber Security. Retrieved from https://www.straitstimes.com/singapore/singapore-to-draw-up-formal-asean-mechanism-for-cyber-security

[78] CSR Singapore. (2019, October 2). ASEAN Member States Agree to Move Forward on a Formal Cybersecurity Coordination Mechanism. Retrieved from https://www.csa.gov.sg/news/press-releases/amcc-release-2019

[79] United Nations General Assembly (2015, July 22). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from https://undocs.org/A/70/174

[80] OHCHR. UN Experts Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools. Retrieved from https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736&LangID=E

[81] The Nation Thailand. (2019, June 03). Thailand to Enforce Weapons Export Controls Starting in 2020. Retrieved from https://www.nationthailand.com/Economy/30370481