GOVERNMENT RESPONSES TO MALICIOUS USE OF SOCIAL MEDIA

Samantha Bradshaw, Lisa-Maria Neudert, Philip N. Howard

ISBN 978-9934-564-31-4
Samantha Bradshaw is a D.Phil. Candidate at the Oxford Internet Institute and a researcher on the Computational Propaganda Project at Oxford University. Samantha has published several journal articles and public policy papers at the nexus of technology, governance and politics. Samantha holds an MA in Global Governance and a BA (joint-honours) in political science and legal studies from the University of Waterloo.

Lisa-Maria Neudert is a DPhil candidate at the Oxford Internet Institute and a researcher with the Computational Propaganda project. Lisa-Maria holds a MSc in Social Science of the Internet from the University of Oxford, a BA in Communication Science from the Ludwig-Maxmilians-University in Munich and an Honors Degree in International Diplomacy from Georgetown University. She was selected as a Fulbright scholar.

Philip N. Howard is a professor and writer. He has written numerous empirical research articles, and published in a number of disciplines, on the use of digital media for both civic engagement and social control in countries around the world. Howard is a statutory Professor of Internet Studies at the Oxford Internet Institute and a Senior Fellow at Balliol College at the University of Oxford.
INTRODUCTION

The manipulation of public opinion regarding social media during critical moments of political life has emerged as a pressing policy concern. During the 2016 Presidential Election in the United States and the Brexit Referendum in the United Kingdom reports about the malicious use of social media and the exploitation of personal data for political gain rose to global prominence, prompting legal and regulatory intervention by governments around the world. But the use of social media to undermine democracy has long been a concern for NATO and the European security community.

Since 2016, at least 43 countries around the globe have proposed or implemented regulations specifically designed to tackle different aspects of influence campaigns, including both real and perceived threats of fake news, social media abuse, and election interference. Some governments are in the early stages of designing regulatory measures specifically for digital contexts so they can tackle issues related to the malicious use of social media. For others, existing legal mechanisms regulating speech and information are already well established, and the digital aspect merely adds an additional dimension to law enforcement.

Our research team conducted an analysis of proposed or implemented regulations and identified a number of interventions. Some measures target social media platforms, requiring them to take down content, improve transparency, or tighten data protection mechanisms. Other measures focus on civil actors and media organisations, on supporting literacy and advocacy efforts, and on improving standards for journalistic content production and dissemination. A third group of interventions target governments themselves, obligating them to invest in security and defence programs that combat election interference, or to initiate formal inquiries into such matters. Finally, a fourth group of interventions take aim at the criminalisation of automated message generation and disinformation.

There has long been a tension between allowing free speech to flourish while limiting the spread of undesirable forms of online content promoting hate, terrorism, and child pornography. Blocking, filtering, censorship mechanisms, and digital literacy campaigns have generally been the cornerstones of regulatory frameworks introduced in most countries, but with the growing challenges surrounding disinformation and propaganda new approaches for addressing old problems are flourishing. This paper provides an updated inventory of these new measures and interventions.
METHODOLOGY

We have created an inventory of the various government initiatives to tackle the multi-dimensional problems related to the malicious use of social media, such as the spread of dis/misinformation, automation and political bots, foreign influence operations, the malicious collection and use of data, and the weaponisation of attention-driven algorithms. We identified cases in three stages. First, we looked at the top-100 countries with the largest number of Internet users in 2016. Based on this list, we conducted an analysis using keywords related to social media manipulation, including fake news, political bots, online or computational propaganda, misinformation, and disinformation. We then searched for these terms in combination with our top 100 countries, as well as the keywords ‘law’, ‘bill’, ‘legislation’, ‘act’, and ‘regulation’ in order to identify instances of government responses to social media manipulation.

Using this approach, we identified a total of 43 cases that are either complete, in progress, or have been dismissed in which governments have introduced regulation in response to the malicious use of social media since 2016. The case studies were last updated in October 2018. We then drafted short case studies for each country to be reviewed by country-specific experts who ensured the accuracy of our information and provided additional country-specific information that could not be gleaned from non-English language bills or news sources. A summary of the various legal and regulatory mechanisms we identified can be found in Appendix 1.

We limited our analysis to legal and regulatory interventions designed in response to social media manipulation, and focused strictly on new or recently updated legal measures proposed in response to allegations of foreign interference in elections around the world, starting with the US election in 2016. For example, both Ghana and Gambia have long-standing legislation designed to tackle digital misinformation, but these countries are not included in our analysis since this legislation was not designed in response to the growing challenge of malicious use of social media. We have not reviewed measures where government legislative or executive branches have expressed interest in regulation, but still lack concrete proposals. We have also excluded pre-existing security-related solutions to disinformation or online propaganda, laws around hate speech, censorship, political campaigning or advertising, foreign intelligence, and other interventions that may have a digital aspect, but are not directly aimed at the growing proliferation of social media manipulation in democracies. Finally, we have not looked into regional or transnational initiatives, but have highlighted some of the more significant efforts initiated by the European Union, NATO, and other international organisations.
ANALYSIS OF MEASURES

Since 2016, 43 governments have proposed or implemented legal or regulatory responses to social media manipulation. A number of countries facing upcoming elections are at the forefront of addressing these issues. The following section explores the themes that have emerged from these various interventions. We have grouped the measures into four categories: (1) Measures Targeting Social Media Platforms, (2) Measures Targeting Offenders, (3) Measures Targeting Government Capacity, and (4) Measures Targeting Citizens, Civil Society and Media Organisations.

Measures Targeting Social Media Platforms

Content Takedowns by Social Media Platforms
Social media companies have become the central information highway for political news and information. Government-monitored removal, blocking, and filtering of illegal content online is a well-established practice in both democracies and authoritarian regimes. Whereas in the past, content takedown enforcement was managed through an Internet Service Provider, governments must now turn to social media companies to remove information deemed harmful. However, given their continued abuse and misuse by politically and economically motivated actors, social media companies have yet to implement sufficient countermeasures against the malicious use of their platforms.

A number of countries are in the process of approving legislation or have already established frameworks designed to address the spread of illegal or undesirable content on social media platforms. These measures typically put the onus on the platform to remove content or shutdown accounts with little government oversight and guidance. Countries such as Brazil, Germany, and South Korea have established or are proposing laws that require social media platforms to take down content deemed illegal by the state, or face hefty fines. However, our analysis concludes that some countries, such as Russia, Vietnam and Zimbabwe, are using similar legislation to legitimise further censorship of speech online. In democracies, there is also a risk of 'collateral censorship' where a lack of transparency around content moderation and blocking could lead to chilling effects in the digital public sphere.

Advertising Transparency
Political advertising in print and broadcast media is subject to tight regulations and standards that ensure the efficiency and
fairness of democratic processes. Several countries have laws regulating campaign spending, messages, scope, and timing. However, as campaigning has ventured into the online realm, with billions of dollars spent on advertising, engagement campaigns, and the curation of voter profiles, lawmakers have yet to extend the same scrutiny to digital contexts. Increasingly, regulators are becoming aware of issues surrounding the transparency of online advertising and are seeking to address them. Some proposed measures for online advertising transparency focus on improving transparency around the purchasers of advertising space and target audiences. The US, France, and Ireland require social network companies to collect and disclose information to users about who paid for an advert or piece of sponsored content, and to share information about the audience that advertisers target. Other efforts are designed to block foreign spending on domestic political campaigns. In addition, advertising giants such as Facebook and Google are engaging in self-regulatory measures, promising more transparency regarding advertising messages and their senders.

Data Protection
The malicious use of social media relies on highly data-driven targeting. Big data is leveraged to strengthen the impact and reach of messages using proprietary software, as well as tools and ad tech features available through private companies. The Cambridge Analytica revelations demonstrated that the data of millions of users has been used to disseminate manipulative news items and polarising information. Data breaches during the last two years at Google and Facebook have underscored the importance of data security, as the data of millions of users has been exposed. Despite these pressing challenges, only a few countries have chosen to implement new data protection measures to combat social media manipulation. Some national initiatives, such as Vietnam's data localisation law, which requires social media data to be stored within the borders of the state, can be used to further governmental control over citizen data. In Europe, the General Data Protection Regulation (GDPR), which came into effect in May 2018, covers many of the data protection issues related to citizens based in the European Union. However, a global framework for data protection has yet to emerge, and even GDPR has gaps in coverage and enforcement that limit its effectiveness to address all problems associated with social media manipulation and data-driven targeting. For example, it remains unclear how social networks with international user bases will apply GDPR in local contexts. Following the implementation of GDPR, Facebook moved the data of 1.5 billion users out of Ireland so users outside of Europe cannot challenge privacy decisions under European law. And while GDPR helps protect elements of privacy for European citizens, it also has unintended consequences to the free flow of information where newspapers and other sources of information are no longer accessible to users based in Europe.
**Measures Targeting Offenders**

**Criminalisation of Disinformation and Automation**

In addition to requiring social media platforms to remove content, much proposed and implemented legislation concerns individuals who produce and/or share disinformation online. Several countries such as Egypt, Indonesia and Kuwait have strengthened government competencies to legally prosecute offenders, resulting in the criminalisation of posting and spreading disinformation online. Monetary fines and increased prison sentences are among the measures for deterring and prosecuting offenders. Other bills, such as in Ireland and California, do not merely prosecute the originators of online disinformation, but also those who maliciously disseminate and amplify it through automation. Rooting their countermeasures in various legal arguments surrounding national security, the disturbance of national order, hate speech, and the provision of false and misleading information, Australia, Indonesia, Ireland, Italy, Malaysia, and the Philippines are among the countries that rely on criminal penalties and fines for producing or sharing disinformation, or for creating and launching a bot campaign targeting a particular political issue. Instances of the misuse of these frameworks to crackdown on political dissidents, minorities, and human rights defenders have already taken place in Iran, Malaysia, Russia, Saudi Arabia, and Tanzania.

**Expanding the Definition of Illegal Content**

The malicious use of social media is a relatively new phenomenon that takes advantage of the scale, targeting opportunities, and ease and speed of content creation and dissemination over the Internet and social media. Existing legislation is often viewed as inadequate in addressing new dynamics and content forms in our continuously evolving information ecosystem. This prompts regulators to revise bills, sharpen enforcement, and propose novel definitions of illegal content online. Thus far, it has been the world's democracies that have pioneered the redefinition of legal frameworks in connection to illegal content. Australian legislation authorises strict punishment for anyone found guilty of communicating information against the 'national interest', particularly with regard to false or distorted content. Germany’s *Network Enforcement Act* explicitly extends the application of the German Criminal Code in cases where freedom of speech and constitutional values are in conflict. And France defers the legal interpretation of fake news and online content to its judiciary, whereby judges rule on prominent untruthful content on a case-by-case basis. Definitions around illegal forms of content in authoritarian countries are often wide-ranging to capture a diverse

---

1) Although Malaysia has since repealed its fake news law, the legislation was widely criticised by human rights activists for providing a new tool for censoring speech online.
collection of information, however, countries such as Saudi Arabia and Egypt have introduced new and even broader definitions of illegal content online.

Measures Targeting Citizens, Civil Society and Media Organisations

Media Literacy and Watchdogs
Countermeasures surrounding media literacy and watchdogs to fight social media manipulation generally focus on long-term educational and advocacy efforts. Tasked with improving public literacy in regard to digital information, practical skills in browsing the Internet for information, and evaluating the quality of content, many countries have begun funding long-term strategies to counter the malicious use of social media. For example, Croatia has funded a new media literacy initiative, rather than simply limiting the spread of malicious information online. Similarly, France is expanding the obligations of media watchdogs to improve public information literacy and exercise scrutiny over non-governmental institutions. Increasingly, these measures focus on improving public literacy, however there are still only a small number of initiatives to bring these skills to government institutions and public servants.

Media Accreditation and Journalistic Controls
Several governments have developed tighter controls over their national media in response to a changing media landscape and the spread of disinformation. Strategies, such as the United States’ enforcement of the Foreign Agents Registration Act, seek to bolster quality journalism while improving transparency regarding information sources. However, other media accreditation strategies are deployed by restrictive regimes to exercise control over journalistic production of all content. For example, Iran and Tanzania have introduced or proposed bills to regulate journalistic research and production of content, resulting in ongoing public scrutiny in these countries regarding limitations on the freedom of the press.

Measures Targeting Government Capacity

Parliamentary Inquiries and Congressional Hearings
Parliamentary inquiries are a government tool often established in emergent or especially problematic political contexts. Inquiries are typically institutionalised within a country’s legal framework, providing a committee with certain tasks and competencies. They are often the starting point for further regulation and action through the creation of policy briefs and recommendation documents. Following the Cambridge Analytica scandal, several countries launched parliamentary inquiries to understand the consequences of social media on democracy. In the UK the Digital, Culture, Media, and Sport Committee carried out an inquiry into the misinformation and digital manipulation of the public and its consequences. As a result of their initial report, the government is developing a
range of regulatory and non-regulatory initiatives to address recommendations such as updating electoral laws for the digital age, protecting personal data, and empowering the electoral commission. In Singapore, the parliament unanimously voted to establish a Select Committee to tackle fake news; the committee has proposed a number of measures, including empowering government to make executive decisions about content moderation and disrupting the flow of digital advertising revenue. In Canada, the House of Commons has recently launched an investigation into data breaches and election integrity, and is carrying out research for its final report. In the United States, a series of congressional hearings have been investigating Russian interference in the 2016 election, the impact of the Cambridge Analytica scandal, and the political and market power of social media platforms in the digital era. At a regional level, the European Union also established a High-Level Expert Group that brought together government representatives, academics, and issue-area experts to put forward recommendations on combating the malicious use of social media, including media literacy, empowering journalists, and protecting the diversity and sustainability of the news ecosystem.

Security and Defence
Several governments have established cybersecurity and information security units within their militaries to address foreign interference in elections. Tasked with improving cybersecurity and citizens’ rights online, these units engage in both the defence of informational infrastructure and strategic cyber warfare operations. As threats of social media manipulation and the spread of misinformation hit the global public agenda, some governments are mandating security and defence authorities to combat these threats, such as Australia’s Election Integrity Task Force. Countermeasures include systematic observation of the online space, identifying offenders, analysing strategies of offense, reporting on problematic information as it rises to prominence, and debunking falsehoods. But security and defence operations remain opaque, with the scope of surveillance and intervention remaining unknown to the public. Brazil, the Czech Republic, Sweden, and Vietnam have introduced or proposed governmental authorities or military units tasked specifically with monitoring and combating various aspects of the malicious use of social media.

Monitoring and Reporting
Some government initiatives focus on monitoring the information ecosystem and providing users with portals to report misinformation. At a regional level, The East StratCom Task Force provides monitoring, training, and capacity building for disinformation campaigns that affect European Union institutions and member state governments. The G7 countries are also working on developing a Rapid Response Mechanism to combat disinformation and foreign interference in
elections. Italy provides one example of a national monitoring initiative where law enforcement has established a monitoring portal citizen can use to report instances of fake news for investigation in the run up to the next election. Another form of monitoring initiative involves taxing citizens for using social media. For example, in Uganda the government has implemented a tax system to generate revenue and limit the amount of 'gossip' being shared on social media. Thus, to access certain online platforms, citizens are expected to pay approximately 200 Uganda shillings (0.05 EUR) per day to use the platforms.
CONCLUSION

There is no simple blueprint solution to tackling the multiple challenges presented by the malicious use of social media. In the current, highly-politicised environment driving legal and regulatory interventions, many proposed countermeasures remain fragmentary, heavy-handed, and ill-equipped to deal with the malicious use of social media. Government regulations thus far have focused mainly on regulating speech online—through the redefinition of what constitutes harmful content, to measures that require platforms to take a more authoritative role in taking down information with limited government oversight. However, harmful content is only the symptom of a much broader problem underlying the current information ecosystem, and measures that attempt to redefine harmful content or place the burden on social media platforms fail to address deeper systemic challenges, and could result in a number of unintended consequences stifling freedom of speech online and restricting citizen liberties.

As content restrictions and controls become mainstream, authoritarian regimes have begun to appropriate them in an attempt to tighten their grip on national information flows. Several authoritarian governments have introduced legislation designed to regulate social media pages as media publishers fine or imprison users for sharing or spreading certain kinds of information, and enforce even broader definitions of harmful content that require government control. As democratic governments continue to develop content controls to address the malicious use of social media in an increasingly securitised environment, authoritarian governments are using this as a moment to legitimise suppression and interference in the digital sphere.

In the future, we encourage policymakers to shift away from crude measures to control and criminalise content and to focus instead on issues surrounding algorithmic transparency, digital advertising, and data privacy. Thus far, countermeasures have not addressed issues surrounding algorithmic transparency and platform accountability: a core issue is a lack of willingness of the social media platforms to engage in constructive dialogue as technology becomes more complex. As algorithms and artificial intelligence have been protective of their innovations and reluctant to share open access data for research, technologies are blackboxed to an extent that sustainable public scrutiny, oversight and regulation demands the cooperation of platforms. Governments have put forward transparency requirements regarding political advertisements online, such as the Honest Ads act in the United States. While some platforms have begun to self-regulate, their self-prescribed remedies often fall short of providing efficient countermeasures and enforcement mechanisms.
Such legislation is important for addressing issues related to particular aspects of foreign interference in elections, such as the artificial inflation of hot button issues, or junk news designed to suppress voter turnout. However, many threats to the democratic process also come from within, and there is currently a lack of transparency regarding how misinformation spreads organically through likes and shares, and also around how political parties use social media to advertise to voting constituencies. Finally, while Europe's GDPR helps prevent some of the challenges arising from the malicious use of social media, and could have helped protect and remedy scandals such as Cambridge Analytica, data protection laws remain highly fragmented. Likeminded democratic governments should work together to develop global standards and best practices for data protection, algorithmic transparency, and ethical product design.
Appendix 1: Summary of National Legal and Regulatory Measures Taken by Governments in Response to the Malicious use of Social Media (2016–2018)
<table>
<thead>
<tr>
<th>Country</th>
<th>Measure</th>
<th>Challenge</th>
<th>Status</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSTRALIA</td>
<td>Draft Bill, Parliamentary Inquiry, Government Task Force (Election Integrity Task Force)</td>
<td>Foreign Interference, Content harmful to national interest</td>
<td>Drafted, Implemented</td>
<td>Implemented</td>
</tr>
<tr>
<td>AUSTRIA</td>
<td>Court Ruling</td>
<td>Hate Speech</td>
<td>Implemented</td>
<td>Non-freedom</td>
</tr>
<tr>
<td>BELGIUM</td>
<td>Government Task Force</td>
<td>Fake News</td>
<td>Implemented</td>
<td>Partially free</td>
</tr>
<tr>
<td>BELARUS</td>
<td>Legal Amendment</td>
<td>Media Regulation</td>
<td>Implemented</td>
<td>Implemented</td>
</tr>
<tr>
<td>BRAZIL</td>
<td>Government Task Force, Draft Bills</td>
<td>Fake News</td>
<td>Implemented, Proposed</td>
<td>Implemented</td>
</tr>
<tr>
<td>CAMBODIA</td>
<td>Legislation</td>
<td>Fake News</td>
<td>Criminalisation</td>
<td>Criminalisation</td>
</tr>
<tr>
<td>CANADA</td>
<td>Parliamentary Inquiry</td>
<td>Foreign Interference, Data Protection</td>
<td>Implemented</td>
<td>Data Protection</td>
</tr>
<tr>
<td>CHINA</td>
<td>Government Task Force</td>
<td>Content harmful to national interest</td>
<td>Implemented</td>
<td>Implemented</td>
</tr>
<tr>
<td>CROATIA</td>
<td>Draft Bill</td>
<td>Hate Speech, Fake News</td>
<td>Proposed</td>
<td>Implemented</td>
</tr>
<tr>
<td>CZECH REPUBLIC</td>
<td>Government Task Force (Centre Against Terrorism and Hybrid Threats)</td>
<td>Foreign Interference, Content harmful to national interest</td>
<td>Implemented</td>
<td>Implemented</td>
</tr>
<tr>
<td>DENMARK</td>
<td>Government Task Force and Media Literacy Campaign</td>
<td>Fake News, Foreign Interference, and Media Literacy</td>
<td>Implemented</td>
<td>Implemented</td>
</tr>
<tr>
<td>EGYPT</td>
<td>Legislation</td>
<td>Fake News, Media Regulation</td>
<td>Implemented</td>
<td>Criminalisation</td>
</tr>
<tr>
<td>FRANCE</td>
<td>Legislation (Proposition De Loi Relative a la lute contre les fausses informations)</td>
<td>Fake News, Foreign Interference, Advertising Transparency</td>
<td>Implemented</td>
<td>Implemented</td>
</tr>
<tr>
<td>GERMANY</td>
<td>Legislation (Network Enforcement Act)</td>
<td>Hate Speech</td>
<td>Implemented</td>
<td>Implemented</td>
</tr>
<tr>
<td>INDIA</td>
<td>Draft Bill</td>
<td>Media Regulation</td>
<td>Dismissed</td>
<td>Freedom</td>
</tr>
<tr>
<td>IRAN</td>
<td>Regulation</td>
<td>Media Regulation, Fake News</td>
<td>Implemented</td>
<td>Implemented</td>
</tr>
<tr>
<td>IRELAND</td>
<td>Draft Bill (The Online Advertising and Social Media Transparency Bill)</td>
<td>Advertising Transparency, Bots and Automation</td>
<td>Proposed</td>
<td>Criminalisation, Advertising Transparency</td>
</tr>
<tr>
<td>ISRAEL</td>
<td>Draft Bill</td>
<td>Content harmful to democratic process</td>
<td>Dismissed</td>
<td>Content Takedown</td>
</tr>
<tr>
<td>ITALY</td>
<td>Reporting Portal</td>
<td>Draft Bill (Regulations to Prevent the Manipulation of Online Information, Guarantee Web Transparency, and Incentivise Media Literacy)</td>
<td>Fake News, Content harmful to democratic process</td>
<td>Implemented, Proposed</td>
</tr>
<tr>
<td>KENYA</td>
<td>Legislation (The Computer and Cyber Crimes Bill 2018)</td>
<td>Fake News</td>
<td>Implemented</td>
<td>Content Takedown, Expanding Definition of Illegal Content</td>
</tr>
<tr>
<td>KUWAIT</td>
<td>Legal Amendment</td>
<td>Fake News</td>
<td>Implemented</td>
<td>Criminalisation</td>
</tr>
<tr>
<td>MALAYSIA</td>
<td>Legislation</td>
<td>Fake News</td>
<td>Repealed</td>
<td>Criminalisation, Expanding Definition of Illegal Content</td>
</tr>
<tr>
<td>NIGERIA</td>
<td>Government Campaign</td>
<td>Media Literacy</td>
<td>Implemented</td>
<td></td>
</tr>
<tr>
<td>PHILIPPINES</td>
<td>Draft Bill (The Anti-Fake News Act of 2017)</td>
<td>Fake News, Hate Speech, Defamation</td>
<td>Dismissed</td>
<td>Content Takedown, Criminalisation, Expanding Definition of Illegal Content</td>
</tr>
<tr>
<td>RUSSIA</td>
<td>Legislation</td>
<td>Fake News, Media Regulation</td>
<td>Proposed</td>
<td>Content Takedown</td>
</tr>
<tr>
<td>SAUDI ARABIA</td>
<td>Government Announcement to national interests, Privacy</td>
<td>Fake News, Content harmful to democratic process</td>
<td>Implemented, Proposed</td>
<td>Criminalisation</td>
</tr>
<tr>
<td>SINGAPORE</td>
<td>Parliamentary Committee (Select Committee on Deliberate Online Falsehoods)</td>
<td>Fake News</td>
<td>Implemented</td>
<td>Parliamentary Inquiry</td>
</tr>
<tr>
<td>SPAIN</td>
<td>Draft Bill</td>
<td>Fake News</td>
<td>Proposed</td>
<td>Data Protection</td>
</tr>
<tr>
<td>SOUTH AFRICA</td>
<td>Draft Bill, Government Task Force</td>
<td>Fake News</td>
<td>Pending Amendments</td>
<td>Content Takedown, Security and Defence</td>
</tr>
<tr>
<td>SOUTH KOREA</td>
<td>Draft Bill</td>
<td>Government Task Force</td>
<td>Fake News</td>
<td>Proposed</td>
</tr>
<tr>
<td>SWEDEN</td>
<td>Government Task Force (Swedish Civil Contingencies Agency and the Defence Commission)</td>
<td>Foreign Interference</td>
<td>Implemented</td>
<td>Security and Defence</td>
</tr>
<tr>
<td>TAIWAN</td>
<td>Educational Reform, Draft Bill (added clause to the Social Order Maintenance Act)</td>
<td>Fake News</td>
<td>Implemented, Proposed</td>
<td>Media Literacy and Watchdog Programs, Criminalisation</td>
</tr>
<tr>
<td>TANZANIA</td>
<td>Legislation (Media Services Act)</td>
<td>Fake News</td>
<td>Implemented</td>
<td>Content Takedown, Criminalisation, Media Accreditation</td>
</tr>
<tr>
<td>THAILAND</td>
<td>Government Task Force</td>
<td>Fake News</td>
<td>Implemented</td>
<td>Monitoring and Reporting</td>
</tr>
<tr>
<td>TURKEY</td>
<td>Government Inquiry</td>
<td>Fake news</td>
<td>Implemented</td>
<td>Parliamentary Inquiry, Criminalisation</td>
</tr>
<tr>
<td>UGANDA</td>
<td>Legislation (The Social Media Tax)</td>
<td>Fake News</td>
<td>Implemented</td>
<td>Monitoring and Reporting</td>
</tr>
<tr>
<td>UNITED KINGDOM</td>
<td>Parliamentary Inquiry (DCMS), Government Task Force (National Security Communications Unit)</td>
<td>Foreign Interference, Fake News</td>
<td>Implemented, Implemented</td>
<td>Parliamentary Inquiry, Security and Defence</td>
</tr>
<tr>
<td>UNITED STATES</td>
<td>Draft Bill (Honest Ads Act), Legislation (Countering Foreign Propaganda and Disinformation Act), Regulation (Foreign Agent Registration Act), Diplomatic (Expelling Diplomats), Senate Bill No. 1001 (State of California), New Media Literacy Law (State of California), Senate Committee Inquiries</td>
<td>Foreign Interference, Advertising Transparency, Bots and Automation, Media Literacy, Data Protection and Election Integrity</td>
<td>Proposed, Implemented, Implemented, Implemented, Implemented, Implemented</td>
<td>Media Accreditation, Advertising Transparency, Parliamentary Inquiry, Data Protection, Security and Defence</td>
</tr>
<tr>
<td>VENEZUELA</td>
<td>Legislation</td>
<td>Hate Speech</td>
<td>Implemented</td>
<td>Criminalisation</td>
</tr>
<tr>
<td>VIETNAM</td>
<td>Draft Bill, Task Force (Force 47)</td>
<td>Fake News</td>
<td>Proposed</td>
<td>Data Protection, Security and Defence</td>
</tr>
<tr>
<td>ZIMBABWE</td>
<td>Draft Bill</td>
<td>Fake news, Revenge Porn, Hate Speech</td>
<td>Proposed</td>
<td>Criminalisation</td>
</tr>
</tbody>
</table>
Endnotes


Daniel Mumbere, "Tanzania Cyber Law Introduces $900 Fees for Bloggers, Compulsory Passwords | Africanews," Africa News, April 2018,


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.