Meta

Meta's submission to the Select Committee on Foreign Interference through Social Media

MARCH 2023

Executive summary

Meta welcomes the opportunity to continue supporting the inquiry by the Select Committee on Foreign Interference through Social Media.

Meta has previously made submissions to the Committee in September 2020 and November 2021, and appeared at a public hearing on 30 July 2021. Given the Committee's continuation in the 47th Parliament, we are providing an update on Meta's efforts to detect and disrupt foreign interference. This submission should be read in conjunction with our previous submissions which outline Meta's approach to other matters in the terms of reference: misinformation, disinformation and electoral integrity.[1]

Foreign interference or influence operations can amplify distrust in the integrity of elections, governance and civic discourse broadly, and undermine the community's confidence in democracy. Combatting these operations is a critical, continuous challenge for governments, industry, media, civil society and academia. Cross-sector cooperation is essential to combat sophisticated bad actors and preserve the community's faith in democracy.

Protecting the integrity of our platform from foreign interference is of paramount importance to Meta. Meta continues to invest significantly in the safety and security of our platforms. We now have more than 40,000 people working on safety and security across the company and we've invested more than US$16 billion (~AU$23 billion) in safety and security since 2016.

This submission outlines Meta's strategy to identify and disrupt coordinated inauthentic behaviour (CIB) which includes our policies, enforcement, partnerships and transparency initiatives. Our approach is continuously informed and updated in response to feedback, research and consultation with government, experts and industry. In Australia, we consult with a range of government, law enforcement and security agencies and think tanks, such as the Australian Strategic Policy Institute.

---

[1] Meta's previous submissions from September 2020 and November 2021 can be found at https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media/ForeignInterference/Submissions

Our efforts are having an impact and we are making progress. In December 2022, we reported that, since 2017, Meta has removed over 200 operations globally for violating our policy against CIB.[2] These networks came from 68 countries and operated in at least 42 languages.

Notably, we worked closely with the Australian Electoral Commission, the Government's Election Integrity Assurance Taskforce, and a range of government and law enforcement agencies in the lead up to the 2022 Australian federal election.

We know that CIB threats are rarely confined to one platform. We report publicly on our findings to enhance transparency and accountability, and we share our findings and threat indicators with industry peers so they too can detect and stop threat activity, and build their responses.

Meta continues to contribute to the debate about effective regulation in this space. Meta is a founding member and signatory to the Australian Disinformation and Misinformation Industry Code.[3] The Code has been a major step in establishing a regulatory framework around industry's work to combat misinformation and disinformation, with other countries around the world looking to emulate this approach. We have also developed principles to guide regulation and legislation around foreign influence operations.

Combatting sophisticated bad actors requires a cross-sectoral approach; we all have a shared interest in building a strong security ecosystem. This collective approach is increasingly important not only within Australia, but across the region. Collaboration between liberal, democratic governments founded on common principles for the internet will be critical as other countries pursue a different and more authoritarian vision for the internet, marked by a heavily surveilled closed internet, data localisation, and very little individual privacy. We would therefore encourage the Committee to consider any further regulatory measures against the broader geo-political context and state of the global internet.

---

[2] B Nimmo, D Agranovich, 'Recapping our 2022 coordinated inauthentic behaviour enforcements', *Meta Newsroom,* 15 December 2022, https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/ and Meta, 'December 2021 Coordinated Inauthentic Behaviour Report', December 2021, https://about.fb.com/wp-content/uploads/2022/01/December-2021-Coordinated-Inauthentic-Behavior-Report-2.pdf

[3] J Machin, 'Facebook's response to Australia's disinformation and misinformation industry code', *Meta Australia Blog*, 21 May 2021, https://australia.fb.com/post/facebooks-response-to-australias-disinformation-and-misinformation-industry-code/

Meta will continue to be a constructive partner for Australian policymakers in considering these policy questions and welcomes the opportunity to engage with this inquiry.

Table of contents

Policies and enforcement

In the social media landscape and beyond, foreign interference relies on two elements: inauthenticity and coordination. Below, we outline are key policies that relate to foreign interference.

Disrupting coordinated inauthentic behaviour

The closest term to foreign interference that Meta uses is coordinated inauthentic behaviour (CIB). Both foreign interference and CIB rely on two elements: inauthenticity - where users misrepresent themselves, through fake profiles or non-transparent behaviours, and coordination - where groups of accounts work together with the intention to deceive users.

Meta defines CIB as “any coordinated network of accounts, Pages and Groups that centrally relies on fake accounts to mislead Meta and people using our services about who is behind it and what they’re doing”.[4] CIB, as we define it, will be slightly broader than the strict interpretation of “foreign interference”, as CIB may include inauthentic coordination by domestic actors, and it may include CIB that is financially motivated (for example, scams) rather than politically motivated. We take action on CIB according to the behaviour of the actors in the network, not the content they post.

In December 2022, we reported that since 2017, Meta has removed over 200 operations for violating our policy against CIB.[5] These networks came from 68 countries and operated in at least 42 languages, with most targeting audiences in their home countries and only around one-third aimed solely at audiences abroad.

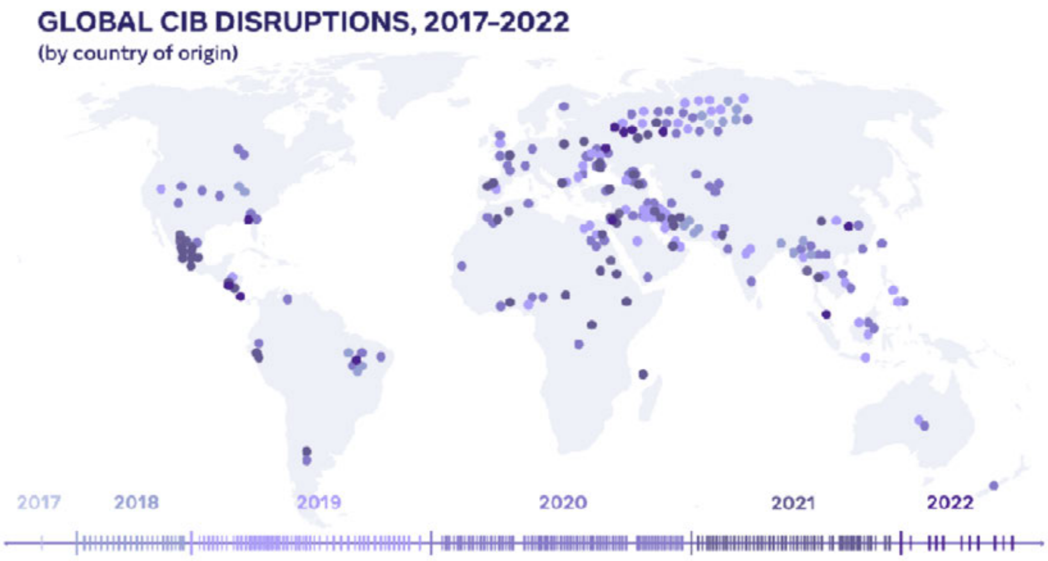
The United States was the most targeted country by global CIB operations we’ve disrupted over the years, followed by Ukraine and the United Kingdom.

---

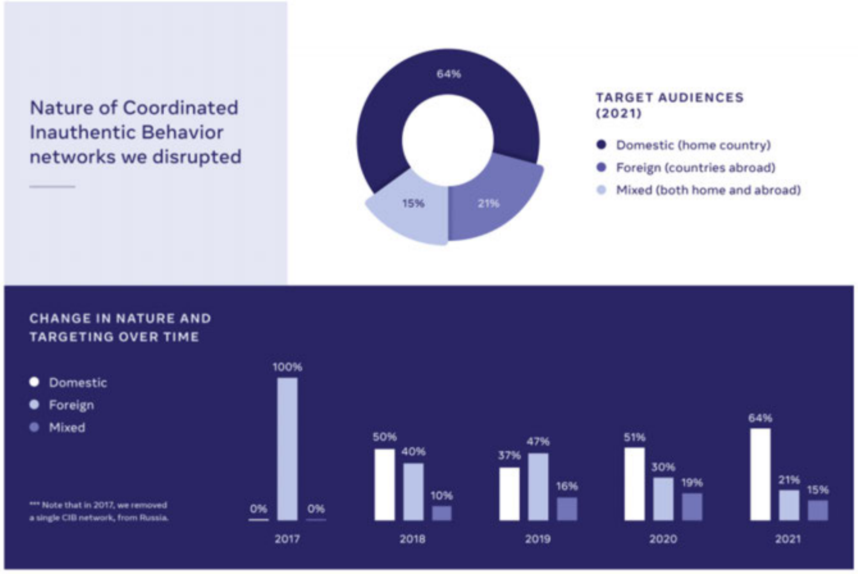
[4] Meta, ‘Threat Report: The State of Influence Operations 2017-2020’, *Meta Newsroom,* May 2021, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

[5] B Nimmo, D Agranovich, ‘Recapping our 2022 coordinated inauthentic behaviour enforcements’, *Meta Newsroom,* 15 December 2022, https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/ and Meta, ‘December 2021 Coordinated Inauthentic Behaviour Report’, December 2021, https://about.fb.com/wp-content/uploads/2022/01/December-2021-Coordinated-Inauthentic-Behavior-Report-2.pdf

Global Coordinated Inauthentic Behaviour Disruptions, 2017 – 2022



Target of Coordinated Inauthentic Behaviour Disruptions, 2017 - 2022[6]



---

[6] We define targets as:

- Domestic: IO that targets public debate in the same country from which it operates.
- Foreign: IO that targets the public debate in a different country from which it operates.
- Mixed: We also see IO campaigns and threat actors that run campaigns that target both domestic and foreign audiences

We also recently reported that we had identified more than 400 malicious android and iOS apps that were designed to steal Facebook login information and compromise people's accounts.[7] These apps were listed on the Google Play Store and Apple's App Store and disguised as photo editors, games, VPN services, business apps and other utilities to trick people into downloading them.

As of end 2022, we have taken action on four instances of CIB operations that targeted Australians.

- In 2020, we removed an operation that operated from many regions around the world including the US, Canada, Australia, New Zealand, Vietnam, Taiwan, Hong Kong, Indonesia, Germany, the UK, Finland and France.[8] It targeted primarily English and Chinese-speaking audiences globally and Vietnam. Our investigation linked this network to Truthmedia, a digital media outlet, which is now banned from our platforms.

- In 2019, we took action against CIB that originated in Macedonia and Kosovo.[9] The individuals behind this activity operated fake accounts to administer Pages sharing general, non-country specific content like astrology, celebrities and beauty tips. They also ran a small number of Pages purporting to represent political communities in Australia, the United Kingdom and the United States. Our investigation benefited from open source reporting, including from the press in Australia.

- In 2019, we took action against CIB that originated in the United Arab Emirates (UAE), Egypt, Nigeria that were promoting content about the UAE.[10] There were multiple sets of activity, primarily in the Middle East and Africa, and some in Europe, North and South America, South Asia and East Asia, and Australia.

- In 2019, we took action against a domestic operation in March 2019 that was linked to local political actors related to the New South Wales state election.

---

[7] D Agranovich, 'Protecting people from malicious account compromise apps', *Meta Newsroom*, 7 October 2022, https://about.fb.com/news/2022/10/protecting-people-from-malicious-account-compromise-apps/

[8] Meta, Coordinated Inauthentic Behavior Report, *Meta Newsroom*, 6 August 2020, https://about.fb.com/news/2020/08/july-2020-cib-report/

[9] N Gleicher, 'Removing Coordinated Inauthentic Behaviour from Iran, Russia, Macedonia and Kosovo, *Meta Newsroom,* 26 March 2020, https://about.fb.com/news/2019/03/cib-iran-russia-macedonia-kosovo/,

[10] N Gleicher, ' Removing Coordinated Behaviour in UAE, Nigeria, Indonesia and Egypt', *Meta Newsroom,* 3 October 2019, https://about.fb.com/news/2019/10/removing-coordinated-inauthentic-behavior-in-uae-nigeria-indonesia-and-egypt/

It is important to note that Meta coordinated with the Government's election integrity assurance taskforce and security agencies in the lead up to the 2022 Australian election, and this is explained in more detail in the 'Partnerships' section below.

During the election, we did not see any evidence of coordinated inauthentic behaviour targeting Australia.

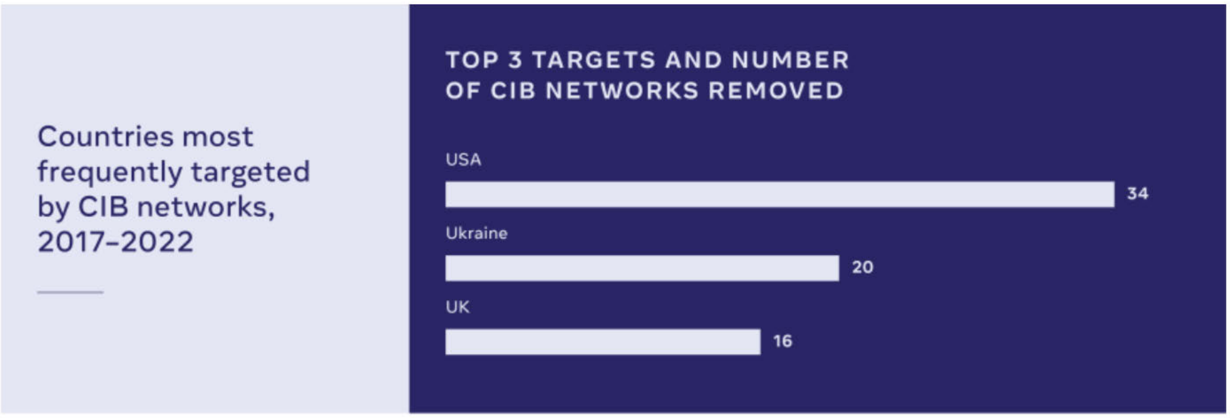
Case study: Meta's CIB response to the war in Ukraine

Since the beginning of the devastating war in Ukraine, Meta has taken a number of steps to combat misuse of our services and help ensure the safety of our community - both in Ukraine and around the world.[11]

To respond to these risks, we rolled out privacy and security measures to help people in Ukraine and Russia protect their accounts from being targeted, and reduce the risk of foreign interference or CIB. We also set up new teams to monitor and respond to emerging threats of inauthentic behaviour.[12]

In 2022, Ukraine was the second most targeted country for CIB operations according to Meta's CIB report.[13]

Targets and CIB networks removed, 2017 - 2022



---

[11] Meta, 'Meta's ongoing efforts regarding Russia's invasion of Ukraine', *Meta Newsroom,* 26 February 2022, https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/

[12] B Nimmo, D Agranovich & N Gleicher, 'Adversarial Threat Report', *Meta,* April 2022, https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf

[13] B Nimmo, D Agranovich, 'Recapping our 2022 coordinated inauthentic behaviour enforcements', *Meta Newsroom,* 15 December 2022, https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/ and Meta, 'December 2021 Coordinated Inauthentic Behaviour Report', December 2021, https://about.fb.com/wp-content/uploads/2022/01/December-2021-Coordinated-Inauthentic-Behavior-Report-2.pdf

We have reported publicly on our efforts to remove CIB related to the war in Ukraine. This war has written a new chapter in our industry's collective understanding of influence operations, both overt and covert. While we've seen some of these elements around the world, this is the first time we've observed attempts at covert influence operations deployed at this scale, alongside a military invasion and subsequent land warfare between two states. In response to military aggression of this magnitude, it's also the first time we've taken the unprecedented step of reducing the distribution of state media outlets.

In February 2023, we released our latest Quarterly Adversarial Threat Report, which outlines our latest efforts.[14] It finds that while Russian-origin attempts at CIB related to Russia's war in Ukraine have sharply increased, overt efforts by Russian state-controlled media have reportedly decreased over the last 12 months on our platform. We saw state-controlled media shifting to other platforms and using new domains to try to escape the additional transparency on (and demotions against) links to their websites.

During the same period, covert influence operations have adopted a brute-force, "smash-and-grab" approach of high-volume but very low-quality campaigns across the internet.

In addition to these insights, we have taken action on the following CIB networks since the war in Ukraine began:

- Removed a network in Russia for abusing our reporting tools to repeatedly report people in Ukraine and in Russia for fictitious policy violations of Facebook policies in an attempt to silence them.[15]

- Detected and disrupted recidivist CIB activity linked to the Belarusian KGB who suddenly began posting in Polish and English about Ukrainian troops surrendering without a fight and the nation's leaders fleeing the country. Prior to that, this particular threat actor primarily focused on accusing Poland of mistreating migrants from the Middle East. On March 14 2022, they pivoted back to Poland and created an event in Warsaw calling for a protest against the Polish government. We disabled the account and event that same day.[16]

---

[14] B Nimmo, M Franklin, D Agranovich, L Hundley, M Torrey, 'Quarterly Adversarial Threat Report', *Meta*, February 2023, https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf

[15] B Nimmo, 'Meta's Adversarial Threat Report, First Quarter 2022', *Meta Newsroom*, 7 April 2022, https://about.fb.com/news/2022/04/metas-adversarial-threat-report-q1-2022/

[16] B Nimmo, D Agranovich, N Gleicher, *'Adversarial Threat Report: Detailed Report'*, Meta, April 2022, https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf

- Took down a network run by people in Russia and Ukraine targeting Ukraine. They ran websites posing as independent news entities and created fake personas across social media platforms including Facebook, Instagram, Twitter, YouTube, Telegram, and also Russian Odnoklassniki and VK.[17]

- Took down a network of Instagram accounts operated by a troll farm in St. Petersburg, Russia, which targeted global public discourse about the war in Ukraine. This appeared to be a poorly executed attempt, publicly coordinated via a Telegram channel, to create a perception of grassroots online support for Russia's invasion by using fake accounts to post pro-Russia comments on content by influencers and media.[18]

- Took down a large network that originated in Russia and targeted primarily Germany, and also France, Italy, Ukraine and the United Kingdom with narratives focused on the war in Ukraine. The operation began in May 2022 and centered around a sprawling network of over 60 websites carefully impersonating legitimate websites of news organisations in Europe, including Spiegel, The Guardian and Bild. There, they would post original articles that criticised Ukraine and Ukrainian refugees, supported Russia and argued that Western sanctions on Russia would backfire. They would then promote these article, original memes and YouTube videos across many internet services, including Facebook, Instagram, Telegram, Twitter, petitions websites Change.org and Avaaz, and LiveJournal.[19]

- Finally, we saw a spike in compromise attempts aimed at members of the Ukrainian military by Ghostwriter, a threat actor tracked by the security community. In a handful of cases, groups posted videos calling on the Army to surrender as if these posts were coming from the legitimate account owners. We blocked these videos from being shared.

---

[17] N Gleicher, 'Updates on our security work in Ukraine', *Meta Newsroom*, 27 February 2022, https://about.fb.com/news/2022/02/security-updates-ukraine/

[18] B Nimmo, D Agranovich, N Gleicher, *'Adversarial Threat Report: Detailed Report'*, Meta, April 2022, https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf

[19] B Nimmo and D Agranovich, *'Removing coordinated inauthentic behaviour from China and Russia'*, Meta Newsroom, 27 September 2022, https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/

Fake accounts

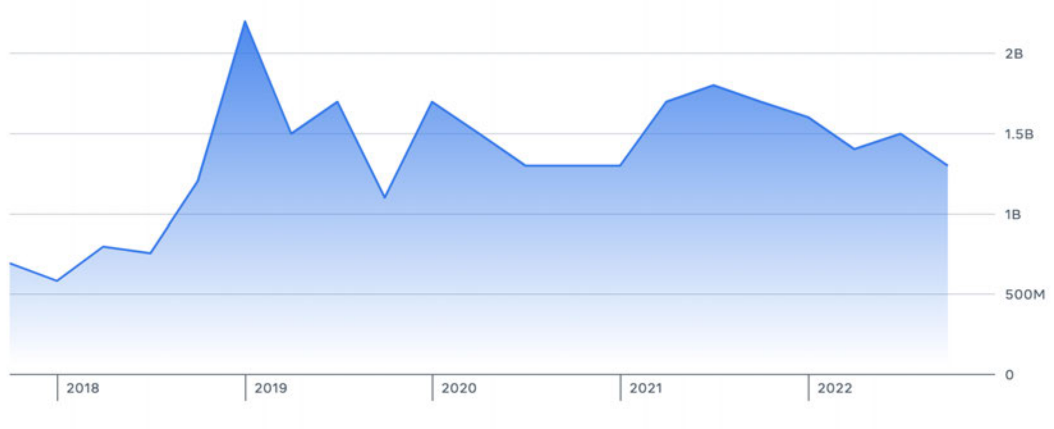
We consider authentic communications to be a central part of people's experience online.[20] People find value in connecting with their friends, family, and issues they care about, and we want them to be able to trust the people and communities they interact with. For this reason, authenticity has long been a requirement of our Community Standards.

We aim to remove fake accounts from our platforms, as they can often be the vehicle for harmful content. These include accounts created with malicious intent to violate our policies, and personal profiles created to represent a business, organisation or non-human entity, such as a pet.

Our ability to detect and remove fake accounts has been improving over the years, and there has been a general decline in the volume of fake accounts found on the platform since 2019.

Our most recent data found that, in Q4 2022 (October to December), we removed 1.3 billion fake accounts on Facebook, and 99.4 percent of these were removed proactively, before they were reported to us.[21]

Number of fake accounts we've taken action on (2018-2022)



---

[20] Meta, *Community Standards - Misrepresentation*, https://www.facebook.com/communitystandards/misrepresentation/

[21] Meta, *Community Standards Enforcement Report Q4 2022 - fake accounts,* https://transparency.fb.com/data/community-standards-enforcement/fake-accounts/facebook/

Partnerships

Combatting foreign interference is a continuous challenge for governments, industry, media, civil society and academia, and cross-sector collaboration is essential. We continue to partner with government and organisations to ensure our efforts are based on expert information and have the most effective impact.

One particular area worth highlighting is Meta's work to prepare for the 2022 Australian federal election. In the lead up to the Australian election, Meta developed a comprehensive strategy that focussed on proactively detecting and removing content that breaches our policies, including detecting and combatting coordinated inauthentic behaviour.

We recognise that each election is different, and it is critical to develop strong partnerships locally to deliver our efforts. We worked closely with the Australian Electoral Commission (AEC), the Government's Election Integrity Assurance Taskforce (EIAT), and a range of government and law enforcement agencies in the lead up to the election.

This involved reviewing content where the AEC expressed concerns about compliance with Australian electoral law. We also worked with the Australian Government's EIAT to undertake scenario planning for different online issues that may arise during an election campaign. We also consulted with experts and academics on possible threats around the election to inform these responses.

In addition to our election-related work, we continue to invest in research and tools to better understand disinformation and coordinated inauthentic behaviour, and inform our approach to these issues. Some recent highlights include:

- Meta supported an analytical paper by First Draft on disinformation and misinformation amongst diaspora groups with a focus on Chinese language.[22] The paper aims to inform policymakers on how to reduce misinformation within Chinese diaspora communities ahead of the next federal election.

---

[22] E Chan, S Zhang, 'Disinformation, stigma and chinese diaspora: policy guidance for Australia', *First Draft website*, 31 August 2021, https://firstdraftnews.org/long-form-article/disinformation-stigma-and-chinese-diaspora-policy-guidance-for-australia/

- We are a major sponsor of the Australian Strategic Policy Institute (ASPI). In late 2020, we launched a CrowdTangle-enabled research pilot where we shared information about recent CIB takedowns with a small group of researchers. ASPI is one of our initial 5 key partners for this archive.[23]

- We funded Dr Jake Wallis from ASPI to undertake a review of disinformation-for-hire, specifically targeting Australia and the Asia-Pacific region. This research was launched in August 2021.[24]

- Meta has facilitated industry efforts to combat cyberthreats through threat signal sharing between industry peers through our ThreatExchange API platform, which we launched in 2015.[25] This program supports the sharing of threat information (e.g. malicious domains hosting malware, phishing scams, malware hashes) to help security professionals in participating organisations better tackle threats by learning from each other's discoveries and making their own systems safer.

Transparency and accountability

We recognise that, as a large company, the decisions we take relating to content or behaviour on our services can be significant. We report regularly on our approach to CIB to provide the community, civil society and governments with greater confidence in our efforts to combat these operations. These are reported through:

- **Our Community Standard Enforcement Report.** Each quarter, we report on metrics for preventing and taking action on content that goes against our Community Standards.[26]

---

[23] B Nimmo, D Agranovich & N Gleicher, 'Adversarial Threat Report', *Meta Newsroom,* April 2022, https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf

[24] Dr J Wallis, 'Influence for hire: the Asia-Pacific's online shadow economy', *Australian Strategic Policy Institute,* 10 August 2021, https://www.aspi.org.au/report/influence-hire

[25] Meta, 'Welcome to ThreatExchange', *Meta for Developers Help Centre*, https://developers.facebook.com/docs/threat-exchange/getting-started/

[26] Meta, *Community Standards Enforcement Report,* https://about.fb.com/news/tag/coordinated-inauthentic-behavior/

- **Monthly Adversarial Threat reports.** Each month we publish a list of CIB networks that we have taken down.[27]

- **Threat Report – State of Influence Operations 2017-2021.** In 2021 we published a strategic report that looks at influence operations (IO) broadly, defined as "coordinated efforts to manipulate or corrupt public debate for a strategic goal", of which CIB is a subset. The report draws on our existing public disclosures and our internal threat analysis to do four things: first, it defines how CIB manifests on our platform and beyond; second, it analyses the latest adversarial trends; third, it uses the US 2020 elections to examine how threat actors adapted in response to better detection and enforcement; and fourth, it offers mitigation strategies that we've seen to be effective against IO.[28]

Discussion on the regulation of foreign interference

We are committed to working with policymakers and partners around the world to meet the challenges posed by foreign interference. This is a continuous challenge for governments, industry, media, civil society and academia, and cross-sector cooperation is essential.

Meta continues to contribute to the debate about effective regulation in this space. For example, Meta has worked constructively with Government and industry in Australia to increase accountability and transparency around our misinformation efforts. In 2020, Meta (then Facebook) became a founding member and signatory to the Australian Disinformation and Misinformation Industry Code.[29]

Since 2020, Meta has publicly released two transparency reports which outline our specific commitments to meet the obligations outlined in the voluntary code. Most recently, we made 45 commitments to combat misinformation and disinformation on our platforms, and we will report again on these efforts in May 2023.[30]

---

[27] Meta, *Community Standards - Coordinated Inauthentic Behaviour,* https://about.fb.com/news/tag/coordinated-inauthentic-behavior/

[28] Meta, 'Threat Report - the State of Influence Operations 2017 - 2020', *Meta Newsroom,* May 2021, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

[29] J Machin, 'Facebook's response to Australia's disinformation and misinformation industry code', *Meta Australia Blog*, 21 May 2021, https://australia.fb.com/post/facebooks-response-to-australias-disinformation-and-misinformation-industry-code/

[30] You can find Meta's two transparency reports for the Australian Disinformation and Misinformation Industry Code here https://digi.org.au/disinformation-code/transparency/

The Code is a credible, world-leading first step in the collaboration between the technology industry and governments to combat misinformation. Two years on, the Code has been an effective framework to increase transparency around companies' efforts to combat misinformation and disinformation, and raise industry standards, so much so, that other countries around the world are looking to emulate this approach.

To support policymakers in considering how best to regulate foreign interference and platform integrity, Meta has also released a set of Recommended Principles for Regulation or Legislation to Combat Influence Operations (IO principles).[31] The principles are:

- Transparency in Ads: Continue to increase transparency for contributions or expenditures for political advertising.
- Reporting on Inauthentic Behaviour: Work with industry and civil society experts to develop minimum disclosure frameworks, collaborative development of transparency best practices, and the sharing of lessons learned.
- Broad Application: Cover IO broadly, rather than focusing on specific tactics only. Because IO manifests differently on different platforms and in their targeting of traditional media, narrow definitions will likely leave loopholes that attackers can exploit.
- Increased Information Sharing: Enable greater information sharing of IO threat signals among tech companies and between platforms, civil society and government, while protecting the privacy of innocent users who may be swept up in these campaigns.
- Deterring Violators: Impose economic, diplomatic and/or criminal penalties on the people behind IO campaigns, understanding that different penalties and mitigations apply in foreign and domestic contexts.
- Supporting Technical Research: Support private and public innovation and collaboration on technical detection of adversarial threats such as manipulated media, including deepfakes.

---

[31] N Gleicher, 'Recommended principles for regulation or legislation to combat influence operations', *Meta Newsroom,* 8 October 2020, https://about.fb.com/news/2020/10/recommended-principles-for-regulation-or-legislation-to-combat-influence-operations/

- Supporting Media and Digital Literacy: Support media and digital literacy efforts to educate people and strengthen societal resilience.

These IO principles promote a holistic approach across government and industry, and aim to enhance our collective capability, as we all have a shared interest in building a strong security ecosystem across Australia.

When considering the domestic regulatory landscape, we would also encourage the Committee to consider any further regulatory measures against the broader geo-political context and state of the global internet.

The open, global internet was founded on liberal, democratic principles, pioneered by US companies. However, the values that underpin the original global internet are increasingly being challenged by a different model pioneered by other strong forces in the region – a heavily surveilled closed internet, data localisation, and very little individual privacy.

Local data storage requirements in particular have broader implications for the state of an open, global internet. Data localisation measures are often intended to facilitate the surveillance or censorship of citizens' online activities and violate individuals' human rights including freedom of speech, expression, access to information, and privacy and due process rights.

For this reason, Meta has proposed a "Bretton Woods" moment for the internet[32] – the creation of a multilateral, international framework for the internet that would agree some inviolable principles of how the global internet operates – such as privacy of the individual, user rights, open data flows across borders, transparency and accountability – among other principles that accord with the liberal democratic origins of the global internet.

Collaboration between liberal, democratic governments founded on common principles for the internet will be critical for combatting foreign interference, particularly in the face of new models for the internet. We would therefore encourage the Committee to consider any regulatory measures against the broader geo-political context and state of the global internet.

---

[32] N Clegg, 'A Bretton Woods for the digital age can save the open internet', *Australian Financial Review*, 16 November 2021, https://www.afr.com/technology/a-bretton-woods-for-the-digital-age-can-save-the-open-internet-20211115-p5994h

Meta will continue to be a constructive partner for Australian policymakers in considering these policy questions, and the best way to approach them, and welcomes the opportunity to engage with this inquiry.