Computational
Propaganda
Research Project

Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation

Samantha Bradshaw, *University of Oxford*
Philip N. Howard, *University of Oxford*

OXFORD
INTERNET
INSTITUTE

UNIVERSITY OF
OXFORD

Contents

EXECUTIVE SUMMARY

The manipulation of public opinion over social media platforms has emerged as a critical threat to public life. Around the world, a range of government agencies and political parties are exploiting social media platforms to spread junk news and disinformation, exercise censorship and control, and undermine trust in the media, public institutions, and science. At a time when news consumption is increasingly digital, artificial intelligence, big data analytics, and "black-box" algorithms are being leveraged to challenge truth and trust: the cornerstones of our democratic society.

In 2017, the first Global Cyber Troops inventory shed light on the global organization of social media manipulation by government and political party actors. This 2018 report analyses the new trends of organized media manipulation, and the growing capacities, strategies and resources that support this phenomenon. Our key findings are:

1. We have found evidence of formally organized social media manipulation campaigns in 48 countries, up from 28 countries last year. In each country there is at least one political party or government agency using social media to manipulate public opinion domestically.

2. Much of this growth comes from countries where political parties are spreading disinformation during elections, or countries where government agencies feel threatened by junk news and foreign interference and are responding by developing their own computational propaganda campaigns in response.

3. In a fifth of these 48 countries—mostly across the Global South—we found evidence of disinformation campaigns operating over chat applications such as WhatsApp, Telegram and WeChat.

4. Computational propaganda still involves social media account automation and online commentary teams, but is making increasing use of paid advertisements and search engine optimization on a widening array of Internet platforms.

5. Social media manipulation is big business. Since 2010, political parties and governments have spent more than half a billion dollars on the research, development, and implementation of psychological operations and public opinion manipulation over social media. In a few countries this includes efforts to counter extremism, but in most countries this involves the spread junk news and misinformation during elections, military crises, and complex humanitarian disasters.

CHALLENGING TRUTH AND TRUST: SOCIAL MEDIA AND DEMOCRACY

Many people are questioning whether social media platforms are threatening democracy. Concentrated in just a few hands, large datasets about public and private life—including data on demographics and public attitudes and opinion—are valuable assets to lobbyists seeking to pass legislation, foreign governments interested in controlling domestic conversations, and political campaign managers working to win an election. While the Internet has certainly opened new avenues for civic participation in political processes—inspiring hopes of a democratic reinvigoration—the parallel rise of big data analytics, "black-box" algorithms, and computational propaganda, are raising significant concerns for policymakers worldwide. In many countries around the world, divisive social media campaigns have heightened ethnic tensions, revived nationalistic movements, intensified political conflict, and even resulted in political crises—while simultaneously weakening public trust in journalism, democratic institutions, and electoral outcomes.

"Cyber troops" are defined here as government or political party actors tasked with manipulating public opinion online (Bradshaw & Howard, 2017). Specifically, we focus on how these actors disseminate computational propaganda over social media platforms. We define computational propaganda as the use of automation, algorithms and big-data analytics to manipulate public life (Howard & Woolley, 2016). The term encompasses issues to do with so-called "fake news", the spread of misinformation on social media platforms, illegal data harvesting and micro-profiling, the exploitation of social media platforms for foreign influence operations, the amplification of hate speech or harmful content through fake accounts or political bots, and clickbait content for optimized social media consumption. This report examines how governmental cyber troops make use of computational propaganda to shape public opinion.

The affordances of social media platforms make them powerful infrastructures for spreading computational propaganda (Bradshaw & Howard, 2018). Social media are particularly effective at directly reaching large numbers of people, while simultaneously micro-targeting individuals with personalized messages. Indeed, this effective impression management—and fine-grained control over who receives which messages—is what makes social media platforms so attractive to advertisers, but also to political operatives and foreign adversaries. Where government control over Internet content has traditionally relied on blunt instruments to block or filter the free flow of information, powerful political actors are now turning to computational propaganda to shape public discourse and nudge public opinion.

The use of social media to subvert elections and undermine trust in democratic institutions is a widespread phenomenon, extending far beyond the actions of a few bad actors. Coordinated manipulation campaigns are taking place domestically in every type of political regime, and foreign operations have targeted several Western and emerging democracies during recent elections. In this year's report, we examine cyber troop activity in 48 countries: Angola, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahrain, Brazil, Cambodia, China, Colombia, Cuba, Czech Republic, Ecuador, Egypt, Germany, Hungary, India, Iran, Israel, Italy, Kenya, Kyrgyzstan, Malaysia, Mexico, Myanmar, Netherlands, Nigeria, North Korea, Pakistan, Philippines, Poland, Russia, Saudi Arabia, Serbia, South Africa, South Korea, Syria, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Venezuela, Vietnam, and Zimbabwe.

A strong democracy requires high-quality news from an independent media, a pluralistic climate of opinion, and the ability to negotiate public consensus. But powerful political actors are increasingly leveraging social media to manufacture consensus, manipulate public opinion, and subvert democratic processes. Building on the global inventory we developed in 2017, we can now look back on a year's worth of trends in the strategies, organization, and resourcing of social media manipulation around the world. Several notable trends have emerged from these data.

1. Political Parties and Disinformation During Elections

With each passing election, there is a growing body of evidence that national leaders, political parties, and individual political candidates are using social media platforms to spread disinformation. Although closely related to some of the dirty tricks and negative campaigning we might expect in close races (and which have always played a part in political campaigning), what makes this phenomenon unique is the deliberate use of computational propaganda to manipulate voters and shape the outcome of elections. In 30 of the 48 countries we examined, we found evidence of political parties using computational propaganda during elections or referenda. In emerging and Western democracies, sophisticated data analytics and political bots are being used to poison the information environment, promote skepticism and distrust, polarize voting constituencies, and undermine the integrity of democratic processes. In more authoritarian regimes, governing parties apply the same strategies as part of their broader efforts to subvert elections. In these cases, social media manipulation, as well as media control, ballot stuffing and police intimidation, all shape the power of ruling elites.

2. Government Agencies Tasked with Combatting Fake News

The growing threat of fake news proliferation—whether real or perceived—is now a significant concern for governments around the world. Since 2016, over 30 countries have introduced legislation designed to combat fake news on the Internet (Bradshaw, Neudert, & Howard, Forthcoming). At the same time, several democracies have established new government agencies or mandated existing organizations to combat fake news and foreign influence operations. The response often involves generating and disseminating counter-narratives or creating reporting, flagging, and fact checking portals to support citizen awareness and engagement. Authoritarian regimes have also developed responses ostensibly to combat the spread of fake news; though they might also be used to stifle speech. In many cases these task forces have become a new tool to legitimize further censorship, and are often used in combination with media law and surveillance capabilities, computational propaganda campaigns, and Internet blocking or filtering to limit freedom of expression and shape online public discourse.

3. Disinformation on Chat Applications

Chat applications such as WhatsApp, Signal, or Telegram are an important medium by which individuals share news and information, coordinate political activity, and discuss politics. In this year's report, there is growing evidence of disinformation campaigns taking place on chat applications. We have seen evidence of social media manipulation campaigns on chat applications in around a fifth of the countries in our sample, many of which are from the Global South, where large public groups on chat applications are a widespread phenomenon.

4. Current and Emerging Strategies for Social Media Manipulation

Government cyber troops make use of a variety of tactics and techniques, and every political campaign uses a different set of tools for the job. Most cyber troops will use online commentators and fake social media accounts to spread pro-government or pro-party messages to populations both domestically and abroad. Political bots are used by cyber troops to flood hashtags with automated messages promoting or attacking particular politicians, or to fake a follower-base on social media. Increasingly they are also used to strategically post particular keywords, in order to game algorithms and cause certain content to trend. Bots are also being used to report legitimate content and accounts on a mass scale, so that social media platforms automatically suspend accounts or remove content until it can be reviewed by a human moderator. We suspect that all these subversive behaviors will continue to evolve as platforms and governments take legal and regulatory steps to curb disruptive activity on social media.

5. The Growing Importance of the Influence Industry

Cyber troops invest significant funds into organizing online manipulation campaigns. Based on preliminary data from a few specific cases around the world, we have already seen tens of millions of dollars being spent on computational propaganda and social media manipulation. While some cyber troop funds are being spent on research and development in military settings, there are an increasing number of purchases being made by political parties to use similar techniques domestically during elections. Often, these funds are used to hire political communication firms that specialize in data-driven targeting and online campaigning. While there are many legitimate businesses that help political parties identify new constituencies and tailor political advertisements to a voter base, there is a growing industry of non-legitimate businesses that use fake social media accounts, online trolls and commentators, and political bots to distort conversations online, help generate a false sense of popularity or political consensus, mainstream extremist opinions, and influence political agendas.

REPORT METHODOLOGY

The research for this report was completed in three stages. First, we conducted a systematic content analysis of news articles reporting on cyber troop activity in our sample of 48 countries. We then supplemented this data with an in-depth secondary literature review. Using this data, a country profile for each country in this report was drafted by a team of research assistants who then consulted country-specific experts on the accuracy and reliability of the publically available information they had collected.

Content analysis is an established research method in communication and media studies (Herring, 2009). It has been used to help understand how the Internet and social media interact with political action, regime transformation, and digital control (Edwards, Howard, & Joyce, 2013; Joyce, Antonio, & Howard, 2013; Strange, Parks, Tierney, Dreher, & Ramachandran, 2013; Woolley, 2016). The qualitative content analysis in this report was conducted to understand the range of state actors who actively use social media to manipulate public opinion, as well as their capacity, strategies and resources. We modeled our content analysis after our 2017 report (Bradshaw & Howard, 2017), using purposive sampling to build a coded spreadsheet of specific variables that appear in news articles. The following keywords were selected and used in combination for our search: astroturf*; bot; Cambridge Analytica; Facebook; fake; fake account; disinformation; government; information warfare; intelligent agent; military; misinformation;

persona management; pro-government; propaganda; psychological operations; psyops; social media; sock puppet*; troll*; Twitter.

In our 2017 report, there were two major limitations to our qualitative content analyses: media bias and language. Media bias is a common limitation to content analysis that uses purposive sampling (Earl, Martin, McCarthy, & Soule, 2004; Joyce et al., 2013). To help mitigate bias, we used LexisNexis and the top three search engine providers—Google, Yahoo! and Bing—which provided hits to a variety of professional, local and amateur news sources. To ensure that only high-quality news sources were used to build our dataset, each article was given a credibility score using a three-point scale. Articles ranked at one came from major, professionally branded news organizations (see Appendix 1). Articles ranked at two came from smaller professional news organizations, local news organizations, or expert commentary and professional blogs (see Appendix 2). Articles ranked at 3 came from content farms, social media posts, or non-professional or hyper-partisan blogs. These articles were removed from the sample.

Language was a second limitation to conducting our qualitative content analysis. For this year's global inventory, we were able to draw on news articles and secondary resources written in English, Spanish, German, Italian, Polish, Portuguese, Russian, and Arabic. We also worked with BBC monitoring who provided an additional portal for collecting and aggregating high-quality news and information on cyber troop activity, as well as translation services for news articles from Malaysia, Kyrgyzstan and Taiwan. Thus, for this year's report, we were able to examine news coverage across 10 different languages. We relied on English-language-only reporting for Armenia, Azerbaijan, Cambodia, Czech Republic, Hungary, Israel, Myanmar, Netherlands, North Korea, Pakistan, Philippines, Thailand, Turkey, and Vietnam.

While we were unable to analyze local news sources for every country in this report, the third phase of our research methodology—consultation with experts—allowed us to peer review the English language reporting and secondary literature we found and discuss additional resources and citations in alternative languages with native speakers. Experts were asked to review the country profiles drafted by research assistants, and (1) fact-check the information and data for accuracy; (2) provide additional citations to openly available material; and (3) provide general feedback on the reliability of the data. We consulted experts for 34 of the 48 countries in our sample, namely: Argentina, Austria, Azerbaijan, Bahrain, Brazil, Colombia, Ecuador, Egypt, Germany, Hungary, India, Iran, Kenya, Malaysia, Mexico, Myanmar, Netherlands, Philippines, Poland, Russia, Saudi Arabia, South Africa, South Korea, Syria, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Venezuela, Vietnam, and Zimbabwe.

This methodology has allowed us to successfully capture a wide range of public documents that shed light on the global distribution of organized manipulation campaigns. There are almost certainly cyber troop operations that have not been publicly documented. While this report is in no way intended to provide a complete picture of how state actors are operating in this space, we can confidently begin to build a bigger picture by piecing together a wide array of publically available information.

ORGANIZATIONAL FORM

Cyber troop activity takes on a variety of organizational forms. Indeed, there are many types of actors who leverage social media to set political agendas and propagate values or ideas. In this report, we focus specifically on cyber troop activity: that is government or political party use of social media to manipulate public opinion. One important feature of the organization of cyber troops is that they often work in conjunction with private industry, civil society organizations, Internet subcultures, youth groups, hacker collectives, fringe movements, social media influencers, and volunteers who ideologically support their cause. While this coordination can also occur informally as a result of overlapping ideologies or values, we have captured examples where formal coordination has occurred. For example, formal organization between industry and political parties appears to have occurred in Austria, Brazil, Colombia, Ecuador, India, Kyrgyzstan, Malaysia, Mexico, Nigeria, Philippines, Poland, South Africa, the United Kingdom and the United States, where political parties and campaign managers have directly hired PR or consulting firms to help spread computational propaganda during elections. Another example of formal coordination that takes place between cyber troops is with volunteers. In countries such as Azerbaijan, Israel, Russia, and Turkey, tech savvy youth are actively recruited by cyber troop organizations to support social media manipulation efforts.

We have documented evidence of the form that cyber troop activity takes in order to comparatively examine the actor types involved (see Table 1). In terms of scope, it is important to note that we do not look at the work of lone wolf actors, hacker collectives, or Internet subcultures who use these platforms for social media manipulation, *unless* they have formally coordinated with cyber troop actors. Thus, we do not capture individual actors who might share the same ideologically goals or values as governments, but who do not work directly in cooperation with them. We also only focus on national initiatives. Thus, government or military coordination with regional organizations such as NATO are not included in this analysis.

Table 1: Organizational Form and Prevalence of Social Media Manipulation

Country	Year of First Report	Government Agencies	Politicians and parties	Private contractors	Civil Society Organizations	Citizens and Influencers
Angola	2017		░			
Argentina	2012	░	▓			
Armenia	2017	░				
Australia	2013	░	▓			
Austria	2005		▓	░		
Azerbaijan	2011	░			▓	
Bahrain	2013	░				
Brazil	2010		▓	█		
Cambodia	2016	█	░			░
China	2011	█		░	░	
Colombia	2016	░	░	░		
Cuba	2017	░			░	
Czech Republic	2017	░	░			
Ecuador	2014	▓	▓	█		
Egypt	2016	░	░			░
Germany	2016	░	░		░	
Hungary	2010	░				
India	2013		░	░		░
Iran	2012	█				
Israel	2008	█			█	
Italy	2016		▓			
Kenya	2013		▓	▓		
Kyrgyzstan	2015		░	░		░
Malaysia	2008	▓	▓	▓	░	
Mexico	2014		█	█	░	
Myanmar	2016	░				
Netherlands	2017		░			
Nigeria	2007	░	░	░		
North Korea	2013	▓				
Pakistan	2017		█			
Philippines	2016	░	▓	▓	░	░
Poland	2015		░	░		
Russia	2012	▓		░	░	░
Saudi Arabia	2013	░		▓	░	░
Serbia	2016	░	░		░	
South Africa	2016		░	▓		
South Korea	2013	░	░			
Syria	2011	▓		░	░	
Taiwan	2010		▓			░
Thailand	2017	░				░
Turkey	2013	░	░			░
Ukraine	2014	░			░	
UAE	2012	░		▓		░
United Kingdom	2014	▓	▓	░		
United States	2008	█	▓	█	░	░
Venezuela	2015	▓	░	▓	░	
Vietnam	2013	░				
Zimbabwe	2018		░			

Source: Authors' evaluations based on data collected. **Note:** This table reports on the types of political actors using social media influence operations, and the number of examples of those organizations found. For government agencies, political parties, civil society groups, and private contractors, ░ = one organization found, ▓ = two organizations found, █ = three or more organizations found. Since it is difficult to assess the number of individual citizens using these tools, evidence of citizen use is indicated by ░.

STRATEGIES, TOOLS AND TECHNIQUES FOR SOCIAL MEDIA MANIPULATION

Messaging and Valence

Cyber troops use a variety of messaging and valence strategies when conducting information operations online (Table 2). Valence is a term that is used to define the attractiveness (goodness) or averseness (badness) of a message, event or thing. A prominent technique of social media manipulation is the use of online commentators who actively engage in conversation and debate with genuine social media users. Their activities span a variety of platforms online, including traditional web forums, blogs, news websites, and social media platforms, and they use a variety of valence strategies when in conversation with real users. We found evidence of government or political party organizations using online commentators to shape discussions on the Internet and social media platforms in three ways: (1) spreading pro-government or pro-party propaganda; (2) attacking the opposition or mounting smear campaigns; or (3) neutral strategies that involved diverting conversations or criticism away from important issues, or fact-checking information.

The second messaging and valence strategy we identified was the use of trolls who target specific individuals, communities or organizations with hate speech or various forms of online harassment (Table 2). These targeted and hateful messages are used as a systematic attempt to persecute minority opinions and political dissent, both in the context of elections and as a tool of social control in authoritarian regimes. We found reports of state-sponsored trolling campaigns targeting political dissidents, members of the opposition, or journalists in 27 of the 48 countries in our sample.

Valence and messaging strategies are usually carried out by cyber troops who operate fake accounts. These accounts are also used to create, disseminate and share junk news and other campaign-crafted information online. We found evidence of fake accounts in 46 of the 48 countries in our sample. We examined three kinds of fake accounts: (1) automated accounts; (2) human accounts; and (3) hybrid or cyborg accounts (see Table 2).

Automated accounts—also known as "political bots"—are pieces of software or code designed to mimic human behavior online. They can be used to perform various manipulative techniques including spreading junk news and propaganda during elections and referenda, or manufacturing a false sense of popularity or support (so-called 'astroturfing') by liking or sharing stories, ultimately drowning out authentic conversations about politics online.

Fake social media accounts are not always automated. In many cases, human operators manually run fake accounts to achieve similar goals, often done by coordinated teams managing a set of accounts. In a few cases, we also found evidence of "cyborg" accounts, whose operators combine automation—to drive volume and speed of activity—with elements of human curation, to make them appear to be legitimate accounts. These hybrid accounts can be the hardest to detect and shut down, since they involve elements of genuine human interaction. While we only found explicit evidence of hybrid accounts being used in 9 of the countries in our sample, we suspect that this activity is much more prevalent in practice, given the still-limited data about the production and use of fake accounts.

Of the 46 countries in our sample operating fake accounts, the most common strategy involves automation. Much of this automated fake account activity is restricted to the platforms that make automation easy—usually Twitter—and there was evidence of 38 countries having automated systems for generating content and interacting with human users. Human operators are used to manage the fake accounts deployed by governments and political parties in 33 countries. In countries where fake account activity is high, we can safely say that both automation and human operators drive disinformation.

Communication Strategies

Cyber troops use a variety of communication strategies to disseminate computational propaganda over social media platforms (Table 3). They create their own content, including fake videos, blogs, memes, pictures, or news websites. These content strategies involve more than simply posting forum comments or replying to genuine user posts, but instead are important sources of junk news, and conspiratorial or polarizing information that can be used to support a broader manipulation campaign.

Content strategies also involve the malevolent takedown of legitimate content or accounts. In addition to amplifying certain messages, cyber troop teams use content strategies to suppress voices online. Increasingly, we are identifying human-operated and automated accounts being used to falsely mass-report legitimate content or users so that their accounts and posts are temporarily (and mistakenly) removed by the social media channel. In Armenia, China, Ecuador and Russia we found evidence of this malevolent reporting of content to stifle individual expression and limit the spread of content online (Table 3).

Increasingly, government actors are creating their own applications, portals or task forces to combat the threat of fake news and foreign influence operations. In some cases, these task forces focus on fact-checking information that is shared across social media, or they allow citizens to report such information to the government or law enforcement agencies. For example, Colombia started a fact-checking imitative for content being shared on WhatsApp, and leading up to the 2018 elections in Italy, law enforcement launched a portal that allowed citizens to report fake news they came across on social media. While there have been many positive responses by governments to begin taking steps to combat computational propaganda, in other instances these applications or portals are used to legitimize censorship or launch astroturfing campaigns. In Brazil, Ecuador, Israel and Serbia we have seen cyber troops create applications or portals to launch astroturfing campaigns.

Finally, other evidence of political communication strategies we identified involves targeting advertisements to specific segments of the population using demographic information or data on user attitudes, or gaming algorithms through search engine optimization techniques to get content to appear higher in search results. The range of platforms on which disinformation is carried out is also growing, with evidence of cyber troop activity on chat applications or other platforms (Instagram, LINE, SnapChat, Telegram, Tinder, WeChat, WhatsApp) in 12 of 48 countries examined.

Table 2: Social Media Manipulation Strategies: Messaging and Valence

Country	Fake Account Type	Pro-Government or Party Messages	Attacks on the Opposition	Distracting or Neutral Messages	Trolling or Harassment
Angola	○ 🤖 ○		■		
Argentina	○ 🤖 ○	■	■		■
Armenia	○ 🤖 ○			■	
Australia	○ 🤖 ○	■	■		
Austria	👤 🤖 ○		■		■
Azerbaijan	👤 🤖 👤⚙	■	■	■	■
Bahrain	👤 🤖 ○		■		■
Brazil	👤 🤖 👤⚙	■	■	■	■
Cambodia	○ 🤖 ○				
China	👤 🤖 ○	■	■	■	■
Colombia	👤 ○ ○		■		■
Cuba	👤 🤖 ○		■	■	■
Czech Republic	○ ○ ○			■	
Ecuador	👤 🤖 ○	■	■		■
Egypt	👤 🤖 👤⚙		■		■
Germany	👤 🤖 👤⚙	■	■		■
Hungary	👤 ○ ○	■	■		■
India	○ 🤖 ○	■	■		■
Iran	👤 🤖 👤⚙	■	■	■	
Israel	👤 🤖 ○	■			
Italy	○ 🤖 ○	■	■		
Kenya	○ 🤖 ○		■		
Kyrgyzstan	👤 ○ ○	■	■		
Malaysia	○ 🤖 ○	■	■		
Mexico	👤 🤖 👤⚙	■	■		■
Myanmar	○ 🤖 ○	■	■		
Netherlands	○ 🤖 ○				
Nigeria	○ ○ ○		■		
North Korea	👤 ○ ○	■	■		
Pakistan	○ 🤖 ○	■	■		
Philippines	👤 🤖 ○	■	■		■
Poland	👤 ○ ○		■		■
Russia	👤 🤖 👤⚙	■	■	■	■
Saudi Arabia	○ 🤖 ○	■		■	
Serbia	👤 🤖 ○	■	■		■
South Africa	👤 🤖 ○	■	■		■
South Korea	👤 🤖 ○	■	■		■
Syria	○ 🤖 ○	■	■		■
Taiwan	👤 🤖 👤⚙	■	■	■	■
Thailand	👤 🤖 ○				
Turkey	👤 🤖 ○	■	■		■
Ukraine	👤 🤖 ○	■	■		■
UAE	👤 🤖 ○	■	■		■
United Kingdom	👤 🤖 ○	■	■	■	■
United States	👤 🤖 👤⚙	■	■	■	■
Venezuela	👤 🤖 ○	■	■	■	
Vietnam	👤 ○ ○	■	■		
Zimbabwe	👤 ○ ○		■		

Source: Authors' evaluations based on data collected. **Note:** This table reports on the messaging and valence strategies of cyber troops. A filled box indicates evidence found. For fake account types: 👤 = human accounts; 🤖 = automated accounts 👤⚙ = cyborg accounts; ○/ ○/ ○ = no evidence found.

Table 3: Observed Strategies for Social Media Manipulation

Country	Content Strategies	Targeted Ads	Task Forces, Portals or Applications	Chat Apps & Other Platforms	SEO
Angola	✔ ✗				
Argentina	✓ ✗	■			■
Armenia	✔ ✖				
Australia	✓ ✗		Counter Info Ops		
Austria	✔ ✗	■			
Azerbaijan	✔ ✗				
Bahrain	✓ ✗				
Brazil	✔ ✗		Astroturf	WhatsApp	
Cambodia	✓ ✗				
China	✔ ✖			WeChat	■
Colombia	✔ ✗		Fact Checking		
Cuba	✔ ✗				
Czech Republic	✔ ✗		Fact Checking		
Ecuador	✔ ✖		Astroturf	WhatsApp	
Egypt	✓ ✗				
Germany	✔ ✗		Counter Info Ops		■
Hungary	✔ ✗				
India	✔ ✗		Astroturf	WhatsApp	
Iran	✔ ✗			Telegram	
Israel	✔ ✗	■	Astroturf	Instagram	
Italy	✔ ✗		Reporting		
Kenya	✔ ✗	■		WhatsApp	■
Kyrgyzstan	✔ ✗				
Malaysia	✓ ✗		Fact Checking		
Mexico	✔ ✗			WhatsApp, SnapChat	■
Myanmar	✔ ✗				
Netherlands	✔ ✗				
Nigeria	✔ ✗	■			
North Korea	✓ ✗				
Pakistan	✔ ✗			WhatsApp	
Philippines	✔ ✗				
Poland	✓ ✗				
Russia	✔ ✖				
Saudi Arabia	✓ ✗				
Serbia	✔ ✗		Astroturf		
South Africa	✔ ✗				■
South Korea	✓ ✗				
Syria	✔ ✗				
Taiwan	✔ ✗		Reporting		
Thailand	✓ ✗			Line, WeChat	
Turkey	✔ ✗	■			
Ukraine	✔ ✗		Fact Checking		
UAE	✔ ✗				
United Kingdom	✔ ✗	■	Counter Info Ops	Tinder	■
United States	✔ ✗	■	Counter Info Ops		■
Venezuela	✔ ✗				
Vietnam	✔ ✗				
Zimbabwe	✔ ✗			WhatsApp	

Source: Authors' evaluations based on data collected. **Note:** This table reports on the observed strategies of cyber troops. A filled box indicates evidence found. For content: ✔ = content creation; ✖ = malevolent content takedown, ✓/ /✗ = no evidence found.

ORGANIZATIONAL BUDGETS, BEHAVIOR AND CAPACITY

Although there is limited public information about the size and operations of cyber troop teams, we can begin to assemble a picture of how much money they budget, how they cooperate, and the kinds of organizational capacities and behaviors they assume (Table 4). First, cyber troop organizations spend significant funds on their activities. In many countries, there are reports of government and military budgets assigning specific funds to conduct psychological operations and information warfare via social media platforms—both against foreign governments but also domestically in many authoritarian regimes. Many high-capacity cyber troop teams, such as in the United States, have large research and development funds that have been spent to conduct research on social networks, or to combat misinformation.

A growing number of political parties are hiring PR firms or data analytics companies to spread disinformation, launch a political bot or trolling campaign, optimize search results, or spread voter suppression messages. Big spending on these private companies is increasingly a common practice, both in Western democracies and emerging democracies. While all political parties will make expenditures for the digital aspects of their campaign, what makes the data collected in this report unique is that it captures what we know about how political parties spend money specifically on disinformation campaigns.

In terms of size, cyber troop teams vary greatly. In some cases, teams are very small, employing just a few workers to propagate ideas and messages across social media over a short period of time, such as during an election campaign. Other teams are larger enterprises that employ hundreds or even thousands of individuals to shape the online information sphere using the various techniques described above.

Different cyber troops have different resources, budgets, expenditures, personnel coordination, and skills required to carry out organized manipulation campaigns. By looking comparatively across the trends of cyber troop activity and organization, we can begin to establish their capacity in relation to one another. For this report, we developed a four-point scale: minimal-low-medium-high (Table 4).

Minimal cyber troop teams are newly formed and often small teams, or teams that were previously active but whose present activities are uncertain. For newly formed teams, they have minimal resources and only apply a few tools or strategies of social media manipulation to a small number of platforms. Minimal teams include: Argentina, Angola, Armenia, Czech Republic, Italy, Kenya, Netherlands, Pakistan, South Korea, and Zimbabwe.

Low cyber troop capacity involves small teams that may be active during elections or referenda, but which then stop activity until the next election cycle. These teams tend to experiment with only a few strategies or tools for social media manipulation, such as using bots to amplify disinformation. Low capacity teams include: Azerbaijan, Australia, Austria, Bahrain, Cambodia, Colombia, Egypt, Germany, Hungary, India, Kyrgyzstan, Myanmar, Nigeria, Poland, South Africa, Taiwan, Tanzania, and Thailand.

Medium cyber troop capacity involves teams that have a much more consistent form and strategy, involving full-time staff members who are employed year-round to control the information space. These medium-capacity teams often coordinate with multiple actor types, and experiment with a wide variety of tools and strategies for social media manipulation. Medium capacity teams include: Brazil, Cuba, Ecuador, Malaysia, Mexico, Iran, North Korea, Philippines, Saudi Arabia, Serbia, Syria, Turkey, Ukraine, United Kingdom, Venezuela, and Vietnam.

High cyber troop capacity involves large numbers of staff, and large budgetary expenditure on psychological operations or information warfare. There might also be significant funds spent on research and development, as well as evidence of a multitude of techniques being used. These teams do not only operate during elections but involve full-time staff dedicated to shaping the information space. High capacity teams include: China, Israel, Russia, UAE, and the United States.

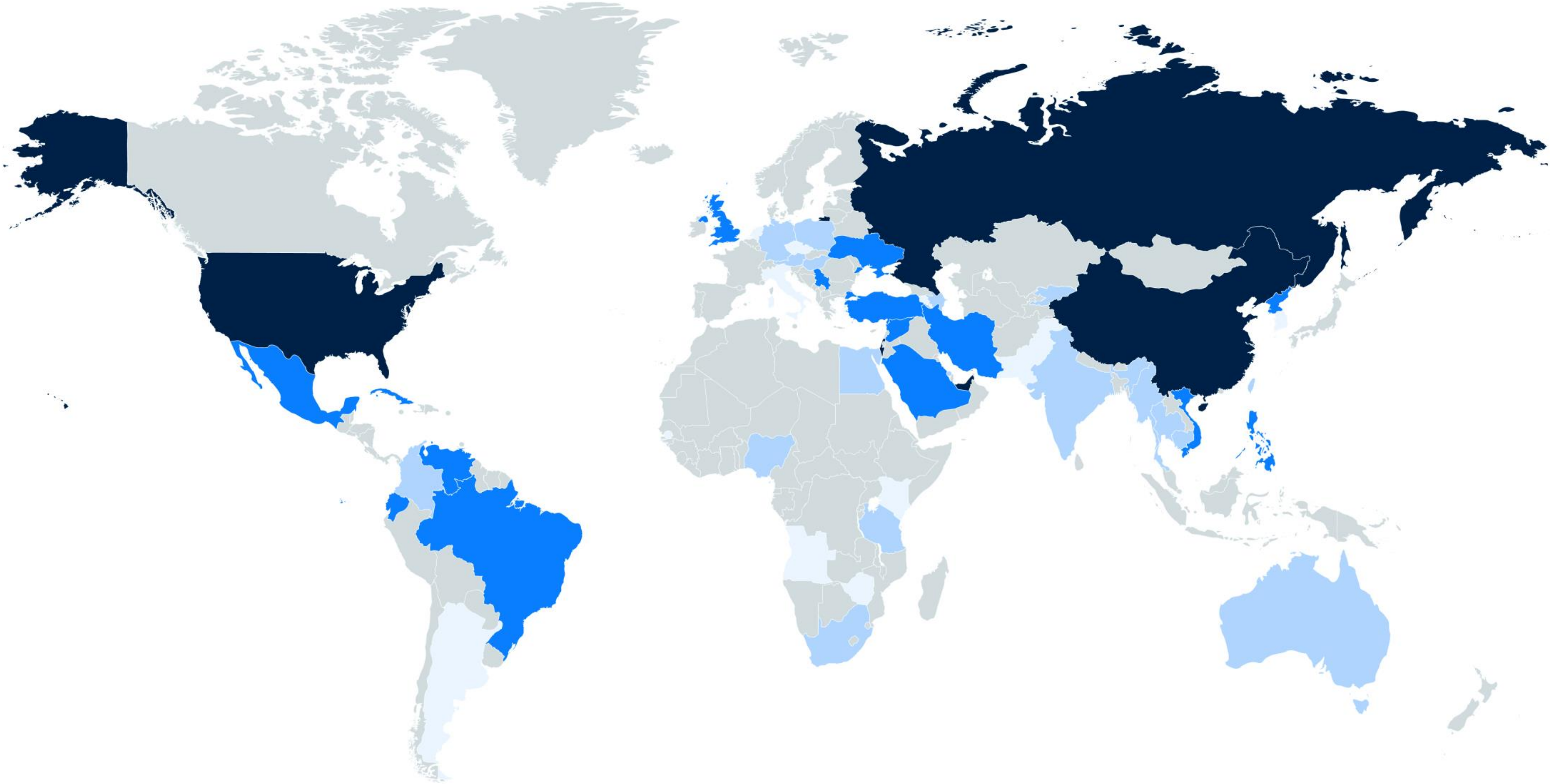
Table 4: Cyber Troop Capacity

Country	Team Size	Resources	Status	Coordination	Capacity
Angola	Newly Formed	..	Temporary	Low	░
Argentina	30-40	Multiple contracts valued at 14 million Pesos and 11 Million Pesos	Previously Active	Low	░
Armenia	Newly Formed	..	Temporary	Low	░
Australia	900	..	Temporary & Permanent	Low	▒
Austria	..	..	Temporary	Low	▒
Azerbaijan	50,000	..	Temporary	Low	▒
Bahrain	..	..	Permanent	Low	▒
Brazil	60	Multiple contracts valued at R10,000,000, R130,000 R24,000	Permanent	Medium	▓
Cambodia	..	..	Temporary & Permanent	Low	▒
China	300,000-2,000,000	..	Permanent	High	█
Colombia	..	..	Temporary	Low	▒
Cuba	..	..	Permanent	Medium	▒
Czech Republic	..	..	Permanent	Low	░
Ecuador	..	Multiple contracts valued at $200,000.	Permanent	Medium	▓
Egypt	..	..	Permanent	Low	▒
Germany	<300	..	Temporary & Permanent	Low	▒
Hungary	..	..	Permanent	Medium	▒
India	..	..	Temporary	Low	▒
Iran	10,000-20,000	..	Permanent	Medium	▓
Israel	400	Multiple contracts valued at $778,000; $100,000,000	Permanent	High	█
Italy	Newly Formed	..	Temporary	Low	░
Kenya	Newly Formed	One contract valued at $6,000,000	Temporary	Low	░
Kyrgyzstan	50	Multiple contracts valued at $2000. $3-4 a day per person	Temporary	Low	▒
Malaysia	..	..	Temporary	Low	▒
Mexico	1,000	Multiple contracts, one valued at $600,000. €520 per month per person	Temporary	Medium	▓
Myanmar	..	..	Temporary & Permanent	Medium	▓
Netherlands	Newly Formed	..	Temporary	Low	░
Nigeria	..	One contract valued at $2,800,000	Temporary	Low	▒
North Korea	200	..	Permanent	Medium	▓
Pakistan	Newly Formed	..	Temporary	Low	░
Philippines	400-500	Multiple contracts valued at $200,000+.	Permanent	Medium	▓
Poland	..	..	Temporary	Low	▒
Russia	400-1000	Annual Budget $10,000,000	Permanent	High	█
Saudi Arabia	..	..	Permanent	Medium	▓

Country	Team Size	Resources	Status	Coordination	Capacity
Serbia	100	Average Monthly Salary €370	Permanent	Medium	▓
South Africa	..	One contract valued at $2,000,000	Temporary	Low	▒
South Korea	<20	..	Previously Active	Low	░
Syria	..	Multiple contracts valued at $4,000	Permanent	Medium	▓
Taiwan	..	..	Temporary	Low	▒
Thailand	Newly formed	..	Permanent	Low	▒
Turkey	6,000	Multiple contracts, one valued at $209,000	Permanent	Medium	▓
Ukraine	20,000-40,000	..	Permanent	Medium	▓
UAE	..	Annual Budget $10,000,000+	Permanent	High	█
United Kingdom	1500	Multiple contracts for elections, total value approximately £3,500,000	Temporary & Permanent	Medium	▓
United States	..	Multiple programs valued at $50,000,000; $200,000,000; $202,000,000	Temporary & Permanent	High	█
Venezuela	500	..	Permanent	Medium	▓
Vietnam	10,000	..	Permanent	Medium	▓
Zimbabwe	Newly formed	..	Temporary	Low	░

Source: Authors' evaluations based on data collected. **Note:** This table reports on cyber troop size, resources, team permanency, coordination, and capacity. For capacity: ░ = minimal capacity, ▒ = low capacity, ▓ = medium capacity, █ = high capacity

Figure 1: Global Cyber Troop Capacity: 2018



Source: Authors' evaluations based on data collected. **Note:** This table reports on cyber troop size, resources, team permanency, coordination, and capacity. See Table 4 for data on global cyber troop capacity. For capacity: ⬜ = minimal capacity, ░ = low capacity, ▓ = medium capacity, █ = high capacity

CONCLUSION

Social media platforms are among the most used applications on the Internet. In the US, 85 percent of the adult population uses the Internet regularly, and 80 percent of those people are on Facebook (Greenwood, Perrin, & Duggan, 2016). Most of the time, social media are not used for politics: they are a place where friends and families connect and reconnect, or where individuals find and share entertainment, popular culture, as well as humorous cat videos. The ubiquity and prominence of social media for everyday life underscores their importance in today's society, and users place high amounts of trust in these platforms. But with their ability to segment audiences and target messages in a quick, cheap and largely unregulated way, it is clear why these platforms have attracted the interest of political operators. Unfortunately, there is mounting evidence that social media are being used to manipulate and deceive the voting public—and to undermine democracies and degrade public life.

We once celebrated the fact that social media let us express ourselves, share content, and personalize our media consumption. It is certainly difficult to tell the story of the Arab Spring without acknowledging that social media platforms allowed democracy advocates to coordinate themselves in surprising new ways: to send their demands for political change cascading across North Africa and the Middle East (Howard & Hussain, 2013). But the absence of human editors in our news feeds also makes it easy for political actors to manipulate social networks. In previous research conducted by the Computational Propaganda Project, we found rather paradoxical evidence of the chilling effect of social media on freedom of speech and political participation. Half of Russian Twitter conversations involve highly automated accounts that actively shape online discourses (Sanovich, 2017). In Brazil, both professional trolls and bots have been used aggressively to drown out minority and dissenting opinions during two Presidential campaigns, one Presidential impeachment campaign, and the major race for the Mayor of Rio (Arnaudo, 2017). Social media have gone from being the natural infrastructure for sharing collective grievances and coordinating civic engagement, to being a computational tool for social control, manipulated by canny political consultants, and available to politicians in democracies and dictatorships alike (Howard and Woolley, 2016).

However, understanding precisely how social media platforms impact public life is difficult (Bradshaw & Howard, 2017). In many democracies it is not even clear that spreading computational propaganda contravenes election laws (Howard, Woolley, & Calo, 2018). It is, however, quite clear that the strategies and techniques used by government cyber troops have an impact, and that their activities violate the norms of democratic practice. We cannot prevent all bad actors from using computational propaganda, but in democracies we can have guidelines discouraging its use. To start to address these challenges, we need to develop stronger rules and norms for the use of social media, big data and new information technologies during elections.

During 2016 and 2017 we saw significant efforts made by Russia to disrupt elections around the world, but also political parties these countries spreading disinformation domestically. Looking at the growth of cyber troop activity from 2017 to 2018 has demonstrated that these strategies are circulating globally. We cannot wait for national courts to sort out the technicalities of infractions after running an election or referendum. Protecting our democracies now means setting the rules of fair play before voting day, not after.

REFERENCES

Arnaudo, D. (2017). *Computational Propaganda in Brazil* (Computational Propaganda Working Paper Series No. 2017.8). Oxford, United Kingdom: Oxford Internet Institute, University of Oxford.

Bradshaw, S., & Howard, P. N. (2017). Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. *The Computational Propaganda Project*. Retrieved from http://comprop.oii.ox.ac.uk/research/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/

Bradshaw, S., & Howard, P. N. (2018). Why does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life. *Knight Foundation Working Paper*. Retrieved from https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf

Bradshaw, S., Neudert, L.-M., & Howard, P. (Forthcoming). Government Responses to Social Media Manipulation. *Computational Propaganda Project Working Paper*.

Earl, J., Martin, A., McCarthy, J. D., & Soule, S. A. (2004). The use of newspaper data in the study of collective action. *Annual Review of Sociology*, 65–80.

Edwards, F., Howard, P. N., & Joyce, M. (2013). Digital Activism and Non-Violent Conflict. Digital Activism Research Project.

Greenwood, S., Perrin, A., & Duggan, M. (2016, November 11). Social Media Update 2016. Retrieved January 13, 2018, from http://www.pewinternet.org/2016/11/11/social-media-update-2016/

Herring, S. C. (2009). Web Content Analysis: Expanding the Paradigm. In J. Hunsinger, L. Klastrup, & M. Allen (Eds.), *International Handbook of Internet Research* (pp. 233–249). Springer Netherlands. https://doi.org/10.1007/978-1-4020-9789-8_14

Howard, P. N., & Hussain, M. M. (2013). *Democracy's Fourth Wave?: Digital Media and the Arab Spring*. New York, NY: Oxford University Press.

Howard, P. N., Woolley, S., & Calo, R. (2018). Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics*, 1–13. https://doi.org/10.1080/19331681.2018.1448735

Howard, P., & Woolley, S. (2016). Political Communication, Computational Propaganda, and Autonomous Agents. *International Journal of Communication*, *10*(Special Issue), 20.

Joyce, M., Antonio, R., & Howard, P. N. (2013). Global Digital Activism Data Set. ICPSR. Retrieved from http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/34625/version/2

Sanovich, S. (2017). *Computational Propaganda in Russia: The Origins of Digital Misinformation* (Computational Propaganda Working Paper Series No. 2017.3). Oxford, United Kingdom: Oxford Internet Institute, University of Oxford.

Strange, A., Parks, B. C., Tierney, M. J., Dreher, A., & Ramachandran, V. (2013). *China's Development Finance to Africa: A Media-Based Approach to Data Collection* (Working Paper No. 323). Retrieved from https://www.cgdev.org/publication/chinas-development-finance-africa-media-based-approach-data-collection

Woolley, S. C. (2016). Automating Power: Social Bot Interference in Global Politics. *First Monday*, *41*(4). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/6161/5300

SERIES ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support of the European Research Council for the research project, "Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe," Proposal 648311, 2015-2020, Philip N Howard, Principal Investigator. Additional support for this study has been provided by the Ford Foundation and the Open Society Foundation. Project activities were approved by the University of Oxford's Research Ethics Committee (CUREC OII C1A15-044). Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders or Oxford University.

For their assistance and advice on this research, we are grateful to Maud Barrett, Beatriz Kira, Cailean Osborne, Jan Rau and Julia Slupska for collecting the preliminary data and drafting country profiles about social media manipulation for the countries outlined in this report. We are also extremely grateful to Dan Arnaudo, Nicole Au, Crofton Black, Ingrid Brodnig, Chipo Dendre, Monika Glowacki, Dean Jackson, Bence Kollanyi, Andreas Krieg, Vidya Narayana, Lisa-Maria Neudert, Sarah Oh, Anna Pleshakova, Akin Unver, and Syddharth Venkataramakrishnan, as well as the many anonymous experts we consulted for this project. Their country-specific expertise and networks were essential for ensuring the reliability and validity of our data. We thank them for their time and assistance in reviewing country profiles, and for providing us with additional sources, citations and data-points to include in this report.

AUTHOR BIOGRAPHIES

Samantha Bradshaw is a doctoral candidate at the Oxford Internet Institute, University of Oxford, a researcher on the Computational Propaganda project, and a Senior Fellow at the Canadian International Council. Prior to joining the team, she worked at the Centre for International Governance Innovation in Waterloo, Canada, where she was a key member of a small team facilitating the Global Commission on Internet Governance. Samantha's research has been featured in numerous media articles, including the *Washington Post*, *the Financial Times* and *CNN*. Samantha holds an MA in global governance from the Balsillie School of International Affairs, and a joint honors BA in political science and legal studies from the University of Waterloo.

Philip N. Howard is Director of the Oxford Internet Institute, and a statutory Professor at Balliol College, Oxford. He writes about information politics and international affairs, and is the author of eight books, including The Managed Citizen, the Digital Origins of Dictatorship and Democracy, and Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up. He has won multiple "best book" awards, and his research and commentary writing has been featured in the New York Times, Washington Post, and many international media outlets. Foreign Policy magazine named him a "Global Thinker" for 2017 and the National Democratic Institute awarded him their "Democracy Prize" for pioneering the social science of fake news.

OXFORD
INTERNET
INSTITUTE

UNIVERSITY OF
OXFORD