ISBN 978-9934-564-66-6

DISINFORMATION AS A GLOBAL PROBLEM – REGIONAL PERSPECTIVES

By Rachael Lim
Researcher, NATO StratCom COE

ISBN: 978-9934-564-66-6
Author: Rachael Lim
Cotributors: Linda Curika, Rueban Manokara

Design: Kārlis Ulmanis

Riga, January 2020
Report compiled based on data available by June 2019

NATO STRATCOM COE
11b Kalciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

Remarks

The assumptions, analyses, views and opinions expressed in this report are those of the author and do not reflect the official policy or position of her employer.

DISINFORMATION AS A GLOBAL PROBLEM – REGIONAL PERSPECTIVES

ISBN: 978-9934-564-66-6
Author: Rachael Lim
Cotributors: Linda Curika, Rueban Manokara

Contents

Introduction

This research project discusses disinformation in the European Union (EU)[a] and Southeast Asia (SEA)[b]. The report examines the characterisation and context of disinformation, provides an overview of its creators and its circulation, where creation refers to production and its underlying motivations and circulation refers to the different ways it is disseminated, amplified and sustained, and rounds up with a discussion on foreseeable trends. It finds that disinformation is ultimately a national security problem, and any assessment of, and response to, disinformation must be formulated with developments in other domains.

In the aftermath of suspected electoral interference in the 2016 US presidential elections and in several European elections in 2016 and 2017, much has been written about disinformation, its definitions, history, manifestations outside of elections and motivations. Generally, the assessed intent is to undermine confidence in legitimate institutions and democratic processes and deepen societal fault lines through entrenching views/beliefs and subverting a society's values. A range of tactics is used. They include creating and capitalising on areas of vulnerability and instability, exploiting political differences and normalising debate on sensitive national

a They are Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

b They are Brunei, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, The Philippines, Singapore, Thailand, Timor-Leste and Vietnam.

KEY TAKEAWAYS

- Disinformation is a perpetual challenge to national security made more complex by sharp power
- Factors outside the information domain provide the conditions by which disinformation and sharp power are exercised
- Regional and national vulnerabilities will continue to be exploited
- The widespread use of digital technologies in communications means that the information environment will become crucial battlegrounds for "like wars"

issues that have had long-standing scientific consensus. Disinformation has been used somewhat interchangeably with information manipulation, information disruption and fake news.

Disinformation will continue to pose a challenge in elections and other democratic processes because[1] it is perpetuated in new ways such as meme warfare[2] and domain cycling[3], which is the tactic of changing domains to avoid detection by fact-checkers and machine-learning models[c]. It is enabled by actors who find new ways to fly under the regulatory radar[4] and those who view it as a profitable business[5] with high returns[6], manifesting in a thriving black market[7] and "hackers for hire"[8, 9].

Disinformation is also regarded as a tool to achieve long-term outcomes such as in influence operations. For example, the European Parliament in November 2016 adopted a resolution stating that Russia's goal was to distort truths, provoke doubt, divide member states, engineer a strategic split between the EU and its North American partners, and discredit EU institutions and transatlantic partnerships as well as to undermine and erode the European narrative based on democratic values, human rights and the rule of law. This is a critical distinction because while there have been robust government, industry, and civil society responses to disinformation per se, the same cannot be said of responses to influence operations due to the latter's more

c For example, a disinformation actor could shut down a site that has been blacklisted and move all content to a new URL.

> Like soft power, sharp power is wielded through proxies – individuals, institutions and communities but it takes place in the grey areas of legal-democratic systems

complex and subjective nature. Consider "soft power". Coined by US political scientist Joseph Nye to describe the ability to get outcomes through attraction and persuasion rather than threats of coercion or offers of payment, it has been used to justify a state's course of action in areas that fall between the lines of what is legitimate and illegitimate. Indeed, soft power could be a "lead indicator" for more offensive actions later.

"Sharp power" was coined to describe influence efforts through distraction and manipulation. According to the National Endowment for Democracy researchers, who coined the term, sharp power **(a)** cuts through the political and information environments in the targeted countries, **(b)** cuts razor-like into the fabric of a society to amplify existing tensions, and **(c)** is malign and aggressive.

Regimes that use sharp power are not necessarily seeking to win hearts and minds but seek to manage their target audiences by manipulating or poisoning the information that reaches them through "preying upon the openness of democratic systems abroad" [10] while "raising barriers to external political and cultural influence at home"[11]. In Nye's view, the line that divides soft and sharp power is "truth and openness… in public diplomacy"[12].

Like soft power, sharp power is wielded through proxies – individuals, institutions and communities but it takes place in the grey areas of legal-democratic systems – not strictly illegal and yet difficult to categorise as traditional foreign espionage[13]. Because issues of national security are inherently subjective, the burden of proof thus falls on national agencies that have to determine when acceptable limits/norms of state behaviour are crossed. Even then, they may not allow for mutual accusations against a state and even if such accusations are publicly made, may be economically and diplomatically costly[14]. In addition, what one region or country might consider as acts of disinformation or sharp power might not be regarded as such by another.

Disinformation through the cyber domain

In the 2018 US midterm elections, the 13 US states that were on the political fence were found to have more malware detections per day than the 37 non-swing states. Politicians and spies were using adware to conduct digital reconnaissance and collect information, after which, more invasive and targeted cyber operations were conducted. Further, a government computer system that interacts with healthcare.gov was hacked leading to sensitive personal data of 75,000 people being compromised. There is potential for these activities to spill over into the mass media space. In the 2014 Ukrainian Presidential election, hackers briefly changed the vote tally on the official election website, and the information was immediately broadcasted on Russian television.

Afternote: *In March 2019, the Department of Homeland Security and the FBI acknowledged that the election infrastructure in all 50 states was targeted beyond the 21 that were confirmed in earlier reports. This included online research and reconnaissance to identify vulnerable databases, usernames and passwords in webpages of state and local websites.*

Scope of Study

This study discusses disinformation in the EU[a] and Southeast Asia (SEA)[b], drawing on examples outside these regions where relevant. Disinformation in this study is defined as "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit"[15].

Disinformation and the use of sharp power is ultimately a national security problem. Therefore, any assessment of disinformation and sharp power must be taken and assessed together with developments in other domains[c, 16]. In this regard, other domains where relevant will be discussed if they provide the conditions[17] by which disinformation is exercised. One example is cyber-mediated disinformation, given the strong intersection and mutually reinforcing elements of the cyber and information spaces. Disinformation campaigns could be complemented and enabled by cyber-

a They are: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

b They are: Brunei, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, Philippines, Singapore, Thailand, Timor-Leste and Vietnam.

c In the Pacific Ocean, China's naval military build-up is a watch area. Quantitatively, the Chinese Navy is now the world's largest, and according to commander of the US Indo-Pacific Command, Adm. Philip S. Davidson, "By building critical asymmetrical capabilities… China is now capable of controlling the South China Sea in all scenarios short of war with the United States."

attacks, including malware attacks, distributed denial of service attacks and integration of backdoor programs[18] (see box story for an example from the 2018 US midterm elections).

Another relevant example is the use of economic pressure, which could be leveraged as a tool of diplomatic pressure in the information domain. Consider China, to which the health of many economies is inextricably tied[19]. Since 2012, China has been the world's largest spender in international tourism globally[20]. Examples over the last few years suggest that the withholding of tourists may be a response to strains in the bilateral relationship[21, 22]. On some occasions, it has spilled over to aggressive media coverage, where at times, articles are published only in English[23], suggesting that the stories were written for the international audience (see box story).

This is salient and has implications for both the EU and SEA because of the wide spectrum of tourism-related Chinese investment in these regions. In Eastern Europe, the focus is on infrastructure development under the Belt and Road initiative; in Southern Europe, in the series of privatisations during and after the euro-zone crisis; and in Western Europe, in high-tech and industrial industries. Eastern European and Western Balkan countries, many of which are part of the EU, have pledged to strengthen tourism-related collaboration, which includes introducing direct flights from China to the region, creating joint tourism packages, and further simplifying visa application procedures. This is in addition to infrastructure development[24] with China under the China+16 framework[25, 26]. In SEA, Chinese visitors continue to be the largest inbound group of tourists. Chinese visitors also spend more per visitor than their Western or Asian counterparts.

Using economic tools as pressure points with spillover to the information space

In 2014, **South Korea**[27] allowed the deployment of the US Terminal High Altitude Area Defence (THAAD) anti-missile system within its borders. For South Korea, it was a way to curb North Korea's nuclear **ambitions** but China viewed THAAD as targeting China and felt that the THAAD's radar capabilities compromised the country's national security. China said it "firmly opposed" the decision and would "resolutely take necessary measures to defend our security interests."

China displayed its displeasure through reducing tourist numbers (state-owned agencies arrange group travel for 58% of China's outbound tourism[28]). Seoul-based multinational conglomerate Lotte, which had agreed to provide land for the THAAD

deployment, was fined over its advertising practices, and a large number of its supermarkets in the country were shut down for alleged fire-code violations. Lotte also reported cyber hacks from China during this time. Certain imported products from Lotte and other Korean brands were banned. At the same time, Chinese customs inspections against South Korean companies intensified. In the entertainment arena, the distribution of South Korean content, including movies and shows, was limited and South Korean celebrities' broadcast airtime was revoked.

Amplified by the news media, these actions gained further traction with Chinese consumers. *Global Times* published daily attacks on South Korea's "erroneous decision". Its media reports encouraged consumers "to become the main force in teaching Seoul a lesson" and to "make it hurt". A patriotic pop song included the lyrics "Chinese sons and daughters must stand up; everybody, stop buying Lotte, make them get out of China fast". According to the South Korean national assembly's budget office, the Chinese boycott cost South Korea US$6.8 billion.

Other SEA countries have had similar experiences. After a boat accident in **Thailand (Phuket)** that resulted in the deaths of Chinese tourists and a viral video of a Thai airport guard punching a Chinese tourist (which Thai Prime Minister Prayuth Chan-Ocha said on Twitter he regretted), there was a 12% dip in the number of Chinese tourists visiting Thailand. The tourism slowdown and the impact of trade disputes were estimated to depress Thailand's economic growth in 2018 from 4.5% to 4.2%.

Most recently, as **Sweden's** diplomatic dispute with China continues over the alleged mistreatment of Chinese tourists in Sweden, and China's detention of a Swedish citizen, China issued a new travel alert warning against travel to Sweden due to the latter's "security situation" [29].

In **New Zealand**, China announced a postponement of the "2019 China-New Zealand Year of Tourism" and a cancellation of the New Zealand prime minister's trip to China. An Air New Zealand flight bound for Shanghai made a U-turn four hours into its journey for improper paperwork[30]. *Global Times* reported[31] that "New Zealand's strained political relationship with China – following the ban of Huawei from building part of its 5G networks – is costing the country more than it can afford." The report added that "the (ban) sparked widespread complaints among Chinese netizens" and "some tourists (were) considering dumping their plans to travel to New Zealand as a way to punish the country." It also quoted a Chinese academic who said that New Zealand's economy was particularly vulnerable to slides in tourism income to which Chinese travellers contributed a large part. The academic said: "offending Chinese tourists is a big thing."

Regional Issues

One of the aims of disinformation is to weaken a country through reducing its ability to resist foreign aggression, change its foreign policy, and create conditions for its inclusion in a foreign country's sphere of influence[32]. This is usually done through exploiting vulnerabilities[33]. Therefore, understanding the information landscape in the EU and SEA requires broad identification of the issues the EU and SEA are facing.

Common to both the EU and SEA is the extremist terrorism threat. The terrorist group ISIS, despite huge losses, is reportedly re-grouping elsewhere. ISIS also claimed responsibility for the multiple Easter Day bombings in Sri Lanka, even though it has no entrenched presence there, because the attackers were inspired by ideology similar to that espoused by ISIS[34]. In SEA, where it had pledged to establish a *wilayat*[a], it continues to be active[35, 36], inspiring home-grown fighters[37]. The threat is expected to worsen. Individuals from more than 100 countries went to Syria to fight for ISIS. On the back of significant territorial losses, the US' withdrawal of most of its troops from Syria, and radicalised individuals and jihadists being released from incarceration, these individuals are expected to return to Europe[38] and SEA[39]. How to manage such foreign fighters remains a challenge[40]. These individuals are now connected and networked[41] and include sleeper cells[42] that have infiltrated parts of Europe and Asia for intelligence and information campaigns meant to mislead authorities about the status of ISIS operatives.

Moreover, the group is already known for using encrypted messaging apps and the dark web to promote itself and recruit new members, their efforts boosted by social media algorithms that inadvertently lead users to visually similar[43] and thus more extremist content[44] through searches. Notwithstanding that ISIS' cyber-crime abilities are regarded as being in their infancy, they may also be considering the use of cyber-attacks, and the dark web to buy illicit malware[45], with some watchers reporting that ISIS propaganda, chatter and online activity had "exploded"[46] two months into 2019. The threat is exacerbated[47] by (a) other groups, e.g. Jemaah Islamiyah in SEA[48], taking centre stage, (b) "e-jihadists"[49], i.e. those who flood social media with violent propaganda memes and hack the personal information of thousands of Americans to create "kill lists", and (c) autonomous cells who hold and are inspired by others with extreme-right beliefs in transnational networks, as the attack on a New Zealand mosque in March 2019 illustrates.

Within the EU, various regions demonstrate different levels of vulnerability. The Balkans, for example, is an arena of geopolitical competition. In the cyber and information realm, the Baltic States continue to come

a An administrative division, e.g., state or province

under attack. Internet trolls exaggerate problems, such as discrimination against **Russian-speakers**, invent events intended to spark outrage, such as an alleged assault by German NATO soldiers on a non-existent Lithuanian orphan, and stir up disputes over divisive issues like immigration[50].

Beyond geography, legislation and policies enacted by certain EU countries have been viewed as incompatible with EU values and democratic norms. The risk is that such divisiveness might open up room for exploitation. Today, a few countries are subject to Article 7[51] proceedings, which is an infringement process outlined in Article 7 of the Treaty on European Union for member states found violating EU fundamental rights.

The rise of eurosceptic political parties[b] advocating de-alignment[c] is an ongoing development that could present another vulnerability to be exploited. While EU membership is generally regarded as an asset and beneficial, countries[d] have seen a rise in support for populist, nationalist, and anti-establishment political parties in response to Europe's economic difficulties and austerity measures in the aftermath of the 2008-2009 global recession and Eurozone crisis. Fears about globalisation, migration[e], a loss of national identity and a growing gap between the international elite and the "true" will of citizens are additional contributory factors. In some parts of Europe, the narrative of small countries being abused and oppressed by stronger powers has historical roots. Therefore, framing the EU as a big power that is once again constraining the sovereignty of the nation is resonant. The narrative of "them vs. us" has helped certain parties to gain popularity. Anti-EU sentiment may also be equated with national or regional pride.

In SEA, the politicisation of ethnic and religious differences[52], a resurgence of nationalism[53], elections, and the ongoing US-China strategic rivalry as well as how it may manifest inside and outside of trade are issues to watch[54]. In the military domain, SEA countries are modernising their armed forces[55] and increasing military spending. A presidential candidate in Indonesia's April 2019 presidential elections advocated for an increase in military spending as part of his election promise[56]. The Stockholm International Peace Research Institute estimated close to $42 billion on regional military spending in 2018[57].

b For example, in Germany, the anti-immigrant and eurosceptic Alternative for Germany party became the first far-right German political party to enter Parliament since the end of WWII.
c This is characterized by the fragmentation of political systems, the rise of populist parties, higher rates of electoral volatility, and an erosion of support for traditionally dominant parties. Source: Foreign Policy.
d For example, in the Czech Republic, 62% of votes went to anti-establishment and populist parties.
e The EU has faced considerable criticism for lacking coherent and effective migration and asylum policies, due to national sovereignty concerns and sensitivities about minorities, integration and identity. A case in point – the Sweden Democrats, a neo-Nazi political party, campaigned exclusively on immigration issues in the 2018 Swedish elections, and was later elected into Parliament with 69 seats, 20 more than the last election cycle.

> As mobile internet becomes more affordable, the implication is that social media and digital platforms will become battlegrounds for "like wars"

It is in this context that disinformation, whether during or outside the election cycle, has risen in salience in recent years, exacerbated by the presence of emerging and potentially powerful groups. For example, think tanks have noted that foreign influence over Europe has spread to the level of political decision-making, notably in three areas: political and economic elites, media and public opinion, and civil society and academia[58].

Media Landscape

The media landscape is an integral feature of the information domain. In the EU, the European Convention on Human Rights, enforced through the European Court of Human Rights, grants "everyone… the right to freedom of expression", which includes "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers" though it does not "prevent States from requiring the licensing of broadcasting, television or cinema enterprises[59]." In addition, a wide range of international government and non-government organisations defend media freedom within the EU.

Meanwhile, media freedom is often touted by western media as "under attack" in SEA. While there is no common SEA law that governs media freedom, western-led thinking is that laws and legislation are abused to prosecute the media and restrict freedom of expression[60].

The issue of media freedom is typically discussed together with the issue of human rights and accountability[61]. The larger point is that democracies are vulnerable to information attacks that turn common political knowledge into contested facts. If people lose sense of what is real, democratic debate suffers. On the other hand, information attacks could benefit more autocratic systems because "…the stability of autocrats' power requires that the public not know how others (are feeling) for there to be constant confusion about which institutions, groups, and views are genuine and which ones are conspiracies, frauds or power-grabs." [62]

Common to both the EU and SEA is the widespread use of social media networks. The Asia-Pacific region was Facebook's fastest growing region by revenue in 2016, an increase of 60% compared to the previous year[63]. SEA countries Indonesia, Philippines, Vietnam and Thailand are four of the top 10 countries by number of Facebook users, numbering 130 million, 70 million, 59 million and 50 million, respectively[64]. The region's six largest countries have 350 million Internet users with online media[65] expected to generate 31 billion dollars by 2025, a 180% increase from 2018[66]. Indonesia, Malaysia, Philippines and Thailand also count among the top 10 most engaged countries globally on mobile devices. As mobile internet becomes more affordable, the implication is that social media and digital platforms will become battlegrounds for "like wars", i.e. the hacking of people and ideas on those networks where "attention is power" and reality can be shaped.[67] In fact, "…'the people' could be seen as a centre of gravity that may be exploited to win future conflicts, potentially without any fighting at all."[68]

Framework of Analysis

Following an examination of the characterisation and context of disinformation, the report will provide an overview of its creators and its circulation, where creation refers to production and its underlying motivations and circulation refers to the different ways it is disseminated, amplified and sustained[69] and discuss foreseeable trends. In examining these issues, open-sourced research, and thereafter published frameworks were used to discuss the findings. Such an approach allows broad observations to surface and provides an initial understanding of the **ways** disinformation is present in the EU and SEA and the conditions that enable it.

Actors & motivations

At the heart of disinformation is falsification and obfuscation. To prevent attribution and for plausible deniability, perpetuators hide behind covers, i.e. false identities, false personas or intermediaries. Nevertheless, these actors can be categorised. For example, actions may be state-directed, state-encouraged or state-aligned (see Table 1 for the definitions of the Atlantic Council[70]). These actions can be used against a foreign entity or on the domestic population.

Table 1: Types and definitions of state involvement

State Involvement	Definition
State-directed	An action that state officials, acting in their capacity as representatives of the government or a government's leadership, have sanctioned or have expressed the desire to achieve
State-encouraged	An action that state officials have not directly ordered or signalled but one in which an individual or entity with good knowledge (usually ascertained from close contact with current or former state officials) of the state's objectives can partake with reasonable assurance that these efforts will be viewed favourably
State-aligned	An action that individuals or entities conduct with the intention to support specific or general state objectives

In both the EU and SEA, instances of state-backed disinformation have been observed. Disinformation in the EU is perpetuated by tactics to distract and demoralise through undermining trust in institutions and dividing citizens[71], augmented by the fragmented operations[72] conceived and generally carried out through amplification channels and by organs and proxies, i.e. "political entrepreneurs"[73] or "patriots"[a]. They include diplomats, spies, criminals, think tanks, oligarchs and journalists.

In SEA countries, all three types of state involvement have been observed, typically originating from political parties or vested interest groups. Foreign-backed actors are present in SEA in various ways, whether through cyber-attacks or as foreign agents of influence[b].

Hardware, software, platforms and data

In coming years, strong demand and supply-driven forces for data could see data taking on a central role in the exercise of disinformation and sharp power. In her book "Surveillance Capitalism", author Shoshana Zuboff describes a new type of capitalism enabled by data. According to Zuboff, "surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to service improvement, the rest are declared as a proprietary 'behavioural surplus', fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into prediction products that anticipate what you will do now, soon, and later. Finally, these 'prediction products' are traded in a new

a When interviewed at the 2017 St Petersburg Economic Forum, the term "patrotic" was used by Russian President Vladimir Putin to describe hackers who "… contribute in a way they think is right, to fight against those who say bad things about Russia." Retrieved from https://www.reuters.com/article/us-russia-economic-forum-putin-cyber/patriotic-russians-may-have-staged-cyber-attacks-on-own-initiative-putin-idUSKBN18S56Y

b While these examples do not fall strictly into the information realm, an argument has been made for their inclusion (see Chapter 1).

Examples from Cambodia and Singapore

In 2018, **Cambodia's** National Election Commission, Ministry of the Interior, and the Cambodian Senate and members of opposition parties were compromised by cyber-attacks found to be consistent with typical Advanced Persistent Threat efforts from a foreign state. In **Singapore**, a prominent academic was permanently banned from Singapore in August 2017 for working with intelligence organisations and agents of a foreign government to influence Singapore's foreign policy and public opinion.

kind of marketplace that I call 'behavioural futures markets'[74]." The supply-driven forces surrounding data described by Zuboff have been demonstrated in investigative reports that detail big technology companies' attempts to capture, mine and sell data as well as to keep users highly engaged within the social media's ecosystem to generate further revenue, most of the time without users' knowledge.

Other big players exist in the data economy, including large third-party commercial companies, state-linked enterprises and app developers[75, 76]. Today, big data companies that collect data[77] on demographics, court and public records, social media and technology use, neighbourhoods, finances, vehicles, purchase behaviour, health and general interest (some estimates point to about 3,000 individual attributes[78]) have international offices in Europe and the Asia Pacific[79] region. Data collection on a massive scale is enabled by data brokers – multi-billion-dollar companies that make a living out of collecting and reselling data[80] from devices that consumers use on a day-to-day basis[81]. They are by no means alone. State-linked organisations are also interested in big datasets, obtained through facial recognition or medical records. At the same time, governments are collecting and compiling data on citizens[82] on national security grounds, raising concerns about how the data will be used now **and in the future**[83].

Rising expectations of how data can improve efficiency will catalyse the proliferation of data-driven applications. Citizens have grown accustomed to a level of user experience and functionality provided by data-powered apps. The user experience will soon be enhanced by wearables, implants, and voice-based technologies. Wearable technology, for example, is increasingly seen as a part of everyday life in helping people to exercise smarter, keeping children safe and improving and enabling greater efficiency at home and at work[84].

Malicious use of data

Clearly, data is tremendously powerful in its fundamental role for powering technologies of the future. In such a landscape the stakes are high, as it relates to the distribution of knowledge - "Who knows?", "Who decides who knows?" (authority) and "Who decides who decides who knows?" (power)[85] with downstream implications in areas such as fair competition and privacy. In addition, because data and the extra network effects that it generates will underpin technologies of the future including 5G networks, Internet-of-things[86], AI-powered applications such as human-like chatbots that can understand context and continuously learn from feedback[87], data is an attractive target for exploitation and manipulation. The wide range of malicious uses includes cyber heists[88], nefarious identity or location-related crime[89], data leaks[90] and theft or disruptions to businesses[91]. Today, parliaments[92], government agencies[93], consumer industries like food and beverages[94], automobiles[95], hospitality, aviation[96], telecommunications[97], devices for children[98], banking and tech companies[99] themselves are already affected and it will be increasingly difficult to find a sector that is not at risk.

In the information environment, data theft, exploitation and manipulation enable disinformation to be exercised by groups against other groups[100] or by states against other states, be they through leaking sensitive information, disrupting critical infrastructure[101] or even as part of a hostile campaign to undermine a nation's international standing[102]. This chapter discusses these issues based on Lund University's **effects-driven** DIDI model[103] (i.e. deception, intention, disruption, and interference) for diagnosing illegitimate influence.

Deception

Definition – The chain of events involves attempts to influence opinion formation by deceptive means such as factually incorrect news reporting or the use of false reports

Data has been manipulated for political gain via the use of fabricated content globally (see box story on "Avoiding detection on social media – an example from Saudi Arabia"). In the EU, much has been written about the consistent tactics observed in (a) creating inauthentic personas impersonating real citizens in the virtual world, (b) supporting and financing real-world protests, and (c) publishing content through fake social media accounts, purchasing social media advertisements and promoted content[104]. Disinformation actors also exploit ideological divides to gain a foothold in the populace. In Muslim-majority Indonesia, conservative Islamic sentiment and doctored online content have been weaponised through low-cost smartphone technology and doxxing[105]. Indonesia's president, no less, has been a victim of hoaxes, with allegations that he

was "…a communist member, anti-Islam, (and) a foreign stooge"[106]. His campaign staff described these hoaxes to be the "toughest challenges in the campaign".

Avoiding Detection on Social Media – An example from Saudi Arabia

A recent incident in which technology was key in a massive disinformation campaign was in the aftermath of the death of *Washington Post* columnist, **Jamal Khashoggi**. Khashoggi was believed to have been targeted for mobilising Saudis to speak out against the Saudi kingdom and initiating the Bee Army – a movement that offers cyber protection to Saudi activists needing a safe platform to speak out to fight the "fly army" [107] – bot accounts.

In the global outcry following Khashoggi's death, analysts observed a massive surge in pro-regime Twitter activity. There was the creation of troll accounts to bury the hashtag of Khashoggi's kidnapping and instead praise Saudi Arabia's crown prince with the hashtag #We_all_trust_Mohammed_Bin_Salman. The kidnapping hashtag was replaced with banal ones like "the kidnapping of ants and cockroaches" deliberately designed to confuse Twitter's algorithms. When these banal hashtags were appropriated by Saudi activists to highlight Khashoggi's plight, the troll accounts tweeted the hashtag at activists with violent threats and images of torture.

According to disinformation experts at the Atlantic Council, this incident highlights how groups behind bots have adapted to evade bans. While botnets were used, the tweets were published sparingly, a move to avoid detection [108].

The Saudi government also reportedly used its cyber army against Jeff Bezos, the owner of the *Washington Post*, which had covered the incident extensively[109].

Intention

Definition – The chain of events is, according to the best available evidence, conducted, controlled or instigated by an actor with perceived hostile intent, i.e. to undermine or otherwise harm society

An intention of hostile event can be assessed through various means, including manipulating any stage of the information process, e.g. tapping data streams, network activities and its concomitant hardware to steal data, and exploiting supply chain vulnerabilities[110]. They could include:

a. **Targeting Global Navigation Satellite Systems (GNSS)**[111, 112]. During NATO's Trident Juncture exercise, held in Norway in October 2018, Global Positioning Satellite (GPS) signals across far northern Norway and Finland failed. Civilian airplanes were forced to navigate manually, and citizens' GPS-powered apps were no longer accurate. By impeding the normal functioning of society through making it much more challenging to access day-to-day essential services like the internet or by jamming, hacking or spoofing GNSS signals[113], a potential adversary can dramatically weaken the target country even without a visible military footprint.

b. **Hijacks on transoceanic cables**. Today, 97% of global communications are transmitted via an estimated 213 independent transoceanic cable systems, which carry $10 trillion worth of financial transfers and data daily[114] with demand likely to grow[115]. Australia blocked Huawei from building a cable that would connect the continent to the Solomon Islands[116] out of the concern that it would offer an entry point to potential hackers. Hijacks would potentially enable access to the information source's networks to steal, modify or corrupt data, add malicious implants to seemingly normal traffic and learn enough to impersonate trusted sources or even break encrypted traffic.

c. **Attacks through routers or Virtual Private Networks (VPNs)**. Attacks on routers may be used as gateways to other Internet-of-Things devices with global impact. This was the case when it was discovered that a piece of malware attributed to Russian state-sponsored hacking group Fancy Bear/APT28 had infected 500,000 routers[117].

These developments have resulted in increasing attention to the possible conduct of state-sponsored spying and information activities through 5G mobile networks[118]. All 28 EU member states will have access to 5G services by 2020[119] and at least seven of

10 SEA countries will have begun to develop and test 5G services[120]. That means national security-related conversations on 5G service providers will continue in the near future.

Case Study: 5G Technologies (see box story) **and Huawei**

The conversation on 5G providers thus far has been driven by countries that have felt the severe economic impact of foreign cyber-espionage activities[121]. For example, the US reached out to its European allies[122] and Japan to try to persuade wireless and internet providers there to avoid telecommunications equipment from China's Huawei[123] on national security grounds[a]. In Europe, the Czech Republic's cyber security institution released a formal warning on the security threats posed by devices developed by Huawei and ZTE[124] in 2018, the first of its kind. The Polish authorities detained and indicted a Huawei executive for allegedly conducting high-level espionage on behalf of the Chinese government[125].

This could put pressure on International Organizations[126] and governments[127, 128, 129] to exclude Huawei from national networks, solidify the positions of countries who are developing 5G networks[130, 131], catalyse concerns by European governments on whether Huawei should be excluded from markets[132] and potentially strain long-standing security partnerships[133, 134]. It also has an impact on Huawei's existing collaborations with academia[135, 136].

These actions have been viewed as an onslaught against China by Chinese citizens, sparking a wave of positive support for Huawei and calls for a boycott of products made in the US[137]. When a poll conducted by CNN asking viewers what they thought were the main reasons for the US' campaign against Huawei resulted in a unanimous "politics", the topic quickly lit up on Weibo, China's most popular social media platform, as a trending topic[138]. Prevalent narratives on Weibo were: (a) the US vs. Huawei battle is politically motivated, especially as it has emerged that the Department of Justice's indictments against Huawei were for events that took place several years ago, with one having already gone through the courts as a civil case[139], (b) the US feels threatened by China, (c) the US is taking desperate measures, and (d) the US is suppressing China. Such comments gained further traction after Meng Wanzhou's WeChat Moments post after her release (see figure 1) as well as reports of the latter's lawsuit against the Canadian government.

In the information space, Huawei has the backing of the Chinese media. Official statements warning of the serious consequences should Huawei be banned from European 5G projects have been

a One concern of the U.S. centres on the use of Chinese telecom equipment in countries that host American military bases. The Defense Department has its own satellites and telecom network for sensitive communications, but most traffic at many military installations travels through commercial networks.

Figure 1 – Posts by Meng

A translation of the text reads: "I am in Vancouver back with my family. I am proud of Huawei! I am proud of the motherland! Thanks to each of you who are concerned about me. Meng Wanzhou"

Figure 3: Huawei ad in the Wall Street Journal on 28 Feb 2019

echoed by state media and academics from state-run think tanks[140, 141]. The Chinese state councillor, in a press conference after meeting the EU's foreign policy chief and EU foreign ministers in March 2019 reiterated China's opposition to "…groundless accusations for political purposes and attempts to bring down a foreign company."[142] A few countries that boycotted Huawei are also experiencing China's diplomatic pushback. The Czech Republic has been threatened with economic retaliation and Czech groups comprising lawmakers and the political elite visiting China have been at the receiving end of intensifying lobbying campaigns[143]. On the other hand, this has led some commentators to suggest[144] that the Chinese government's visible backing for an organisation in trouble is a signal to other Chinese individuals and organisations that the state will step in should they be in the same situation.

Huawei is pushing back on what it says are unfounded claims[145]. The company is suing[146] or threatening to sue[147, 148], taking out ads in high-reach media (see figures 3 & 4) and sending warning shots to its commercial partners for sponsoring research institutions that have an "unhealthy fixation" with Huawei[149, 150]. Its senior leadership[151] publicly denounces what it says are unbacked claims and is "going on the attack". In a reverse narrative, Huawei's chairman has[152] said that the US is trying to suppress a rising technological competitor and "collect it all", a reference to the National Security Agency's PRISM programme that allowed the NSA to collect data.

Huawei could retain its current dominance despite government warnings[153] as it remains attractive to consumers[154], price competitive[155], complies with local regulations[156], and has made restitution in

Poland[157, 158] (where Huawei's HQ for Central and Eastern Europe and Scandinavia is located). Essentially, it is because Huawei lacks an equal strategic competitor in terms of market share[159, 160]. Before the US blacklisting, sales of Huawei's mobile handsets had surpassed those of Apple. In the EU, Huawei also has one-third market share in telecommunications equipment and any replacement of backbone equipment would come at a cost of billions of dollars[161]. In response to the US ban, Huawei has ramped up indigenous R&D capability to eliminate dependence on US products[162]. Consequently, AI chips produced by Huawei may eventually rival those currently in the market. Huawei Chairman Ren Zhengfei has said that while they did not expect the US to "…attack Huawei in so many aspects", he expects a revival in 2021[163].

Governments and industry[164] in EU countries are also taking a more calibrated approach[165] towards Huawei, with the EU pressing ahead with 5G collaboration projects between the EU and China[166] and industry players requesting the US to present facts to back its claims. Germany[167] and [168] the UK appear to have gone with a "middle ground" approach thus far, choosing to stipulate that network operators must put in place risk-management measures. Hungary and Slovakia have publicly backed Huawei[169]. Italy has said that the issue is about foreign equipment manufacturers and not Huawei per se[170]. Even within Poland and the Czech Republic[171], there are divisions among government officials on how the situation with regard to Huawei should be approached[172]. In SEA, Philippines-based network operator Globe Telecom will go ahead with Huawei for its 5G commercial networks[173]. Thailand, a US ally, will continue to launch a Huawei 5G testbed[174] to "make observations which will be useful to either confirm or disconfirm the allegations". Huawei is also providing telecoms equipment for 5G trials in Singapore and Malaysia.

Figure 4: Huawei's outdoor ad in New Zealand

Providing the 5G Service – What's At Stake? [175]

5G technologies will support next-generation digital applications, ushering in a sea change in communications. These apps are likely to be the building blocks of future smart cities and digital economies, which are predicted to be the next key driver of economic growth. 5G will be an enabler in the following ways: First, it will significantly increase the speed of wireless communications. Ultra-fast flowing mobile data means that whoever controls the networks, through either hardware or software, controls access to the voluminous data that passes through these networks. Second, while earlier generations of mobile technology focused mainly on connecting people in better ways, 5G connects things, even previously unconnected ones, through machine-to-machine data transmissions. Embedded with software, these devices can "talk" to each other, and can be remotely monitored or controlled. While data transmission can take place over a network connection approved by the owner of the device, it may be programmed to upload or download data wirelessly over an unregulated spectrum when it passes a receiver point[176]. Consequently, control of the networks by undesirable actors could result in not just espionage but sabotage, significantly raising the risk of bringing down critical infrastructure. Lastly, choices made among competing 5G standards will have an impact on who has the best understanding of how the technology is implemented – whether in silicon, software, network infrastructure, cloud or in resolving technological, political and policy challenges. This has knock-on effects on economic returns, cyber security, intelligence and how secrets may be protected or stolen. On economic returns alone, industry predicts[177] that the IoT market will reach 30.7 billion devices in 2020, and more than twice that number in 2025. In 2020, annual revenues could exceed 470 billion for IoT vendors selling hardware, software and comprehensive solutions.

Thus, 5G has been regarded as a proxy battlefield for global technological, economic and eventually, military supremacy[178,179].

According to *The Diplomat*, "from the geoeconomic perspective, 5G networks could become such a game-changer that the technology tilts the balance between the world's first and second most advanced economy. The geoeconomics also applies to other states at the periphery of the two superpowers. Whichever superpower successfully deploys 5G can claim to replicate this model in other countries and exert geopolitical, economic, and technological influence over these states. Therefore, 5G has the potential to be the next leverage tool that the United States and China can wield in the great power competition to redraw the lines between the U.S. and Chinese camps – especially in Northeast, Southeast, and South Asia."

China's Huawei and ZTE have come under fire as potential security risks despite protests that they are private companies, as Chinese laws require companies doing business in China to share data that the government deems necessary for national security reasons[180, 181]. As intelligence officers could work with Chinese companies to steal industrial secrets to advance their own economy despite the strict data laws in regions like Europe, the integrity, flow and use of data is thought to be at potential risk if it flows through Huawei's and ZTE's 5G systems. There are also concerns that Huawei could build backdoors into its products.

China's advanced research in AI technologies[182], laws that disadvantage competitors and the absence of ethical restrictions are also part of the equation. More importantly, Huawei exemplifies the four conditions that ex Google China President Kai Fu Lee believes are required to become an AI superpower[183]– big amounts of data, dedicated entrepreneurs, skilled AI scientists and a friendly policy environment. According to Lee, "China's highly competitive startup environment[184] is forging the world's most shrewd and persistent entrepreneurs, and China's weird 'intranet' has created the world's most data-rich internet environment, so when you add on the other two factors – the emergence of more AI scientists and the Chinese government's policy support – Silicon Valley's advantage will melt away."

Disruption

Definition – The chain of events (that) undermines or harms society and/or otherwise hinders the normal functioning of societal institutions, or shows the potential to do so.

Disruption manifests itself when intelligence gathering turns into influence operations. The "hack, leak and amplify approach" in the 2016 US presidential elections and the Macron presidential campaign are examples of how strategic leaks of data are used to influence. These hack-and-leak incidents "fit into a building pattern of breaches with the seeming aim of shaking confidence in the political establishment or undermining important players in it"[185].

One of the ways disruption is carried out is via cyberattacks, considered a top global risk in 2019[186]. In the Asia-Pacific region, cyber security incidents have resulted in estimated losses of US$1.745 trillion[187]. More than just the economic impact, cyberattacks can include deliberate actions by state actors to influence a population over time, slowly changing the dynamics and opinions of a nation[188] and eroding confidence in governments. Both the EU and SEA provide ongoing examples of the use of cyberattacks to achieve these objectives. In Europe, they include:

1 Use of integrated cyber and electromagnetic capabilities to geo-locate Ukrainian and Enhanced Forward Presence troops, intimidating soldiers and their relatives with demoralising and threatening text messages;

2 Cyberattacks which have compromised the EU's COREU network used to relay diplomatic messages on issues related to nuclear proliferation, arms control, human rights, and regional diplomatic talks;

3 IT security incidents related to power and water supplies and telecommunications equipment[189]

4 Attacks on 104 employees from 6 EU countries from September to December 2018 [190] that targeted "think tanks and non-profit organisations working on topics related to democracy, electoral integrity and public policy and that are often in contact with government officials."

In SEA, cyber-attacks that targeted Cambodia's 2018 elections were thought to be potential precursors of "soft war" as Indonesia, Thailand and the Philippines hold elections in 2019[191]. The cyber hack into Singapore's public health system in 2018 that resulted in the theft of hundreds and thousands of patients' information was also believed to have been state-linked.[192] Cyber security experts later concluded it was a part of a wider pattern aimed at Singapore's healthcare, media, telecoms and engineering sectors and would benefit an intelligence-gathering operation that was targeting the defence, telecommunications and energy sectors operating in SEA and Russia[193, 194].

> Cyberattacks can include deliberate actions by state actors to influence a population over time, slowly changing the dynamics and opinions of a nation and eroding confidence in governments.

Disruption can also occur through targeting weak links such as contractors and vendors or unsecured legacy systems. Through targeted attacks on contractors and subcontractors who have no direct reason to be on alert against foreign state-sponsored attacks or agents and degradation[a], hackers can undermine capacity to respond to disinformation and other influence operations, or work their way up the data chain[195].

Interference

Definition – The chain of events involves actors, especially foreign actors or their proxies that have little or no business in interfering with the issue at hand; involvement in the issue encroaches on the sovereignty of the state.

Amplifying sentiment is unsurprisingly one of the most widely used methods in interference and has been observed globally – in Asia-Pacific, Europe, US[196] and South Asia. The modus operandi is to use all available means to achieve the widest possible reach in a process that has been described as "data craft". This includes:

- psychological profiling and targeting of social media posts at people most liable to fall for them via advertisements that align with their interests
- use of botnets to push hashtags to trending status and boost the reach of messages
- planting compromised individuals as key staff members in social media companies

Sentiment amplification is contagious and could be used to shift online conversations into the mainstream through stimulating a domino effect. Some estimates point to 25 - 30 times more fake information from automated accounts on the extreme left and the extreme right than there is genuine, real-life conversation[197].The Arab Spring movements showed how it could be used to mobilise for change. At the same time, it may be exploited. Social media accounts known to promote the views of a foreign state were found to have inflated facts and amplified negative sentiments[198] on France's

a Process of wearing down through activity, creating anxiety and sowing discord, confusion and fatigue

#giletsjaunes movement, to an extent that portrayed French law enforcement agencies as being on the verge of chaos.

Hashtag wars in the lead up to Indonesia's 2019 presidential elections have gone viral online[199], sparked offline campaigns[200] and resulted in aggressive behaviour towards supporters of the incumbent[201]. In the rest of SEA, Twitter users in Thailand, Myanmar and Cambodia had reported the emergence of thousands of bot-like accounts. These accounts used names common in their respective countries, accompanied by regionally authentic languages and profile pictures[202]. These accounts followed local politicians, journalists, scholars and celebrities, but did not tweet or accrue any followers[203].While the objective and source of these bot accounts is undetermined, it implied that infrastructure was being built for data-mining[204], sale or on-demand-use.

Near-term Developments

Low barriers to entry, limited technological difficulty and replicable tools of more sophisticated technologies will pose continued challenge for societies with regard to addressing disinformation. Since January 2018, more than one million people daily have come online for the first time in their lives. SEA has had 70 million new internet users since 2015 – the third largest number of internet users in the world, and more are expected to join. Indonesia launched its first Internet-only satellite with Elon Musk's SpaceX rocket, which is expected to provide internet connectivity for 10,000 Indonesian villages this year[205]. Malaysia is the second country (after Hungary) to run trials on Terragraph, a new wireless technology that would support the demand for data in highly built-up urban areas[206]. As examples of hoaxes, misinformation and violence elsewhere suggest, the ability to manipulate people into action is greater when they first gain access to digital communications[207]. As developed societies grapple with ageing populations, another concern is also digital immigrants' vulnerability to misinformation and polarization of views[208].

Cyber-attacks will continue for myriad reasons, for example, hackers seeking reputational gains[209]. This includes attacks on election infrastructure (as Finland experienced in April 2019[210] on its online election results service), day-to-day, low-level strikes on social media and industrial control systems, transportation networks and health care providers because of old or poorly maintained infrastructure[211] as well as global cyber espionage campaigns against critical infrastructure[212, 213]. The Cambodian PM's Facebook account was reportedly hacked into in February 2019[214].

Disinformation actors are also resilient. They learn from mistakes and develop new strategies to sidestep[215] monitoring and other regulatory activities with evolving techniques. These techniques are enabled by[216] black-hat hackers that allow **for hidden** identities and locations through stolen identities available for sale on the

dark web[217], and even after discovery, to bounce back quickly. The playbook for disinformation is now "in the wild" for anyone to use, with the potential for other groups to build cheaper and quicker versions of the same capability[218]. Thus, disinformation tactics observed in the US and Europe can be expected to recur in other countries. Social media companies have announced that Bangladesh, Brazil, Venezuela and Iran have used social media content to widen political and social divisions. Other broad shifts include:

a. **Technical "hacks"**. This includes the use of VPNs, which can obscure physical locations, and linking accounts to international cell phone numbers that will better match the accounts' supposed location. It also includes breaking into computing devices to open social media accounts[219] and false flag attacks[220], where instead of hiding their identities, operatives paste a new, invented or borrowed one over it. This was the case in South America, where an Advanced Persistent Threat group masqueraded as official institutions to steal data [221]. Cyber experts[222] and researchers looking into suspected state-sponsored attacks have identified several evolutions in tradecraft. Some methods that have fallen out of action are re-invented to create something new[223]. Sometimes, much less tailored malware and less sophisticated command and control communications[224] are used to "blur the line between state-supported attacks and the activities of online activists and profiteering cyber criminals"[225]. This includes the use of publicly available hacking tools (available on cybercrime forums) and blending in by running attack traffic over widely used ports. A common method is wireless attacks[226] that include Bluetooth and other devices that rely on wireless connectivity as well as privatisation of offensive cyber-capabilities through cyber mercenaries. Further underscoring the role of cyber in future conflicts, Russia's State Duma has approved draft legislation to disconnect the entire country from the global Internet to test the robustness of Runet – its in-country internet service – and its cyber infrastructure[227] to prepare for potential isolation from the rest of the world[228]. This move is similar to what China did in the early 2000s when it built its own internet infrastructure[229]. Ahead of the country's elections, Indonesia's military commander ordered the military policy corps to upgrade its digital skills to deal with cybercrimes on digital and social media platforms[230].

b. **Content "hacks"**. This includes the following:

- home-grown misinformation[231] and disinformation[232];
- the shift from words to images, or "meme warfare", which are useful for non-native speakers who are looking to spread disinformation in another country, and more effective as they are more likely to avoid detection and removal by text-based filters,
- the intentional mixing of legitimate speech and influence operations, where the spread of information is disguised through proxies or through the artificial amplification of genuine voices whose statements support disinformation objectives[233], and
- coordinated fake activity[234].

Content "hacks" will be exacerbated by deep fakes, which are synthesised audio-visual content that has the potential to be highly realistic, especially when weaved into authentic content. With such technologies, even maps[235] – usually thought to be authoritative sources of information – could be manipulated.

c. **Platform "hacks"**. The slow-drip effect of content manipulation could wreak damage in the long-term. This can happen when disinformation is shared via short-time content[236] like Instagram stories or through dark social[a]. Dark social media will continue to grow[237] as social media users around the world seek more private spaces to communicate[238]. Younger audiences are moving towards private apps to read and discuss news[239]. Encrypted end-to-end mobile messaging applications are examples of a dark social medium[240]. WhatsApp, for example, has over a billion monthly active global users and was downloaded more times than Facebook in 2018[241]. While journalists have effectively used WhatsApp groups for good to distribute news when covering political development in places with censorship, the increased use of free applications and ability to broadcast messages has resulted in lynchings, sectarian clashes and waves of political misinformation and disinformation in what has been termed "WhatsApp Propaganda" [242] (see case studies of WhatsApp in India and Brazil). In Malaysia[243], the message of government corruption was spread via WhatsApp even as the details of the 1MDB scandal were too complex to resonate in rural towns and villages. In Indonesia, where 40% of the 142 million Internet users use WhatsApp, the app has been said to enable the spread of fake news in the country, for example, about child kidnappings. WhatsApp has

a Social sharing that is invisible to the public and occurs outside of what can be measured by web analytics platforms.

also been seen as responsible for the low success rate of the national vaccination campaign, after reports on the dangers of immunisation[244] were circulated on family group chats.

Responses

There is a need for multi-faceted solutions to the many dimensions of the problem[245] and a need to scope the issue to better identify the stakeholders involved and the processes required to respond at the structural, societal and governmental levels[246]. NATO STRATCOMCOE Director Jānis Sārts has used the term "digital security" to describe the space between the need to protect critical infrastructure and hardware, and the need to protect society against disinformation. Digital security points to the need to examine data-driven technological possibilities and its impact more deeply. As a start, it includes ensuring that content is securely transmitted from source to receiver and the accuracy of the content that is consumed, as well as the cognitive domain by which the society understands the information.

Governments are responding with legislation[247], collaboration and building in-country capabilities. For example, Europe's new General Data Protection Regulation imposes fines on companies if regulators are not notified about a data breach within 72 hours. The European Commission Action Plan will include a rapid alert system, which tracks election influence online[248]. The European External Action Service East StratCom task force's[b] budget will also be increased by 160% to 5 million euros. In SEA, ASEAN information ministers have agreed on an ASEAN Framework and Joint Declaration to Minimise the Harmful Effect of Fake News, with the majority of SEA countries enhancing or drawing up new cyber and information-related legislation[249].

Governments are also actively holding big technology companies to account[250] through closer partnerships, especially ahead of elections[251]. The EU, for example, launched a new code against disinformation

b The task force comprises a volunteer network of 500 NGOs, diplomats, think-tanks and media professionals who send in examples of fake news, which are then debunked in the task force's newsletter and on Facebook and Twitter.

in October 2018[252] that laid out a series of guidelines for social media companies. These companies have also testified at high-level governmental hearings and are being held accountable for how they might be addressing disinformation on their platforms[253]. This includes:

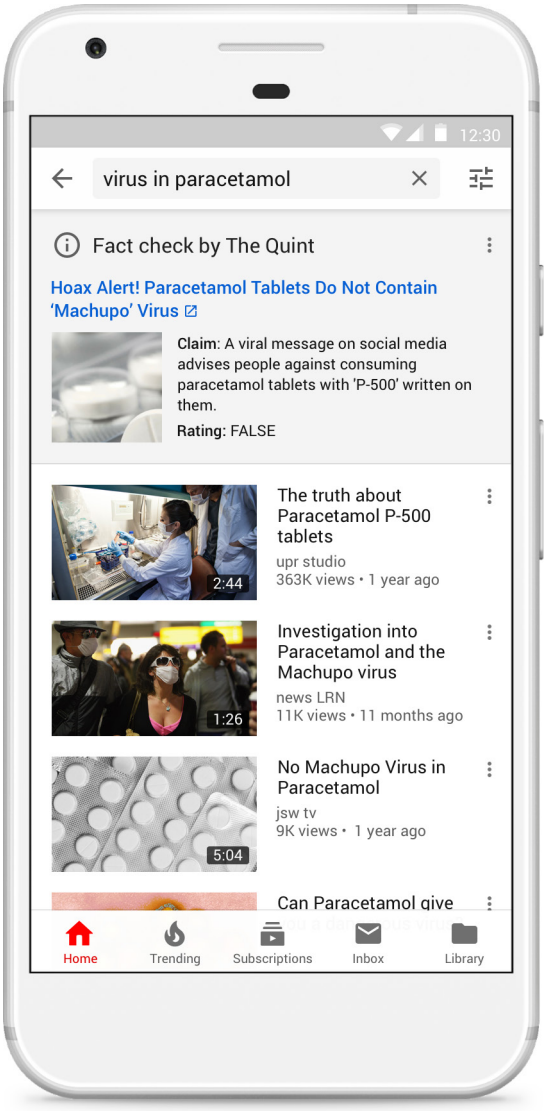
a. increasing the human and technological resources[254] for platform oversight, including an independent board planned by Facebook to handle "edge cases"[255]
b. greater transparency in political advertising[256]
c. strengthening partnerships with local fact-checking initiatives[257, 258],
d. setting up regional centres that directly support elections and providing digital literacy training[259],
e. free security tools that guard against cyber-attacks made available to political parties and organisations involved in elections[260] and
f. enhanced platform features

For example, YouTube launched "information panels" in India for a limited number of users, which provide fact checks when certain terms and phrases are searched for (see figure)[261, 262]. WhatsApp is reportedly[263] building a "search by image" function that will allow users to upload received images to Google to reveal similar messages that will enable users to better judge image authenticity.

Looking ahead, big tech companies can be expected to be a part of national conversations on regulation[264] and in the near-term will have to proactively work with governments and parliamentarians for greater transparency and accountability[265]. Governments will wield greater power when it comes to forcing these companies to comply with local norms[266], rules and regulations as non-compliance could result in a suspension of the company's right to operate. Even though big tech companies have addressed disinformation campaigns with some success[267, 268], these measures address symptoms rather than the root causes. Their revenue-generating models inadvertently provide a conducive environment for disinformation to thrive[a] [269]. Regulation of the technical architecture and mathematical formulas that determine what a user sees is being explored. Another development to look out for is the prosecution of unauthorised mobile activity. While early cases of such prosecution are targeted at those who steal and extort money from victims through SIM-card related manipulation[270], legislation down the road could be expanded to target those who peddle disinformation on the black market.

Civil society has also come on board to address the challenge, with cross-border grassroots efforts and media organisations collaborating or complementing government

a For example, to generate revenue through selling more advertisements, Facebook's algorithms push out "engaging" content based on users' past history, which could expand their exposure to more falsehoods. YouTube keeps users engaged by offering suggestions for videos, which can also be more extreme. Google's search algorithms could further encourage filter bubbles.



Information panels by YouTube

efforts to combat disinformation. For example, Lithuania and the Czech Republic have citizen "elves" who debunk falsehoods. Media organisations can also be expected to play a larger role in this area. For example, Comprova or "Prove it", a Brazilian ground-up initiative[271] comprising 24 national newspapers and television networks sought to verify and debunk[272] content that was being shared in politically motivated WhatsApp groups or Facebook pages in the lead up to the October 2018 elections. Other examples include the *New York Times*, which asked its readers[273] to send in a tip should they come across "false information being spread deliberately to confuse, mislead or influence voters ahead of the 2018 midterm elections" and the *Washington Post*, which launched a WhatsApp channel dedicated to its coverage of India's elections[274].

Staff of big tech companies are coming together in collective action to advocate against projects that are against the values they espouse[275]. Ahead of the May 2019 European Parliament elections, 19 media outlets from 13 countries collaborated on a fact checking project to address issues[276] related to the elections, legislation, politics and migration. In line with steps taken thus far at the national level, media in countries like Australia are examining data-related investments[277]and calling out politicians' associations with foreign state-affiliated associations and individuals.

Even while there is currently momentum to address disinformation on social media and elsewhere, policy makers must be aware of new challenges that come with new technologies and tools. In the next 10-20 years, visual and audio search will become more prevalent as social media companies like Facebook deepen capabilities in these areas[278].

Case Study: WhatsApp in India[279, 280, 281, 282, 283, 284, 285, 286, 287]

BACKGROUND

India is WhatsApp's biggest market, with 250 million (and growing) monthly users. Users in India forward more messages, photos, and videos than in any other country in the world. Up to 75% of users are in groups, organised by caste, income level and religion though most groups comprise fewer than 10 people. WhatsApp has teamed

THE ISSUE

Between January 2017 and July 2018, there were an estimated 33 deaths arising from 69 incidents linked to false rumours that circulated on WhatsApp. To defuse tensions and prevent further **rumour-mongering**, India shut down the Internet. There were 116 instances of **shut downs** in 2018, significantly more than the 79 instances in 2017, 31 instances in 2016 and 3 instances in 2015.

GOVERNMENT RESPONSE

India's Union IT Minister met WhatsApp's CEO, telling the latter to take "suitable steps" to prevent the misuse of the platform. The government has also requested WhatsApp to trace the origins of misinformation spread through the platform.

WHATSAPP'S RESPONSE

As a generic measure, from Jul 2018, WhatsApp users will only be able to forward messages to 20 others at once, from 100 previously. In India, the criteria are stricter. The upper limit is 5, and WhatsApp has removed the "quick forward" button from audio, video and images.

In addition, WhatsApp is working with local non-profit organisations, the Digital Empowerment Foundation and the NASSCOM (National Association of Software and Services Companies) Foundation, to hold training sessions for community leaders in 10 states where there have been cases of violence and where there will be state polls before the end of 2018, and to conduct digital literacy training.

up with Reliance Jho, a local telecommunications provider, to produce "WhatsApp" phones i.e. mobile handsets that come pre-installed with WhatsApp, and in some instances, offer access to only WhatsApp and selected apps, sometimes for as little as $20.

Ahead of upcoming elections, local fact checkers say misinformation has spread from Facebook to WhatsApp.

In March 2019, India published a set of draft regulations that would require platforms to break end-to-end encryption, and to algorithmically filter out objectionable content.

WhatsApp has also taken out print, radio and TV advertisements as well as held roadshows to ask users to check the veracity of information received as a forward before sharing it with others. It has also worked with a third-party fact-checking service and appointed a grievance officer for users to report complaints and concerns, including those about fake news.

Globally, WhatsApp says it removes more than two million suspicious accounts monthly.

Case Study: WhatsApp in Brazil [288, 289, 290, 291]

BACKGROUND

Internet access is very expensive in Brazil. A broadband connection can cost up to 15% of a household's income. Thus, mobile plans with unlimited data are rare. Instead, mobile carriers offer "zero rating" plans with free access to specific applications, usually Facebook, WhatsApp and Twitter. Nearly three in four Brazilian

THE ISSUE

WhatsApp was used significantly in the recent Brazilian elections. Supporters of presidential candidate Bolsonaro had "mass-shot" misinformation directly to millions of Brazilian phones in spam message campaigns, some smearing Bolsonaro's opponents. They included doctored photos, audio clips manipulated to misrepresent opponents' policies, and fake "fact-checks" discrediting authentic news stories.

Supporters included marketing firms that had used Bolsonaro's supporter database and third-party databases of phone numbers, targeting by location and income

THE CONSEQUENCE

Following these findings, independent agencies started investigating the impact of the smear campaign. Comprova, an amalgamation of 24 newsrooms in Brazil, used a tool called Zendesk, through which they could access WhatsApp's API to respond to citizens' queries as to whether a piece of information was factual. Aos Fatos, a Brazilian fact-checking start-up, opened a WhatsApp business account to receive

INDUSTRY AND GOVERNMENT RESPONSE

After Folha's investigative report was published, WhatsApp issued an op-ed to apologise. More than 100,000 spam accounts were banned, forwarded messages are clearly labelled as such, and rules on group messaging were tightened, e.g., limiting the message forwarding feature from 250 to 20 messages. WhatsApp has also partnered with Brazilian fact-checking organisations.

Ban more than 100,000 accounts[292]

internet users had these prepaid mobile-internet plans in 2016. In summary, most Brazilians have unlimited social media access but very little access to the rest of the Internet, with WhatsApp being used by more than half of Brazilians.

levels. An investigative report by Folha, a local broadsheet, found that some of these firms purchased contracts worth up to 3.2 million US dollars. Shortly before the elections, Folha found that a Brazilian business lobby had paid for the multi-million-dollar campaign. This was likely an illegal campaign contribution as companies are forbidden from donating to political campaigns and procuring a candidate's supporter database.

misinformation reports and send users verified content. Aos Fatos also crowd-sourced from over 6,000 WhatsApp subscribers more than 700 false or misleading posts. The researchers found that these posts were shared at least 3.5 million times from August to October in a coordinated way, moving from WhatsApp to Facebook and vice versa to create a perception that the information was universal and true.

Brazil's highest electoral court also created an advisory board on internet and elections to investigate disinformation in Brazil's 2018 elections, and propose regulations to limit its impact in future political processes.

Foreseeable trends

Increasing sophistication in disinformation and sharp power tools will be enabled by advances in technology, most notably artificial intelligence (AI). While AI is more about automation than intelligence[293] at the moment[294], it is here to stay. AI is being "democratised" through heavy investment by both the private[a] and public sectors[b] and open sourced algorithms and hardware[295], making it cheaper and less difficult to use. Developments in superconducting technology, which will contribute to higher levels of efficiency in data processing, will also translate into energy-saving data centres essential for superior and affordable computer processing power[c] that underpins AI operations.

AI is increasingly prominent as a solution to decades-long challenges like famine[296] and more pervasive in daily living[297] in areas such as e-commerce (e.g., product recommendations), communications (e.g., machine translation, chatbots), worker productivity[298], speech and facial recognition, education, and even in space[299]. It has powered digital assistants and voice-operated interfaces like Amazon's Alexa and Google Assistant and will be the basis for augmented reality[300] and virtual reality applications and technologies like self-driving cars. Healthcare-devices will be able to intuit deeper health data directly from users through cheap wearable devices[301].

In the area of cyber-attacks, corporations looking to prevent data breaches and fight hackers are looking to AI for a solution. Machine learning is able to search for common characteristics in millions of malware files to identify new attacks and track hackers. AI helps[302] overcome the challenge of identifying unknown threats, provides more precise verification in areas of identification, and is able to sift through alerts, determine which ones are most important, and then automate the responses[d].

AI, like other technological tools, is a double-edged sword, where for all its benefits, it could be leveraged for harm. It could

a In North America, the private sector invested some $15 billion to $23 billion in AI in 2016, according to a McKinsey Global Institute report. Facebook will double its AI research division to 400 staff by 2020.

b DARPA is investing $2 billion dollars over the next five years in new programmes advancing AI. This is in addition to $2bn dollars on AI R&D in the 2017 fiscal year. Current projects include cyber-security, the detection of AI-created fake audio or video, and "human-computer symbiosis" programmes targeting the interactions between people and machines.

c According to Top500, a website, China has overtaken the US in terms of the largest number of supercomputers, with 202 supercomputers compared to the US' 143. Japan, Germany, France and the UK are ranked third to sixth, with 35, 20, 18 and 15 supercomputers respectively. China also accounts for 35.4% of the world's supercomputing powers, compared to the second-placed US at 29.6%.

d For example, security systems can mine and analyse information on registries and online databases to find clues about the infrastructure that criminals set up to launch attacks, such as domain names of websites and IP addresses associated with the devices they use for hacking.

KEY TAKEAWAYS

- Increasing sophistication in disinformation and sharp power tools will be enabled by advances in technology, most notably AI
- A key development to watch is the possible bifurcation of the internet in the next decade, one led by the US and the other by China
- Disinformation and the use of sharp power is ultimately a national security problem. Any assessment of disinformation and sharp power must be taken and assessed together with developments in other domains
- Expect stronger, collective responses from governments and civil society to disinformation and sharp power

supercharge malware and phishing, which would allow authentic behaviours to be mimicked with greater accuracy. Machine learning models can be manipulated to carry out open-sourced attacks and trust attacks[303]. An AI hacking arms race is also possible, where instead of humans writing the code for cyber-attacks, software will begin to train other software[304]. There are also concerns over the rise of deep attacks[305], which is when AI-generated content is used to evade AI security controls, further increasing the risks of erroneous attribution, miscalculation and escalation. Data-powered devices and the inter-connectivity of IoT could also result in greater regularity of spyware and malware installed in phones[306] to at best, siphon off data and at worst, take over "smart" devices remotely[307] without the owner's knowledge and without leaving any trace. AI is already leveraged by cyber criminals, where attackers have used machine learning to tailor the language of a phishing email to individuals.

In the area of disinformation, the next generation of bots will look and behave increasingly like real people with advances in facial recognition[308] and natural-language processing[309] enabled by large data harvests. Given that one-to-one targeting of the target audience is already widely practised today, "smarter" propaganda bots could seek out, approach and cultivate vulnerable users over private chat channels. As bots learn to understand context and intent through analysing data, generative adversarial networks will become more adept at engaging in conversation and delivering customised false or biased information that tricks[310] or creates more

credence to entrench an individual's worldview. Language modelling (similar to how auto-complete works) can also generate coherent "news" reports[a, 311]from large volumes of unprocessed data[312].

Driving advances in AI applications are the US and China. While American companies lead in terms of AI patents with IBM and Microsoft taking top spots, Chinese research groups, universities and organisations hold 17 of the top 20 spots in total patent filings. China today has nine of the world's top 20 technology companies; the US has the other 11.[313] China has 227 of the world's 500 super computers; the US has 109[314]. The US has Silicon Valley; China is a major player in the semiconductor market[315] with heavy, albeit slowing, investment in the technology industry[316] and with AI increasingly permeating all strata of Chinese society with AI schools[317] and AI farms hiring large numbers of young people. A recent AI index confirms the predominance of the US and China in AI[318].

A key development to watch is thus the possible bifurcation of the internet in the next decade, one led by the US and the other by China. Google founder Eric Schmidt is of the view that it is an inevitable outcome given the scale of the companies and services being built in China, the immense wealth being generated and the Belt and Road Initiative. His view has been echoed by former Google China head Dr Kai Fu Lee, who has described the development as "splinternet", referring to a scenario where the internet is fragmented, governed by separate regulations and run by different services[319]. Such a development is not inconceivable. China's 829 million internet users, its technology sector's business models as well as domestic laws determining the players in its market have created an entirely alternative infrastructure for apps and content from the US. In SEA, Chinese firms have used blockchain technology and FinTech to engineer technological leapfrogs that have shaped a new kind of digital landscape that deviates from decades-old legacy banking systems and traditional frameworks used by firms such as Amazon and PayPal[320].

The ongoing developments on Huawei provide another indicator of how US-China rivalry might play out for the rest of the world. Even as the US persuades its allies and partners to exclude Huawei from building 5G networks, Huawei has announced that it will support Saudi Arabia's 5G development[321] and has deployed more than 10,000 5G sites across South Korea in collaboration with local conglomerate LG[322]. US allies, the United Arab Emirates[323] and Bahrain, where the US Navy's Fifth Fleet is headquartered, have also said that they would use Huawei's equipment to build wireless networks and commercial

a In this experiment, while the quotes and statistics in the AI-generated articles were made up, AI researchers acknowledge that it represents a groundbreaking shift in capabilities.

5G networks[324]. On the African continent, Huawei has built 70% of 4G networks, and its networks have been lauded for enabling millions to move into the formal financial system[325].

At the same time, both the US and China are pursuing their own form of international expansion. The United States has Google and Facebook with Australia, North America and Europe on board. China has focused on markets like SEA, the Middle East and Africa with products that are a better fit for the demographics there[326]. Mergers, acquisitions and consolidations across big tech companies in both will add further complexity and generate new dynamics (see examples below).

Example 1 – ByteDance and Musical.ly

China's ByteDance, which is behind the most downloaded app in 2018, TikTok, does not rely on social connections to figure out what to show users. To determine preferred content, it algorithmically analyses elements like (a) geo-location, (b) the faces, voices, music and objects in the video that a user watches for the longest time and (c) users' likes, comments and shares. In November 2017, ByteDance bought Musical.ly, a US-based music video app, which enabled it to successfully break into the US market.

Example 2 – Tencent and Reddit

China's Tencent has invested in US-based Reddit[327] which generated a vigorous online backlash among those concerned about possible censorship on Reddit[328]. Users have reported "the most active and aggressive" activity on the site by pro-China accounts to spread what is believed to be Chinese propaganda through coordinated "upvoting" and burying messages that are "anti-China"[329]. Reddit, currently disallowed in China, is known as the "front page of the Internet" because it allows users to share links on any subject and vote so the most popular content is most prominently seen.

AI supremacy has other implications on the information front, for example, in exerting political influence and shaping discourse domestically and internationally. With AI, virtual reality might be used to recreate major events from the past. The availability of such services can be expected to grow as the business of censorship becomes increasingly profitable[330].

The information space will be where the US and China continue to engage in tit-for-tat rivalry[331], against a backdrop of the warming Russia-China relationship[332, 333], where "…China and Russia have steadily converged in their positions on key regional strategic issues"[334]. The US has become

more proactive about cyber indictments, briefing the private sector on how Chinese-government backed hackers will have increasingly sophisticated cyber tools to steal proprietary data[335]. Cyber companies are also publicly attributing cyber-attacks to China[336] as challenging as attribution is.

Chinese cyber companies are mirroring the US' claims of the presence of professional hackers whose aim is to infiltrate key Chinese sectors[337]. New technology players in China's mobile sector such as Xiaomi[338, 339] and social media apps like TikTok[340, 341] developed by Chinese technology firms are also finding a growing[342] and receptive market beyond China; the global popularity of the latter matching that of Facebook and Instagram[343, 344].

The issues of disinformation and influence will continue in perpetuity. It is a global problem that plays on existing beliefs, values and sentiments[345]. The cross-pollination and cross-migration of tactics from country to country and region to region must be expected. The speed of technological advances means it will be increasingly challenging to distinguish between fact and fiction as well as between soft and sharp power. For government communications, key to navigating these complexities is a repeated articulation of the principles and values that the country stands by. This is the strong foundation on which layers of robust response mechanisms can stand. The mechanisms for early detection and effective response include key civil society stakeholders and legislation, continually sensitising the domestic population to the possibility of disinformation and influence, and staying alert.

. . . . .

Endnotes

1 (2019, March 13). Fake news about French "yellow vests" gets 100 million Facebook hits. *The Local France.*

2 Bogle, A. (2019, January 20). Instagram spreads political misinformation and Australian elections are vulnerable. *ABC*.

3 Funke, D. (2019, January 30). Want to get away with posting fake news on Facebook? Just change your website domain. *Poynter*.

4 Wang, S. (2019, February 26). Celebrities exploting data to boost social media popularity in China. *CGTN.*

5 Workman, M. & Hutcheon, S. (2019, March 15). Facebook trolls and scammers from Kosovo are manipulating Australian users. *ABC.*

6 Brokes, F. (2019, February 26). How to build a disinformation business.

7 NATO Stratcom COE (2018). The black market for social media manipulation.

8 Thomas, E. (2019, January 24). Hackers for hire pose growing international security risk. *The Strategist.*

9 Stone, J. (2019, February 27). 20-year-old pleads guilty to DDos-for-hire scheme that netted $550,000. *cyberscoop.*

10 Walker, C. & Ludwig, J. (2017, December 5). From 'soft power' to 'sharp power': Rising authoritarian influence in the democratic world.

11 Ibid.

12 Nye, J. S. (2018, January 4). China's soft and sharp power. *Project Syndicate.*

13 Cole, J. M. (2018, October). The hard edge of sharp power. *Macdonald-Laurier Institute*.

14 Haciyakupoglu, G. (2019, February 12). Southeast Asia's battle against disinformation. *The Diplomat*.

15 European Commission. (2018). *A multi-dimensional approach to disinformation*.

16 (2019, March 17). China knows America's greatest military weakness (and is planning to exploit it).

17 Cederberg, A., Eronen, P. & Mustonen, J. (2018). Regional cooperation to support National Hybrid Defence Efforts. (1/2017). Hybrid COE.

18 (2018, March 17). "Some indicators" Singapore was target of information warfare recently, says academic. *Channel Newsasia.*

19 Chau, D. (2019, January 15). Australia's fortunes are linked to China's economy – for better or worse. *ABC*.

20 UN World Tourism Organisation (2013, Apr 4). China – the new number one tourism source market in the world.

21 Nithin, C. (2018, September 26). Chinese tourists are Beijing's newest economic weapon. *Foreign Policy.*

22 (2018, October 9). Chinese tourist arrivals to Malaysia plunge during Golden Week. *The Straits Times.*

23 Roy, E. A. (2019, February 15). Huawei ban: Chinese state media claims tourists avoiding New Zealand. *The Guardian.*

24 Crawford, A. & Martin, P. (2018, October 19). China is forced to reconsider its route into Eastern Europe. *Bloomberg.*

25 (2018, September 19). Croatia, China and others sign tourism cooperation agreement.

26 (2018, September 21). Balkan countries spy potential in Chinese tourism. *Balkan Insight*.

27 (2017, March 17). China is whipping up public anger against South Korea. *The Economist.*

28 Coca, N. (2018, September 26). Chinese tourists are Beijing's newest economic weapon. *Foreign Policy.*

29 Shi, J. & Elmer, K. (2018, December 24). China renews warning against travelling to Sweden amid ongoing diplomatic row. *South China Morning Post.*

30 Matsumoto, F. & Sun, N. (2019, February 16). New Zealand tourism faces Huawei backlash from China. *Nikkei Asian Review.*

31 Li, X. (2019, February 13). Chinese travelers wary of NZ as strains increase. *Global Times.*

32 Yong, C. (2018, September 20). Select committee on fake news: Russian trolls divided societies and turned countries against one another. *Straits Times.*

33 (2018, October). *Deterrence by resilience – Are democracies proactive enough in protecting Western values* presented at the 2018 Riga Conference, Riga, Latvia.

34 Chellaney, B. (2019, April 26). Asia is the new ground zero for Islamist terror. *The Strategist.*

35 (2019, February 2). Philippines' Minister "certain" church bombers were Indonesians. Tempo.

36 (2019, March 10). Torture fears as Malaysia deports foreigners linked to terror group. *South China Morning Post.*

37 Koller, S. (2019, March 14). Counter-terrorism yearbook 2019: Western Europe. *Australian Strategic Policy Institute.*

38 Britton, B. (2019, February 17). Trump tells Europe to take back ISIS fighters, warns they could be released. *CNN*.

39 Marone, F. (2018, December 11). Foreign fighters: A problem for Asian countries, too. *Italian Institute for International Political Studies.*

40 (2019, February 18). Trump wants Europe to take back ISIS fighters. That's tricky. *ABC.*

41 Willsher, K. (2018, December 19). Returning jihadists "threaten new wave of terror in Europe". *Guardian.*

42 Speckhard, A. & Shajkovci, A. (2019, February 5). ISIS smuggler: Sleeper cells and "undead" suicide bombers have infiltrated Europe. *Daily Beast.*

43 (2019, April 17). Notre-Dame fire reveals tech companies' struggle to combat misinformation. *Washington Post.*

44 Rohmah, A. (2019, January 20). How social media helps spread extremist content in Indonesia, and what's being done about it. *South China Morning Post.*

45 Spong, R. (2018, September 18). Europol warns on Daesh cyber threat. *Arab News*.

46 Dunn, B. (2019, February 6). Investigative report: United cyber caliphate & Islamic State making returns to the hacking scene in 2019?

47 Ravndal, J. A. (2019, March 16). The dark web enabled the Christchurch killer. *Foreign Policy.*

48 Chalk, P. (2019, March 21). Where next for Jemaah Islamiyah? ASPI.

49 Swenson, K. (2019, March 21). She seemed like a normal web-savvy teen. She was actually waging "e-jihad" with ISIS hackers. *Wall Street Journal.*

50 (2019, January 31). How the Baltic States resist Russia. *The Economist.*

51 This is an infringement process outlined in Article 7 of the Treaty on EU for member states found violating EU fundamental rights.

52 Griffiths, J. (2019, February 19). In the new Malaysia, signs of an older, uglier politics. *CNN.*

53 Palatino, M. (2013, April 6). Don't let the flames of nationalism engulf Southeast Asia. *The Diplomat.*

54 Emmerson, D. K., & Simon, S. W. (1993). Regional issues in Southeast Asian security. Vol 4, No. 2. The National Bureau of Asian Research.

55 Laksmana, E. (2019, February 8). Journey to the east? The rebalancing of Indonesia's force structure. *ASPI*.

56 Maulia, E. (2019, April 1). Opposition candidate Subianto demands boost in Indonesia's military. *Nikkei Asian Review.*

57 SIPRI Military Expenditure Database.

58 Benner, T., Gaspers, J., Ohlberg, M., Poggetti, L. & Shi-Kupfer, K. (2018). Authoritarian advance – Responding to China's growing political influence in Europe. *GPPI & MERICS.*

59 European Convention on Human Rights.

60 Rajagopalan, M. (2018, January 2). The press is under attack in Southeast Asia, and it's only going to get worse. *Buzzfeed News.*

61 (2018, December 28). Best of the Interpreter 2018: Press freedom in Southeast Asia. *Lowy Institute*.

62 (2018, November 27). Using information security to explain why disinformation makes autocracies stronger and democracies weaker.

63 Tostevin, M. (2017, August 30). Vietnam's Facebook Dissidents Test the Limits of Communist State. *Reuters*.

64 (2018, January). Leading countries based on number of Facebook users as of July 2018 (in millions).

65 This covers online advertising, online gaming, video and music on demand.

66 Anadan, R. & Sipahimalani, R. (2018, November 19). Southeast Asia's accelerating internet economy. [Blog Post].

67 Singer, P. W. & Brooking E. (2018, October 2). The future of war will be "liked". *Foreign Policy.*

68 Layton, P. (2019, April 11). Non-technical measures can help reduce Australia's vulnerability to foreign influence. *ASPI*.

69 Kalsnesn, B. (2018, September). Fake News. *Oxford Research Encyclopedia (Communication)*.

70 Galante, L. & Ee, S. (2018). Defining Russian Election Interference: An analysis of select 2014 to 2018 cyber enabled incidents. *Atlantic Council Sowcroft Centre for Strategy and Security*.

71 (2018, February 22). Russian disinformation distorts American and European democracy. *The Economist.*

72 Hutchings, S. (2018, April 4). We must rethink Russia's propaganda machine in order to reset the dynamic that drives it. [Blog post]. *The London School of Economics and Political Science*.

73 Galeotti, M. (2018, March 5). I'm sorry for creating the "Gerasimov Doctrine". *Foreign Policy*.

74 Naughton, J. (2019, January 20). "The goal is to automate us": welcome to the age of surveillance capitalism. *The Observer.*

75 (2019, March 21). Health apps pose "unprecedented" privacy risks. *BBC*.

76 Teo, Y. (2019, March 24). The right of privacy: death by a thousand cuts? – Analysis.

77 Mirani, L. & Nisen, M. (2014, May 27). The nine companies that know more about you than Google or Facebook. *Quartz.*

78 Melendez, S. & Pasternack, A. (2019, March 2). Here are the data brokers quietly buying and selling your personal information. *Fast Company.*

79 DataLogix, for example, has global contacts in 9 of 10 SEA countries.

80 NATO StratCom Centre of Excellence (2019). *Malicious use of data*. Manuscript submitted for publication.

81 Cox, J. (2019, January 11). AT&T to stop selling location data to third parties after Motherboard investigation. *Motherboard.*

82 Zheng, W. (2019, February 2). Happy lunar new year: how big security data is scanning the holiday crowds in China. *South China Morning Post.*

83 Geltzer, J. & Jones, B. (2019, January 10). Weapons of mass consumerism: Why China wants your personal information.

84 PwC (2016). The wearable life.

85 Naughton, J. (2019, January 20). "The goal is to automate us": welcome to the age of surveillance capitalism. *The Observer.*

86 Australian Signals Institute (2018, October 29). Mike Burgess, Director-General ASD, speech to ASPI national security dinner.

87 Castellanos, S. (2018, March 30). Allstate's "Digital Colleague" Amelia answers questions for call centre rep. *The Wall Street Journal.*

88 (2019, January 30). Bangladesh to sue Philippine bank over $81M cyber heist.

89 Seals, T. (2019, January 30). Attackers can track kids' locations via connected watches.

90 (2019, January 14). Millions of Chinese CVs exposed on cloud server. *BBC*.

91 Barboza, T., James, M. & Ryes, E. A. (2018, December 30). Foreign cyberattack hits the printing of big US newspapers. *The Sydney Morning Herald.*

92 Kwai, I. (2019, February 7). Australian parliament reports cyberattack on its computer network. *New York Times.*

93 Whittaker, Z. (2019, April 16). Hackers publish personal data on thousands of US police officers and federal agents. *Tech Crunch.*

94 Cimpanu, C. (2019, February 12). Dunkin' donuts accounts compromised in second credential stuffing attack in three months. *ZDNet.*

95 Lyngaas, S. (2019, March 30). Toyota data breach affects up to 3.1 million customers. *Cyberscoop.*

96 (2019, January 30). Airbus reports breach into its systems after cyber-attacks. *Euronews.*

97 Cox, J. (2019, January 31). Criminals are tapping into the phone network backbone to empty bank accounts. *Motherboard*.

98 Hill, R. (2019, February 4). European commission orders mass recall of creepy, leaky child-tracing smart watch. *The Register.*

99 Cox, J. (2019, April 15). Hackers could read your Hotmail, MSN and Outlook emails by abusing Microsoft Support. *Motherboard.*

100 MacKinnon, A. & Groll, E. (2019, January 28). Hackers turn the tables on Russia. *Foreign Policy.*

101 Zengerle, P. & Chiacu, D. (2019, January 29). US spy chiefs break with Trump on many threats to the US. *Reuters*.

102 Ives, M. (2019, January 29). Data breaches dent Singapore's image as a tech innovator. *New York Times.*

103 Pamment, J.; Nothhaft, H.; Agardh-Twetman, H. & and Fjällhed, A. (2018). Countering Information Influence Activities: The State of the Art. *Lund University*.

104 Cormier, A. & Leopold, J. (2018, December 20). Russian agents sought secret US treasury records on Clinton backers during 2016 campaign. *Buzzfeed News.*

105 Paterson, T. (2018, October 5). Weaponisation of religious sentiment in Indonesia's cyber space. *The Strategist*. [Blog Post].

106 (2019, March 17). Jokowi campaign team says they're overwhelmed by hoaxes. *Tempo.*

107 Groll, E, (2018, October 19). The kingdom's hackers and bots. *Foreign Policy.*

108 Collins, B. & Wodinsky, S. (2018, October 19). Twitter pulls down bot network that pushed pro-Saudi talking points about disappeared journalist. *NBC News*.

109 (2019, April 1). Amazon CEO Jeff Bezos had phone hacked by Saudis "intent on harming him", security chief claims. *ABC.*

110 The US Department of Defense "Strategy for Operating in Cyber Space" refers to supply chain vulnerabilities as one of the central aspects of the cyber threat.

111 Braw, E. (2018, December 17). The GPS wars are here. *Foreign Policy*.

112 O'Dwyer, G. (2019, March 9). Norway accuses Russia of jamming its military systems.

113 Edwards, J. (2019, April 14). The Russians are screwing with the GPS system to send bogus navigation data to thousands of ships. *Business Insider.*

114 Sunak, R. (2017). Undersea cables: Indispensable, insecure. *Policy Exchange*.

115 Satariano, A. (2019, March 10). How the Internet travels across oceans. *The New York Times.*

116 Wroe, D. (2017, July 26). Australia refuses to connect to undersea cable built by Chinese company. *The Sydney Morning Herald.*

117 Tung, Liam. (2018, May 29). FBI to all router users: Reboot now to neuter Russia's VPNFilter malware. *ZDNet.*

118 Fire, R., Chase, S., & Freeze, C. (2018, December 5). CSIS director warns of state-sponsored espionage threat to 5G networks. *The Globe and Mail.*

119 (2018, November 29). Towards 5G. *European Commission*.

120 Ariffin, E. (2018, November 15). The potential of 5G in Southeast Asia. *The ASEAN Post.*

121 Xu, V. X. (2018, November 28). New Zealand blocks Huawei, in blow to Chinese telcom giant. *The New York Times.*

122 (2019, February 10). Pompeo to raise Huawei concerns on central Europe visit. *The Straits Times.*

123 Woo, S. & O'Keefe, K. (2018, November 23). Washington asks allies to drop Huawei. *The Wall Street Journal.*

124 (2018, December 19). Cyber security centre warns against use of Huawei devices in critical state infrastructure. *CZ*.

125 Hinshaw, D. (2019, January 11). Chinese Huawei executive is charged with espionage in Poland. *The Wall Street Journal.*

126 Emmott, R. Chee, F. Y. & Plucinska, J. (2019, January 30). Exclusive: EU considers proposals to exclude Chinese firms from 5G networks. *Reuters.*

127 (2019, January 17). Question of Huawei involvement in Latvian 5G network unresolved. *LSM.lv*.
128 Fadden, R. (2019, January 20). For the security of Canadians, Huawei should be banned from our 5G networks. *The Globe and Mail.*
129 Marinas, R. (2019, March 5). Exclusive: Romania's opposition seeks Huawei ban in infrastructure. *Reuters.*
130 (2019, January 10). Norway is considering whether to exclude Huawei from building 5G network, justice minister says, citing espionage fears. *South China Morning Post.*
131 (2019, February 4). Norway intelligence service issues Huawei warning. *France 24.*
132 (2019, January 13). Poland calls for "joint" EU-NATO stance on Huawei after spying arrest. *The Guardian.*
133 Chrysoloras, N. & Bravo, R. (2019, February 7). Huawei deals for tech will have consequences, US warns EU. *Bloomberg*.
134 Pancevski, B. & Germano, S. (2019, March 11). Drop Huawei or see intelligence sharing pared back, US tells Germany. *The Wall Street Journal.*
135 Chen, L. (2019, January 18). Oxford University suspends donor ties with Chinese tech giant Huawei as national security fears mount. *South China Morning Post.*
136 Power, J. (2019, March 14). British universities wrestle with anxiety over links to Chinese tech giant Huawei: investigation. *The South China Morning Post.*
137 Koetse, M. (2019, January 29). The Huawei case sparks anti-American, "support Huawei" sentiments on Weibo.
138 Koetse, M. (2019, February 21). CNN question "What do you think is the main reason behind the US campaign against Huawei?" goes trending on Weibo.
139 Thomas, E. (2019, March 5). The Huawei indictments: allegations and politics. *The Lowy Institute.*
140 Elmer, K. (2019, February 7). EU ban on Chinese technology in 5G revolution would hit trade, investment and cooperation, analysts say. *South China Morning Post.*
141 Chen, Q. (2019, March 11). Poland "faces 5G delay" by 2-3 years without Huawei: envoy. *Global Times.*
142 (2019, March 18). China rejects "abnormal" US spying concerns as EU pushes trade. *Reuters.*
143 Santora, M. & de Goeij, H. (2019, February 12). Huawei was a Czech favourite. Now? It's a national security threat. *The New York Times.*
144 Lian, Y. (2019, March 13). China requires its citizens and corporations to conduct espionage for the state. Did Huawei comply? *The New York Times.*
145 Santora, M. (2019, February 8). Huawei threatens lawsuit against Czech Republic after security warning. *The New York Times.*
146 (2019, March 7). Huawei sues US government over product ban. *BBC*.
147 Wang, Z. (2019, February 14). Huawei says doesn't wish to escalate further with Czech cyber watchdog. *Xinhua.*
148 (2019, February 25). Huawei seeks solution to Czech security warning, readies legal means: paper. *Reuters.*
149 Coleman, Z. (2019, February 24). Huawei comes out swinging against critics. *Nikkei Asian Review.*
150 Duke, J. (2019, February 14). Huawei heaps pressure on Telstra, Google over think tank funding. *The Sydney Morning Herald.*
151 Vanderklippe, N. (2019, March 26). Top Huawei executive says not even Xi Jinping could compel it to help China spy in other countries. *Globe and Mail.*
152 Doffman, Z. (2019, February 28). Huawei claims US onslaught is because their 5G technology prevents widespread NSA spying. *Forbes.*
153 Davidson, J. (2019, February 4). Are employees with Huawei phones a security risk for your company? *Financial Review.*
154 Vaswani, K. (2019, February 8). Why Asia isn't hanging up on Huawei. *BBC*.
155 Redrup, Y. (2019, February 4). How Huawei chairman John Lord plans to win in Australia despite 5G and NBN bans. *Financial Review.*
156 Stubbs, J. (2019, February 4). Exclusive: Huawei needs 3-5 years to resolve British security fears – letter. *Reuters.*
157 (2019, February 7). Huawei offers to build centre for cyber security in Poland. *Reuters*.
158 (2019, February 13). China's Huawei says ready to work with Poland to build trust. *Channel NewsAsia.*
159 Schulze, E. (2019, April 21). The US is attacking Huawei and China – without its own 5G strategy. CNBC.
160 Venzon, C. (2019, February 12). Philippines' wireless leader pushes on with Huawei 5G launch. *Nikkei Asian Review.*
161 Barfield, C. (2019, February 25). Huawei, 5G wireless, and the battle for Europe. *American Enterprise Institute.*
162 (2019, June 6). Huawei digs in for a drawn-out battle with Trump's white house. *Bloomberg.*
163 (2019, June 17). Huawei CEO says underestimated impact of US ban, sees US$100 billion revenue dip. *Channel News Asia.*
164 Stubbs, J. (2019, February 27). Europe calls for facts not fears in Huawei security row. *Reuters.*
165 Barnes, J. & Satariano, A. (2019, March 17). US campaign to ban Huawei overseas stumbles as allies resist. *The New York Times.*
166 Elmer, K. (2019, February 10). China-EU 5G research project to continue despite growing concerns about Huawei. *South China Morning Post.*
167 (2019, January 17). Germany considers barring Huawei from 5G networks. *Reuters*.
168 Scroxton, A. (2019, February 18). NCSC signals UK may take softer line on Huawei.

169 Hinshaw, D. & Woo, S. (2019, February 10). US campaign against Huawei faces challenge in Eastern Europe. *The Wall Street Journal.*

170 Follain, J. (2019, February 19). Trump's Huawei threats dismissed in Italian pivot toward China. *Bloomberg.*

171 Yang, X. & Wang, Z. (2019, February 16). Interview: Huawei aims to resolve cyber security controversy in Czech Republic in "friendly and reasonable way". *Xinhua.*

172 Heijmans, P. (2019, March 6). The US-China tech war is being fought in central Europe. *The Atlantic.*

173 Chua, K. H. (2019, February 13). Huawei gets vote of confidence from Philippines' Globe Telecom, which says security concerns somewhat overblown. *South China Morning Post.*

174 (2019, February 8). Thailand launches Huawei 5G testbed, even as US urges allies to bar Chinese gear. *CNBC.*

175 Blumenthal, D. (2018, December 12). Huawei is the doorway to China's police state. *National Interest*.

176 Howell, B. (2019, February 22). Security in the Internet of things: Is Huawei the only risk? *American Enterprise Institute.*

177 Columbus, L. (2016, November 27). Roundup of Internet of Things Forecasts and Market Estimates, 2016. *Forbes.*

178 Morell, M. & Kris, D. (2018, December 14). It's not a trade war with China. It's a tech war. *The Washington Post*.

179 Tham, J. (2018, December 13). Why 5G is the next front of US-China competition. *The Diplomat*.

180 Corera, G. (2018, December 19). Looking for China's spies. *BBC*.

181 Finley, K. (2019, January 17). Huawei's many troubles: Bans, alleged spies and backdoors. *Wired.*

182 (2018, October 10). China's Huawei takes aim at Qualcomm, Nvidia with new AI chips. *Bloomberg.*

183 Custer, C. (2018, August 30). Kai-fu Lee: China's next step toward its "AI future". *Tech in Asia.*

184 Liao, R. (March 12). China's Qutoutiao is burning millions of dollars to take on Tiktok parent. *Tech Crunch.*

185 Eddy, M. (2019, January 4). Hackers leak details of German lawmakers, except those on far right. *The New York Times.*

186 World Economic Forum (2019). The global risks report 2019.

187 Microsoft Asia News Centre (2018, May 18). Cybersecurity threats to cost organisations in Asia Pacific US$1.75 trillion in economic losses.

188 Ibid.

189 (2019, February 17). Germany sees big rise in security problems affecting infrastructure. *Reuters.*

190 (2019, February 20). New steps to protect Europe from continued cyber threats. [Blog Post]

191 Kanematsu, Y. (2018, August 18). Fears of Chinese cybermeddling grow after Cambodian election. *Nikkei Asian Review*.

192 Tham, I. (2018, August 7). SingHealth breach work of a typical state-linked group. *Straits Times.*

193 Watts, J. M. (2019, March 6). Group that stole Singapore health records persistently attacked country. *Wall Street Journal.*

194 Yu, E. (2019, March 6). Hacker group behind SingHealth data breach identified, targeted mainly Singapore firms. *ZDNet.*

195 Smith, R. & Barry, R. (2019, January 10). America's electric grid has a vulnerable back door – And Russia walked through it. *The Wall Street Journal.*

196 Barnes, J. E. (2018, December 21). Russians tried, but were unable to compromise midterm elections, U.S. says. *The New York Times.*

197 Mak, T. (2018, October 1). What can citizens to fight foreign disinformation campaigns? *NPR.*

198 Matlack, C. (2018, December 8). Pro-Russia social media takes aim at Macron as yellow vests rage. *Bloomberg.*

199 (2018, April 22). War of hashtags: #2019StillJokowi vs #2019ChangePresident. *The Jakarta Post.*

200 Dewi, S. W. & Swaragita, G. (2018, May 1). Why an anti-Jokowi hashtag could be his strongest foe so far. *The Jakarta Post.*

201 Cook, E. (2018, May 4). Indonesia election race heats up with social media war. *The Diplomat.*

202 Ruiz, T. (2018, April 20). Someone's building a Twitter bot army in Thailand. *Khaosod English*.

203 O'Byrne, B. (2018, April 2) Twitter bots begin following Southeast Asian opinion-makers. *The Phnom Penh Post*.

204 Russell, J. (2018, April 20). Twitter Doesn't Care that someone is building a bot army in Southeast Asia. *Tech Crunch.*

205 Harsono, N. (2019, February 26). Indonesia launches first Internet-only satellite with SpaceX rocket. *Jakarta Post.*

206 (2019, February 18). Malaysia second country to run Facebook's Terragraph trials. *The Star.*

207 WhatsApp suggests a cure for virality (2018, July 26). *The Economist*.

208 Silverman, C. (2019, April 3). Old, online and fed on lies: how an ageing population will reshape the internet. *Buzzfeed.*

209 Cimpanu, C. (2019, April 15). A hacker has dumped nearly one billion user records over the past two months. *ZDNet*.

210 (2019, April 11). DoS attack against election results portal under investigation in Finland. *Helsinki Times*.

211 Wheeler, T. (2018, September 12). In Cyber War, There Are No Rules. *Foreign Policy.*

212 (2019, September 19). Malicious Hacking Activity Increasingly Targeting Critical Infrastructure.

213 Musil, S. (2018, December 12). Global hacking campaign targets critical infrastruture. *CNET*.

214 (2019, March 1). Cambodia PM's Facebook hacked. *The Manila Times.*
215 Collins, B. (2018, November 6). In secret chats, trolls struggle to get Twitter disinformation campaigns off the ground. *NBC News*.
216 Cimpanu, C. (2019, February 17). Hacker puts up for sale third round of hacked databases on the dark web. *ZDNet.*
217 Williams, C. (2019, February 11). 620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts. *The Register.*
218 Stamos, A. (2018, Aug 22) How the US has Failed to Protect the 2018 Election – and Four Ways to Protect 2020.
219 Sebenius, A. (2019, March 9). Russian internet trolls are apparently switching strategies for 2020 US elections. *Time.*
220 Pawlak, P. (2018). Protecting and defending Europe's cyber space. In Popescu, N. & Secrieru, S. (Eds.). *Hacks, leaks and disruptions – Russian cyber strategies* (p.15).
221 Stone, J. (2019, February 21). Blind eagle, a new APT group, poses as Columbia's cyber police to steal business secrets. *Cyberscoop.*
222 Newman, L. H. (2018, November 20). Russia's elite hackers may have new phishing tricks. *Wired*.
223 (2019, February 28). Chinese cyber-espionage group customises old, public tools.
224 Leyden, J. (2018, December 17). State-backed hackers switch to inferior tactics to avoid being fingered for attacks. *The Daily Swig*.
225 Estonian Foreign Intelligence Service (2019). International security and Estonia 2019.
226 Violino, B. (2019, February 4). Cyberattacks to watch for in 2019. *ZDNet*.
227 Maza, C. (2019, February 11). Russia prepares for cyberwar by cutting all domestic Internet from the World Wide Web. *Newsweek*.
228 (2019, February 12). Russian lawmakers pass first draft of Internet-isolation legislation.
229 Jee, C. (2019, March 21). Russia wants to cut itself off from the global internet. Here's what that really means. *MIT Technology Review.*
230 Nasution, R. (2019, February 8). Indonesia military police corps ordered to upgrade digital skills. *Antara.*
231 Funke, D. (2019, April 17). Why fact-checkers couldn't contain misinformation about the Notre Dame fire. *Poynter.*
232 Kelly, J. (2019, March 29). When it comes to social media manipulation, we're our own worst enemy. *The Washington Post.*
233 Ferran, Lee. (2018, October 25). In social media "arms" race, tech giants chase evolving trolls and bots. *Abcnews*.
234 Gleicher, N. (2019, March 26). Removing coordinated inauthentic behaviour from Iran, Russia, Macedonia and Kosovo. [Press release].
235 Schwab, C. (2018, September 5). The Next Great Fake News Threat? Bot-Designed Maps. *Fast Company.*
236 Wardle, C. (2018). Forget deepfakes: Misinformation is showing up in our most personal online spaces. *Nieman Lab*.
237 Newman, N. (2018). Trust, misinformation and the declining use of social media for news: Digital News Report 2018. *Reuters Institute for the Study of Journalism.*
238 Rigillo, N. (2018, September 26). WhatsApp can be dangerous. *The Washington Post.*
239 Kalogeropoulos, A. (2018) The Rise of Messaging Apps for News. *Reuters Institute for the Study of Journalism.*
240 Some authors have argued that by using metadata and human content moderation, WhatsApp can stop the spread of false information and remove misinformation from its networks.
241 Singh, M. (2019, January 16). App Annie: WhatsApp is now Facebook's most popular app.
242 Dias, N. (2017, Aug 17). The era of WhatsApp propaganda is upon us. *Foreign Policy*.
243 Lim, I. (2019, January 20). Smartphone boom in rural Malaysia, WhatsApp gossip behind BN's GE14 downfall? *Malay Mail.*
244 (2019, January 16). Top 10 Indonesian hoaxes of 2018.
245 Vasu, N., Ang, B., Teo, T., Jayakumar, S., Faizal, M., and Ahuja, J. (2018). Fake News: National Security in the Post-Truth Era.
246 Sarts, J. (2019, March 25). Emerging trends in social media.
247 (2019, April 2). Factbox: "Fake news" laws around the world. *Reuters.*
248 (2018, December 6). European action plan against disinformation well-received in Estonia. *ERR*.
249 Ministry of Law Singapore (2019, April 1). New bill to protect society from online falsehoods and malicious actors. [Press Release]
250 (2019, January 29). EU urges internet firms to intensify fake news fight. *Channel NewsAsia.*
251 Chee, F. Y. (2018, September 26). Facebook, Google to tackle spread of fake news, advisors want more. *Reuters.*
252 Scott, M. (2018, October 7). Why we're losing the battle against fake news. *Politico*.
253 European Commission (2019, March 20). Code of practice against disinformation: Commission takes note of the progress made by online platforms and urges them to step up their efforts. [Press Release].
254 (2018, September 6). How Social Media Platforms Dispense Justice. *The Economist*.
255 Sin, Y. (2019, February 20). Facebook's independent oversight board could include Singapore experts.

The Straits Times.
256 Gill, P. & Moynihan, R. (2019, January 26). Here's how global tech giants are tackling "fake news" ahead of elections in the world's largest democracy. *Business Insider*.
257 Thaker, A. (2019, January 29). A Facebook team in Singapore will tackle the fake news threat to the 2019 Indian election. *Quartz India*.
258 Rai, S. (2019, April 22). How 11 people are trying to stop fake news in the world's largest election. *Bloomberg*.
259 Cohen, D. (2019, March 5). Facebook unveils the We Think Digital educational portal in Singapore.
260 Cimpanu, C. (2019, February 11). Microsoft and Google expand security tools to political parties in Canada, Europe. *ZDNet*.
261 Binder, M. (2019, March 8). YouTube starts to fact-check search results. *Mashable*.
262 Dixit, P. (2019, March 7). YouTube is rolling out a feature that shows fact-checks when people search for sensitive topics. *Buzzfeed News*.
263 (2019, March 13). WhatsApp Beta for Android 2.19.73: what's new?
264 Zuckerberg, M. (2019, March 30). Mark Zuckerberg: The internet needs new rules. Let's start in these four areas. *The Washington Post*.
265 Platiau, C. (2019, February 7). Google began censoring search results in Russia, reports say.
266 Horbelt, S. (2019, February 14). Indonesia threatened to ban all of Instagram due to this one gay artist.
267 Resnick. P. (2018, November 5). Unlike in 2016, there was no spike in misinformation this election cycle. *Nieman Lab*.
268 Allcott, H., Gentzkow, M. & Yu, C. (2018). Trends in the Diffusion of Misinformation on Social Media. Stanford University.
269 Tiku, N. (2018, December 4). Study revives debate about Google's role in filter bubbles. *Wired*.
270 (2019, February 6). More alleged SIM swappers face justice.
271 Kaiser, A. J. (2018, September 26). The Brazilian group scanning WhatsApp for disinformation in run-up to elections. *The Guardian*.
272 Sultan, Z, (2018, October 12). As Brazil fights election misinformation, fact-checking sites work overtime. *Columbia Journalism Review*.
273 (2018, September 17). If You See Disinformation Ahead of the Midterms, We Want to Hear From You. *The New York Times*.
274 (2019, April 17). The Washington Post launches WhatsApp channel on India's elections. *The Washington Post*.
275 Weigel, M. & Tarnoff, B. (2019, February 7). The stark political divide between tech CEOs and their employees. *The New Republic*.
276 Funke, D. & Benkelman, S. (2019, March 21). 19 fact-checkers are teaming up to fight misinformation about the EU elections. *Poynter*.
277 Seo, B. (2019, February 4). Alibaba's Aussie cloud push struggles against extra China tech scrutiny. *Financial Review*.
278 In Feb 2019, Facebook bought visual search start-up Grok Style. Citation: Johnson, K. (2019, February 8). Facebook acquires visual search start up GrokStyle.
279 Mclaughin, T. (2018, September 5). Disinformation is spreading on WhatsApp in India – and it's getting dangerous. *The Atlantic*.
280 Burgess, M. (2018, October 18). To fight fake news on WhatsApp, India is turning off the Internet. *Wired*.
281 (2018, 29 Aug) WhatsApp to train users on dangers of fake news.
282 (2018, December 7). Government meets with WhatsApp over tracing of fake news: source. *Channel NewsAsia*.
283 Rai, S. (2018, December 3). How Facebook uses "WhatsApp phones" to tap next emerging market. *Bloomberg*.
284 Thaker, A. (2018, December 4). WhatsApp is now betting on Indian primetime television to fight fake news. *Quartz India*.
285 (2019, March 18). The wrong way to fight fake news. *Bloomberg*.
286 Chaturvedi, A. (2019, March 18). WhatsApp, NASSCOM foundation join hands to help curb misinformation. *The Economic Times*.
287 Purnell, N. (2019, March 31). Fake news runs wild on WhatsApp as India elections loom. *The Wall Street Journal*.
288 Broderick, R. (2018, October 18). As Facebook shows off its "election war room", a massive "WhatsApp scandal hits Brazil". *Buzzfeed News*.
289 Belli, L. (2018, December 5). WhatsApp skewed Brazilian election, proving social media's danger to democracy.
290 Nalon, T. (2018, December 17). Here's how WhatsApp might fix its misinformation problem. *Poynter*.
291 Rinehart, A. (2018, November 29). What WhatsApp "API access" meant for Comprova.
292 Frier, S. & Camillo, G. (2018, October 19). WhatsApp bans more than 100,000 accounts in Brazil election. *Bloomberg*.
293 Metz, R. (2019, March 16). Why AI is still terrible at spotting violence online. *CNN*.
294 Schmelzer, R. (2018, November 19). Sorry, but your bots are stupid. *Forbes*.
295 Taulli, T. (2018, November 24). What to expect for AI in 2019. *Forbes*.
296 Holley, P. (2018, Sep 23). The World Bank's Latest Tool for Fighting Famine: Artificial Intelligence. *The Washington Post*.
297 Brynjolfsson, E., Hui, X. & Liu, M. (2018, Sep 18). Artificial Intelligence can Transform the Economy. *The Washington Post*.
298 Mochizuki, T. (2018, October 4). Your afternoon pick-me up, reimagined. *The Wall Street Journal*.

299 American Association for the Advancement of Science (2018, October 31). *Artificial intelligence bot trained to recognize galaxies* [Press Release].

300 Pierce, D. (2019, February 10). It's the real world – with Google maps layered on top. *Wall Street Journal.*

301 Bindley, K. (2019, January 6). Blood pressure, baby's pulse, sperm potency: home health devices are tracking more than ever. *The Wall Street Journal.*

302 Janofsky, A. (2018, Sep 18). How AI can help stop cyberattacks. *The Wall Street Journal.*

303 Byrne, C. (2019, January 7). The new ways we could get hacked (and defended) in 2019. *Fast Company.*

304 Hille, K. (2018, October 22). Taiwan to share Chinese hacks data with private companies. *Financial Times.*

305 Williams, O. (2018, December 31). The future of cyberattacks, according to the team behind the world's largest threat database. *New Statesman.*

306 (2018, September 8). Iran targeting civilians in mobile phone surveillance Ops. *The Malaysian Insight.*

307 Schapiro, A. A. (2018, Oct 2). Spyware hijacks smartphones, threatens journalists around the world. *Columbia Journalism Review.*

308 Roberts, J. (2019, March 27). The business of your face. *Fortune.*

309 Neudert, L. (2018, Aug 22). Future Elections May Be Swayed By Intelligent, Weaponised Chatbots.

310 Tucker, P. (2019, March 31). The newest AI-enabled weapon: "deep-faking" photos of the earth.

311 Piper, K. (2019, February 14). An AI helped us write this article. *Vox.*

312 (2019, February 14). Better language models and their implications. [Blog Post]

313 Sullivan, J. (2018, October 1). Engaging with China: Eyes wide open. *Forbes.*

314 Clark, D. (2019, March 18). Racing against China, US reveals details of $500 million super computer. *The New York Times.*

315 Trilo, P. & Webster, G. (2018, December 7). China's efforts to build the semiconductors at AI's core. *New America.*

316 (2019, March 7). China's formerly white-hot tech sector is in the doldrums. *The Economist.*

317 Zhao, R. (2019, April 1). You can now major in "artificial intelligence" in China.

318 (2019, June 2019). US and China lead new index on AI development the Cambrian AI Index. *Straits Times.*

319 Kharpal, A. (2019, February 3). The "splinternet": How China and the US could divide the internet for the rest of the world. *CNBC.*

320 Capri, A. (2018, May 3). China's major tech firms will dominate SE Asia's emerging markets: who wins and who loses? *Forbes.*

321 Chu, D. (2019, February 22). Huawei to help Saudi Arabia become world's top 5G countries. *Global Times.*

322 Reichert, C. (2019, February 25). MWC 2019: Huawei builds 5G network across Korea with LG Plus. *ZDNet.*

323 Satariano, A. (2019, February 26). UAE to use equipment from Huawei despite American pressure. *The New York Times.*

324 Cornwell, A. (2019, March 26). Bahrain to use Huawei in 5G rollout despite warnings. *Reuters.*

325 Mackinnon, A. (2019, March 19). For Africa, Chinese-built internet is better than no internet at all. *Foreign Policy.*

326 Gardels, N. (2018, Sep 24). The Great AI duopoly. *The Washington Post.*

327 Constine, J. (2019, February 11). Reddit confirms $300m series d led by China's Tencent at $3B value. *Tech Crunch.*

328 (2019, February 11). Reddit: Censorship fears spark criticism of Tencent funding reports. *BBC.*

329 Silverman, C. & Lytvynenko, J. (2019, March 14). Reddit has become a battleground of alleged Chinese trolls. *Buzzfeed.*

330 (n.d.). The Chinese Communist Party's newspaper has spun out an incredibly lucrative censorship business.

331 Wang, C. (2019, March 19). AI race between China, US shifts to talent in battle for dominance. *Global Times.*

332 Miller, C. (2019, March 1). The new Cold War's warm friends. *Foreign Policy.*

333 Drenzer, D. (2019, April 3). China and Russia are not breaking up anytime soon. *The Washington Post.*

334 Franchell, B. (2019, March 29). Foreword: The China-Russia entente and the Korean peninsula. *The national bureau of Asian Research.*

335 Lyngaas, S. (2019, February 6). DHS briefs industry on shift in Chinese hacking that "increases the risk for all of us".

336 Lyngaas, S. (2019, February 6). Hack of billion-dollar Norwegian firm is tied to Chinese espionage group APT10.

337 Needlam, K. (2019, February 19). China the world's biggest hacking victim, Chinese report says. *The Sydney Morning Herald.*

338 (2019, February 9). Xiaomi MI 9 certified in Singapore, hints at release outside of China.

339 Lancaster, M. (2019, February 27). Xiaomi MI 9 European availability reaches Netherlands.

340 Tik Tok, which merged with a California-based company in 2018, was fined by the US government in Feb 2019 for illegally collecting data on children below 13 years old. Reference: Timberg, C. & Romm, T. (2019, February 27). The US government fined the app now known as Tik Tok $5.7 million for illegally collecting children's data. *The Washington Post.*

341 Biancotti, C. (2019, January 11). The growing popularity of Chinese social media outside China poses new risks in the

West. *Pearson Institute for International Economics.*
342 Kwang, K. (2019, February 7). China's TikTok video app brings old-school social media fun back to Singapore users. *Channel NewsAsia.*
343 Lucas, L. (2019, March 4). China's TikTok passes 1bn global downloads. *Financial Times.*
344 Ramli, D. & Banjo, S. (2019, April 18). The kids use Tik Tok now because data-mined videos are so much fun. *Bloomberg.*
345 Buchanan, E. (2019, April 11). The great Brexit distraction. *Foreign Policy.*

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org