THE GLOBAL ORGANIZATION OF SOCIAL MEDIA DISINFORMATION CAMPAIGNS

Samantha Bradshaw, Oxford University, samantha.bradshaw@oii.ox.ac.uk
Philip N. Howard, Oxford University, philip.howard@oii.ox.ac.uk

Word Count: 3952

Paper Submitted to the Journal of International Affairs
29 July 2018

INTRODUCTION

The manipulation of public opinion over social media platforms has emerged as a critical issue facing contemporary digital society. There are many dimensions to this problem: junk news is spreading like wildfire over social media platforms during key moments of public life; bots are amplifying opinions at the fringe of the political spectrum; patriotic trolls are harassing individuals to suppress speech online; the economic model that supports high-quality news and journalism is increasingly strained by social media advertising; strategic data leaks targeting political campaigns are undermining the credibility of world leaders and democratic institutions; and the lack of transparency around how social media firms operate is making regulatory interventions difficult.

Studying the darker side of political communication—such as misinformation campaigns, negative campaigning, and information operations—may seem like a boutique domain of inquiry. It may also seem like a specialized subtopic for international communication scholars, or simply another aspect of national security and military crises as digital becomes ubiquitous. But several kinds of evidence are now emerging that reveals the global the social organization of misinformation online.

Governments and political parties around the world are spending significant resources to generate content, direct public opinion, and manipulate the opinion of foreign and domestic audiences via social media.[1] These "cyber troops" are state-sponsored organizations tasked with conducting disinformation campaigns on the Internet. Disinformation takes many forms,[2] but cyber troop activity involves the *purposeful* distribution of fake, misleading, fabricated or manipulated content. These actors rely on "computational propaganda"—or the use of automation, algorithms and big data analytics—in order to influence or deceive social media users.[3] Unlike lone-wolf coders, hacker collectives, or non-state actors who also use social media to express speech or achieve political goals, cyber troops are publicly funded and often highly coordinated government actors who use social media to spread disinformation and attempt to generate false consensus. These strategies not only serve as another tool for control in repressive regimes to restrict freedom of expression, but also erodes the quality of democracy by undermining trust in leaders, media, and institutions.

This paper discusses the global organization of social media disinformation, looking comparatively at government actors across regime types. Drawing on data collected from the Computational Propaganda Project's 2017 investigation into the global organization of social media manipulation, we examine how governments and political parties around the world are using social media as a tool of information warfare, on both domestic and foreign audiences.

---

[1] Bradshaw, Samantha and Philip N. Howard. 2017. Troops, Trolls and Troublemakers: A Global Inventory of Social Media Manipulation. *Computational Propaganda Project Working Paper.* Bradshaw, Samantha and Philip N. Howard. 2018. Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. *Computational Propaganda Working Paper.*

[2] Wardle, Claire. 2017. Fake News, Its Complicated. https://firstdraftnews.org/fake-news-complicated/

[3] Woolley, Samuel C. and Philip. N. Howard. 2016. Automation, Algorithms, and Politics: Political Communication, Computational Propaganda, and Autonomous Agents. *International Journal of Communication,* 10 pp. 4882-4890.

We highlight the broad trends of this phenomenon, drawing conclusions about the form, organization, and capacity these institutions assume.

POWER AND COUNTER-POWER: TECHNOLOGY AND THE STATE

The study of technology and information has been central to the domain of international studies. Scholars have dedicated significant resources to understanding how technology disrupts power and politics, enhances or constrains human rights, reorganizes political interactions and institutions, and elevates cyberspace as a new domain of conflict. Much of the literature assumes that low barriers to entry and reduced communication costs afforded by technology has altered the balance of power in favour of minor political players. This assumption has informed a wave of research that has explored issues such as terrorist recruitment and coordination online,[4] the disruptive power of marginal social movements,[5] and independent coder and hacker collectives performing discursive political actions.[6] Indeed, many singular and small-scale actors have achieved impressive political gains by using the internet to catch authoritarian elites off-guard during the Arab Spring.[7]

Looking broadly at one small slice of previous scholarship on technology, power, and counter-power, research has tended to focus on (1) the growing role and capacity of non-state actors, (2) cases that are regionally specific or limited in scope (3) and cases that are serendipitous in success. While there is a growing body of important research on these modular phenomena, there is no reason we should expect that transferring norms of technology use should only involve social movements and democracy advocates.[8] Many kinds of political actors can learn—and learn across geographic borders and regime types—how to successfully adapt technology to implement digital solutions to support their own public interests or goals.[9] Indeed, many authoritarian regimes have successfully leveraged the Internet and social media technologies to exert further control and censorship over freedom and information.[10] And states—who have sometimes been viewed as disadvantaged by the shift in communication power—can learn to exploit social media architecture to re-assert control and sovereignty in cyberspace.

---

[4] Bernard, Rose. 2017. These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of the Islamic State. *Journal of Cyber Policy,* 2(2) pp. 255-265.

[5] Owen, Taylor. 2015. Disruptive Power: The Crisis of the State in the Digital Age. Oxford Studies in Digital Politics: Oxford.

[6] Beyer, Jessica L. 2014. "Expect Us: Online Communities and Political Mobilization" Oxford University Press: Oxford. Coleman, Gabriella. 2014. "Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous" Singapore Books.

[7] Howard, Philip N. and Muzammi M. Hussain. 2013. "Democracy's Fourth Wave? Digital Media and the Arab Spring." Oxford University Press: Oxford. Margetts, Helen, Peter John, Scott Hale, and Taha Yasseri. 2015. "Political Turbulence: How Social Media Shape Collective Action." Princeton University Press: Princeton.

[8] Beissinger, Mark R. 2007. Structure and Example in Modular Political Phenomena: The Diffusion of Bulldozer/Rose/Orange/Tulip Revolutions. *Perspectives in Politics,* 5(2) pp. 259-276. Howard, Philip N. 2010. "The Digital Origins of Dictatorship and Democracy."

[9] Dobson, William. 2012. The Dictators Learning Curve. Tyranny and Democracy in the Modern World. Vintage Press: London

[10] MacKinnon, R. 2011. Chinas Networked Authoritarianism. *Journal of Democracy,* 22(2) pp. 32-46. Pearce, K. E. and Kendzior S. 2012. Networked Authoritarianism and Social Media in Azerbaijan. *Journal of Communication,* 62(2) pp. 283-298.

With increasing evidence of Russian involvement in the UK's Brexit Referendum and interference with the US election of November 2016 social media manipulation has proven to be a powerful tool for political influence.[11] Up until then, most public concern and academic inquiries on cyber power have been preoccupied with the "hard power" capabilities that affect both the cyber and real-world domains, such as cyber-crime and data theft, attacks that damage critical infrastructure, or online surveillance.[12] Over the past five years, international affairs have become replete with examples of how governments have leveraged social media to manipulate public opinion, assigning personnel and financial resources to disinformation and propaganda campaigns online. These campaigns focus less on the ability to obtain desired outcomes through coercion or material resources, but instead employ what scholars have referred to as "soft power" and persuasion,[13] framing and agenda setting,[14] ideological hegemony,[15] symbolic power,[16] or sharp power[17] to achieve desired outcomes. This emerging domain of inquiry should be treated as central to the study of international studies as it provides an opportunity to both expand and refine the concept and exercise of cyber power, and acts as a countervailing example of state power in the digital age.

THE ORGANIZATION OF SOCIAL MEDIA MANIPULATION

This section draws on the Computational Propaganda Project's 2017 investigation into state-sponsored social media manipulation, which presented an investigation of the political economy and organizational behaviour of global cyber troops in 28 countries. These countries included: Argentina, Australia, Azerbaijan, Bahrain, Brazil, China, Czech Republic, Ecuador, Germany, India, Iran, Mexico, North Korea, Philippines, Poland, Russia, Saudi Arabia, Serbia, South Korea, Syria, Taiwan, Turkey, Ukraine, United Kingdom, United States, Venezuela, and Vietnam. The inventory captured the various actors, across many regime types, that used disinformation campaigns on social media in an attempt to influence public opinion. It relied upon open sources of information such as news reports, academic and think tank studies, and government documents, combined with expert consultations, to publish a country-by-country report of government-sponsored social media disinformation campaigns worldwide.[18]

---

[11] Department of Justice. 2018. United States of America v. Internet Research Agency (18 U.S.C. 2,371,1349,1028A)

[12] Deibert, R. 2013. *Black Code: Surveillance, Privacy and the Dark Side of the Internet.* Signal: Toronto. Zetter, K. 2014. Countdown to Zero Day. New York: Crown Publishers. Healey, J. 2017. Cyber Warfare in the 21st Century: Threats, Challenges and Opportunities. House Committee on Armed Services.

[13] Nye, J. 1990. Soft Power. Foreign Policy, 80 pp,153-171. Nye, J. (2004). *Soft Power. The Means to Success in World Politics.* New York: Public Affairs Press.

[14] Bacharach P. and Baratz, M. S. 1963. Decisions and Nondecisions: An Analytical Framework. *The American Political Science Review* 57(3) pp. 632-642,

[15] Lukes, S. 1970. *Power: A Radical View.* London: Palgrave.

[16] Bourdieu, P. 1979. Symbolic Power. *Critique of Anthropology, 4(13-14) pp. 77-85.*

[17] Walker, C. and Ludwig, J. 2017. The Meaning of Sharp Power. *Foreign Affairs,* November.

[18] Bradshaw, Samantha and Philip N. Howard. 2017. Troops, Trolls and Troublemakers: A Global Inventory of Social Media Manipulation. *Computational Propaganda Project Working Paper*

While national contexts are always important to consider, we suggest it is also worth trying to generalize about the experience of organized disinformation campaigns by regime type to develop a broad, comparative understanding of this phenomenon. Table 1 highlights four key trends in the capacity, organization, form and targets that computational propaganda takes on across regime type.

Table 1: A Comparative Redux of Government Capacity for Social Media Manipulation Around the World

Regime Type (countries studied)	Modal Actors	Level of Formal Organization	Level of Capacity	Modal Targets
Democracy (Argentina, Australia, Brazil, Czech Republic, Ecuador, Germany, India, Israel, Mexico, Philippines, Poland, Serbia, South Korea, Taiwan, United Kingdom, United States)	Political Party	Medium	4.63	Domestic
Authoritarian (Azerbaijan, Bahrain, China, Iran, North Korea, Russia, Saudi Arabia, Turkey Venezuela, Vietnam)	Government	High	4.4	Domestic
Crisis State (Ukraine, Syria)	Government	Low	3.5	Domestic

Source: Authors, calculated based on data collected from *Bradshaw & Howard 2017. Troops, Trolls and Troublemakers: The Global Organization of Social Media Manipulation.*

MODAL ACTORS

Column one, modal actor types, presents the modal actor active across the regime types. For each country we sought evidence that government agencies and political parties were employing computational propaganda, either through their own capacity or working alongside civil society groups, private citizens, or independent contractors. Based on the data we collected, we calculated the modal actor present in each regime by counting the number of actors identified in each case.

In authoritarian regimes, the modal actor types are government ministries. For example, this represents cyber troops who work for Vietnam's ministry of Education, or the Internet Research Agency in Russia. Most of the authoritarian states in our sample (Bahrain, China, Iran, North Korea, Saudi Arabia, Venezuela and Vietnam) had a government organization responsible for OMS. Often, these organizations were part of a larger cybersecurity team tasked with securing cyber infrastructure and content, such as Bahrain's National Cyber Crime Unit, or Iran's Supreme Council of Cyberspace. This finding fits into the broader work on

censorship and repression by authoritarian regimes who leverage technology to exert control over cyberspace.[19]

In contrast, the modal actor type in democracies are political parties. In twelve out of the sixteen countries we identified, we found evidence of political parties using computational propaganda (Argentina, Australia, Brazil, Germany, India, Mexico, Poland, Philippines, Serbia, Taiwan, United States, United Kingdom). These actors would often target domestic audiences during elections or other important political events such as referenda.

Level of Formal Organization

Level of Formal Organization presents the level of formality among cyber troop teams. Here, we collected evidence on the organizational behaviour of cyber troops, such as coordination across teams, clear levels of hierarchy, and reward structures (such as evidence of performance bonuses or scholarships). We used a simple calculation to determine the level of formal organization where evidence of each variable was added up and averaged across regime type. This column is based on a low-medium-high scale: a score of 1-3 meant a low level of organization was found, 3-7 was considered medium, and 7 or above was considered high.

Authoritarian regimes have the highest level of formal organization, Teams often work in a structured environment with managers and reporting structures. Cyber troops are assigned daily or weekly tasks, such as making a certain number of posts or friending real people. Staff will also receive formal training. In some cases, scholarships and other forms of recognition are awarded to encourage more activity online. This is not surprising given the amount of control these kinds of regimes already exert over their populations.

Democracies have a slightly lower degree of formal organization. This is in part because teams that work with political parties often form around an election and dissolve when the campaign has ended. When coordination does occur. it is usually around military interventions that use tools of computational propaganda to combat terrorism or counter extremism online. These psychological operations, often carried out in a military setting, are more formally organized, with major investments made into research and development.

Level of Capacity

Level of Capacity presents the capacity of cyber troop teams to conduct disinformation campaigns online. Different teams use different tools and techniques to manipulate public opinion, such as political bots, content creation, targeted advertisements, fake personas, and trolling or harassment. We collected evidence of the existence of these capacities in each regime type, then calculated the average number of tools found across regime types to determine the level of capacity.

---

[19] Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2008. Access Denied. Cambridge: MIT Press; MacKinnon, Rebecca. 2012. Consent of the Networked: The Worldwide Struggle for Internet Freedom. Basic Books.

Democracies have the highest level of capacity to conduct disinformation campaigns. This is not surprising since much of the research and innovation in this area began in democratic military settings, as defence organizations invested resources into understanding how ideas go viral on social media. Today however, most of the innovation around tools and techniques occurs around election cycles with political parties and strategic communication firms driving innovation. A common tool used in democracies are political bots, which amplify follower counts on social media, and get certain stories or hashtags trending.[20] In Argentina, Australia, Brazil, Germany, Ecuador, Mexico, the Philippines, Taiwan, the United States and the United Kingdom, we found evidence of political bots being used by political parties to distort political conversations by generating high follower counts or amplifying certain hashtags or narratives over others.

Although they are highly coordinated, authoritarian regimes have a slightly lower level of capacity for conducting disinformation campaigns. While there are a few authoritarian regimes that have invested significant funds and developed sophisticated tools for disseminating disinformation, most authoritarian regimes rely on blunt tools to silence freedom of speech such as trolling, harassment and targeting journalists or political dissidents with hate speech or threats. Indeed, trolling journalists has been recognized as a new and widespread threat to freedom of the press and freedom of expression around the world.[21] In Azerbaijan, Bahrain, Russia, and Turkey we found evidence of state-sponsored trolling behaviour.

MODAL TARGETS

Finally, modal targets represents the most common target for coordinated disinformation campaigns. We collected evidence of various incidents where cyber troops were used to shape the public debate. Some incidents focused on domestic audiences, such as the use of computational propaganda as a tool of social control and censorship. Other incidents focused on foreign adversaries, such as foreign influence operations. Then, we organized this information by regime type to calculate the modal targets of each regime type.

Across all three regimes, the modal target was domestic audiences. In democracies, this tended to be political parties using OMS during elections. In authoritarian regimes, OMS is used as another tool of censorship and repression. In only a few instances did we find cyber troops using OMS on foreign audiences. Examples here include Russia targeting the United States as well as Baltic and European countries, but also foreign operations between China and Taiwan, North and South Korea or Israel and Palestine

[20] Woolley, Samuel and Philip Howard. 2017. Computational Propaganda Worldwide: Executive Summary. Computational Propaganda Working Paper Series. Oxford: UK.
[21] Reporters Without Boarders. 2018. Online Harassment of Journalists: The Trolls Attack"
https://rsf.org/en/news/rsf-publishes-report-online-harassment-journalists

LIMITATIONS

While the findings of this paper serve to inform a broader understanding of the global organization of social media manipulation, there are several limitations to this methodology that should be considered. First, data about OMS is spotty at best. Many of these activities occur in secretive military contexts, or behind the proprietary walls of private actors. Thus, painting a complete picture of OMS activities online by government actors is extremely difficult, and there will be gaps in the data and cases collected. The cases we identified are no way exhaustive about the extent to which governments and political party actors use OMS. Nevertheless, they are important to begin inventorying to start developing a broader understanding of this phenomenon and the implications for democracy.

Second, the data collected for the analysis was based on open source information in the English language. While expert consultations were conducted to ensure the accuracy of data collected in non-English country-specific contexts, we only consulted individuals once we had identified a case of OMS. Thus, there are many other cases that might have not been captured because of the language used.

Finally, we used very simplistic measures to calculate the modal actor types, level of formal organization, level of capacity and modal targets. Although a more rigorous model could be adopted with more data points, this simplistic model demonstrates a few important differences that are already emerging between regime types and how different actors use social media to manipulate public opinion. These insights are important for beginning to establish insights into this phenomenon and encourage further research on this topic.

CONCLUSION

Cyber troops invest significant funds and resources in an attempt to sway public opinion over social media. Increasingly, governments and political parties around the world are investing in the tools and techniques of computational propaganda to shape the outcomes of elections,[22] disrupt diplomatic efforts,[23] and undermine peace building efforts.[24] It is valuable to know this because it means those of us who investigate such phenomena have bigger objects and subjects of study. But it also means that even the most traditional ways of analysing the causes and consequences of modern peace, conflict, trade, diplomacy, and myriad other international process must consider that political actors have a significant new tool for political communication--and for disrupting the political signals of rival actors.

By taking a global perspective on computational propaganda and the actors involved in spreading disinformation over social media, we can identify emerging trends and track the

[22] Howard, Philip N., Bence Kollanyi, Samantha Bradshaw and Lisa-Maria Neudert. 2017. Social Media, News and Political Information During the US Election: Was Polarizing Content Concentrated in Swing States? Computational Propaganda Project Data Memo. September 28.

[23] Powers, Shawn and Markos Kounalakis. 2017. Can Public Diplomacy Survive the Internet? Bots, Echo Chambers and Disinformation. *United States State Department, Advisory Commission on Public Diplomacy.* May.

[24] Aastha, Nigam, Dambanemuya Henry K., Joshi Madhav, and Chawlaw Nitesh V. 2017. Harvesting Social Signals to Inform Peace Processes Implementation and Monitoring. *Big Data,* 5(4) pp. 337-355.

evolution of this phenomenon over time. It is clear that more state actors are attempting to exploit social media in order to exercise power in the digital age. From 2017-2018 we have already seen the size of our sample grow, with more political parties and governments beginning to experiment with computational propaganda.[25] Domestic and international affairs have become proliferated with examples of state actors using and abusing social media to achieve political goals. These examples demonstrate the changing nature of cyber power, and the addition of computational propaganda to the arsenal of cyber warfare. As innovation continues in areas such as artificial intelligence, machine learning, the Internet of Things, and big data analytics, we can assume that the nature and strategy of computational propaganda will also evolve over time. It will be important for scholarship to understand how power is assumed and exercised through computational propaganda, and the consequences of this phenomenon for society and democracy.

[25] Bradshaw, Samantha and Philip N. Howard. 2018. Challenging Truth and Trust: The Global Organization of Social Media Manipulation. COMPROP Working Paper Series.

BIBLIOGRAPHY

Aastha, Nigam, Dambanemuya Henry K., Joshi Madhav, and Chawlaw Nitesh V. 2017. Harvesting Social Signals to Inform Peace Processes Implementation and Monitoring. *Big Data,* 5(4) pp. 337-355.

Bacharach P. and Baratz, M. S. 1963. Decisions and Nondecisions: An Analytical Framework. *The American Political Science Review* 57(3) pp. 632-642,

Beissinger, Mark R. 2007. Structure and Example in Modular Political Phenomena: The Diffusion of Bulldozer/Rose/Orange/Tulip Revolutions. *Perspectives in Politics,* 5(2) pp. 259-276.

Bernard, Rose. 2017. These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of the Islamic State. *Journal of Cyber Policy,* 2(2) pp. 255-265.

Beyer, Jessica L. 2014. "Expect Us: Online Communities and Political Mobilization" Oxford University Press: Oxford.

Bradshaw, Samantha and Philip N. Howard. 2017. Troops, Trolls and Troublemakers: A Global Inventory of Social Media Manipulation. *Computational Propaganda Project Working Paper.*

Bradshaw, Samantha and Philip N. Howard. 2018. Challenging Truth and Trust: The Global Organization of Social Media Manipulation. COMPROP Working Paper Series.

Bourdieu, P. 1979. Symbolic Power. Critique of Anthropology, 4(13-14) pp. 77-85.

Coleman, Gabriella. 2014. "Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous" Singapore Books.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. 2008. Access Denied. Cambridge: MIT Press

Deibert, R. 2013. *Black Code: Surveillance, Privacy and the Dark Side of the Internet.* Signal: Toronto.

Department of Justice. 2018. United States of America v. Internet Research Agency (18 U.S.C. 2,371,1349,1028A)

Dobson, William. 2012. The Dictators Learning Curve. Tyranny and Democracy in the Modern World. Vintage Press: London

Healey, J. 2017. Cyber Warfare in the 21st Century: Threats, Challenges and Opportunities. House Committee on Armed Services.

Howard, Philip N. 2010. “The Digital Origins of Dictatorship and Democracy.” Oxford University Press: Oxford

Howard, Philip N. and Muzammi M. Hussain. 2013. “Democracy’s Fourth Wave? Digital Media and the Arab Spring.” Oxford University Press: Oxford.

Howard, Philip N., Bence Kollanyi, Samantha Bradshaw and Lisa-Maria Neudert. 2017. Social Media, News and Political Information During the US Election: Was Polarizing Content Concentrated in Swing States? Computational Propaganda Project Data Memo. September 28.

Lukes, S. 1970. Power: A Radical View. London: Palgrave

MacKinnon, Rebecca. 2011. Chinas Networked Authoritarianism. *Journal of Democracy,* 22(2) pp. 32-46.

MacKinnon, Rebecca. 2012. Consent of the Networked: The Worldwide Struggle for Internet Freedom. Basic Books.

Margetts, Helen, Peter John, Scott Hale, and Taha Yasseri. 2015. “Political Turbulence: How Social Media Shape Collective Action.” Princeton University Press: Princeton.

Nye, J. 1990. Soft Power. Foreign Policy, 80 pp,153-171.

Nye, J. (2004). Soft Power. The Means to Success in World Politics. New York: Public Affairs Press.

Owen, Taylor. 2015. Disruptive Power: The Crisis of The State in the Digital Age. Oxford Studies in Digital Politics: Oxford.

Pearce, K. E. and Kendzior S. 2012. Networked Authoritarianism and Social Media in Azerbaijan. *Journal of Communication,* 62(2) pp. 283-298.

Powers, Shawn and Markos Kounalakis. 2017. Can Public Diplomacy Survive the Internet? Bots, Echo Chambers and Disinformation. *United States State Department, Advisory Commission on Public Diplomacy*. May.

Walker, C. and Ludwig, J. 2017. The Meaning of Sharp Power. *Foreign Affairs,* November.

Woolley, Samuel and Philip Howard. 2017. Computational Propaganda Worldwide: Executive Summary. Computational Propaganda Working Paper Series. Oxford: UK.

Zetter, K. 2014. Countdown to Zero Day. New York: Crown Publishers.