Wi-Fi in Warzones: How Do Armed Organizations Capture the Information Advantage?



Laura Courchesne
St. John's College
Candidate Number: 1073788
Word Count: 74,628
August 17, 2022

Final dissertation material submitted in partial fulfillment of the requirements for the degree of DPhil in International Relations in the Department of Politics and International Relations at the University of Oxford

Table of Contents

Project Overview **3**

Introduction **4**
Review of the Literature 10
Overview and Contributions 19

Paper 1 - The Armed CTO: Towards a Theory of ICT Adoption **23**

The Evolving ICT Environment 29
Existing Theories of Technology Adoption 38
Disruptive Attribute Theory: The Role of Intervening Variables in ICT Adoption 42
Exploring the Range of ICT Adoption 52
The Communist Party of Nepal - Maoists (CPN-M) 55
Los Zetas of Mexico 63
Russia, Russian Armed Forces 69
People's Republic of China, People's Liberation Army 74
Discussion 82
Conclusion 86

Paper 2 - What's New about the New Information Environment? How Private Firms Shape the Landscape for Strategic Competition **89**

The Internet Landscape, Strategic Interaction, and Private Actors 96
Characterizing the Online Information Landscape 109
Platform Governance in the Real World 123
Islamic State and Non-State Armed Groups 124
Russia 127
China 130
Discussion and Policy Implications 133

Paper 3 - Twitter and the Taliban: Patterns, Paradoxes, and the Power of Platforms **138**

Non-State Armed Groups on Social Media 143
ICT and the Taliban 149
The Taliban Online 159
Quantitative Analysis: Twitter Activity During 2021 Takeover 167
Methods 170
Results 173
Discussion 194
Conclusion 198
Appendix 1 201
Appendix 2 217

Project Conclusion **219**

Bibliography **228**

Project Overview

From the social media-driven inceptions of civil wars in Libya and Syria to the recent cyber-augmented Russian invasion of Ukraine, information and communications technology (ICT) plays an integral role in the operational success of armed organizations in modern combat. Increased access to ICT, coupled with ease of adoption and low investment costs, have enabled armed organizations - both state militaries and non-state armed groups - to incorporate ICT as a critical component of organizational operations. States have increasingly co-opted and manipulated the online environment to their benefit, leveraging social media platforms such as Facebook, Twitter, and YouTube to monitor internal dissent, influence foreign populations, and propagate incendiary ideas abroad. Meanwhile, rebel groups have leveraged Google Maps, Google Earth, WhatsApp, and Skype to supplement kinetic operations, correct mortar fire, engage in information collection, and communicate with one another and civilians. And yet, international relations scholarship has failed to account for the diversity of armed organizations' use of ICT, as well as the forces contributing to patterns of adoption and adaptation. Existing models of military technology adoption are often centered on the impact of organizational factors, overlooking the role of technological attributes and focused primarily on the behaviors of states.

This article-based dissertation aims to explore the impact of the new information landscape and how armed organizations respond to the strategic challenges of modern ICT. Paper 1 (*The Armed CTO: Towards a Theory of ICT Adoption*) introduces disruptive attribute theory, presenting four intervening variables for understanding ICT adoption by states and non-states. The paper leverages case studies across conflicts, technologies, and organizations to engage in a plausibility probe. Case studies include the creation of a national radio network by the Los Zetas drug cartel of Mexico, the use of satellite phones by the CPN-Maoists of Nepal during a national suspension of phone service, Russian reliance on state-owned social media platform VKontakte during its occupation of eastern Ukraine, and the weaponization of Facebook and Twitter by the Chinese military to wage influence operations in Taiwan. Paper 2 (*What's New about the New Information Environment? How Private Firms Shape the Landscape for Strategic Competition*), co-authored with Dr. Jacob N. Shapiro, focuses on the modern information environment, arguing that social media platforms have created a fundamentally new landscape for strategic competition. Using a series of case studies, we highlight how social media policies alter the environment for influence operations along three key dimensions: resource constraints, audience access constraints, and content constraints. This analysis also presents a large dataset (n = 163) of platform policy changes categorized by strategic impact. Finally, Paper 3 (*Twitter and the Taliban: Patterns, Paradoxes, and the Power of Platforms*) engages in an in-depth analysis of a novel dataset of 112,354 tweets from 63 Taliban-linked Twitter accounts. It reviews the Taliban's social media presence throughout the group's 2021 takeover of Afghanistan, comparing online activity with on-the-ground events and highlighting the use of platform features to amplify their influence campaign.

Wi-Fi in Warzones: How Do Armed Organizations Capture the Information Advantage?

Introduction

On February 24, 2022, Russia began its invasion of Ukraine, launching missile and artillery attacks on major cities.[1] Since then, the war has been broadcast online: photos and videos uploaded by civilian journalists highlighting the human costs of the conflict in real-time, disinformation spread by Russian-linked actors justifying the 'special military operation,' and selfie videos filmed by the Ukrainian president, Volodymyr Zelenskyy, calling on the international community to take action.[2] The invasion highlights the centrality of information and communications technology (ICT) to modern conflict, as all sides struggle for supremacy on multiple information fronts: internationally, domestically, and in the physical conflict space.

Since the inception of the conflict, Russia has weaponized social media, attempting to undermine international support for their opponent. Russian disinformation is advancing narratives online that the Ukrainian government is a neo-Nazi regime engaged in genocide, that the U.S. is supporting the development of biological weapons in Ukraine, and that the Russian invasion is lawful because Ukraine "never registered its borders with the United Nations."[3] So far, these

---

1 "Timeline: The events leading up to Russia's invasion of Ukraine," *Reuters*, March 1, 2022, https://www.reuters.com/world/europe/events-leading-up-russias-invasion-ukraine-2022-02-28/.

2 Craig Timberg and Drew Harwell, "Social media fuels new type of 'fog of war' in Ukraine conflict," *The Washington Post,* February 24, 2022, https://www.washingtonpost.com/technology/2022/02/24/ukraine-russia-war-twitter-social-media; Aja Romano, "Reckoning with the war meme in wartime," *Vox*, February 25, 2022, https://www.vox.com/culture/2022 /2/25/22950655/ukrainian-invasion-memes-political-cartoons-controversy; Eliot Higgins, "These are the Cluster Munitions Documented by Ukrainian Civilians," *Bellingcat*, March 11, 2022, https://www.bellingcat.com/news/rest- of-world/2022/03/11/these-are-the-cluster-munitions-documented-by-ukrainian-civilians/.

3 Rebecca Kern, Mark Scott, Clothilde Goujard, "Social media platforms on the defensive as Russian-based disinformation about Ukraine spreads," *POLITICO*, March 24, 2022, https://www.politico.com/news/2022/02/24/social-media-platforms-russia-ukraine-disinformation-00011559; Jessica Brandt, Valerie Wirtschafter, and Adya Danaditya, "Popular podcasters spread Russian disinformation about Ukraine biolabs," *Brookings Institution*, March 23, 2022, https://www.brookings.edu/techstream/popular-podcasters-spread-russian-disinformation-about-ukraine-

information campaigns have found support on the Chinese internet, with users praising Vladimir Putin and the Russian state on regional social media platforms, Weibo and WeChat. Meanwhile, Chinese government officials are taking to Twitter to contradict Western reporting of the conflict.[4]

Domestically, Putin has eliminated all independent media and engaged in efforts to criminalize discussion, going so far as to ban the broadcast of specific words, including 'war,' 'assault,' or 'invasion.'[5] Facebook and Instagram were banned on March 21, with the Russian government citing the platforms' facilitation of "extremist activities."[6] The government has also passed a new law, which penalizes discussion of the war in Ukraine with prison sentences of up to 15 years. Russian users are prevented from uploading new content to TikTok and have faced disruption of service on Twitter. In a bid to access external information, Russian civilian demand for VPNs has increased dramatically.[7] In Russian-occupied territories in eastern Ukraine, Ukrainians have been forced to use Russian SIM cards, which are preventing users from sending images and videos and accessing the internet.[8]

biolabs/; Maria Giovanna Sessa, "Ukraine conflict disinformation: worldwide narratives and trends," *EU Disinfo Lab*, https://www.disinfo.eu/publications/ukraine-conflict-disinformation-worldwide-narratives-and-trends/.

[4] Li Yuan, "Why the Chinese Internet Is Cheering Russia's Invasion," *The New York Times,* February 27, 2022, https://www.nytimes.com/2022/02/27/business/china-russia-ukraine-invasion.html.

[5] Maya Vinokour, "Russia's Media Is Now Totally in Putin's Hands," *Foreign Policy,* April 1, 2022, https://foreignpolicy .com/2022/04/05/russia-media-independence-putin/; AFP, "Russia Bans Media Outlets From Using Words 'War,' 'Invasion'," *The Moscow Times*, https://www.themoscowtimes.com/2022/02/26/russia-bans-media-outlets-from- using-words-war-invasion-a76605.

[6] Pjotr Sauer, "Russia bans Facebook and Instagram under 'extremism' law," *The Guardian*, March 21, 2022, https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and-instagram-under-extremism-law.

[7] Shannon Bond and Bobby Allyn, "Russia is restricting social media. Here's what we know," *NPR*, March 21, 2022, https://www.npr.org/2022/03/07/1085025672/russia-social-media-ban; Adam Satariano, "Russia Intensifies Censorship Campaign, Pressuring Tech Giants," *The New York Times*, February 26, 2022, https://www.nytimes.com/ 2022/02/26/technology/russia-censorship-tech.html.

[8] Anshel Pfeffer, "Russian forcing occupied Ukrainians to use its mobile network," *Haaretz*, March 28, 2022, https:// www.haaretz.com/world-news/europe/.premium-occupiers-forcing-ukrainians-to-switch-to-russian-cell-phone-networks-1.10703781.

Meanwhile, in the physical battlespace, Russian forces have seemingly struggled to adopt and deploy secure ICT, using walkie-talkies and push-to-talk radios broadcasting on unencrypted frequencies.[9] Russian soldiers are depending on the same commercial cell phone networks used by Ukrainians. There are also numerous reports of Russian soldiers using their own personal phones to call family members. In response, military leaders are confiscating cell phones in an attempt to enforce greater information security. Using open-source methods, the investigative organization Bellingcat recorded Russian fighters using unencrypted communications to report the death of a top officer's nephew.[10] When Ukraine banned all numbers with a Russian country code from their networks, Russian soldiers began to steal Ukrainian phones.[11] Shockingly, private citizens are also seemingly able to monitor Russian communications: "Russian military transmissions over unsecured lines have been so prevalent [...] that amateur radio enthusiasts have tuned into them online using sites such as Web SDR."[12]

But Ukrainians and their leaders have proven resilient and adept at capturing international support through social media. A selfie video from president Zelensky, posted on February 25, was viewed 3 million times in the first hour.[13] Zelensky's official Instagram has amassed 16.6 million

---

9 "Why Russian radios in Ukraine are getting spammed with heavy metal," *The Economist,* March 28, 2022, https://www.economist.com/the-economist-explains/2022/03/28/why-russian-radios-ukraine-war-intercepted-heavy-metal; Alex Horton and Shane Harris, "Russian troops' tendency to talk on unsecured lines is proving costly," *The Washington Post*, March 27, 2022, https://www.washingtonpost.com/national-security/2022/03/27/russian-military- unsecured-communications/.

10 Jack Detsch and Amy Mackinnon, "'The Ukrainians Are Listening': Russia's Military Radios Are Getting Owned," *Foreign Policy*, March 22, 2022, https://foreignpolicy.com/2022/03/22/ukraine-russia-military-radio/.

11 Ibid.

12 Alex Horton and Shane Harris, "Russian troops' tendency to talk on unsecured lines is proving costly," *The Washington Post*, March 27, 2022, https://www.washingtonpost.com/national-security/2022/03/27/russian-military-unsecured-communications/.

13 Anjana Susarla, "Why Zelenskyy's 'selfie videos' are helping Ukraine win the PR war against Russia," *The Conversation*, March 1, 2022, https://theconversation.com/why-zelenskyys-selfie-videos-are-helping-ukraine-win-the-pr-war-against-russia-178117; Steven Erlanger, "How Volodymyr Zelensky rallied Ukrainians, and the world, against Putin," *The New York Times*, February 27, 2022, https://www.nytimes.com/2022/02/27/world/europe/volodymyr-zelensky-ukraine - russia.html.

followers as of April 7, 2022.[14] Zelensky has also engaged in direct and personalized communication with Ukrainian civilians using the messaging platform Telegram.[15] Recognizing this threat, Russian-linked accounts have tried to undermine the efficacy of Ukrainian information campaigning. For example, a deepfake video of Zelensky emerged online in March encouraging Ukrainian soldiers to lay down their weapons and surrender.[16]

Ukraine's vice prime minister and minister of digital transformation, Mykhailo Fedorov, has also taken to social media to ask private companies to limit Russian access to ICT. He called on Facebook to block Russian-based users from creating new accounts on the platform. He wrote to Apple's CEO Tim Cook, pleading for the company to block Russian access to the Apple Store.[17] SpaceX CEO, Elon Musk, provided Starlink internet satellites to Ukrainians as a result of a Twitter exchange between Fedorov and Musk. By the end of March 2022, Musk had sent thousands of Starlink internet kits to Ukraine.[18]

Private companies are also countering Russia's ICT capacity. Google eliminated the monetization capacities of Russian state-funded media channels and Facebook is now preventing

---

[14] See Zelensky's Instagram page (zelenskiy_official) at https://www.instagram.com/zelenskiy_official/

[15] Sam Sabin and Laurens Cerulus, "3 reasons Moscow isn't taking down Ukraine's cell networks," *POLITICO,* March 7, 2022, https://www.politico.com/news/2022/03/07/ukraine-phones-internet-still-work-00014487.

[16] Bobby Allyn, "Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn," *NPR*, March 16, 2022, https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia; Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," *WIRED,* March 17, 2022, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.

[17] Sarah Fischer, "Internet becomes battleground in Russia's Ukraine invasion," *Axios*, February 27, 2022, https://www.axios.com/internet-key-battleground-russia-ukraine-b39b49a2-79ff-4fdf-af15-1dee5217c867.html.

[18] Brett Molina, "Ukraine confirms arrival of Starlink satellite internet hardware after plea to Elon Musk," *USA Today,* March 1, 2022, https://www.usatoday.com/story/tech/2022/03/01/starlink-ukraine-elon-musk-satellite-internet/9328753002/; Mike Ives, "Satellite internet terminals, sent by Elon Musk, arrive in Ukraine," *The New York Times*, March 1, 2022, https://www.nytimes.com/2022/02/28/world/europe/elon-musk-satellite-internet-ukraine.html; Michael Sheetz, "Elon Musk's SpaceX sent thousands of Starlink satellite internet dishes to Ukraine, company's president says," *CNBC*, March 22, 2022, https://www.cnbc.com/2022/03/22/elon-musk-spacex-thousands-of-starlink-satellite- dishes-sent-to-ukraine.html.

Russian media from running advertisements.[19] A U.S.-based mobile phone app, Premise, suspended service in Ukraine after the Ukrainian government claimed that the app was used by Russians to identify potential locations to airstrike.[20] Separately, Polish programmers built a tool to send targeted messages, including footage of the conflict and video clips of Western media reporting, to millions of Russian cell phone numbers and email addresses.[21]

Russia's invasion offers a timely case study of ICT's importance in modern conflicts.[22] Paradoxically, despite its reputation as a global military power, Russia seemingly failed to prepare an effective strategy for deploying information communications technologies and appears so far to be losing the online information war to Ukraine. This case is emblematic of broader questions relating to ICT's adoption in combat: What determines patterns of ICT use? What kinds of organizations are better suited to gain an information advantage in modern conflicts? And does the technology itself matter?

Modern information and communications technology (ICT) is defined as technology that is used to transmit, store, access, create, or exchange information across distances instantaneously. To achieve this level of speed and scale, these technologies convert information into alternative forms, such as radio waves (in the case of radios, landlines, and cell phones) and bits (in the case of computers and the internet) to facilitate transmission. Increased access to ICT, coupled with ease of adoption

---

19 Sarah Fischer, "Internet becomes battleground in Russia's Ukraine invasion."

20 Byron Tau, "Premise Mobile-Phone App Suspends Ukraine Activities After Accusations Fly," *The Wall Street Journal*, February 26, 2022, https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-02-26/card/premise-mobile-phone-app-suspends-ukraine-activities-after-accusations-fly-8FDnhZe9raunaIJ4HV66.

21 Bojan Pancevski, "Using a New Cyber Tool, Westerners Have Been Texting Russians About the War in Ukraine" *The Wall Street Journal,* March 22, 2022, https://www.wsj.com/articles/using-a-new-cyber-tool-westerners-have-been-texting-russians-about-the-war-in-ukraine-11647100803.

22 Jon R. Lindsay, *Information technology and military power* (Cornell University Press, 2020).

and low investment costs, has enabled state militaries and non-state armed groups to incorporate these technologies as critical components of military operations and strategy.[23] However, international relations scholarship on military technology adoption is often focused on the role of organizational factors, treating technology homogeneously and orienting to the adoption behaviors of states. As a result, the field has failed to account for the diversity of armed organizations' use of ICT nor provided adequate frameworks for anticipating how ICT will be weaponized and the types of organizations that can gain an information advantage. The Russia-Ukraine case highlights four important factors that this project explores in-depth. These factors reflect specific features of ICT as a category of technology that, when paired with existing theory on the role of organization and resources, help to better account for the variation and seemingly counterintuitive behaviors of armed groups' adoption of ICT.

First, sharing infrastructure with an opponent, often required when deploying ICT, introduces strategic tradeoffs and significant interaction effects. For example, Russian forces rely on local Ukrainian telecom networks and communications infrastructure to coordinate. Consequently, destroying those cell towers would harm their operations, even if this action would also impact their Ukrainian opponent.

Second, modern ICT causes private technology companies to have an outsized role in conflicts. For example, Ukrainian officials are pleading directly to Silicon Valley executives to remove ICT access from their opponent. Companies themselves are developing ideological policies, deciding who has access to their platform and how politically motivated actors can use it.

[23] Non-state armed groups (NSAGs) are defined as "armed organizations operating outside the control of the state and willing and able to use force to achieve their objectives," see Benedetta Berti, "What's in a name? Re-conceptualizing non-state armed groups in the Middle East," *Palgrave Communications*, Vol. 2, No. 1 (2016), pp. 1-8.

Third, the increasing ubiquity and diffusion of ICT can cause armed organizations to engage in unintentional adoption, with individual soldiers using technologies independent of organizational mandates. For example, Russian soldiers are using their own personal cell phones to communicate, introducing security and intelligence risks.

Fourth, ICT's capacity for customization and ability to support multiple functions can result in counterintuitive conflict outcomes. Even as compared to other military technologies, developing a sophisticated, adaptive organizational strategy for technology adoption and deployment is vital due to the inherent breadth of applications. Despite being comparatively less-resourced, Ukraine is seemingly winning the information war on social media. The Ukrainian government's specific style of deploying ICT, which reflects its tremendous potential for customization, highlights how ICT can help tip the balance in favor of weaker actors. This includes Zelensky's specific mode of personal and direct communication with the world. His selfie videos, often including other senior government leaders, with the frontlines in the backdrop, successfully contrast the cold, detached denial of official Russian state messaging.

Review of the Literature

This project seeks to contribute to two key research streams related to the use of technology in conflict: (1) theories of technology adoption by state militaries, and (2) the relationship between ICT and political violence, with a focus on conflict actors' use of social media.

Technology Adoption

Traditional international relations scholarship equates technology with military power, advocating for the pursuit of large-scale, highly destructive technologies as essential for states' strategic

advantage, governing outcomes of war and conflict.[24] Posen (1984) highlights the need for states to constantly innovate, moving towards the creation, adoption, and deployment of cutting edge technologies.[25] Rosen (1991) similarly underscores the urgency for states to innovate, delineating the wartime and peacetime mechanisms contributing to differing forms of technology creation and adoption.[26] As a result, the literature is often overly fixated on "big threats and exquisite technologies."[27] The field's preoccupation with nuclear weapons exemplifies this approach.[28] And while understanding how and when states develop and wield these types of technologies is critical, it often comes at the expense of exploring other crucial technological questions: do non-state armed groups adhere to the same strategies and rationales as states in adopting and using technology? Do all forms of technology abide by the same principles of adoption and use? And do existing models help us to accurately understand or predict variation in adoption?

Scholarship on military technology adoption can be divided into two key theoretical approaches. The first treats both the adopter and the type of adopted technology as constants, focusing instead on the importance of diffusion and comparative adoption.[29] This includes epidemic and contagion theories of adoption.[30] Many of these models argue for an advantage of backwardness,

---

[24] Martin Van Creveld, *Technology and war: From 2000 BC to the present* (Simon and Schuster, 2010).

[25] Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca NY: Cornell University Press, 1984).

[26] Stephen P. Rosen, *Winning the Next War: Innovation in the Modern Military* (Ithaca, NY: Cornell University Press, 1991).

[27] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford University Press, 2019).

[28] Scott D. Sagan, "Why do states build nuclear weapons?: Three models in search of a bomb," *International Security*, Vol. 21, No. 3 (1996), pp. 54-86; Robert Jervis, *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon*, (Cornell University Press, 1989).

[29] Kenneth N. Waltz, *Theory of international politics* (Reading, Mass.: Addison-Webley, 1979); Edwin Mansfield, "Technical change and the rate of imitation," *Econometrica: Journal of the Econometric Society* (1961), pp. 741-766; Barbara Wejnert, "Integrating models of diffusion of innovations: A conceptual framework," *Annual review of sociology*, Vol. 28, No. 1 (2002), pp. 297-326.

[30] Corey M. Angst, Ritu Agarwal, Vallabh Sambamurthy, and Ken Kelley, "Social contagion and information technology diffusion: The adoption of electronic medical records in US hospitals," *Management Science*, Vol. 56, No. 8 (2010), pp. 1219-1241; Manus I. Midlarsky, Martha Crenshaw, and Fumihiko Yoshida, "Why violence spreads: The contagion of international terrorism," *International Studies Quarterly*, Vol. 24, No. 2 (1980), pp. 262-298.

wherein less developed states can free ride on the innovation and research of more advanced states, closing military-technological gaps quickly through imitation.[31] Waltz (1979)'s description of the international system presumes that states will opt to "imitate the military innovations contrived by the country of the greatest capability and ingenuity," resulting in the "weapons of major contenders… to look much the same all over the world."[32]

The second approach explains patterns of technological adoption by studying the organizational attributes of the states and non-state armed groups involved.[33] This literature has provided evidence that organizational features - including doctrine, process, and resources - are crucial in shaping adoption behaviors.[34] Among the most prominent models is Horowitz (2007)'s adoption-capacity theory. Horowitz argues that "once states have necessary exposure," adoption is determined by the two organizational factors of financial intensity and organizational capacity.[35] Capacity is argued to include "human capital, tacit knowledge, and organizational practices."[36] Further, adoption-capacity theory contends that being the first to innovate, or the supposed 'first-mover advantage', does not guarantee mastery over the technology nor long-term superiority over your opponent. In considering ICT adoption through the lens of adoption-capacity theory, its

---

31 Alexander Gerschenkron, *Economic Backwardness in Historical Perspective: A Book of Essays* (Cambridge, Mass.: Belknap, 1962), pp. 5–30; Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1981), pp. 176–177; Kenneth Waltz, *Theory of International Politics*, pp. 74, 127.

32 Kenneth Waltz, *Theory of International Relations,* pp. 111–114.

33 See Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics* (Harvard University, 2007); Michael C. Horowitz, "Nonstate actors and the diffusion of innovations: The case of suicide terrorism," *International Organization*, Vol. 64, No. 1 (2010), pp. 33-64; Eszter Hargittai, "Weaving the Western Web: Explaining differences in Internet connectivity among OECD countries," *Telecommunications policy*, Vol. 23, No. 10-11 (1999), pp. 701-718; Sampsa Kiiski and Matti Pohjola, "Cross-country diffusion of the Internet," *Information Economics and Policy*, Vol. 14, No. 2 (2002), pp. 297-310.

34 Eliot A. Cohen, "Change and transformation in military affairs," *Journal of Strategic Studies*, Vol. 27, No. 3 (2004), pp. 395-407; Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*; Kimberly Marten Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955 - 1991* (Princeton University Press, 1993).

35 Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics*.

36 Michael C. Horowitz, Shahryar Pasandideh, Andrea Gilli, and Mauro Gilli, "Correspondence: Military-Technological Imitation and Rising Powers," *International Security*, Vol. 44, No. 2 (2019), pp. 185-192.

diffusion among armed organizations is viewed as a product of lowered financial intensity. Specifically, it argues that "cheaper and more widely available information age technologies could lower the barriers for groups seeking to challenge state authority, meaning it will become increasingly easy for new groups to spring up in virtual environments and exchange information across borders."[37] Throughout this project, this literature is treated as important but incomplete. In particular, the factors highlighted by adoption-capacity theory have a presumed role in explaining aspects of the adoption behaviors of the states and non-states discussed.

A nascent literature has taken a third approach, one furthered by this thesis project, arguing that technology's attributes are also crucial for explaining differences in the adoption process. As highlighted by Gilli and Gilli (2018), attributes of the technology may matter in ways beyond imposing on organizational capacity and resource requirements. The authors argue that existing theory ignores the impact of "the exponential increase in the complexity of military technology" since the second industrial revolution.[38] Complexity reduces diffusion and adoption of technologies by heightening the barriers to entry. Actors seeking to develop a more complex technology must now possess (1) the requisite resources (baseline levels of scientific, technical, and industrial infrastructure) and (2) the requisite knowledge base (the expertise and organizational wherewithal to institute the process and structure of development). Thus, as technological complexity increases, fewer states are able to meet the demands necessary to imitate and produce the technology for themselves.

[37] Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics*, p. 26.
[38] Andrea Gilli and Mauro Gilli, "Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage," *International Security*, Vol. 43, No. 3 (2018), pp. 141 - 189.

More recently, scholars have also begun to study the implications of emerging technology on global politics, with a specific emphasis on the consequences of weaponizing artificial intelligence.[39] Cronin (2019) highlights the impact of open technological innovation, which is enabling a broad range of politically-motivated actors to acquire autonomous weapons, AI, and smartphones.[40] Lindsay (2020) additionally emphasizes the important connection between information technology and military power.[41] Emerging technologies are argued to have an impact on global politics, but this effect is "mediated by the ability of military organizations [...] to use them effectively in relevant military scenarios and in the pursuit of political ends." [42]

Crucially, all three approaches provide sparse evidence of the factors shaping different patterns of adoption by non-state actors. Cronin (2019) argues that the scope of studies on technology adoption and innovation should be extended to non-state actors who are empowered by newly emerging technologies.[43] While, there are numerous studies on specific terrorism-related innovations, including suicide bombings, improvised explosive devices (IEDs), and CBRN (chemical, biological, radiological and nuclear) attacks, the field lacks comprehensive modeling for when and how these actors adopt and use technology. [44]

---

[39] Valerie M. Hudson, *Artificial intelligence and international politics*, (Routledge, 2019); James Johnson, "Artificial intelligence & future warfare: implications for international security," *Defense & Security Analysis*, Vol. 35, No. 2 (2019), pp. 147-169; Kenneth Payne, "Artificial intelligence: a revolution in strategic affairs?," *Survival*, Vol. 60, No. 5 (2018), pp. 7-32; Greg Allen and Taniel Chan, *Artificial intelligence and national security,* (Cambridge, MA: Belfer Center for Science and International Affairs, 2017).

[40] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford University Press, 2019).

[41] Jon R. Lindsay, *Information technology and military power*.

[42] Michael C. Horowitz, "Do emerging military technologies matter for international politics?," *Annual Review of Political Science* Vol. 23 (2020), pp. 385-400.

[43] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*.

[44] Michael C. Horowitz, "Nonstate actors and the diffusion of innovations: The case of suicide terrorism," *International Organization*, Vol. 64, No. 1 (2010), pp. 33-64l; Magnus Ranstorp, and Magnus Normark, *Unconventional Weapons and International Terrorism* (Abingdon, UK: Routledge, 2009); Magnus Ranstorp and Magnus Normark, *Understanding Terrorism Innovation and Learning* (Oxon: Routledge, 2015); Nicole A. Tishler, "Trends in terrorists' weapons adoption and the study thereof," *International Studies Review*, Vol. 20, No. 3 (2018), pp. 368-394; Paul Gill, "Tactical innovation and the provisional Irish Republican Army," *Studies in Conflict & Terrorism*, Vol. 40, No. 7 (2017), pp. 573-585; Gary A.

ICT and Political Violence[45]

Research on ICT and political violence has primarily focused on cell phones, particularly exploring the relationship between cell network coverage and rates of violence.[46] For example, Shapiro and Weidmann (2015) found that increased mobile phone communications were linked to decreases in violence in Iraq.[47] Macías-Medellín and Atuesta (2021) highlight that different forms of ICT can have different effects on levels of violence. While mobile phones enabled rebels to organize violence, the internet increased the public visibility of violence, heightening the risk of repercussions from the community.[48] There also exists a substantive historical literature on the role of radio in conflict, including its use as a tool to instigate violence and as a mode for counterpropaganda.[49]

Ackerman, "“Designing Danger” Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue," *Journal of Strategic Security*, Vol. 9, No. 1 (2016), pp. 1-11.

45 Political violence is defined as “the infliction of physical harm” that “explicitly and directly aims to impact governance” as defined in Stathis N. Kalyvas, *The landscape of political violence* (New York: Oxford University Press, 2019).

46 See Nils B. Weidmann, "Communication, technology, and political conflict: Introduction to the special issue," *Journal of Peace Research* Vol. 52, No. 3 (2015), pp. 263-268; Jan H. Pierskalla and Florian M. Hollenbach, "Technology and collective action: The effect of cell phone coverage on political violence in Africa," *American Political Science Review*, Vol. 107, No. 2 (2013), pp. 207-224; Jacob N. Shapiro and David A. Siegel, "Coordination and security: How mobile communications affect insurgency," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 312-322; Eli Berman, Joseph H. Felter, and Jacob N. Shapiro, *Small Wars, Big Data* (Princeton University Press, 2018); Catie Snow Bailard, "Ethnic conflict goes mobile: Mobile technology’s effect on the opportunities and motivations for violent collective action," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 323-337; Jacob N. Shapiro and Nils Weidmann, "Talking about killing: Cell phones, collective action, and insurgent violence in Iraq," *Collective Action, and Insurgent Violence in Iraq* (2011); Jacob N. Shapiro and Nils B. Weidmann, "Is the phone mightier than the sword? Cellphones and insurgent violence in Iraq," *International Organization*, Vol. 69, No. 2 (2015), pp. 247-274; Marco Manacorda and Andrea Tesei, "Liberation technology: Mobile phones and political mobilization in Africa," *Econometrica*, Vol. 88, No. 2 (2020), pp. 533-567; T. Camber Warren, "Explosive connections? Mass media, social media, and the geography of collective violence in African states," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 297-311.

47 Jacob N. Shapiro and Nils B. Weidmann, "Is the phone mightier than the sword? Cellphones and insurgent violence in Iraq."

48 Martín Macías-Medellín and Laura H Atuesta, "Constraints and military coordination: How ICTs shape the intensity of rebel violence," *International Interactions*, Vol. 47, No. 4 (2021), pp. 692-719.

49 See Stefano Gagliarducci, Massimiliano Gaetano Onorato, Francesco Sobbrio, and Guido Tabellini, "War of the waves: Radio and resistance during World War II," *American Economic Journal: Applied Economics*, Vol. 12, No. 4 (2020), pp. 1-38; Alex Armand, Paul Atwell, and Joseph F. Gomes, "The reach of radio: Ending civil conflict through rebel demobilization," *American economic review*, Vol. 110, No. 5 (2020), pp. 1395-1429; Darryl Li, "Echoes of violence: Considerations on radio and genocide in Rwanda," *Journal of Genocide Research*, Vol. 6, No. 1 (2004), pp. 9-27; Scott Straus, "What is the relationship between hate radio and violence? Rethinking Rwanda's “Radio Machete,”" *Politics & Society*, Vol. 35, No. 4 (2007), pp. 609-637; Christine L. Kellow, and H. Leslie Steeves, "The role of radio in the Rwandan genocide," *Journal of communication*, Vol. 48, No. 3 (1998), pp. 107-128; Benjamin Barber and Charles Miller, "Propaganda and Combat Motivation: Radio Broadcasts and German Soldiers’ Performance in World War II," *World Politics*, Vol. 71, No. 3 (2019), pp. 457-502; Maja Adena, Ruben Enikolopov, Maria Petrova, Veronica Santarosa, and Ekaterina Zhuravskaya, "Radio and the Rise of the Nazis in Prewar Germany," *The Quarterly Journal of Economics*, Vol. 130, No. 4 (2015), pp. 1885-1939.

This literature base also explores factors impacting adoption and usage, highlighting the importance of organization and technology. For example, Shapiro and Siegel (2015) found that insurgents face tradeoffs when considering cell phone usage. While coverage reduces organizational costs of communication, it increases the likelihood that insurgents can be monitored by opponents through tracing methods tied to cell phone use and improves human intelligence tied to community reporting.[50] Rød and Weidmann (2015) investigated state deployment of ICT and concluded that regime type matters, influencing strategic considerations surrounding usage.[51]As summarized by Dafoe and Lyall (2015) in their seminal review, several mitigating mechanisms impact the role of ICT in political violence, including technology costs, ICT penetration rates, and the goals and strategies of the adopting actors. The authors also identify four key areas for further research: (1) understanding the role of ICT in conflict duration, onset, and termination, (2) examining technology other than cell phones, (3) expanding the types of effects measured, beyond rates of violence, and (4) understanding the causes of geospatial and temporal variation in ICT usage and adoption by conflict actors.[52]

There also exists an emerging literature on social media and the internet and its role in reshaping conflict.[53] Zeitzoff (2017) argued that social media has four key points of impact: (1) reducing costs to communicate, (2) increasing the speed and scope of information sharing, (3) increasing the need for scholarly focus on "strategic interaction and competitive adaptation" and (4)

---

[50] Jacob N. Shapiro and David A. Siegel, "Coordination and security: How mobile communications affect insurgency."
[51] Espen Geelmuyden Rød and Nils B. Weidmann, "Empowering activists or autocrats? The Internet in authoritarian regimes," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 338-351.
[52] Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 401-413.
[53] See Anita R. Gohdes, "Studying the Internet and Violent conflict," *Conflict Management and Peace Science*, Vol. 35, No. 1 (2018), pp. 89-106; Thomas Zeitzoff, "How social media is changing conflict," *Journal of Conflict Resolution*, Vol. 61, No. 9 (2017), pp. 1970-1991; Barbara F. Walter, "The new new civil wars," *Annual Review of Political Science*, Vol. 20 (2017), pp. 469-486; Peter Warren Singer and Emerson T. Brooking, *LikeWar: The weaponization of social media* (Eamon Dolan Books, 2018).

introducing a new source of information. Critically, he argues that "social media's influence on conflict defies simplistic explanations that argue that it privileges incumbents or challengers."[54] Walter (2017) emphasizes massive increase in rebel group use of the internet, including the proliferation of terrorist-linked websites. She argues that social media has six potential impacts on the future of civil wars, including benefiting citizens rather than elites, its ability to facilitate coordination and recruitment, incentivizing framing of rebel ideology and aims in global terms, and increasing funding channels.[55]

In the last decade, literature has emerged examining the weaponization of social media by non-state armed groups. But much of it focuses on the Islamic State, with a smaller set of studies on a limited number of other prominent groups including Al-Shabaab, Hamas, and Hezbollah.[56] These studies tend to be narrowly focused, and generally explore how group ideology is promoted through social media messaging. By contrast, Loyle and Bestvater (2019) conducted one of the first comprehensive studies of non-state armed group use of social media, examining the behavior of 55 rebel groups on Twitter. The authors found that rebel groups typically use social media to spread messaging targeted at international audiences.[57]

---

54 Thomas Zeitzoff, "How social media is changing conflict."

55 Barbara F. Walter, "The new new civil wars."

56 See Scott Gates and Sukanya Podder, "Social media, recruitment, allegiance and the Islamic State," *Perspectives on Terrorism*, Vol. 9, No. 4 (2015), pp. 107-116; Tamar Mitts, Gregoire Phillips, and Barbara F. Walter, "Studying the impact of ISIS propaganda campaigns," *The Journal of Politics*, Vol. 84, No. 2 (2022); Imran Awan, "Cyber-extremism: Isis and the power of social media," *Society*, Vol. 54, No. 2 (2017), pp. 138-149; Ken Menkhaus, "Al-Shabaab and social media: A double-edged sword," *Brown Journal of World Affairs*, Vol. 20 (2013); David Mair, "# Westgate: A case study–how Al-Shabaab used Twitter during an ongoing attack," In *Violent Extremism Online*, (Routledge, 2016), pp. 65-86; Hyunjin Seo, "Visual propaganda in the age of social media: An empirical analysis of Twitter images during the 2012 Israeli–Hamas conflict," *Visual Communication Quarterly*, Vol. 21, No. 3 (2014), pp. 150-161; Gabriel Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," *New Media and Innovative Technologies,* Vol.22 (2008); Benjamin T. Jones and Eleonora Mattiacci, "A manifesto, in 140 characters or fewer: Social media as a tool of rebel diplomacy," *British Journal of Political Science*, Vol. 49, No. 2 (2019), pp. 739-76.

57 Cyanne E. Loyle and Samuel E. Bestvater, "# rebel: Rebel communication strategies in the age of social media," *Conflict Management and Peace Science*, Vol. 36, No. 6 (2019, pp. 570-590.

There also exists a newly developing literature on state use of social media, particularly to advance political aims globally, spurred by documentation of Russian influence operations during the 2016 U.S. presidential election.[58] Literature on states online tends to focus on either domestic repression or foreign influence operations.[59] Research on foreign influence operations is relatively nascent but documents many states deploying "computational propaganda—the use of automation, algorithms, and big data analytics—to influence or deceive social-media users."[60] At least 51 countries have been targeted in 78 foreign influence efforts and 25 domestic influence efforts (when governments use social media to target their own citizens) from 2011 through early-2021, including well-documented campaigns by China, Iran, Russia, Saudi Arabia, United Arab Emirates, and Venezuela.[61] States use this online coercion to gain the advantage, weaponizing "the digital domain to disrupt, spy, and degrade."[62] Scholars underscore the potential for disinformation and state-sponsored influence operations to behave as tools for global instability.[63]

---

[58] See Figure 1 in Jon Bateman, Elonnai Hickok, Laura Courchesne, Isra Thange, and Jacob N. Shapiro, "Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research," *Carnegie Endowment for International Peace*, June 28, 2021, https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence- operations-key-findings-and-gaps-from-empirical-research-pub-84824.

[59] Aim Sinpeng, "State Repression in Cyberspace: The Case of Thailand," *Asian Politics & Policy*, Vol. 5, No. 3 (2013), pp. 421-440; Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, (Oxford University Press, 2021); Steven Feldstein, "The road to digital unfreedom: How artificial intelligence is reshaping repression," *Journal of Democracy*, Vol. 30, No. 1 (2019), pp. 40-52, Herbert Lin, "The existential threat from cyber-enabled information warfare," *Bulletin of the Atomic Scientists*, Vol. 75, No. 4 (2019), pp. 187-196.

[60] Samantha Bradshaw and Philip N. Howard, "The global organization of social media disinformation campaigns," *Journal of International Affairs*, Vol. 71, No. 1.5 (2018), pp. 23-32.

[61] Diego A. Martin, Jacob N. Shapiro, and Michelle Nedashkovskaya, "Recent trends in online foreign influence efforts," *Journal of Information Warfare*, Vol. 18, No. 3 (2019), pp. 15-48; Diego A. Martin, Jacob N. Shapiro, and Julia G. Ilhardt, "Version 2.0: Recent trends in online foreign influence efforts," August 5, 2020, https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_online_influence_efforts_v2.0_aug_5_2020.pdf.

[62] Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy bears and digital trolls: Cyber strategy with a Russian twist," *Journal of Strategic Studies,* Vol. 42, No. 2 (2019), p. 212-234.

[63] Herbert Lin, "The existential threat from cyber-enabled information warfare."

Overview and Contributions

Paper 1, entitled *The Armed CTO: Towards a Theory of ICT Adoption*, introduces disruptive attribute theory, presenting a set of four critical intervening variables for understanding ICT adoption by states and non-state groups. It argues that four attributes of ICT are overlooked by existing models, which privilege the role of organizational capacity and resources in determining technology adoption.[64] Disruptive attribute theory argues the following: (1) ICT introduces distinct and strategic interaction effects, imposed by overlaps in infrastructure use by multiple conflict-relevant actors, (2) ICT increases the influence of third-party and private sector actors, who are often responsible for introducing, maintaining, and controlling ICT infrastructure in conflict zones, (3) the ubiquity and dual-use nature of ICT creates different modes of technology acquisition by armed organizations, notably individual fighters adopting ICT independently of an organizational mandate, and (4) ICT allows for customization and a wider range of applications, dramatically broadening the number of deployment strategies available to groups. These four key features of ICT act as intervening variables within existing theories of technology adoption, increasing or decreasing demands on the organizational capacity of adopting groups.

Using a qualitative case studies to support a plausibility probe, this paper analyzes the ICT adoption patterns of four armed organizations: the CPN-Maoists of Nepal's adoption of satellite phones, the creation of a national radio network by Los Zetas of Mexico, Russia's coercive purchase of social media platform VKontakte during the Russian military's occupation of eastern Ukraine, and the use of traditional and online media by the Chinese military in an influence

64 Michael Horowitz, *The diffusion of military power: Causes and consequences for international politics*; Michael C. Horowitz, "Nonstate actors and the diffusion of innovations: The case of suicide terrorism"; Michael C. Horowitz, Shahryar Pasandideh, Andrea Gilli, and Mauro Gilli, "Correspondence: Military-Technological Imitation and Rising Powers".

operation targeting Taiwan.[65] This analysis serves a critical function in theory development by assessing the applicability of the model across technologies and types of armed actors. The paper compares and contrasts technology adoption by a broad range of actors involved in political violence: two powerful states, a rebel group, and a drug cartel. It offers a technology-centric model for understanding variation in adoption and usage patterns of ICT and contributes to eliminating a gap in studies of ICT adoption by non-state armed groups.

Paper 2, *What's New about the New Information Environment? How Private Firms Shape the Landscape for Strategic Competition*, focuses on the modern information environment, arguing that social media platforms have created a fundamentally new landscape for strategic engagement between states (with some consideration of non-states). Co-authored with Dr. Jacob N. Shapiro, the paper offers an in-depth application of the second factor of disruptive attribute theory, presented in Paper 1: the role and importance of private actors. States increasingly engage in the online environment, leveraging social media to monitor internal dissent, influence their own populations, and propagate incendiary ideas abroad. Those information operations happen on a landscape that is created, controlled, and actively altered by social media platforms that serve huge swathes of the world. This introduces a fundamentally new dynamic in world politics: private companies can now remake the landscape of inter-state competition.

Using a series of case studies, the paper offers a conceptual framework for understanding and anticipating the effects of policies on online influence operations, along three key constraints: content, resource, and audience access. Underlying this analysis is a novel dataset of 163 platform

[65] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, (MIT Press, 2005), pp. 20-22, 45.

policies categorized by strategic impact, which has broader utility in supporting research on the efficacy of countermeasures.[66] The paper conceptualizes the online landscape as a changing, adaptive environment that imposes constraints and challenges, where control rests squarely with private actors. Understanding the new 'rules of the game,' including which algorithmic and policy changes impose significant effects on influence operations, will allow scholars of influence operations and soft power to avoid conflating changes in state behavior with changes to underlying goals. The paper argues that policymakers aspiring to blunt the informational advantages of autocratic opponents should view social media companies as potential strategic partners and seek to make friends with the 'mapmakers.'

Paper 3, *Twitter and the Taliban: Patterns, Paradoxes, and the Power of Platforms,* reviews the Taliban's Twitter activity, includes a novel analysis of 112, 354 tweets from 63 accounts run by senior leaders, spokesmen, and avowed members. It pursues a descriptive quantitative methods approach to establish the scope and scale of the Taliban's presence on Twitter and the ways in which the group used the platform throughout the 2021 takeover.

This research established several key trends in the Taliban's online activity: (1) the frequency and intensity of the Taliban's Twitter activity appears to track with key events in the conflict, and (2) the Taliban documented and advertised their movements online as they took the country and moved toward Kabul, (3) the Taliban made use Twitter's platform features to amplify their messaging and engage in both domestic and international outreach, including developing specialized hashtags to

[66] Laura Courchesne, Julia Ilhardt, and Jacob N. Shapiro, "Review of social science research on the impact of countermeasures against influence operations," (Harvard Kennedy School Misinformation Review, 2021); Helen Innes and Martin Innes, "De-platforming disinformation: conspiracy theories and their control," *Information, Communication & Society*, (2021), pp. 1-19.

push specific propaganda narratives and leveraging mentions to attempt to garner a response from humanitarian organizations, key political players, and journalists. Overall, it establishes that the Taliban invested considerable time and organizational resources to develop and amplify a sophisticated and coordinated campaign in real-time. The real-time nature of the group's posts highlights the Taliban's perception that social media was an important tool to augment their military and political goals (irrespective of the reality of its efficacy). This analysis also demonstrates that Twitter took minimal action against Taliban content on their platform, even when it violated stated policies about sensitive media (i.e., images and videos of gore and violence, posts inciting violence).

Taken together, the three papers argue that attributes of information and communications technology matter for explaining adoption behaviors of armed organizations. These attributes impact both state and non-state actors in conflicts, contributing to widespread variation in behavior. In particular, social media and its features present novel challenges for armed organizations seeking to control the information environment. Power over platforms rests squarely in the hands of private actors and their decisions reshape the landscape of online strategic engagement between states (and non-states). As a technology, social media can be weaponized by any politically motivated group and, if left unchecked, support real world aims and battlefield success. Specifically, the Taliban operated on Twitter with impunity, leveraging the platform to spread their messaging globally throughout their takeover of Afghanistan. Increasingly, analysis of conflict dynamics in the modern era will require a nuanced and comprehensive understanding of the power of ICT.

Paper 1

The Armed CTO: Towards a Theory of ICT Adoption

Introduction

From the social media-driven inceptions of civil wars in Libya and Syria to the cyber-augmented Russian invasion of Ukraine, information and communications technology (ICT) is playing an integral role in the operational success of armed organizations in modern combat.[67] ICT is an essential tool in states' efforts to propagate and control information flows during conflict. And critically, the pervasive diffusion of new forms of ICT, particularly cell phones and internet access, empowers an unprecedented range of actors to adopt and use this technology in novel ways.[68] Scholars have argued that modern ICTs are altering the fundamental nature of how political violence is organized.[69] Increased access to ICT, coupled with ease of adoption and low investment costs, have seemingly enabled a wide range of armed organizations - both state militaries and non-state armed groups - to incorporate ICT as a major component of organizational operations and strategy. But as highlighted by Dafoe and Lyall (2015),"variation in the adoption and use of [ICT] by different organizations remains an important empirical puzzle."[70] This variation matters. And yet, existing

[67] Matt Herbert, "Libya's War Becomes a Tech Battleground," *Institute for Security Studies*, October 8, 2019, https://issafrica .org/iss-today/libyas-war-becomes-a-tech-battleground; Melik Kaylan, "Syria's War Viewed Almost in Real Time," *The Wall Street Journal*, September 27, 2013, https://www.wsj.com/articles/syria8217s-war-viewed-almost-in-real-time- 1380305826; Mykola Makhortykh and Maryna Sydorova, "Social media and visual framing of the conflict in Eastern Ukraine," *Media, War & Conflict*, Vol. 10, No. 3 (2017), pp. 359-381.

[68] Cyanne E. Loyle and Samuel E. Bestvater, "# rebel: Rebel communication strategies in the age of social media," *Conflict Management and Peace Science*, Vol. 36, No. 6 (2019), pp. 570-590.

[69] See Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 401-413; Nils B. Weidmann, "Communication, technology, and political conflict: Introduction to the special issue," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 263-268; Barbara F. Walter, "The new new civil wars," *Annual Review of Political Science*, Vol. 20 (2017), pp. 469-486.

[70] Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda."

scholarship on military technology adoption focuses principally on the role of organizational factors, neglecting the impact of technological attributes in shaping adoption decisions and behaviors.[71]

Modern conflicts, including the Taliban's success in Afghanistan and the Ukrainian military's resilience in the face of Russian invasion, underscore the ability of weaker actors to challenge or defeat powerful states.[72] ICT is often characterized as a critical tool for empowering weaker actors, acting as the impetus for social uprisings, providing organizations with novel methods for coordination, communication, and intelligence collection, and reshaping global perceptions of conflicts.[73] In particular, modern ICT is argued to "lower the barriers for groups seeking to challenge state authority, [making it] increasingly easy for new groups to spring up in virtual environments and to exchange information across borders."[74] At the moment, we lack an understanding of the ICT capacities of non-state armed groups broadly and the online operations of states beyond a select few, namely Russia, China, and Iran.[75] Global attention has focused on the

---

[71] For a brief review of the literature see Jon Schmid and Jonathan Huang, "State adoption of transformative technology: Early railroad adoption in China and Japan," *International Studies Quarterly*, Vol. 61, No. 3 (2017), pp. 570-583. For an exemplative theory, see Michael Horowitz, *The diffusion of military power: Causes and consequences for international politics* (Harvard University, 2007).

[72] Gavin Butler, "How Social Media Helped 'Taliban 2.0' Take Control of Afghanistan," *Vice News*, August 19, 2021, https://www.vice.com/en/article/z3x5we/social-media-helped-taliban-control-afghanistan; Anjana Susarla, "Why Zelenskyy's 'selfie videos' are helping Ukraine win the PR war against Russia," *The Conversation*, March 1, 2022, https://theconversation.com/why-zelenskyys-selfie-videos-are-helping-ukraine-win-the-pr-war-against-russia-178117; Brian Todd, "How Zelensky is using social media to dominate the information war," *CNN Situation Room,* March 9, 2022, https://www.cnn.com/videos/media/2022/03/09/volodymyr-zelensky-social-media-ukraine-todd-dnt-intl-tsr-vpx.cnn; Wynne Davis, "Ukraine appears to have stalled Russia's advance. Here's what that could mean," *NPR*, March 18, 2022, https://www.npr.org/2022/03/18/1087314355/russia-ukraine-invasion-latest-analysis.

[73] Philip N. Howard, Aiden Duffy, Deen Freelon, Muzammil M. Hussain, Will Mari, and Marwa Maziad, "Opening closed regimes: what was the role of social media during the Arab Spring?," *Available at SSRN 2595096* (2011); Gadi Wolfsfeld, Elad Segev, and Tamir Sheafer, "Social media and the Arab Spring: Politics comes first," *The International Journal of Press/Politics*, Vol. 18, No. 2 (2013), pp. 115-137; Nils B. Weidmann, "Communication, technology, and political conflict: Introduction to the special issue," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 263-268.

[74] Michael Horowitz, *The diffusion of military power: Causes and consequences for international politics*, p. 16.

[75] See Tamar Mitts, Gregoire Phillips, and Barbara F. Walter, "Studying the impact of ISIS propaganda campaigns," *The Journal of Politics*, Vol. 84, No. 2 (2022); Imran Awan, "Cyber-extremism: Isis and the power of social media," *Society*, Vol. 54, No. 2 (2017), pp. 138-149; Ken Menkhaus, "Al-Shabaab and social media: A double-edged sword," *Brown Journal of World Affairs*, Vol. 20 (2013), p. 309; David Mair, "# Westgate: A case study–how Al-Shabaab used Twitter during an ongoing attack," In *Violent Extremism Online* (Routledge, 2016), pp. 65-86; Hyunjin Seo, "Visual propaganda in the age of social media: An empirical analysis of Twitter images during the 2012 Israeli–Hamas conflict," *Visual Communication*

success of the Islamic State's social media branding and the breadth of Russia's online influence operations leaving major gaps in research. For example, will other non-state armed groups replicate the Islamic State's pattern of adopting social media? Is it merely a question of organizational capacity or does ICT impose unique challenges for adoption and use by armed organizations? Other groups appear to use the same technology as the Islamic State but in very different ways. For instance, both Hamas and Hezbollah primarily use proxy social media accounts, leveraging the influence and reach of national media organizations and local charities. The content they seek to promote is far more subtle in its branding, with few direct mentions of the organization or overt depictions of violence.[76] Their apparent goal is to operate in the open, but in a way that does not garner international attention (and importantly, that of the private companies whose platforms they operate on). Others forgo the technology altogether. Among rebels operating in Libya, while the majority of armed groups have access to cell phones and the internet, only a small minority opted to develop a social media presence.[77] It is more than likely that many groups use social media successfully in more targeted ways, aimed at a more limited, domestic audiences or communicating directly with funders and supporters in ways that are invisible to an outside observer. Replicating the adoption and usage patterns of the Islamic State may not be feasible for other organizations or may not inherently advantage an armed group in a particular civil war context. Another essential question is whether a low-capacity state could develop a similar program of online information operations as Russia. Recent research suggests that a range of states have been actively pursuing influence operations

Quarterly, Vol. 21, No. 3 (2014), pp. 150-161; Gabriel Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," *New Media and Innovative Technologies,* Vol.22 (2008); Diego A. Martin, Jacob N. Shapiro, and Michelle Nedashkovskaya, "Recent trends in online foreign influence efforts," *Journal of Information Warfare*, Vol. 18, No. 3 (2019), pp. 15-48; Diego A. Martin, Jacob N. Shapiro, and Julia G. Ilhardt, "Version 2.0: Recent trends in online foreign influence efforts," August 5, 2020, https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_online_influence_efforts_v2.0_aug_5_ 2020.pdf.

[76] Sheera Frenkel and Ben Hubbard, "After Social Media Bans, Militant Groups Found Ways to Remain," *The New York Times*, April 19, 2019, https://www.nytimes.com/2019/04/19/technology/terrorist-groups-social-media.html.

[77] For examples of social media use by rebel groups in Libya, see Laura Courchesne and Brian McQuinn, "After the Islamic State: Social Media and Armed Groups."

online, including China, Iran, Saudi Arabia, United Arab Emirates, and Russia.[78] More states will likely follow suit or are already doing so in ways which have yet to be identified. As of yet, we lack a comprehensive account of how most armed organizations engage with social media.[79]

Why do armed organizations differ in their adoption and use of modern information and communications technology (ICT)? What explains this variation in behavior? I argue that four key attributes of ICT, unaccounted for in existing organization-centric models of technology adoption, provide important insights for understanding and anticipating the range of ICT adoption behaviors by armed organizations. These attributes reflect inherent characteristics of ICT as a category of military technology, imposing constraints, challenges, and opportunities for organizational capacity. The proposed model, entitled the disruptive attribute theory, aims to delineate a set of key variables and mechanisms for explaining variations in and counterintuitive patterns of ICT adoption by state militaries and non-state armed groups. This article presents four intervening variables, reflecting qualities of modern ICT, that interact with organizational variables presented in existing theory to impact adoption outcomes:

(1) First, ICT's shared infrastructure introduces distinct and strategic interaction effects. ICT use by armed organizations is often conditional on publicly available infrastructure. For

[78] Diego A. Martin, Jacob N. Shapiro, and Michelle Nedashkovskaya, "Recent trends in online foreign influence efforts," *Journal of Information Warfare*, Vol. 18, No. 3 (2019), pp. 15-48; Diego A. Martin, Jacob N. Shapiro, and Julia G. Illhardt, "Version 2.0: Recent trends in online foreign influence efforts," Empirical Studies of Conflict Project, August 5, 2020, https://scholar.princeton.edu/sites/ default/files/jns/files/trends_in_online_influence_efforts_v2.0_aug_5_2020.pdf.
[79] Laura Courchesne and Brian McQuinn, "After the Islamic State: Social Media and Armed Groups," *War on the Rocks,* April 9, 2021, https://warontherocks.com/2021/04/after-the-islamic-state-social-media-and-armed-groups/; Herbert, "Libya's War Becomes a Tech Battleground"; Antonia Ward, "ISIS's use of social media still poses a threat to stability in the Middle East and Africa," *Georgetown Security Studies Review* (2018); Joby Warrick, "Private money pours into Syrian conflict as rich donors pick sides," *Washington Post*, June 15, 2013, https://www.washingtonpost.com/world/ national-security/private-money-pours-into-syrian-conflict-as-rich-donors-pick-sides/2013/06/15/67841656-cf8a-11e2-8845-d970ccb04497_story.html.

example, phone lines, wireless networks, and radio networks often exist in conflict contexts as a public good. Unless an organization is willing and able to create independent, self-supported infrastructure spanning the geography of their operations, their use of ICT will rely on infrastructure used by both civilians and their opponent(s). This overlap in reliance on the same physical infrastructure introduces strategic challenges for adoption, including the calculus of whether continued access to ICT is worth the cost of permitting the same access to an opponent.

(2) Second, ICT increases the role and importance of private sector actors. These actors are often responsible for introducing and maintaining ICT in a conflict setting. They make decisions that shape an armed organization's strategic considerations, such as the geographical reach of ICT infrastructure and who has access to it. As a result, armed organizations must either partner with or coerce private actors as a means of securing control. If these strategies are not possible, armed organizations will adopt and use ICT in patterns constrained by the decisions of third-party actors or forgo the technology altogether.

(3) Third, the ubiquity of ICT results in modes of acquisition that differ from other forms of military technology. ICT's global diffusion is driven by non-conflict-related forces and aims. This inadvertent introduction of new technologies into a conflict context should be distinguished from the intentional, strategic acquisition of a technology by an armed organization. In the case of ICT, armed groups and state militaries often adopt ICT not from a desire to close a technological gap in war but because of adoption behaviors in non-military settings. Members of an organization often already use ICT, such as cell phones or social media, independent of and prior to joining the group. This can result in intra-organizational variation in usage patterns and challenges in

controlling vulnerabilities introduced by adoption, as individual members adopt ICT separate from organizational decision-making.

(4) Fourth, ICT allows for customization and a wide range of applications. Usage patterns for military technology are often considered in a binary way (use or non-use), primarily due to the more limited applications. For example, there is a finite range of ways an armed actor can use a gun or a tank. However, when it comes to ICT, there is more variability and breadth of application. A computer or smartphone can be used to support kinetic operations, engage in cyber warfare, deploy influence operations, engage in recruitment, communicate with funders, liaise with the local community, and build an international brand. Importantly, ICT can be used for external purposes, such as propaganda and recruitment, or internal actions, including communication and coordination. Different functions impose different strains on organizational capacity. The same organization may opt for differing approaches to ICT depending on the intended purpose, exhibiting variation in their use of more advanced forms of technology.

To explore the role and relevance of these factors, this article uses case studies to engage in a plausibility probe and support initial theory building.[80] This article analyzes patterns of ICT adoption among four diverse armed organizations: the CPN-Maoists of Nepal (2005), Los Zetas of Mexico (2006 - 2016), the Russian military (2014 - 2017), and the Chinese military (2020). This analysis serves a critical function in theory development by assessing the applicability of the model across varied settings, time periods, technologies, and types of armed organizations.

[80] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, (MIT Press, 2005), pp. 20-22, 45, 75; John Gerring, "What is a case study and what is it good for?," *American Political Science Review*, Vol. 98, No. 2 (2004), p. 341-354; Harry Eckstein, "Case study and theory in political science," *Case study method* (2000), pp. 119-164.

The article proceeds as follows: first, it begins by outlining historical modes of information control in conflict settings and the impact new forms of ICT have on traditional dynamics, followed by a brief review of the existing theoretical literature on technology adoption. It then provides an expanded overview of disruptive attribute theory, its connection to existing theory, and its utility in explaining the behavior of armed organizations. Next, it explores the relevance and applicability of the model using four qualitative case studies of armed organizations, detailing their organizational structure and ICT adoption patterns. In the final section, the paper concludes by highlighting future research streams for testing the model and the implications of this framework for international relations theory.

The Evolving ICT Environment

Historically, physical control over the conflict space enabled control over the information environment. During World War I, the British Army "used telegraph cables and telephones to communicate between the front-line soldiers and commanders. But heavy artillery bombardment meant these lines of communication were easily broken. They were also easily intercepted by the German Army, as were the very basic wireless telegraph sets used by the British Army."[81] Further, "despite efforts to protect the wire lines, they were frequently cut at critical times as the result of the intense artillery fire."[82] As illustrated by the efforts of various states during both World Wars in developing newer, adaptable, and more secure ICT, state militaries were often the originators of

[81] Elizabeth Bruton, "Communication Technology," *International Encyclopedia of the First World War*, last updated December 9, 2014, https://encyclopedia.1914-1918-online.net/article/communication_technology.
[82] George Raynor Thompson, "Military Communication," *Britannica Encyclopedia*, last updated April 25, 2018, https://www.britannica.com/technology/military-communication/.

information and communications technologies in historical conflicts.[83] During the Falklands War in 1982, the British military sought to control the flow of external information by limiting media coverage. Any information that reached the international community came either from the Ministry of Defense briefings or journalists accompanying the British taskforce. This policy exemplified the close relationship between traditional military power and the information environment in historical conflicts: by physically controlling a space, one could exert control over the information environment.[84]

During the Gulf War of the 1990s, US military forces held daily military briefings that incorporated smart-bomb videos captured by the infrared radar system used to guide missile deployment. This technology pioneered new possibilities for using video footage in enabling armed forces to 'capture' the information environment. Video footage of the conflict rested squarely under US military control. These videos allowed the US military to more effectively and persuasively accomplish two key information goals: 1) convince the domestic populace of the validity of the war effort and 2) showcase their technical prowess to the international community.[85] Selective bans on access to Western journalists further amplified this control. The structure of the information environment and information flows in historical conflicts meant that control could be successfully exerted through physical capture of the conflict space. ICT infrastructure was typically located within the bounds of the physical conflict space, which enabled control by powerful, well-resourced actors. Crucially, new technologies have shifted power over information flows away from formalized

[83] Dean Juniper, "The First World War and Radio Development," *The RUSI Journal*, Vol. 148, No. 1 (2003), pp. 84-89; Greg Myre, "From Wristwatches To Radio, How World War I Ushered In The Modern World," *NPR*, April 2, 2017, https://www.npr.org/sections/parallels/2017/04/02/521792062/from-wristwatches-to-radio-how-world-war-i-ushered-in-the-modern-world; Michael S. Sweeney, *Secrets of victory: The Office of Censorship and the American press and radio in World War II* (University of North Carolina Press, 2001).
[84] William Merrin, *Digital war: A critical introduction* (Routledge, 2018), pp. 5 - 6.
[85] Ibid., p. 9.

channels overseen by the state. Instead, private sector actors are now playing a prominent role, responsible for introducing and maintaining modern ICT infrastructure in conflict settings.

By the time of the Kosovo conflict in 1999, civilians were using the internet to become active participants in the information ecosystem. One such civilian, Father Sava Janjic, was labeled the 'cyber-monk,' using his monastery's website to successfully broadcast news and images of the conflict in real-time.[86] This shift showcases how newer forms of ICT began to empower non-state actors and overcome prior constraints, which had traditionally advantaged more powerful, resource-rich states. Exerting control over the information environment was no longer as closely linked to physical occupation. Additionally, prior technical constraints limiting ICT usage at a larger scale to more sophisticated actors continued to fade. Fast forward to the civil wars in Libya and Syria, non-state armed groups are using these same information campaigning tactics, but with less resource-intensive technology and the assistance of publicly available social media platforms.[87]

Modern ICT is characterized by Weidmann (2015) as differing from older forms in the following ways: its (1) "pervasiveness [...] as regards speed and coverage", (2) the "nature of the information transmitted" and (3) "the type of network" used, including broadcast and peer-to-peer networks.[88] For the purposes of this article, modern information and communications technology (ICT) is defined as technology that is used to transmit, store, access, create, or exchange information across distances instantaneously. To achieve this level of speed and scale, these technologies convert information into alternative forms, such as radio waves (in the case of radios, landlines, and cell

[86] Ibid., pp. 20 - 22.
[87] Melik Kaylan, "Syria's War Viewed Almost in Real Time," *The Wall Street Journal*, September 27, 2013, https://www.wsj.com/articles/syria8217s-war-viewed-almost-in-real-time-1380305826.
[88] Nils B. Weidmann, "Communication, technology, and political conflict: Introduction to the special issue." Journal of Peace Research 52, no. 3 (2015): 263-268.

phones) and bits (in the case of computers and the internet), to facilitate transmission across networks.[89] This definition is inclusive of technologies including radio, cell phones, computers, and the internet.

Social media, in particular, has been an important force in modern conflict, empowering a broad range of actors to engage in a wide array of actions, including developing a global brand, recruiting at a mass scale, soliciting new funders, and liaising directly with local communities.[90] Moreover, the online landscape has created new opportunities and challenges for armed organizations seeking to gain an advantage over the information environment. For example, performing an information operation across borders and simultaneously in several conflict contexts is much less costly and resource intensive.

The potential applications of social media by armed organizations are still emerging. Some non-state armed groups are beginning to approach information operations in similar ways to the Russian military, with reports of Hezbollah sending its members to 'fake news training camps' to learn the basics of doctoring images and videos.[91] Further, the role of private actors is ever increasing, with actions taken by Western-based social media companies, including Twitter,

---

89 For additional definitions of modern ICT, see Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda"; Farid Shirazi, Ojelanki Ngwenyama, and Olga Morawczynski, "ICT expansion and the digital divide in democratic freedoms: An analysis of the impact of ICT expansion, education and ICT filtering on democracy," *Telematics and Informatics*, Vol. 27, No. 1 (2010), pp. 21-31; Robin Mansell, Chrisanthi Avgerou, Roger Silverstone, and Danny Quah, *The Oxford handbook of information and communication technologies,* (Oxford Handbooks, 2007).

90 Laura Courchesne and Brian McQuinn, "After the Islamic State: Social Media and Armed Groups;" Matt Herbert, "Libya's War Becomes a Tech Battleground"; Antonia Ward, "ISIS's use of social media still poses a threat to stability in the Middle East and Africa"; Joby Warrick, "Private money pours into Syrian conflict as rich donors pick sides."

91 Wil Crisp and Suadad al-Salhy, "Exclusive: Inside Hizbollah's fake news training camps sowing instability across the Middle East," *The Telegraph*, August 2, 2020, https://www.telegraph.co.uk/news/2020/08/02/exclusive-inside-hezbollahs-fake-news-training-camps-sowing/.

Facebook, and YouTube, eliminating scores of assets of state influence operations.[92] Non-state armed groups have also dealt with social media bans, adapting to the demands and constraints of a new information environment.[93] For example, both Hamas and Hezbollah both developed adaptive social media strategies in response to Facebook and Twitter targeting their accounts with flags on content and account bans. They relied on community member information propagation instead of official accounts and provided detailed instructions to supporters on permissible content to post in accordance with platform policies.[94]

The Syrian civil war is one of the more notable examples of the complex dynamics of state and non-state adoption of ICT. Since the inception of the conflict in 2011, non-state armed groups have uploaded hundreds of thousands of videos and images to social media platforms, detailing their occupation of territory and military victories, showcasing their ammunition and arms, and outlining their ideological motivations.[95] These platforms have also provided groups with opportunities to gain international recognition and support, as well as develop and maintain strong relationships with newfound financial backers. As highlighted by Walter (2017), non-state armed groups "are embracing the Internet and adapting their strategies and tactics to exploit a radically new information environment."[96] Several Syrian rebel groups posted "videos on YouTube thanking [sponsors from Gulf states] for past assistance and pleading for more,"[97] as well as videos

[92] Elizabeth Culliford, "Facebook removes Russian Network that Targeted Influencers to Peddle Anti-Vax Message," Reuters, August 10, 2021, https://www.reuters.com/technology/facebook-removes-russian-network-that-targeted-influencers-peddle-anti-vax-2021-08-10/.
[93] Sheera Frenkel and Ben Hubbard, "After Social Media Bans, Militant Groups Found Ways to Remain."
[94] Ibid.
[95] Liam Stack, "Watching Syria's War," *The New York Times*, last accessed September 8, 2021, https://www.nytimes.com/ interactive/projects/watching-syrias-war; Andy Greenburg, "Google's New YouTube Analysis App Crowdsources War Reporting," WIRED, April 20, 2016, https://www.wired.com/2016/04/googles-youtube-montage-crowdsources-war -reporting/; Melik Kaylan, "Syria's War Viewed Almost in Real Time."
[96] Barbara F. Walter, "The new new civil wars." *Annual Review of Political Science*, Vol. 20 (2017), pp. 469-486.
[97] Joby Warrick, "Private money pours into Syrian conflict as rich donors pick sides."

confirming the acquisition and use of weapons. This content forms the backbone of non-state armed group information campaigns to solicit awareness, brand themselves globally, gain publicity, and garner support over the course of the Syrian conflict.

WhatsApp, an online messaging platform with end-to-end encryption, became one of the primary communications tools for Syrians during the conflict.[98] As reported by a civilian living in Idlib: "In Raqqa, locals rely entirely on WhatsApp as well as other platforms such as Skype, Telegram, Facebook Messenger and Viber, to communicate. Cell towers have been out of operation since Raqqa's infrastructure was heavily damaged last year during intense fighting to oust ISIS, suspending landlines and mobile phone networks. In Idlib, where there is no Syrian network coverage, residents have two choices to place a phone call: WhatsApp or Turkish phone networks."[99] Another civilian in Aleppo is reported as saying: "Even when the internet is not that good we can use WhatsApp, it doesn't cost a lot and even if the connection is weak, it works well. We get information usually like this."[100]

Importantly, Syrian rebels used WhatsApp to communicate and coordinate with each other. Rebel groups were documented as alternating between online messaging platforms and walkie-talkies to communicate with civilians, medics, and other rebel groups about incoming attacks. A rebel group's choice of messaging technology depended on internet coverage. In Homs, when internet

98 Rima Abdelkader and Emmanuelle Saliba, "Syrians Trapped in Aleppo Using WhatsApp to Post Cries for Help," *NBC News*, December 14, 2016, https://www.nbcnews.com/storyline/aleppos-children/syrian-dispatches-call-help-n696166.
99 Sunniva Rose, "Syrians worry about regime proposal to ban WhatsApp calls," *The National*, October 18, 2018, https://www.thenationalnews.com/world/mena/syrians-worry-about-regime-proposal-to-ban-whatsapp-calls-1.782118.
100 Lauren Said-Morehouse, "How Syrian activists use WhatsApp to tell the world their stories," *CNN*, September 28, 2016, https://www.cnn.com/2016/09/28/middleeast/whatsapp-syria-aleppo-activists/index.html.

access failed, they would "hook walkie-talkies up to the loudspeakers in the minarets of mosques," to warn civilians about air raids.[101]

In March 2012, the Syrian state banned WhatsApp from national networks. The intended goal of this strategy was to "disrupt the rebel opposition's cellular privacy" by curtailing access to the technology.[102] Gohdes (2015) found that the Syrian state's ICT strategy included targeted blackouts in areas where opposition groups were most active.[103] And yet, there is evidence that both civilians and armed groups easily found ways to circumvent these bans. One of the largest opposition groups, the Free Syrian Army, continued to promote links on their website to download the app and actively shared a WhatsApp contact number. Rebels were still able to access the platform to "use the messaging service to organize, share news, track government security forces and warn of national army movements."[104] As one civilian stated: "In southern Syria, people are tapping into the Jordanian cellular networks, and in the north, near Aleppo, they are jumping on Turkish ones [...]. In other parts of the country it is possible to access WhatsApp using a satellite connection."[105]

---

101 Maya Gebeily, "Secret Syria network warns of air raids over WhatsApp," *The Times of Israel*, January 21, 2016, https://www.timesofisrael.com/secret-syria-network-warns-of-air-raids-over-whatsapp/.
102 Alessandria Masi, "Facebook's $19 Billion App Is Hugely Popular Among The Syrian Opposition," *Business Insider*, February 23, 2014, https://www.businessinsider.com/whatsapp-is-hugely-popular-among-syrian-rebels-and-activists -2014-2.
103 Anita R. Gohdes, "Pulling the plug: Network disruptions and violence in civil conflict"; Andy Brownstone, "Meet the Libyan rebels on the front line," *BBC Newsbeat*, May 24, 2011, http://www.bbc.co.uk/newsbeat/13505340; Joshua Keating, "Firing mortars? There's an app for that," *Slate*, September 18, 2013, https://slate.com/news-and-politics/2013/09/video-of-free-syrian-army-using-an-ipad -to-aim-mortars.html; Elhanan Miller, "Syrian opposition uses home-made rockets and Google technology, video reveals," *The Times of Israel*, August 20, 2012, http://www.timesofisrael.com/syrianopposition-uses-home-made-rockets-google-technology-new video-reveals/.
104 Alessandra Masi, "Facebook's $19 Billion App Is Hugely Popular Among The Syrian Opposition," *Business Insider,* February 23, 2014, https://www.businessinsider.com/whatsapp-is-hugely-popular-among-syrian-rebels-and-activists-2014-2.
105 Ibid.

WhatsApp and other publicly available online communications platforms also became a tool to report ceasefire violations between the Syrian government and rebels.[106] A U.S. State Department official claimed that during the February 2016 ceasefire, "the bulk of violations reported to the United States have come by email and WhatsApp. Reports tend to be a grab-bag of firsthand and secondhand accounts of varying reliability, some backed up with YouTube videos."[107]

The failures of the Syrian state's ban of WhatsApp on national networks are illustrative of several key points regarding the evolving nature of ICT in modern combat. First, historical models of absolute state (or superior actor) control over communication networks are becoming less applicable. Both Syrian civilians and rebel groups quickly found ways to circumvent the ban and were able to quickly resume their use of WhatsApp. Second, investment and acquisition costs for ICT are much lower. Civilians, non-state armed groups, and state militaries can now rely on publicly available infrastructure. This infrastructure, such as the encryption capacities and operating system of the WhatsApp platform, is also maintained by a separate actor, enabling organizations to invest resources and time elsewhere. And in the case of WhatsApp, access to and use of the platform is free. These features help to level the playing field when actors face more powerful and better-resourced opponents. Third, the increasing ubiquity essentially eliminates the possibility of total information control by armed organizations over a conflict environment. This ubiquity is a by-product of the increased prominence and influence of third-party actors whose decisions (where to place physical infrastructure, whom to provide access to, what type of content can be shared) shape

[106] Melissa Wall and Sahar El Zahed. "Syrian citizen journalism: A pop-up news ecology in an authoritarian space." *Digital Journalism*, Vol. 3, No. 5 (2015), pp. 720-736.
[107] Sam Heller, "The Syrian Ceasefire Is Held Together by an Unlikely Group of Frenemies — and WhatsApp," *Vice*, March 16, 2016, https://www.vice.com/en/article/xw3kvw/the-americans-russians-and-the-un-are-keeping-syrias-shaky-ceasefire-afloat-with-whatsapp-text-messages.

strategic considerations.[108] Fourth, the multitude of actors operating in a conflict space often rely on the same physical infrastructure for information needs. The preexisting usage behaviors and internet penetration rates of civilians can influence the adoption patterns of non-state armed groups and the strategic considerations of states.

Armed groups' use of modern information and communications technology to support their efforts also extends beyond leveraging internet access to use social media. Rebel groups in several conflicts have been documented as using online platforms such as Google Maps, Google Earth, WhatsApp, and Skype to supplement kinetic operations, correct mortar fire, engage in information collection, and communicate with one another and civilians.[109] The barriers that once prevented less technically proficient, under-resourced actors from engaging in large-scale information operations and long-range communications while waging war appear to have dissipated. Further complicating matters is the overlap in the use of the same ICT infrastructure by civilian communities. The newfound ubiquity, technical ease of adoption, and reliance on an infrastructure developed, maintained, and controlled by a private actor requires a reexamination of assumptions of military power and technological superiority. Historical models of information control and ICT adoption during active conflicts, which traditionally favored powerful and well-resourced state actors, have become much harder to apply. Given these changes to the nature of information flows in modern conflicts and widespread accessibility to ICT, understanding the nature of the organizational limits on ICT adoption becomes an important empirical question. As emphasized by Dafoe and Lyall

[108] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford University Press, 2019).

[109] Anita R. Gohdes, "Pulling the plug: Network disruptions and violence in civil conflict," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 352-367; Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda."

(2015), "insurgent organizations can [...] display considerable spatial and temporal variation in their engagement with ICT."[110] This paper seeks to answer why.

Existing Theories of Technology Adoption

Scholarship on military technology adoption can be divided into two key theoretical approaches. The first treats both the adopter and the type of adopted technology as constants, focusing instead on the importance of diffusion and comparative adoption.[111] Rather, it assumes that what matters most is the pre-existing spread of a given technology and the pressure to adopt. This includes epidemic and contagion theories of adoption.[112] Notably, Kenneth Waltz (1979)'s description of the international system presumes that states will opt to "imitate the military innovations contrived by the country of the greatest capability and ingenuity," resulting in the "weapons of major contenders… to look much the same all over the world."[113] Many existing models that fall under this category presume an advantage of backwardness, wherein less developed states can free ride on the innovation and research of more advanced states, closing military-technological gaps quickly through imitation.[114]

---

110 Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda."

111 Kenneth N. Waltz, *Theory of international politics* (Reading, Mass.: Addison-Webley, 1979); Edwin Mansfield, "Technical change and the rate of imitation," *Econometrica: Journal of the Econometric Society* (1961), pp. 741-766; Barbara Wejnert, "Integrating models of diffusion of innovations: A conceptual framework," *Annual review of sociology*, Vol. 28, No. 1 (2002), pp. 297-326.

112 Corey M. Angst, Ritu Agarwal, Vallabh Sambamurthy, and Ken Kelley, "Social contagion and information technology diffusion: The adoption of electronic medical records in US hospitals," *Management Science*, Vol. 56, No. 8 (2010), pp. 1219-1241; Manus I. Midlarsky, Martha Crenshaw, and Fumihiko Yoshida, "Why violence spreads: The contagion of international terrorism," *International Studies Quarterly*, Vol. 24, No. 2 (1980), pp. 262-298.

113 Kenneth Waltz, *Theory of International Relations* (Reading, Massachusetts: Addison-Webley, 1979), pp. 111–114.

114 Alexander Gerschenkron, *Economic Backwardness in Historical Perspective: A Book of Essays* (Cambridge, Mass.: Belknap, 1962), pp. 5–30; Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1981), pp. 176–177; Kenneth Waltz, *Theory of International Politics*, pp. 74, 127.

The second approach explains patterns of technological adoption by studying the organizational attributes of the states and non-state armed groups involved.[115] This literature has provided evidence that organizational features - including doctrine, process, and resources - are crucial in shaping adoption behaviors.[116] The most prominent theory is Michael C. Horowitz's adoption-capacity theory, which emphasizes the importance of organizational and financial attributes in determining the successful adoption and use of a military technology. Horowitz argues that "once states have necessary exposure," adoption is determined by two primary factors, financial intensity and organizational capital.[117] Capital is argued to include "the intangible assets needed by organizations to transform in the face of major military innovations" such as "human capital, tacit knowledge, and organizational practices."[118] Financial intensity is defined as "the investments required to purchase the physical hardware associated with an innovation, along with the relative ability of states to make those investments."[119] Further, adoption-capacity theory contends that being the first to innovate, or the supposed 'first-mover advantage,' does not guarantee mastery over the technology nor long-term superiority over your opponent.

---

115 See Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics* (Harvard University, 2007); Michael C. Horowitz, "Nonstate actors and the diffusion of innovations: The case of suicide terrorism," *International Organization*, Vol. 64, No. 1 (2010), pp. 33-64; Eszter Hargittai, "Weaving the Western Web: Explaining differences in Internet connectivity among OECD countries," *Telecommunications policy*, Vol. 23, No. 10-11 (1999), pp. 701-718; Sampsa Kiiski and Matti Pohjola, "Cross-country diffusion of the Internet," *Information Economics and Policy*, Vol. 14, No. 2 (2002), pp. 297-310.

116 Eliot A. Cohen, "Change and transformation in military affairs," *Journal of Strategic Studies*, Vol. 27, No. 3 (2004), pp. 395-407; Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars*; Kimberly Marten Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955 - 1991* (Princeton University Press, 1993).

117 Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics*.

118 Michael C. Horowitz, Shahryar Pasandideh, Andrea Gilli, and Mauro Gilli, "Correspondence: Military-Technological Imitation and Rising Powers," *International Security*, Vol. 44, No. 2 (2019), pp. 185-192.

119 Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics*, p. 9.

However, a nascent literature highlights the importance of the technology and its features in the adoption process.[120] As highlighted by Gilli and Gilli (2018), attributes of the technology may matter in ways beyond capacity and resource requirements. They argue that existing theory ignores the impact of technological factors, including "the exponential increase in the complexity of military technology" since the second industrial revolution.[121] They contend that a technology's complexity reduces diffusion and adoption of technologies by heightening the barriers to entry. Actors seeking to develop a more complex technology must now possess (1) the requisite resources: baseline levels of scientific, technical and industrial infrastructure and, (2) the requisite knowledge base: the expertise and organizational wherewithal to institute the process and structure of development. Thus, as technological complexity increases, fewer states are able to meet the demands necessary to imitate and produce the technology for themselves.

While there is tremendous value in an assumption of technological neutrality, which allows for a focused exploration of the role of the international system or organization, the impact of technology's attributes in shaping patterns of behavior must not be overlooked. Horowitz underscores this point, writing that "for understanding the future of warfare, it will therefore be critical to assess how many factors influence the diffusion of military technologies, including system complexity, unit costs, and whether the underlying technology comes from private-sector or military research."[122] Further, the majority of scholarship on technology adoption focuses on states at the expense of theory development for non-state armed actors. As articulated by Cronin (2019), "in

[120] For an overview see Jon Schmid and Jonathan Huang, "State adoption of transformative technology: Early railroad adoption in China and Japan," *International Studies Quarterly*, Vol. 61, No. 3 (2017), pp. 570-583.
[121] Andrea Gilli and Mauro Gilli, "Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage," International Security, Vol. 43, No. 3 (2018) , pp. 141 - 189.
[122] Michael C. Horowitz, Shahryar Pasandideh, Andrea Gilli, and Mauro Gilli, "Correspondence: Military-Technological Imitation and Rising Powers."

most studies of military technological innovation, the focus is on state use of force against other states, as if the weapons, strategy, and tactics used by non-state individuals and groups [....] are virtually irrelevant."[123]

In response to these gaps, this article identifies four additional factors, reflective of attributes of ICT, that influence adoption by state militaries and non-state armed groups. As will be outlined, these four factors behave as "missing" intervening variables within Horowitz's adoption-capacity theory. Currently, adoption-capacity theory predicts widespread adoption of modern ICT by a range of actors. Specifically, it argues that "cheaper and more widely available information age technologies could lower the barriers for groups seeking to challenge state authority, meaning it will become increasingly easy for new groups to spring up in virtual environments and exchange information across borders."[124] More directly, it posits that the ubiquity and low cost of modern ICT lowers the required financial intensity needed by organizations, thereby increasing the rate of adoption. But this explanation fails to account for seemingly counterintuitive adoption behaviors related to ICT, including lack of adoption despite financial means, regression to less advanced forms of ICT, and intentional destruction of ICT infrastructure. Developing a robust organizational and technological understanding of ICT adoption in conflict is crucial for forecasting future trends and understanding the logic of adoption behaviors. As technology becomes more complex and diffused, understanding state and non-state attempts at information control will require a better understanding of the communications networks, associated physical infrastructure, and the private actors involved in facilitating ICT.

123 Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*.
124 Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics*, p. 26.

Disruptive Attribute Theory: The Role of Intervening Variables in ICT Adoption

Adoption-capacity theory argues that two primary organizational attributes, financial intensity and organizational capital, determine adoption outcomes. When a technology requires a high-level of financial intensity and a high-level of organizational capital, fewer organizations will be able to adopt. When a technology requires a low-level of financial intensity and a low-level of organizational capital, more organizations will be able to adopt it. A summary of these variables and adoption outcomes are outlined in Figure 1.

Figure 1. Horowitz's Adoption Capacity Theory (Titled 'Table 2.2 System - Level Diffusion of Technology' in *Diffusion of Military Power*)[125]

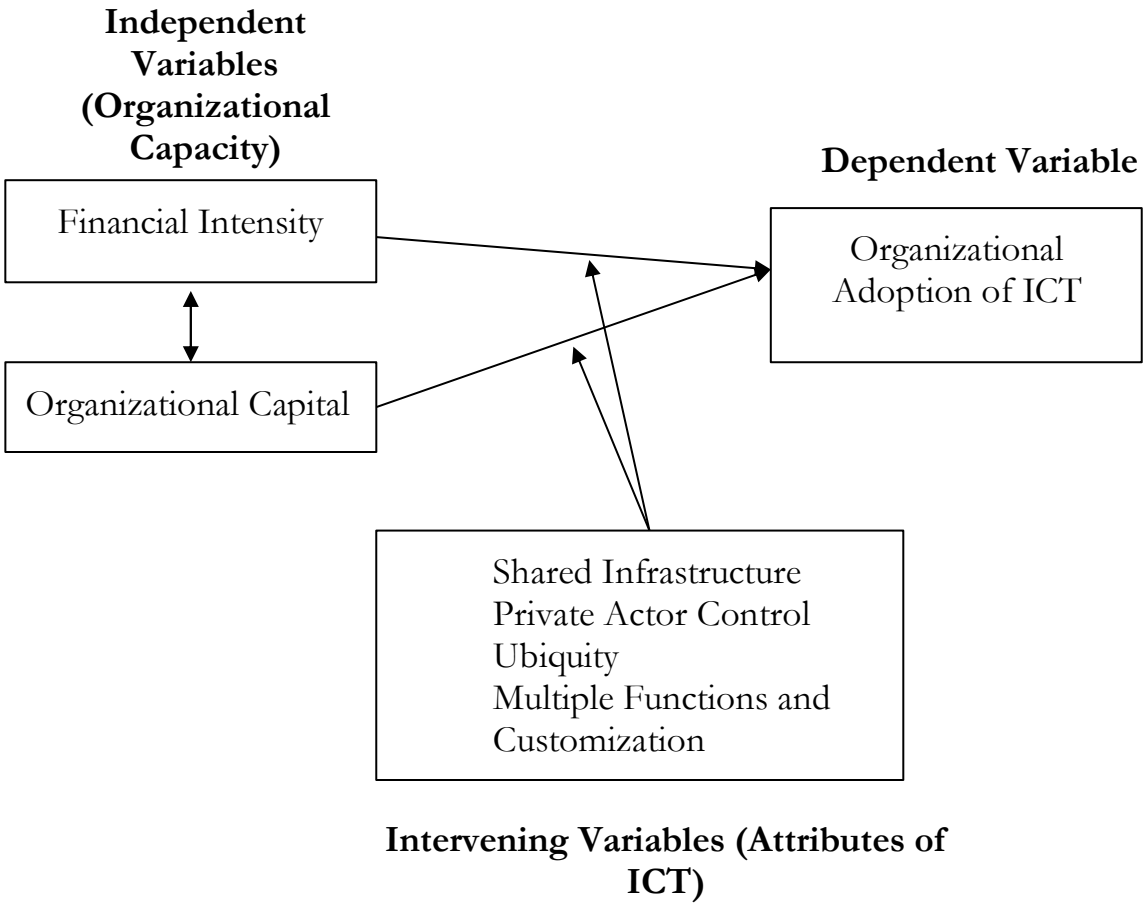
		Level of financial intensity required to implement a major military innovation	
		Low	High
Level of organizational capital required to implement major military innovations	Low	Rate/extent fast	Rate/extent medium
	High	Rate/extent medium	Rate/extent slow

Adoption-capacity theory presents two key independent variables (financial intensity and organizational capital) that shape the dependent variable (technology adoption by armed organizations or at a macro-level, the degree of technological diffusion in the international system). Organizations are argued to have certain levels of organizational capital and resources at their disposal that determine their ability to adopt a given technology. Using adoption-capacity theory as

[125] Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics,* p. 40.

the baseline model, this article argues that in considering adoption outcomes of ICT, four additional intervening variables must be considered. These intervening variables increase or decrease the level of organizational capital and financial intensity required to adopt ICT. Figure 2 provides a simple, high-level diagram of the relationship between adoption capacity theory and these intervening variables.

Figure 2. Intervening Variables Impacting ICT Adoption: A Modified Diagram of Horowitz's Adoption-Capacity Theory



These four intervening variables, (1) shared infrastructure, (2) private actor control, (3) ubiquity, (4) multiple functions and customization, can increase or decrease organizational demands placed on state militaries and non-state armed groups in adopting ICT. Even if at first glance an organization may appear to possess both the financial intensity and organizational capital to adopt an ICT (for example, cell phones, which are cheap, ubiquitous, and are relatively straightforward to adopt and use), this adoption outcome may not occur. Why? ICTs impose additional hidden demands on organizations seeking to adopt. These intervening variables are outlined in detail below:

1. Shared Infrastructure - ICT introduces distinct and strategically important interaction effects. These effects stem from overlaps in reliance on shared physical infrastructure by different conflict actors and local civilian communities. As compared to other forms of military technology, the use of information and communications technology is often predicated on publicly accessible infrastructure. This infrastructure is either owned by a state government or a private business. In the context of a civil war, both the state military and an opposing rebel group may use the same national telephone networks to communicate, as was the case in the Syrian conflict. Further complicating matters is the use of this public ICT infrastructure by civilians. Berman et al. (2018) discuss the strategic and game theoretical consequences generated by the introduction of civilian tip lines in various conflict settings.[126] Armed actors were forced to decide between destroying phone lines altogether or managing the risk to exploit other strategic benefits, including communication, coordination of operations, and the ability to remotely detonate IEDs. For example, in Iraq, while Al Qaeda destroyed water and electricity infrastructure, it spared the cell phone towers. As described by one observer, the "insurgents must have believed that on balance ICT helped their cause more

[126] Eli Berman, Joseph H. Felter, and Jacob N. Shapiro, *Small Wars, Big Data* (Princeton University Press, 2018).

than hurt it."[127] Shapiro and Siegel (2015) found that insurgents in Afghanistan, India, and Iraq all faced tradeoffs when considering cell phone usage. While increased coverage reduced organizational costs of communication, it increased the likelihood that the insurgents could be monitored by opponents through tracing methods tied to cell phone use and through human intelligence tied to community reporting.[128]

In contrast with existing literature on the role of technology in determining military power, an opponent's use of information and communications technology matters beyond a desire to mimic or exceed their technological arsenal.[129] Due to overlaps in reliance, additional strategic considerations are imposed that in turn shape organizational decisions. This produces variations in ICT adoption, as different organizations react differently to this strategic calculus: some will still adopt, some will modify their usage patterns to minimize vulnerabilities, while others will opt out of the technology altogether. For example, certain armed organizations may revert to older forms of technology to avoid detection or destroy infrastructure to prevent opponent access to an ICT, as was the case with the Taliban's approach to cell phone towers in certain parts of Afghanistan.[130]

2. Control by Private Actors - ICT increases the role and importance of private sector actors. With modern ICT, private actors have grown in importance, often responsible for introducing, maintaining, and controlling ICT infrastructure in conflict settings. An armed organization's ability to work with, coerce, or avoid detection by these third-party actors influences whether an ICT will

[127] Ibid., p. 88.
[128] Jacob N. Shapiro and David A. Siegel, "Coordination and security: How mobile communications affect insurgency," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 312-322.
[129] Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca NY: Cornell University Press, 1984); Kenneth Waltz, *Theory of International Politics*.
[130] Ibid., p. 86; Antonio Giustozzi, *Koran, Kalashnikov, and Laptop* (Columbia Univ. Press, 2008).

be adopted and how it will be used. While other forms of military technology can be dual use, the role and control possessed by private sector actors is comparatively negligible. By contrast, with ICT, coping with the influence of private actors is a critical strategy consideration for armed organizations. These private actors decide where to place infrastructure and to whom they provide access to. Rød and Weidmann (2015) investigated state deployment of ICT and found that the actor deploying ICT infrastructure matters, influencing strategic considerations surrounding usage.[131] Similarly, Dafoe and Lyall (2015) argued that "ICTs are often deployed strategically to promote certain interests, and thus the effects of ICTs could depend on which groups are in power."[132]

In the case of social media platforms, access is predicated on both the physical infrastructure providing internet access and the platform itself. For example, the Islamic State faced bans on many prominent social media platforms, including Facebook and Twitter.[133] Access to this technology was determined by the private actor. Opponents of the Islamic State (namely Western states) were forced to liaise with social media platforms to curtail the group's access. Final decision-making power remained with the private companies, however. This impact is similarly illustrated by the Syrian government's attempt to prevent Syrian rebel group access to WhatsApp: even though the platform was banned on national networks, rebel groups enjoyed continued access by leveraging Jordanian networks because the private actor (WhatsApp) allowed them continued access to their platform.

131 Espen Geelmuyden Rød and Nils B. Weidmann, "Empowering activists or autocrats? The Internet in authoritarian regimes," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 338-351.
132 Ibid.
133 Julia Greenberg, "Why Facebook and Twitter Can't Just Wipe Out ISIS Online," *WIRED,* November 21, 2015, https://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/; David Ingram, "Facebook says it is taking down more material about ISIS, al-Qaeda, *"Reuters,* April 23, 2018, https://www.reuters.com/article/facebook-extremism-int/facebook-says-it-is-taking-down-more-material-about-isis-al-qaeda-idUSKBN1HU2PY.

By contrast, the Taliban coordinated deals with private actors. As emphasized by Berman et al. (2018): "In 2008, the Taliban began sporadically demanding that mobile companies shut down their towers at night. Why only at night? Apparently, the Taliban were motivated by a concern with tips, since citizens could phone in tips at night with less risk of being spotted than during the daytime. But the Taliban seemed to also have a second concern: ISAF could triangulate mobile signals to track the nighttime activities of their operatives. The Afghan government rallied the three main mobile providers to keep the towers running. The Taliban responded by blowing up the towers and killing mobile company employees. By 2010 the mobile companies caved to Taliban pressure."[134]

3. Ubiquity - The ubiquity of ICT results in modes of acquisition that differ from other forms of military technology. ICT's global diffusion is driven by non-conflict-related forces and aims. This is in contrast to the underlying assumption of most technology adoption models, wherein states undertake intentional acquisition. Much of the existing literature hinges on the agency of states in the adoption process. In the case of ICT, armed groups and states adopt not because of a desire to close a military-technological gap but because of adoption behaviors in non-military settings. Many types of ICT, including phone lines and internet access, are introduced for development purposes in a given environment, and thus, actors adopt and adapt following civilian adoption.

As a result, adoption, integration, and use of ICT may occur as a result of passive rather than traditional 'active' acquisition. For example, members of a state military or armed group may separately possess cell phones, and the organization must then decide how to account for them in their technology strategy. This mode of adoption may result in vulnerabilities that organizational

[134] Eli Berman Joseph H. Felter, and Jacob N. Shapiro, *Small wars, Big data*, p. 86.

doctrine and processes fail to anticipate. For example, U.S. soldiers accidentally gave away the location of military bases in Afghanistan and the Sahel region of Africa through their use of a social running app, Strava, on their mobile phones.[135] Meanwhile, Russian soldiers occupying eastern Ukraine in 2015 posted updates and photos of their operations to their own personal social media accounts, contradicting official state narratives that the military was not directly involved in supporting Ukrainian separatists.[136] Current models fail to account for the potential impact of a bottom-up mode of military adoption driven by non-conflict-related aims. Due to its importance and diffusion in non-military and non-conflict settings, ICT inherently exhibits differences in adoption, diffusion, and usage patterns, necessitating a modified analytical approach.

4. Multiple Functions and Customization - ICT allows for customization and a wider range of applications. Usage patterns for military technology are often considered in a binary way, primarily due to their more limited range of functions. For example, there is a more finite range of ways a military can use a gun. However, when it comes to ICT, there is more variability. What is meant by adoption or use may vary from organization to organization. In the case of ICT, it is not a question of use or non-use, but a question of repertoire. For instance, the usage patterns of cell phones may include a wide array of behaviors and strategic applications: intra-organizational communication, developing social media campaigns, liaising with funders, addressing local communities, and the remote detonation of IEDs. Adoption of or access to the same technology does not predict identical, or even similar, usage patterns. The inherent ability to customize ICT

135 Liz Sly, "U.S. soldiers are revealing sensitive and dangerous information by jogging," *The Washington Post,* January 29, 2018, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html.
136 "Russian soldiers face ban on selfies and blog posts," *BBC*, October 5, 2017, https://www.bbc.com/news/world-europe-41510592; Dmitry Volchek and Claire Bigg, "Ukrainian bloggers use social media to track Russian soldiers fighting in east," *The Guardian*, June 3, 2015, https://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine.

means that usage patterns can vary dramatically among armed organizations. For example, while most armed groups in Syria and Libya had access to smartphones and internet access, many opted out of using social media as a means of garnering international support.[137] For some groups, using certain features appeared to introduce vulnerabilities that were perceived as too strategically risky. Reflecting this broad range of applications, organizations may also adopt varying forms of ICT depending on function. For example, a group may opt to use cutting edge ICT for external functions, such as promoting propaganda over social media to foreign audiences, while relying on a more low-tech approach for internal communication, due to the potential risks of opponent intelligence gathering. As a result, spatiotemporal and intraorganizational variation may be an inherent byproduct of the ICT's ability to be deployed for a wide range of purposes. Adopting ICT may impose different vulnerabilities, depending on the intended function, that the organization may be more or less equipped to deal with.

Table 1 outlines each of the four variables (broken down by the specific source of impact), intervening effects on the independent variables of financial intensity and organizational capital (by increasing or decreasing demands on organizations), and anticipated adoption outcomes (broken down by potential adoption behaviors). In considering adoption outcomes, adoption-capacity theory characterizes this dependent variable as binary (whether the technology adopted or not adopted). Further theorization is needed to understand and categorize the range of behaviors that may fall under the adoption or lack of adoption of a technology. However, given the different kinds of documented adoption behaviors, including destroying ICT infrastructure or reverting to older technologies (importantly, these behaviors are not mutually exclusive), this column provides further description of how the impact of these intervening variables may specifically manifest.

[137] Laura Courchesne and Brian McQuinn, "After the Islamic State: Social Media and Armed Groups."

Table 1. Impact of Intervening Variables on IVs and DV

Intervening Variables	Financial Intensity	Organizational Capital	Adoption Outcome	
1 - Shared Infrastructure			**Adopted**	**Not Adopted**
Infrastructure used by opponent	**Increases the need for resources.** Organizations must invest resources to cope with the challenges imposed (surveillance and monitoring by opponent; opponent vying for control over infrastructure), and opportunities (ability to impact opponent's ICT capacity) created by opponent use of shared infrastructure.	**Increases the need for processes.** Organizations must develop strategies to cope with the challenges imposed (surveillance and monitoring by opponent; opponent vying for control over infrastructure), and opportunities (ability to impact opponent's ICT capacity) created by opponent use of shared infrastructure.	1. Organizations adopt ICT despite vulnerabilities imposed by sharing infrastructure with their opponent. 2. Organizations adopt and enforce processes to minimize vulnerabilities. 3. Organizations adopt and take advantage of opponent's dependence (i.e., surveillance).	3. Organizations opt out of the technology and revert to a comparatively "older" form of ICT. 4. Organizations create an alternative technology and associated infrastructure. 5. Organizations destroy technology to deprive access to opponents.
Infrastructure used by civilians	**Increases the need for resources.** Organizations must invest resources to cope with vulnerabilities imposed (civilian tip lines; denying civilian access to infrastructure could undermine support for the group) and opportunities (able to exert control over civilian's access to information) created by civilian use of shared infrastructure.	**Increases the need for processes.** Organizations must develop strategies to cope with vulnerabilities imposed (civilian tip lines; denying civilian access to infrastructure could undermine support for the group) and opportunities (able to exert control over civilian's access to information) created by civilian use of shared infrastructure.	1. Organizations adopt and exert control over infrastructure, enforcing selective bans on access to control information flows from and to civilians. 2. Organizations adopt and take advantage of civilian access to share pro-organization propaganda.	3. Organizations engage in destruction of technology to deprive access to civilians.

2 - Controlled by Private Actors Private actor decision-making controls access to infrastructure	**Increases the need for resources.** Organizations must invest resources to overcome challenges of private actor control over access and use of technology.	**Increases the need for processes.** Organizations must develop strategy and processes to overcome challenges of private actor control over access and use of technology.	1.Organizations purchase infrastructure from private actors to gain control. 2. Organizations coerce or bribe private actors to provide access or cede control. 3. Organizations adopt technology constrained by private actor decisions.	4. Organizations revert to comparatively 'older' form of ICT. 5. Organizations create an alternative technology and infrastructure.
3 - Ubiquity Widespread diffusion of ICT in conflict settings	**Decreases the need for resources.** Reduces the need for an organizational investment to create or acquire technologies due to cheaper and widely available technology.	**Decreases the need for processes for acquiring or creating technologies. But potentially increases the need for new processes for integrating new technology.** Reduces the need for organizational processes to create or acquire technologies due to cheaper and widely available technology. But the availability of new technology increases the need for processes allowing for organizational integration.	1. Widespread adoption of cutting-edge ICT. Organizations outsource for access to new technologies, rather than engage internal development.	2. New processes required for the integration of new technologies are too challenging for the organization and they opt not to adopt.
Adoption in non-military settings and by individual fighters	**Decreases the need for resources.** Reduces need for organizational investment as the group can rely on technology (i.e., cell phones) adopted by individual members.	**Increases the need for processes.** Organizations must develop processes to cope with individual adoption and use of technology independent of a central decision/mandate.	1. Organizations introduce and enforce codes of conduct regarding personal ICT usage. 2. Bottom-up adoption of ICT by individual fighters introduces vulnerabilities and mistakes.	3.Organizations confiscate individuals' ICT, reverting to a more low-tech but controlled approach.

4 - Multiple Functions and Customization A single technology can be used for a wide range of functions	**Decreases need for resources.** A single technology is able to support multiple organizational functions, reducing the need to invest in acquiring or developing additional technologies.	**Increases need for processes.** Vulnerabilities introduced by the adoption of ICT may vary by function. Organizations must develop different processes to address the vulnerabilities (and opportunities) presented by each of these functions. For example, using a cell phone for external communication vs. internal coordination imposes different kinds of organizational requirements.	1. Organizations adopt more advanced forms of ICT for certain functions.	2. Organizations may opt for a comparatively "older" form of ICT for a particular function.

Exploring Patterns of ICT Adoption

In considering empirics for appropriately exploring disruptive attribute theory, I opted to use a qualitative case study approach as a plausibility probe to analyze a range of armed organizations and technologies and to support initial theory building.[138] The goal of this plausibility probe is "to show that the argument is sufficiently grounded in the evidence to justify further research and additional testing."[139] A case study approach was chosen for this initial exploration. As articulated by Gerring (2017), "qualitative data are likely to be more important when not much is known about a subject and when the goal of the researcher is to develop a new concept, uncover a new hypothesis,

138 Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences*, (MIT Press, 2005), pp. 20-22, 45, 75; John Gerring, "What is a case study and what is it good for?," *American Political Science Review*, Vol. 98, No. 2 (2004), p. 341-354; Harry Eckstein, "Case study and theory in political science," *Case study method* (2000), pp. 119-164.

139 Harry Eckstein, *Regarding politics: Essays on political theory, stability, and change*, (Univ of California Press, 1992), pp. 148 - 152; Dominic D.P. Johnson and Dominic Tierney, "Bad world: The negativity bias in international politics," *International Security*,Vol. 43, No. 3 (2018), p. 126.

or shed light on unknown causal mechanisms. Qualitative data are ideal for exploratory analysis."[140] George and Bennett (2005) further underscore the value of case studies for engaging in initial theory development.[141]

These cases were chosen based on available data and documentation of ICT adoption, as well as to highlight how the variables identified by disruptive attribute theory impact a variety of organizational types and capacities. This analysis opted for a 'diverse' case selection approach. As defined by Gerring (2008), this selection strategy involves using multiple cases that highlight the full range of variation of a specific factor of interest.[142] For the purposes of this plausibility probe, the goal is to establish the presence of these intervening variables across various forms of ICT and impact on different types of organizations. The cases selected allow for review of the theory's applicability for both states (China and Russia) and non-states (Los Zetas and CPN-Maoists), as well as a range of modern information and communications technology: radio (Los Zetas), cell phones and satellite phones (CPN-M), social media platforms (Russia), and a multi-modal approach to ICT (China). These cases are also important in that they feature seemingly counterintuitive adoption outcomes that are unaccounted for in existing theory of military technology adoption: (1) the CPN-M reverted to an 'older' technology after they were denied access to phone lines. They continued using this technology even after access had resumed; (2) Los Zetas made a massive investment in developing their own proprietary national radio network despite the ubiquity of and access to existing ICT infrastructure; and (3) Russia purchased privately-owned social media platform VKontakte despite previously accessing the technology for free. These cases also represent a range

[140] John Gerring, "Qualitative methods," *Annual Review of Political Science*, Vol. 20 (2017), pp. 15-36.
[141] Alexander L. George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (MIT Press, 2005), pp. 20-22, 45.
[142] John Gerring, "Case selection for case-study analysis: Qualitative and quantitative techniques," In *The Oxford Handbook of Political Methodology*, (2008).

of actors engaged in political violence: the paramilitary wing of a drug cartel, a rebel group involved in a civil war, and two powerful state actors. Given existing gaps in theory surrounding technology adoption by non-state armed groups, who are critically important actors in the landscape of political violence, this analysis seeks to offer a needed technological comparison of patterns between state and non-state and to explore whether similar forces apply universally across actor types.[143]

For the purposes of this plausibility probe, these case studies "take the form of modest or rather diffusely designed comparative studies, as preludes to more ambitious and tighter ones."[144] While this article is the first (to the author's knowledge) to explicitly explore determinants of ICT adoption by armed organizations, a potential null hypothesis could be the predicted adoption outcome articulated by Horowitz and other scholars: the ubiquity and low cost ICT leads to widespread adoption of the most advanced form of technology organizations can access.[145] If this explanation holds true, we would expect to observe (1a) adoption of advanced forms of ICT in most cases, unless (1b) the organization is very poorly resourced or functionally incapable of integrating technology (i.e., the organization fails to meet the low baseline of attributes identified in adoption-capacity theory). If disruptive attribute theory holds true, we would expect (2a) a lack of modern ICT adoption, with organizations instead reverting to 'older' forms of ICT and forgoing adoption of the predicted technology, or (2b) if adopted, organizations invest heavily into the development of sophisticated processes that control for the vulnerabilities imposed.

143 Stathis N. Kalyvas, *The landscape of political violence*, (New York: Oxford University Press, 2019).
144 Harry Eckstein, "Case study and theory in political science."
145 Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics;* Alexander Gerschenkron, *Economic Backwardness in Historical Perspective: A Book of Essays* (Cambridge, Mass.: Belknap, 1962), pp. 5–30; Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1981), pp. 176–177; Kenneth Waltz, *Theory of International Politics*, pp. 74, 127.

The Communist Party of Nepal - Maoists (CPN-M)

The Communist Party of Nepal - Maoists (CPN-M) operated as a non-state armed group in Nepal from February 1996 until May 2006, growing in size and organizational sophistication over the course of the decade.[146] The organization originated as a splinter group, separating from the Communist Party of Nepal's Unity Centre (CPN-UC) due to ideological differences regarding the best means to achieve political change. CPN-M instead sought to engage in armed struggle to pursue their strategic aims. The geography of Nepal was viewed as ideal for the successful implementation of guerilla warfare tactics, and the group was able to amass popular support throughout the country.[147] CPN-M's primary ideological objective was to capture state power and establish a new people's democracy, naulo janba. Its ideology was derived from a mixture of Marxism, Leninism, and Maoism.[148] The group produced and disseminated a large body of work outlining their doctrine and operations.[149] The group was led by Pushpa Kamal Dahal, referred to as Chairman Prachanda. He remained the principal leader for the entirety of the group's existence.[150]

CPN-M Organization

Organizationally, the group was hierarchical in structure. The group grew in size over time, but by 2005, CPN-M had an estimated force of 30,000 members.[151] In conceptualizing conflict intensity, UCDP recorded a total of 11,181 deaths resulting from the conflict between state forces and CPN-

---

146 Mahendra Lawoti, "Evolution and growth of the Maoist insurgency in Nepal," In T*he Maoist Insurgency in Nepal*, (Routledge, 2009) pp. 25-50.
147 Krishna Hachhethu, "Maoist insurgency in Nepal: An overview." *The Naxal Challenge: Causes, Linkages and Policy Option*, (2008) pp. 136-52.
148 International Crisis Group, "Nepal's Maoists: Their Aims, Structure and Strategy," Asia Report, No. 104 (2005).
149 Deepak Thapa, "Understanding the Maoist movement of Nepal, Vol. 10," *Centre for Social Research and Development* (2003).
150 Kiyoko Ogura, "Seeking state power: The communist party of Nepal (Maoist)," *Berghof Transitions Series*, No.3 (2008).
151 Krishna Hachhethu, "The Communist Party of Nepal (Maoist): Transformation from an insurgency group to a competitive political party." *European Bulletin of Himalayan Research* Vol. 33, No. 34 (2009) pp. 39-71.

M.[152] The group engaged in ceasefire agreements on two separate occasions, 2001 and 2003, before signing the final Comprehensive Peace Agreement (CPA) in 2006. In the aftermath, and as a consequence of the peace agreement, CPN-M transitioned into a political party which operated within the newly modified government of Nepal.[153]

The group emerged in February 1996 with only a few hundred ill-equipped fighters.[154] In the early stages of the group's formation and military engagement, it possessed limited resources, lacking necessary weapons and uniforms. Despite this, they were "well planned and highly organized," engaging in several synchronous attacks designed to support broader strategic aims.[155] The group organized itself into three preliminary units: fighting, security, and volunteer, with variation in cohesion between these units reflecting function and geographical location. CPN-M continued to develop organizationally, increasing in size and creating new units to anticipate strategic demand, before defeating state police forces in early 2001.[156]

The CPN-M's organizational structure is borrowed from the CPN-UC, and other Maoist-inspired groups, adhering to the "three magic weapons" of party, army, and a united front. The organizational structure of the CPN-Maoists can aptly be described as a highly interconnected system composed of various specialized subgroups dedicated to differing functions.[157] CPN-M formalized its military structure beginning in 1998, increasing in sophistication and size over time.

---

[152] Ralph Sundberg, Kristine Eck, and Joakim Kreutz. "Introducing the UCDP non-state conflict dataset." *Journal of peace research* Vol. 49, No. 2 (2012, pp. 351-362.
[153] Krishna Hachhethu, "The Communist Party of Nepal (Maoist): Transformation from an insurgency group to a competitive political party."
[154] Krishna Hachhethu, "Maoist insurgency in Nepal: An overview."
[155] Kiyoko Ogura, "Seeking state power: The communist party of Nepal (Maoist)."
[156] International Crisis Group, "Nepal's Maoists: Their Aims, Structure and Strategy."
[157] Deepak Thapa, "Understanding the Maoist movement of Nepal."

The army was composed a supreme commander (who was also the chairman), a general staff composed of the same individuals as the party's standing committee, then divisional command (divided into western, special central but later mid-central, and eastern), nine brigades, twenty-nine battalions, companies, platoons, and squads. There were also locally organized militias which were poorly armed and typically received the least amount of training; they operated in a relatively autonomous manner.[158]

The CPN-M contained three massive divisions dedicated to different but complementary functions, further divided into additional subgroups performing specialized tasks.[159] An international department existed which sought to expand the organization through the recruitment and mobilization of expatriate Nepalis, primarily in India. CPN-M leveraged these specialized units to secure funding sources and resources for training and combat. There were also departments dedicated to tasks such as publishing, broadcasting, health, policy, education, and human rights.[160]

Throughout its existence as an armed organization, the CPN-M exhibited notably high-levels of cohesion, engaging in synchronous military action and deliberate reassessment of procedures to promote unity. CPN-M was characterized by its prolonged indoctrination of recruits and rigorous daily political training programs within its cadres. It was also known for its strict discipline and integrated command over its subgroupings. The group was composed of numerous, geographically widespread subgroups which had the structural capacity to behave autonomously.[161]

---

158 Kiyoko Ogura, "Seeking state power: The communist party of Nepal (Maoist)."
159 Paul K. Davis, Eric V. Larson, Zachary Haldeman, Mustafa Oguz, and Yashodhara Rana, *Understanding and influencing public support for insurgency and terrorism* (Santa Monica, CA: RAND National Defense Research Institute, 2012).
160 International Crisis Group, "Nepal's Maoists: Their Aims, Structure and Strategy."
161 Paul K. Davis, Eric V. Larson, Zachary Haldeman, Mustafa Oguz, and Yashodhara Rana, *Understanding and influencing public support for insurgency and terrorism*, (Santa Monica, CA: RAND National Defense Research Institute, 2012).

CPN-M ICT Usage

A report from the International Crisis Group in 2005 describes the CPN-M as "skilled propagandists, producing their own publications, running FM radio stations, and using the domestic and international media to promote their point of view."[162] They are described as possessing:

> "Radio sets and cordless telephones adapted to function as walkie-talkies. The turn to e-mail and the internet started in November 2001. Following the breakdown of the ceasefire, the Maoists' unofficial mouthpiece, the weekly newspaper Janadesh, was shut down and its journalists went underground. While print publications were maintained clandestinely, the growing use of the internet in Nepal led to the Maoists adopting it as a primary means of communication. The faxing of press statements to selected journalists was gradually overtaken by email distribution within the country and far beyond. Maoist political and news websites collect press releases and offer access to online versions of Maoist publications in Nepali and English. According to one researcher, "Nepal's Maoists are the first among all of the world's communist movements to make good use of communications technology."[163]

They were also described as "the largest users of satellite phones in the country."[164] Crucially, the group "exploited the growth in mobile phone connectivity" in Nepal, which began in 2000.[165] The importance of ICT to CPN-M's operations was tested during the national suspension of phone services on February 1, 2005. In order to target the CPN-M's ICT infrastructure, the Nepalese

[162] International Crisis Group, "Nepal's Maoists: Their Aims, Structure and Strategy."
[163] Ibid.
[164] International Crisis Group, "Nepal's Maoists: Their Aims, Structure and Strategy."
[165] Ibid.

government shut off all public telecommunications for an extended period. This ban in telecommunications services applied to all land lines, cell phone lines, and internet access.[166] Landline phones were reactivated on February 7, cell phone lines on May 1, and prepaid cell phone services on August 22. [167]

The state and the military justified this shutdown over claims that the CPN-M were using pre-paid mobile SIM cards that prevented the government from identifying group members.[168] The CPN-M frequently planted roadside bombs that were remotely detonated using these mobile phones. Prior to national shutdown, the state would often engage in selective shutdowns in specific areas and for specific times to prevent targeted attacks on the king.[169] Ang, Tekwani, and Wang (2012) note:

> "Captured Maoists invariably had a mobile phone on them. Tracing the mobile phone numbers led only to prepaid users, who were not registered and so had complete anonymity. According to the managing director of Nepal Telecom, the charges for the pre-paid service probably made Nepal one of the cheapest places to own a mobile phone: incoming calls, including SMS (short message service), are free and so with careful use of SMS and limited outgoing calls, a card of US $10 could last six months before it expired. The shutdown in

166 Peng Hwa Ang, Shyam Tekwani, and Guozhen Wang, "Shutting down the mobile phone and the downfall of Nepalese society, economy and politics," *Pacific Affairs*, Vol. 85, No. 3 (2012), pp. 547-561.
167 United States Department of State, *U.S. Department of State Country Report on Human Rights Practices 2005 - Nepal* , 8 March 2006, https://www.refworld.org/docid/441821a829.html.
168 International Crisis Group, "Nepal's Maoists: Their Aims, Structure and Strategy."
169 Peng Hwa Ang, Shyam Tekwani, and Guozhen Wang, "Shutting down the mobile phone and the downfall of Nepalese society, economy and politics."

mobile phone service was intended to stop anonymous prepaid users; when the service resumed, all users—including pre-paid ones—had to register."[170]

The shutdown was achieved due to state-owned Nepal Telecommunications (NT)'s monopoly over the market.[171] During the shutdown, NT was able to provide the Nepalese government and military access to a newly developed CDMA (a type of radio communications system) network, which they planned to operate in parallel with the older system. Thus, state forces were able to continue using ICT with minimal interruption. [172]

The shutdown's impact on CPN-M operations only lasted for two weeks. Initially, operations slowed, and the transport of food and medicine was impacted. But the group opted to use "high-powered walkie talkies that had a range of 10 to 15 kilometers."[173] In response to this suspension of services, Maoists pivoted to relying on "ACeS satellite phones with SIM cards smuggled in from Thailand and the Philippines."[174] As a result of this modification to ICT strategy, the Maoists "had the most advanced telecommunications network in Nepal" and became the largest users of satellite phones in the country.[175] Landline services were also restored fairly quickly, which enabled CPN-M to resume usage on the communications network that depended on this infrastructure. The state was forced to resume access to landlines due to civilian reliance on this

---

170 Ibid.

171 Gopal Sharma, "Nepal frees top leader, restores some mobile phones," *Reuters,* May 2, 2005, https://reliefweb.int/report/nepal/nepal-frees-top-leader-restores-some-mobile-phones.

172 Peng Hwa Ang, Shyam Tekwani, and Guozhen Wang, "Shutting down the mobile phone and the downfall of Nepalese society, economy and politics."

173 Kunda Dixit, "Keep in touch: Satellite phones may be the only way to communicate in the event of a natural disaster," Nepali Times, March 26, 2010, http://archive.nepalitimes.com/news.php?id=16929#.YKPRRjsZ7q8.

174 Kunda Dixit, "Keep in touch: Satellite phones may be the only way to communicate in the event of a natural disaster," Nepali Times, March 26, 2010, http://archive.nepalitimes.com/news.php?id=16929#.YKPRRjsZ7q8.

175 Peng Hwa Ang, Shyam Tekwani, and Guozhen Wang, "Shutting down the mobile phone and the downfall of Nepalese society, economy and politics."

service. In addition, CPN-M had access to public communication offices described as "staffed privatized telephone booths" which offered services such as "faxes, phone card sales and, often, Internet access."[176] As described by one observer, the CPN-M "communications network appeared to be functioning better than that of the government."[177]

Application of the Theory

Initially, the CPN-M followed predicted adoption behaviors of existing theory. They were early users of advanced ICT, adopting the internet and mobile phones soon after the technology was introduced in Nepal. In particular, cell phones enjoyed widespread adoption intra-organizationally, with documentation of high rates of cell phone ownership and use by individual fighters. Noting this, the Nepalese government took advantage of their power over the publicly owned infrastructure that the CPN-M relied on to use this technology. Grappling with their opponent's power over and use of this infrastructure, the CPN-M reverted to using satellite phones. While they used landlines once service was returned, the CPN-M continued to use satellite phones, becoming the largest user base of this technology in Nepal. Importantly, civilian reliance on this same infrastructure became the key impetus for the resumption of access.

Variable 1. Shared Infrastructure The Nepalese state, the CPN-M, and Nepalese civilians all relied on the same telecommunications infrastructure: Nepal Telecom, a state-owned company with a monopoly over the market. However, the Nepalese government could not effectively benefit from the vulnerabilities created by CPN-M use of the network, as prepaid users did not need to register and could thus operate with anonymity. Rather than exploiting the overlap in reliance to gather

[176] Ibid.
[177] International Crisis Group, "Nepal's Maoists: Their Aims, Structure and Strategy."

intelligence, the Nepalese state decided to target CPN-M operations through the temporary elimination of communications services. This approach was largely ineffective, and the true impact was felt by civilians who also depended on this network, leading to protests and condemnation of the decision. In response, CPN-M opted to further minimize reliance, choosing to transition to a more low-tech approach that was less dependent on this shared infrastructure.

Variable 2. Control by Private Actors In the case of Nepal, local infrastructure and telecommunications were state-owned, minimizing the role of private sector actors. Depending on which networks they provided access to and whether they were privately owned, there may have been some effects imposed by CPN-M reliance on SIM cards sourced from Thailand and the Philippines. Additionally, there may have been some effects created from sourcing the satellite phones from Singapore. In this case, there is not enough available information to determine impact on adoption outcomes.

Variable 3. Ubiquity Regarding mobile cell phone adoption, CPN-M strategy appears to reflect a passive acquisition approach. Most captured members of CPN-M had a cell phone, despite internal organizational calls to minimize usage in order to prevent information leaks. Their increased use by CPN-M fighters also reflects the role of the emerging ICT sector, which led to the diffusion of mobile phones across Nepal.

Variable 4. Multiple Functions and Customization CPN-M used ICT for various documented purposes, including propaganda, internal communications, and appeals to the international diaspora. This reflected their intensive approach to ideology and indoctrination. They opted against any

explicit technological innovation involving ICT and across functions preferred to revert to older technologies when faced with a vulnerability that could advantage their opponent.

Los Zetas of Mexico

Los Zetas originated as the paramilitary wing of the La Compañía drug smuggling organization, operating across Mexico from 2006 through present day. Over the course of their organizational development, the group grew in numbers, sophistication, and independence. Beginning in 2006, the group sought to construct a proprietary, encrypted radio network, which spanned from "core Los Zetas territories in Nuevo León and Tamaulipas, into central Mexico and through the gulf states as far south as the border with Guatemala."[178] The formal military training of Los Zetas members informed their prioritization of information and communications technology as an integral part of their operations.[179]

Los Zetas Organization

Los Zetas were composed of former Mexican special forces (GAFE) members, adhering to a highly centralized command structure. As articulated by a retired U.S. army colonel, Los Zetas had:

> "a paramilitary mindset...a chain of command, an appreciation of what technology can do to enhance paramilitary capabilities. If you're a military guy who started such a group, one of your first concerns is communications. You can build communication networks at a

[178] See an excellent summary of Los Zetas' ICT capacity and development of the radio network by James Halverson, "Los Zetas and proprietary radio network development," *Journal of Strategic Security*, Vol. 9, No. 1 (2016), pp. 70-83.
[179] For additional resources on Los Zetas see Patrick Radden Keefe, "Cocaine Incorporated," *The New York Times*, June 15, 2012, http://www.nytimes.com/2012/06/17/magazine/how-a-mexican-drugcartel-makes-its-billions.html; Damon Tabor, "Radio Tecnico: How the Zetas Cartel Took Over Mexico with WalkieTalkies," *Popular Science*, March 25, 2014, http://www.popsci.com/article/technology/radio-tecnico-how-zetas-cartel-took-overmexico-walkie-talkies; Michael Weissenstein, "Mexico's cartels build own national radio system," *Associated Press*, December 26, 2011, https://www.seattletimes.com/nation-world/mexicos-cartels-build-own-national-radio-system/.

relatively low expense if you have the expertise. So, it's quite possible to build, say, a network for a low-level handheld radio carried by a taxi driver that can be picked up, re-transmitted, boosted up, and sent anywhere you want to send it, and even encrypted after it's transmitted."[180]

Los Zetas' organizational structure included numerous communications experts. In the earliest stages of the radio network's development, decisions were likely made and guided by the leadership of La Compañía. This control over decision-making shifted over time, until it came under the purview of Heriberto Lazcano-Lazcano, leader of Los Zetas (from 2004 - 2012), as the group evolved into an autonomous organization. Lazcano-Lazcano was characterized as "the person with the single most influence over decisions regarding the network's creation and expansion."[181]

Los Zetas were described as possessing a "vast telecommunications network involving two-way radios, encrypted, secure radio networks, computers and burner cell phones."[182] The radio network was selected as a valuable alternative to existing cell phone networks. Cell phones made the group vulnerable to monitoring by Mexican authorities and cellular service often failed to reach rural areas of Mexico where Los Zetas often operated.[183]

---

180 Sam Clements, "Los Zetas Drug Cartel Has Their Own Radio Network," *VICE*, January 2, 2013, http://www.vice.com/read/the-los-zetas-drug-cartel-have-theirown-radio-network.

181 James Halverson, "Los Zetas and proprietary radio network development."

182 Robert J. Bunker ,"Mexican Cartel Operational Note No. 1: Mexican Military Operations against Los Zetas Communications Networks," *Small Wars Journal* (2011); Robert J. Bunker and Alma Keshavarz, "Narco Radio C2 and CCTV Networks Reader," *Small Wars Journal -- El Centro eBook*, (2019); Lisa J. Campbell, "Los Zetas: operational assessment," *Small Wars & Insurgencies*, Vol. 21, No. 1 (2010), pp. 55-80.

183 Spencer Ackerman, "Radio Zeta: How Drug Cartels Stayed Networked," *WIRED,* December 27, 2011, https://www.wired.com/2011/12/cartel-radio-mexico/.

To develop the national network, Los Zetas built a specialized technical team led by Jose Luis Del Toro Estrada, referred to as El Técnico. This team included individuals with specialized technical expertise in the creation and installation of radio networks. Later on, after a mass DEA crackdown which resulted in the capture of Estrada, Los Zetas switched to a new model of accessing expertise. The group began to kidnap and force engineers and technicians with backgrounds in telecommunications "into slave labor for as long as they were useful."[184] This includes an estimated "thirty-six telecommunications professionals who went missing between 2009 and 2012."[185]

For Los Zetas, investing in this network (which is estimated to have cost them tens of millions), was both financially possible and viewed as a valuable investment to support the organization's operations.[186]

Attributes of a Radio Network

The proprietary radio network was the most substantial and resource-intensive ICT project undertaken by the group. There is some evidence that early-stage prototyping occurred in the border town Matamoros in 2004, with the installation of a local radio network. Structurally, the radio network system "was believed to make use of many hundreds of antennas and signal repeaters, which, under the control of a series of command centers, offered service in vital areas of operation."[187] Territory under Los Zetas' control was divided into 'plazas.' The leader of each of these plazas "has the responsibility for establishing nodes on the network -- getting the antennas in

184 Ibid.
185 Ibid.
186 Ibid.
187 James Halverson, "Los Zetas and proprietary radio network development."

place, concealing them as necessary, making sure the signal-boosting repeaters extend the network's reach, equipping cartel personnel with handheld radios, and replacing what the security forces destroy."[188] The sourcing of the radio network material is unknown. Los Zetas were intentional about camouflaging infrastructure, including painting antennas to match the surrounding environment, and were intentional about placing both antennas and signal repeaters in "remote, hard to reach areas."[189]

Los Zetas pursued different installation strategies for urban and rural areas. In urban areas, they first mapped the local spectrum of frequencies to avoid interference from existing networks. They then installed physical components and infrastructure, sometimes co-opting existing radio infrastructure, including existing radio repeaters, which are used to receive and boost signals. In rural areas, infrastructure was designed to maximize reach over long distances. Towers were built at the highest point in a given topography and attached with various antennas and repeaters. One grouping of towers in Veracruz provided coverage over a 100-mile radius, which included ten towns and cities. Many of these towers relied on solar panels for power.

Los Zetas also developed command and control centers and computer systems to manage the network. Over time this central system was able to give instructions to specific towers. One raid conducted by Mexican forces also found equipment for "ground to air radio communication." As described by an in-depth journalistic report, "much of the infrastructure -- the towers, the receivers -- is cheap enough to be easily replaced. The network is 'low-cost, highly extendable and maintainable.'"[190]

---

[188] Spencer Ackerman, "Radio Zeta: How Drug Cartels Stayed Networked."
[189] James Halverson, "Los Zetas and proprietary radio network development."
[190] Spencer Ackerman, "Radio Zeta: How Drug Cartels Stayed Networked."

Patterns of ICT Usage

The primary functions of the radio network were operational coordination and intelligence gathering. The radio network was viewed as a way to more effectively support ongoing control of territory and engage in active monitoring. The network served as an "early warning reconnaissance system," with regional operatives using handheld devices to alert the organization of the presence of state forces in a given territory. One news article reported that the radio network was primarily utilized for operational and tactical purposes, as "bosses only communicate through the Internet. The radio network is for lookouts and lower-level players."[191] There were also documented instances of Los Zetas operatives hijacking Mexican military radio networks to broadcast threatening messages. These incidents are involved intentionally compromising the operational security of the group's radio network. In one case, a repeater was installed on the roof of a police station.[192] The radio network also offered tactical support to a wide range of activities, notably drug trafficking and smuggling, enabling consistent monitoring of and rapid response to territories under their control. The radio network as a critical tool in the expansion of their activities.[193]

Application of the Theory

Los Zetas pursued an unorthodox adoption strategy from the group's inception. Noting the risks imposed by their use of cell phones, the group sought to invest millions in creating a national radio network. When they lacked internal technical expertise, they kidnapped engineers to build up their organizational capacity. Most interestingly, they opted for a technology that was both less technologically sophisticated (radio, as opposed to cell phones, although they occasionally used

191 Ibid.
192 James Halverson, "Los Zetas and proprietary radio network development."
193 Spencer Ackerman, "Radio Zeta: How Drug Cartels Stayed Networked."

burner phones), and imposed far greater demands on financial intensity and organizational capital. The group's perception of the technological alternative, reliance on shared infrastructure and the vulnerabilities opponent access imposed, was perceived as sufficiently risky to revert to a comparatively older technology and create their own ICT infrastructure. Another forcing mechanism may have been ICT's lack of ubiquity in certain areas of their operations (rural Mexico), elevating the financial intensity of adopting either radio or cell phones.

Variable 1. Shared Infrastructure. Los Zetas pursued an innovative ICT strategy, with a central goal of avoiding overlaps in infrastructure reliance with state police and military forces. The aim was to reduce vulnerabilities (such as detection) introduced by depending on the same physical ICT infrastructure. Organizationally, it mirrored the approach typically taken by state militaries, contrasting the approach of most non-state armed groups, who often lack the organizational capacity and resources to develop and maintain this level of infrastructure.

Variable 2. Control by Private Actors. In developing their own radio network, Los Zetas pursued a deliberate strategy to avoid third-party actors altogether. They kidnapped and coerced experts from the private sector into developing a system for them. By building their own infrastructure, they could avoid the potential strategic impact of decisions made by private sector actors, such as the location and range of radio infrastructure.

Variable 3. Ubiquity This is an example of an intentional acquisition. Los Zetas quite clearly and deliberately chose to invest a massive amount of resources into acquiring and developing radio infrastructure. This adoption was not a byproduct of the proliferation of radio technology in Mexico. Los Zetas' investment decision represented an approach that mirrors state militaries, likely a

byproduct of members' backgrounds working for the Mexican military. Also important to note is the lack of commonly accessible ICT infrastructure in certain rural areas where they operated, that may have forced them to make a greater organizational investment than they would have otherwise.

Variable 4. Multiple Functions and Customization. This variable was present. The radio network was used for a wide range of functions, including communication, intelligence gathering, and hijacking of other networks to threaten members of state forces. The customization of the network was also extensive: networks were paired with specific iterations of antennas and repeaters to expand the scope of reach and eventually consolidated into a central command system that allowed for direct control. For different functions, the group opted for more advanced (computers, cell phones) or less advanced (radio), depending on their ability to control for risk.

Russia, Russian Armed Forces

In the post-Soviet Union era, Russia has sought to emulate the U.S.'s approach to developing and integrating information and communications technology and building up C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) capacity. In 2008, a shift occurred in Russia's investment strategy and general approach to ICT (and C4ISR broadly).[194] The change placed an emphasis on greater centralization and private sector partnerships. The Russian military also created specialized subunits dedicated to electronic warfare.

In 2014, Russia created the National Defense Management Center (NDMC) to support the consolidation and modernization of C4ISR systems and capacity. The intention of the NDMC was

194 Andrew Radin, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, *The Future of the Russian Military: Russia's ground combat capabilities and implications for US-Russia competition* (RAND Corporation Santa Monica United States, 2019), p. 47.

to pursue "the integration of existing communications systems within a single network, as well as the development of UAVs, space-based intelligence, surveillance, and reconnaissance (ISR), and other sensors."[195] Russia is described as having "laid the foundations for a C4ISR infrastructure more complicated and interconnected than the U.S. interagency, with both the potential risks and benefits of greater centralization."[196] The goal of this approach, according to Western analysts, appeared to be to gain the advantage in "net-centric" warfare, that is, information and electronic warfare. This new organizational strategy made ICT integration, adoption, and effective use paramount.

Russia's current organizational model for pioneering, innovating, and incorporating cutting edge ICT is to use a state-owned holding company to consolidate relevant 'private' sector industries for military use. The Russian government uses a holding company called 'Rostec' or, State Corporation for Assistance to Development, Production and Export of Advanced Technology Industrial Product Rostec, to centralize control over the domestic industry for C4ISR technologies.

The Russian government also actively helped to subsidize the domestic ICT industry and pursued "import substitution to resolve foreign dependence."[197] The Russian military has sought to engage in "major investment in networks to improve effectiveness and centralization [...] [along with] emulation of Western investments in reconnaissance strike complex, including UAVs, space, etc."[198] In spite of this, Russian ICT innovation remains limited by the capacity of the domestic ICT sector and its cutoff from Western technologies due to sanctions.[199]

---

[195] Ibid., p. 54.
[196] Ibid., p. 54.
[197] Ibid., p. 50.
[198] Ibid., p. 50.
[199] Ibid., p. 54.

Russia has also invested heavily in their technical capacity for electronic warfare, intended to target radio and online networks of opponents. Senior military leaders have publicly emphasized the need for electronic warfare capacities. Reflecting this organizational prioritization, "since 2011, Russia has delivered a number of advanced [electronic warfare] systems to the Ground Forces, at the company, battalion, and brigade levels, which seek to jam VHF radio, radio-controlled fuses, and GPS. UAVs with [electronic warfare] capabilities also complement existing airborne systems."[200]

VKontakte - Russian Control of Social Media Platforms as a Military Tool

One key example of Russia's acquisition of ICT and information warfare tools from the private sector is its coercive and indirect purchase of VKontakte. VKontakte was used as a key tool for Russia's information warfare efforts in Ukraine, supporting Russian annexation of Crimea and military activity in the Donbas region. VKontakte, described as a Facebook for Russian speakers, is an online social media platform created by Russian entrepreneur Pavel Durov in 2006. In 2012 and 2013, VKontakte was among the most popular websites for Ukrainians, second only to Google search in terms of daily users.[201] On January 24, 2014, Durov was forced to sell his stake in the company to Russian government proxies (specifically, Kremlin-affiliated business magnates), bringing the social media platform under government control.[202] In February 2014, Russian soldiers took over key positions in Crimea in the aftermath of the Maidan revolution in Ukraine, which had resulted in the removal of Russian-aligned Ukrainian president Viktor Yanukovych. In March 2014, a forced referendum occurred, confirming the "validity" of Russia's annexation of Crimea. In April

200 Ibid., p. 55.

201 Dinissa Duvanova, Alexander Semenov, and Alexander Nikolaev, "Do social networks bridge political divides? The analysis of VKontakte social network communication in Ukraine," *Post-Soviet Affairs,* Vol. 31, No. 3 (2015), pp. 224-249.

202 Nickolay Kononov, "The Kremlin's Social Media Takeover," *The New York Times*, March 10, 2014, https://www.nytimes.com/2014/03/11/opinion/the-kremlins-social-media-takeover.html.

2014, pro-Russia separatist groups, interspersed with Russian paramilitary and intelligence, began fighting for control over the Donbas region in eastern Ukraine.[203]

Throughout this conflict, VKontakte was used to supplement military action on the ground, particularly in the Donbas region. For example, pro-Russian separatist groups, supported by members of the Russian military, were able to solicit donations over VKontakte. A journalistic investigation showcased one "pro-Russian group battling for control over the Ukrainian port city of Mariupol solicit[ing] donations for equipment on VKontakte, Russia's most popular social network. It wrote "help is very much needed" and listed ways to transfer money."[204] Analysis of the VKontakte activity of pro-Russian groups, including the Novorossiya Militia, demonstrated that online activity correlated strongly with events happening on the battlefield. Makhortykh and Sydorova (2017) found "that social media such as Vkontakte were intensively used for framing the conflict during the peak of violence in summer 2014."[205] This use of VKontakte allowed groups to brand themselves and propagate a narrative to both local and regional audiences regarding the validity of their cause.

However, Ukrainian groups also operated on and used VKontakte to support their activities.[206] In response to the vulnerabilities this created, Ukraine instituted a ban on VKontakte in May 2017. In addition to providing the opposing side visibility into Ukrainian operations, cybersecurity experts claimed that VKontakte posed "a greater danger as launchpads for hacking

---

203 Michael Kofman, Katya Migacheva, Brian Nichiporuk, Andrew Radin, and Jenny Oberholtzer, *Lessons from Russia's operations in Crimea and Eastern Ukraine*, (Rand Corporation, 2017).
204 Jo Becker and Steven Lee Myers, "Russian Groups Crowdfund the War in Ukraine," *The New York Times,* June 11, 2015, https://www.nytimes.com/2015/06/12/world/europe/russian-groups-crowdfund-the-war-in-ukraine.html.
205 Mykola Makhortykh and Maryna Sydorova, "Social media and visual framing of the conflict in Eastern Ukraine," *Media, War & Conflict*, Vol. 10, No. 3 (2017), pp. 359-381.
206 Ibid.

attacks."[207] However, the ban did not apply to Russian occupied territories and many Ukrainian civilians found ways around the ban to continue using the platform.[208]

Application of the Theory

Russia adopted one of the most advanced forms of technology available, in the form of social media platform VKontakte. However, it did so in a way that imposed greater financial demands on the organization. Rather than take advantage of a technology that was freely accessible, Russia adopted the technology in a way that accounted for two key concerns: (1) the technology was owned and controlled by a private actor, and (2) the technology was used by the populations of its opponents (namely Ukraine). Controlling for these risks and opportunities, Russia coercively purchased the platform in order to gain total control over the technology.

Variable 1. Shared Infrastructure Russia preempted possible interaction effects caused by subsuming VKontakte under its control, in line with a broader technology acquisition strategy. Ukraine recognized the vulnerabilities created by military members and Ukrainian civilians relying on the platform well into the conflict and attempted to institute a ban.

Variable 2. Control by Private Actors Russia quickly recognized the strategic importance of private sector actors in shaping a possible landscape of engagement with other states and domestic

[207] Thomas Grove, "Russian Social Media Seen as Threat to Ukraine and to Cybersecurity," *The Wall Street Journal,* May 29, 2017, https://www.wsj.com/articles/russian-social-media-seen-as-threat-to-ukraine-and-to-cybersecurity-1496055606.

[208] Sebastian Bay, Giorgio Bertolin, Nora Biteniece, Edward H. Christie, Anton Dek, R. Fredheim, J. Gallacher, Kateryna Kononova, and Tetiana Marchenko. "Responding to Cognitive Security Challenges." *NATO STRATCOM Centre of Excellence, January* (2019).

political opponents. As a result, they opted to coercively assume control of the platform, purchasing the company using government proxies.

Variable 3. Ubiquity For the Ukrainians and the Russians, this was an instance of unintentional acquisition. A third-party actor created and deployed the technology, and both sides attempted to cope with the strategic ramifications of adoption by military members and broader society. For the Ukrainians, the military was forced to adapt after realizing the vulnerabilities created, due to widespread use among Ukrainian civilians and military members. Once the threat and vulnerabilities became apparent for the Russians, they developed an acquisition strategy that allowed for total control over the platform's technology.

Variable 4. Multiple Functions and Customization The Russian-backed groups were able to use the platform to communicate with communities, delineate their operations, and solicit funding. It was also used as a means of intelligence gathering and had the potential to be used to facilitate cyberattacks. There is not much evidence of instances when the group used different types of ICT for different functions.

People's Republic of China, People's Liberation Army (PLA)

In the face of a new information environment, China's military, the People's Liberation Army (PLA), underwent several organizational shifts to better integrate new forms of information and communications technology. One goal of this organizational restructuring was to consolidate information operations into a specialized sub-unit that could operate across services. Strategically, development of ICT and ICT-related organizational capacity prioritized four key principles: (1) integration, (2) dual peacetime / wartime use, (3) centralization, and (4) innovation. Additionally,

their articulated strategy involved leveraging civilian ICT for military use and engaging in leap-frog development, by copying or acquiring more advanced foreign technologies.

The PLA's organizational structure had remained fairly consistent since the 1950s, designed to place the Chinese Communist Party in charge over military decision-making and operations. This included a "dual command system" wherein "unit commanders shared responsibility with political commissars."[209] In the 1990s, in response to witnessing US technology during the Gulf War and the power of emerging forms of ICT, PLA military theorists began emphasizing the importance of information technology and of developing a networked system for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). In 2000, the PLA began prioritizing the development of a command automation system which would include command and control, intelligence and surveillance, communications, electronic countermeasure, early warning, and information support capabilities. Computers were intended to form the backbone of this system. By 2010, this system utilized fiber optic cables, wireless communications, and satellite communications.[210]

Patterns of use and type of ICT available varied intra-organizationally and by geography. China has historically been divided into military regions, with the most recent reform in 2016, resulting in a system of five theater commands.[211] In 2010, this system included seven military

[209] Joel Wuthnow and Phillip Charles Saunders, *Chinese military reform in the age of Xi Jinping: Drivers, challenges, and Implications*, (Government Printing Office, 2017).
[210] Kevin Pollpeter, "Toward an Integrative C4ISR System: Informationization and Joint Operations in the People's Liberation Army," In *The PLA at Home and Abroad: Assessing the Operational Capabilities of China's Military (*Carlisle: Strategic Studies Institute, 2010).
[211] Shannon Tiezzi, "It's Official: China's Military Has 5 New Theater Commands," *The Diplomat*, February 2, 2016, https://thediplomat.com/2016/02/its-official-chinas-military-has-5-new-theater-commands/.

regions. During this time, ICT capacity and usage varied between military regions (MR). One report documented ICT capacity in the Chengdu MR as follows:

> "[it] is said to use a combination of optical fiber networks, satellite networks, program-controlled switched telephone networks, computer networks and teleconferencing networks. Optical fiber cables now cover 98 percent of the units at the regiment or battalion level and above, as well as key border defense posts and entry ports. Military program-controlled switched telephone networks and satellite networks cover all units at the company level and above. Regional computer networks and teleconferencing systems have been established in combat units at the regimental level and above. In addition, a digitized broadband communications network connects all campaign and tactical level units horizontally and vertically. "[212]

By contrast, in the Nanjing MR, there was evidence of the military "taking over or renting civil telecommunication lines from the commercial sector," rather than creating their own secured networks.[213] The development and acquisition of ICT was left up to individual subunits (in particular, the military regions), which had relative autonomy in determining usage and acquisition patterns for ICT. This time in the PLA's organizational history was characterized by, "bureaucratic stove piping within the PLA [that] led to different services relying on different information systems, MRs developing C4ISR capabilities that were incompatible with other MRs, and operations in the information domain being managed by different organizations."[214] Individual MRs often established

[212] Kevin Pollpeter, "Toward an Integrative C4ISR System: Informationization and Joint Operations in the People's Liberation Army," p. 202.
[213] Ibid., p. 213
[214] Ibid., p. 213

or developed their own joint C4ISR systems, independent of other MRs. Crucially, "while the services have been good at establishing communications with subordinate units, they have largely ignored connectivity with their sister services."[215] This compartmentalization of the C4ISR system meant that ICT adoption and use was uneven intra-organizationally. Additionally:

> "Communication problems [arose] due to the incompatibility of technology. Units use different models and generations of weapons and equipment and there are differences in the technology levels of services and combat arms or even between different operational units within a service or combat arm. One of the main sources of this incompatibility is the decentralized nature of PLA technology development where individual units are provided funding to develop their own technology but pay no attention to connecting with other units." [216]

By early 2016, under Chinese president Xi Jinping, the PLA instituted several structural reforms which addressed these long-standing issues. In particular, these reforms sought to prioritize C4ISR across its branches and address problems of integrating the capabilities of different services became a key impetus for organizational change. Additionally, these "core problems were accompanied by other structural weaknesses, including a defense R&D system that did not adequately utilize advances in civilian science and technology (S&T)."[217] These reforms established a new specialized unit called the Strategic Support Force, tasked with managing the PLA's "electronic

[215] Ibid., p. 217
[216] Ibid., p. 216
[217] Joel Wuthnow and Phillip Charles Saunders. *Chinese military reform in the age of Xi Jinping: Drivers, challenges, and Implications*.

warfare, cyberwarfare, and psychological operations, among other high-tech missions."[218] This unit has been described as operating across joint forces and supporting all services.[219] Specific operational and tactical roles include: "early warning, managing space satellites (including the Beidou navigation satellites), and provid[ing] defense in the electromagnetic and cyber domains."[220] The SSF also harnessed civilian technical expertise in its efforts, with the development and sponsorship of projects "involving the joint efforts of industry, civilian research institutes, and military academies."[221]

Chinese Influence Operations and Taiwan

The People's Republic of China (PRC) has long sought Taiwan's "reunification" with the mainland under its "One-China" principle. Over the years, China has employed various methods to coerce and intimidate Taiwan into reunification. The PLA has prepared contingencies in the event that armed force is necessary. So far, the PLA and PRC's primary tactics have been information warfare, cyber-attacks and increasing the "the frequency and scale of patrols of PLA bombers, fighter jets, and surveillance aircraft over and around Taiwan."[222] In particular, online influence operations have been a key tool in China's effort to disrupt Taiwan domestic elections and to promote pro-China sentiment among the Taiwanese. During the 2020 Taiwanese presidential election, China launched targeted influence operations aimed at altering voting outcomes.

---

218 Lindsay Maisland, "China's Modernizing Military," Council on Foreign Relations, February 5, 2020, https://www.cfr.org/backgrounder/chinas-modernizing-military.

219 Kevin Pollpeter, "Toward an Integrative C4ISR System: Informationization and Joint Operations in the People's Liberation Army."

220 Joel Wuthnow and Phillip Charles Saunders. *Chinese military reform in the age of Xi Jinping: Drivers, challenges, and Implications*.

221 Ibid.

222 Lindsay Maizland, "Why China-Taiwan Relations Are So Tense," Council on Foreign Relations, May 10, 2021, https://www.cfr.org/backgrounder/china-taiwan-relations-tension-us-policy.

China's online operations consisted of promoting advantageous narratives on social media platforms to prompt skepticism of Taiwan's ruling Democratic Progressive Party (DPP). As compared to its rival party Kuomintang (KMT), DPP holds less favorable opinions towards relations with China (as perceived by the Chinese government). China's online operations leveraged Facebook, Twitter, Instagram, YouTube, as well as regional platforms PTT (described as Taiwan's version of Reddit) and LINE (a messaging platform similar functionality to WhatsApp).[223]

Chinese influence operations peddled multiple contentious and incendiary narratives intended to undermine the credibility of the DPP. These included casting doubt on DPP presidential candidate Tsai Ing-wen's doctoral degree, spreading false stories about the LGBTQ+ community, critiquing Taiwan's Anti-Infiltration (foreign interference) bill, questioning the integrity of the election results, and discrediting a Chinese whistleblower who had called attention to Chinese influence operations. According to one report, this involved "the Chinese cyber army and content farms creat[ing] and/or circulat[ing] in Taiwan's cyberspace fake stories on polarizing issues."[224] The PLA's Strategic Support Force is characterized as the organizing force behind the content farms and troll factories producing online disinformation. In October and December 2019, a few months prior to the election, Facebook was able to remove scores of Chinese assets connected to this influence operation. Additionally, LINE launched a fact-checking program during the election that led to the removal and correction of more than 30,000 stories shared by users.[225]

---

223 Nick Monaco, Melanie Smith, and Amy Studdart, "Detecting Digital Fingerprints: Tracing Chinese Disinformation in Taiwan," Graphika Report, August 25, 2020, https://graphika.com/reports/detecting-digital-fingerprints-tracing-chinese-disinformation-in-taiwan/.

224 Aaron Huang, "Combatting and Defeating Chinese Propaganda and Disinformation," HKS Belfer Center for Science and International Affairs, (July 2020).

225 Ibid., pp. 35-36.

Some of this interference also came in the form of traditional media: China was able to funnel false stories through Taiwanese media outlets. Specifically, "China has been able to pass much of its propaganda as news stories, even though they were paid advertisements. China also has been able to influence and direct numerous media organizations because it is a major source of their advertisement revenue."[226] This vulnerability is exacerbated by the Taiwanese government's hesitancy to regulate freedom of speech within the press and media.

Application of Theory

China adopted key forms of modern ICT, leveraging its features to wage influence operations against its opponent, Taiwan. China adopted the technology because of the vulnerabilities and risks imposed, namely the shared use of ICT infrastructure in the form of social media (which enabled China to access Taiwanese civilians), private actor control over ICT infrastructure in Taiwan (which enabled China to bribe Taiwanese media companies into ceding access), and the ubiquity of ICT (which limited Taiwan's ability to wrangle back control over information flows). China also faced some constraints in adoption, in the form of asset removals and bans on the platforms of privately owned social media platforms.

Variable 1. Shared Infrastructure China leveraged interaction effects imposed by the shared use of and access to ICT infrastructure to target Taiwanese citizens during the 2020 election to undermine the ruling party leading the Taiwanese government. However, Taiwan had limited means to reduce China's access, constrained by its commitment to freedom of speech and the fact that social media companies are privately owned. As a result, China was able to weaponize shared ICT infrastructure to access the Taiwanese population.

[226] Ibid., p. 19.

Variable 2. Control by Private Actors China recognized the strategic importance of two sets of private actors, the Taiwanese media and social media platforms. China was able to exert influence over traditional media by catering to the profit-motivations of media companies. Leveraging the media's dependence on advertising revenue, China was able to push its own narratives through channels owned by private actors. Unfortunately, Chinese operations were targeted by platforms including Facebook, Twitter, and LINE, without much ability to counter the removal of their assets. This case highlights two kinds of interactions armed organizations can have with private actors over ICT.

Variable 3. Ubiquity For both Taiwan and China, this was an instance of unintentional acquisition. A separate actor created the technology (social media and traditional media), and both sides attempted to cope with the strategic ramifications of adoption by the military and broader society. In this case, China weaponized the dual-use nature of ICT to target Taiwanese civilians. For Taiwan, they dealt with the consequences and vulnerabilities created by ICT's widespread use by civilians. While Taiwan has engaged in some efforts to curb the spread of Chinese influence, including the 2019 Anti-Infiltration Bill, which seeks to criminalize behaviors that contribute to the success of foreign influence efforts, countermeasures are limited.

Variable 4. Multiple Functions and Customization Chinese influence operations were able to leverage multiple ICT-based features to develop their campaign, including spreading rumors and false stories, promoting pro-China propaganda, and evaluating Taiwanese response to its information campaigns. It is unclear whether they opted for different forms of ICT for different functions.

Discussion

Disruptive attribute theory is not meant to wholly replace existing theory, but rather highlight that in the case of ICT, technology cannot be treated as a constant. The attributes of ICT matter in explaining variation in patterns of adoption and usage by armed organizations, an established puzzle in the literature.[227] Through case study analysis of four varied organizations, both state and non-state, this paper sought to explore the relevance of disruptive attribute theory's explanatory power and further theory building around the impact of ICT's attributes on adoption and use.

Despite organizational differences in capacity, the groups analyzed all exhibit patterns of behavior unaccounted for by standard models. Due to overlaps in the use of physical ICT infrastructure, the CPN-M reverted to an older form of technology, satellite phones, to evade the consequences of the Nepalese government's national shutdown of phone lines. Further, this shutdown proved wildly unsuccessful for the state, as they received backlash from the civilian population who also depended on this infrastructure. Los Zetas dealt with the same problem of overlaps in dependence by creating their own, separate radio network. Los Zetas perceived the vulnerabilities of public infrastructure to outweigh the cost of developing a free-standing system that they could exert total control over. While Mexican forces removed pieces of the radio network's infrastructure where they could find it, the system remained operational for years, supporting the communication and intelligence needs of Los Zetas. Russia dealt with the problem of private actor power, by subsuming control of a popular social media platform through a coercive purchase. This approach proved successful, aiding in military operations in Donbas, even amidst attempts by the Ukrainian government to ban the platform networks. Civilian users easily circumvent this ban to

[227] Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda."

continue accessing the site. Finally, the Chinese state leveraged both traditional media and social media to propagate influence operations targeting Taiwan. The control that private actors have over the media environment in Taiwan meant that the Chinese state could use financial means to achieve its goals. However, this same third-party control became a constraint on social media. The decisions made by platforms, including Facebook and LINE, reduced the effectiveness of Chinese operations. Table 2 provides a comparative review of each case by variable.

Table 2. Comparison of Adoption Behaviors by Case

Variable	CPN - M	Los Zetas	Russia	China
1 - Shared Infrastructure. ICT introduces distinct and strategically important interaction effects.	Nepal's government initiated a nation-wide shutdown of cell phone services. In response, CPN-M reverted to an older technology: satellite phones.	Los Zetas build their own radio infrastructure to eliminate possible interaction effects and vulnerabilities imposed by relying on existing infrastructure.	Russia preempted possible interaction effects by subsuming VKontakte under their control. Ukraine attempted to counteract these effects by instituting a ban of the platform on national networks.	China weaponized shared ICT infrastructure (social media platforms) to access the Taiwanese population.
2 - Control by Private Actors. ICT increases the role and importance of third-party and private sector actors.	Nepal Telecom was state owned, but untraceable SIM cards used by the CPN-M were made and sold by private actors.	Los Zetas pursued a deliberate strategy to avoid third-party actors altogether. They kidnapped and coerced experts from the private sector into developing a system for them	Russia quickly recognized the strategic importance of private sector actors and opted to coercively assume control of the platform.	China was able to exert influence over traditional media by catering to the profit-motivations of media companies. Chinese operations were targeted by platforms without much ability to counter the removal of their assets.

3 - Ubiquity. The ubiquity of ICT creates different modes of technology acquisition by armed organizations: the source and form of technological diffusion matter.	CPN-M were intentional about acquisition of satellite phones and walkie-talkies post-shutdown. However, fighter adoption of cell phones partly reflects national growth of this industry.	This is an example of an intentional acquisition. Los Zetas quite clearly and deliberately choose to invest massive resources into acquiring and developing radio infrastructure.	For the Ukrainians and the Russians, this was an instance of private actors introducing a technology of relevance in a conflict context. A third-party actor created and deployed the technology, and both sides attempted to cope with the strategic ramifications.	For both Taiwan and China, this was an instance of private sector actors developing technologies that were then adopted into ICT strategy after their diffusion.
4 - Multiple Functions and Customization. ICT allows for customization and a wider range of applications.	ICT was used for several operational purposes: propaganda, internal communications and remote detonation of IEDs.	ICT was used for a wide range of functions, including communication, intelligence gathering, and hijacking of other networks to threaten members of state forces. Los Zetas also engaged in customization of the radio network.	ICT was used to communicate with communities, delineate their operations, solicit funding, gather intelligence and launch cyberattacks.	In this case, ICT was principally used for influence operations.

As was documented, in many cases the predicted outcomes of the null hypothesis were absent. Both CPN-M and Los Zetas opted for alternative technologies, not because of a lack of cheaply available and easily adoptable technology (1b), but rather because constraints imposed by key features of ICT which encouraged pursuit of comparatively 'older' technologies (satellite phones and radio) (2a). While Russia and China both adopted the expected technologies (1a), they faced greater organizational demands than predicted (2b), forced to coercively purchase infrastructure (in the case of Russia's purchase of Vkontakte), bribe private actors for access (as was seen with China's coordination with Taiwanese media companies), or continually develop new assets after private actor decision-making reduced their ability to operate (evidenced by China facing moderation by Facebook, Twitter and LINE). Further, these cases highlighted how the ubiquity of ICT plays an

underappreciated role, resulting in bottom-up adoption separate from organizational mandate. This was particularly prevalent in the case of the CPN-Maoists. These case studies provide less evidence of the role and importance of the fourth variable. Further research is needed to conceptualize and delineate what contributes to differences in adoption of ICT by function.

This case study approach faces several limitations. Due to the inherent differences of time period, organizational structure, access to resources, conflict contexts, and technologies deployed, cross-case comparisons for the purpose of establishing a clear, specific causal mechanism are challenging. Rather, this variability showcases the relevance of disruptive attribute theory *in spite of* highly disparate conditions facing armed organizations. However, robust theory testing is needed to establish disruptive attribute theory's full explanatory power. For the purposes of theory building, these cases highlight how the model can be deployed to evaluate the behaviors of various organizations, involving a range of ICTs in different types of conflict.

Further, it is important to emphasize that disruptive attribute theory provides an added analytical layer that must be considered in conjunction with existing theories of technology adoption. As was highlighted in these four cases, organizational capacity and financial intensity, as outlined by Horowitz's adoption-capacity theory, do matter. However, they are not the only influencing factors.

There are certainly limitations to this plausibility probe. The primary goal of this analysis is to highlight the presence of the variables presented by disruptive attribute theory and their potential role in shaping adoption outcomes. Future studies should involve explicit theory testing of the impact on organizational capital, financial intensity and adoption outcomes of each intervening variable identified. Additional research is needed to understand the interaction between the factors

outlined by disruptive attribute theory and adoption-capacity theory. For example, there may be contextual factors which exacerbate or decrease the impact of the variables outlined. This may include, for example, the timing of a new ICT sector's introduction to a conflict setting, the state of origin of private actors (many social media platforms are U.S.-based and may therefore exhibit ideological or preferential treatment of certain actors leveraging their platforms), the degree of privatization of the ICT market in a country, and proximity to neighboring markets and networks.

Conclusion

Technology's attributes play an important role beyond what is captured by existing models. In considering ICT, theory must be refined to think about the varied strategic impositions of different categories of military technology. Specifically, this paper argued that attributes of information and communications technology introduce a set of strategic opportunities, constraints, and tradeoffs that contribute to variation in patterns of adoption by armed organizations. This article addressed three key gaps in the literature on adoption: (1) it gave proper consideration to the role of technology's attributes in the adoption behaviors of armed groups, (2) it explored the theoretical relevance for both state and non-state actors, and (3) it offered a framework for considering the empirical puzzle that is variation in ICT usage among and within armed organizations. Disruptive attribute theory, coupled with the case studies presented, also highlight many vital lessons and implications for understanding the adoption and use of ICT by armed organizations.

First, both states and non-state are constrained in their behavior by similar forces, reflecting the attributes of ICT when deployed as a military technology. These constraints reflect the attributes of the technology, rather than solely organizational capacity. Importantly, existing models of military technology adoption fail to account for the unique effects of specific categories of technology, such

as whether communications technology, transportation technology, artificial intelligence or traditional weaponry might all exhibit different logics of adoption and usage. ICT is deserving of special attention because of its growing role in global conflicts.

Second, it underscored the importance of studying adoption patterns, rather than simply considering it as binary. [228] Whether technology is adopted in some capacity does not tell the whole story. Analyzing the diversity in patterns of use are critical in shaping understanding the future of ICT. As highlighted by Berman et al. (2018), some non-state armed groups may opt to destroy phone lines, sacrificing a more advanced mode of communication in favor of safeguarding their operations from being compromised by civilian tip lines.[229] In this case, it is not a simple calculus of choosing not to use a particular kind of technology. Rather, it is about sacrificing one's own access to a technology to simultaneously deprive an opponent. In the case of ICT, technological imitation or movement toward the more complex is neither inevitable nor inherently advantageous. The more technologically advanced form of ICT will not necessarily be adopted by groups, even when controlling for resource constraints. This appears to be a choice that singularly applies to ICT as a category of technology.

Third, an opponent's strategy and decision to adopt technology matters. This impact goes beyond the traditional emulation model (as captured by the 'advantage of backwardness' and 'arms race' models of thinking). Instead, opponent decisions to use ICT can introduce interaction effects, resulting in a complex array of strategic trade-offs.

---

[228] Michael C. Horowitz, "Nonstate actors and the diffusion of innovations: The case of suicide terrorism," *International Organization*, Vol. 64, No. 1 (2010), pp. 33-64; Matthew Fuhrmann and Michael C. Horowitz, "Droning on: Explaining the proliferation of unmanned aerial vehicles." *International Organization,* Vol. 71, No. 2 (2017), pp. 397- 418; Michael C. Horowitz, *The diffusion of military power: Causes and consequences for international politics*.

[229] Eli Berman, Joseph H. Felter, and Jacob N. Shapiro, *Small Wars, Big Data.*

Fourth, the ICT adoption patterns of the civilian population and the decisions of the private sector actors developing and maintaining ICT matter. The impact of ICT's dual-use nature and increasing ubiquity remains under-examined. The forces driving its introduction into conflict settings, namely private actors, influence the strategic considerations and decisions armed organizations make regarding adoption and usage. It may be that armed groups and states adopt ICT not because of a desire to close a military-technological gap but because of adoption behaviors in non-military settings. ICT follows a fundamentally different acquisition model.

More indirectly, by highlighting the need for incorporating factors reflecting the technological attributes, this research contributes to key debates in international relations around the impact and trajectories of emerging technologies, such as artificial intelligence. Finally, this research also contributes to ongoing discussion surrounding state regulation of social media platforms and internet governance, by stressing the importance of private actors in shaping the strategic calculus of states.

Understanding ICT adoption and usage patterns is increasingly essential, as the online information age presents new opportunities and challenges for organizations at war. The forms of information that can be collected, promoted, and controlled have changed and increased dramatically with the introduction of new forms of technology. The use of ICT, particularly for cyber and influence operations, is fast becoming a common tactic employed by state actors and non-state armed groups. Disruptive attribute theory underscores the need to think holistically about the organizational limitations and opportunities imposed by ICT on armed actors, from states to non-state armed groups, to begin building a better picture of how ICT will shape the future of conflict.

Paper 2

What's New about the New Information Environment? How Private Firms Shape the Landscape for Strategic Competition

By Laura Courchesne and Jacob N. Shapiro

Introduction

What shapes the landscape for strategic competition in the information age? Over the last decade, states have increasingly co-opted and manipulated the online environment to their benefit, leveraging social media to monitor internal dissent, influence foreign populations, and propagate incendiary ideas abroad. This problem is only growing: existing actors are increasing their activities while new states appear to be developing and strengthening technical capacities for engaging in the online information space.[230] At least 51 countries have been targeted in 78 foreign influence efforts and 25 domestic influence efforts (when governments use social media to target their own citizens) from 2011 through early-2021, including well-documented campaigns by China, Iran, Russia, Saudi Arabia, United Arab Emirates, and Venezuela.[231] Cyber-enabled foreign interference occurred in at least 41 elections between 2010 and 2020, with North Korea and Iran increasing their activities in 2019 and 2020.[232] Beyond covert operations, states also leverage social media to promote narratives

[230] Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation," *Working Paper (Oxford, UK),* Project on Computational Propaganda (2019).
[231] Diego A. Martin, Jacob N. Shapiro, and Michelle Nedashkovskaya, "Recent trends in online foreign influence efforts." *Journal of Information Warfare*, Vol. 18, No. 3 (2019), pp. 15-48; Diego A. Martin, Jacob N. Shapiro, and Julia G. Ilhardt, "Version 2.0: Recent trends in online foreign influence efforts," August 5, 2020, https://scholar.princeton.edu/sites/ default/files/jns/files/trends_in_online_influence_efforts_v2.0_aug_5_2020.pdf; Additional data available at https://esoc.princeton.edu/publications/trends-online-influence-efforts.
[232] Sarah O'Connor, Fergus Hanson, Emilia Currey, and Tracy Beattie, "Cyber-enabled foreign interference in elections and referendums," *Australian Strategic Policy Institute*, 2020.

through official diplomatic, governmental, or state-affiliated media accounts.[233] Jensen, Valeriano, and Maness (2019) characterize the online information landscape created by social media platforms as a critical tool that state actors are using to achieve "strategic ends [...] employing cyber coercive instruments as part of long-term competition between rivals."[234]

States are effectively interacting on a landscape that is fundamentally different in many respects. One critical, under-appreciated aspect of this new environment is that it is created, controlled, and actively altered by privately held companies with global reach. Changes to platform policies, from new content standards to changes in algorithmic curation tools, can be likened to sudden shifts in physical landscapes. Much like a storm can convert a packed dirt road into an inaccessible route, render an area inaccessible to drones, or prevent a landing from sea, so too can platforms shut down or open up opportunities for state operations in the online environment. This was notably illustrated in February 2021, when Facebook denied access to accounts run by Myanmar's military, effectively eliminating a key mode of engagement for the government of one of the most Facebook-engaged populations in the world.[235] And importantly, this landscape is changing at an evolving rate. Since 2016, 14 mainstream platforms have announced close to a hundred policies explicitly targeting influence operations. Of these new policies, 66 were announced in 2020, a dramatic increase from 17 in 2019 (and see Figure 1 for the growing rate of new policies broadly).[236]

---

233 Jessica Brandt and Bret Schafer, "How China's 'wolf warrior' diplomats use and abuse Twitter," *Brookings Institution*, October 28, 2020, https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/.
234 Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy bears and digital trolls: Cyber strategy with a Russian twist," *Journal of Strategic Studies,* Vol. 42, No. 2 (2019), pp. 212-234.
235 Paul Mozur, Mike Isaac, David E. Sanger, and Richard C. Paddock, "Facebook Takes a Side, Barring Myanmar Military After Coup," *The New York Times*, February 24, 2021, https://www.nytimes.com/2021/02/24/technology/facebook-myanmar-ban.html.
236 Kamya Yadav, "Platform Interventions: How Social Media Counters Influence Operations," *Carnegie Endowment for International Peace, Partnership for Countering Influence Operations*, January 25, 2021, https://carnegieendowment.org/2021/01/25/platform-interventions-how-social-media-counters-influence-operations-pub-83698.

However, governments across the globe have struggled with how to engage social media companies. American legislators criticize Google, Facebook, and Twitter for their role in enabling Russian interference in the 2016 U.S. presidential election and their broader failure to eliminate state influence operations (IOs) from their platforms.[237] Russia responded to Facebook's ban on Russian-state advertising in 2017 by threatening retaliation, tacitly acknowledging the strategic importance of the platform's actions.[238] More recently, the U.S. government claimed that the social media platform TikTok, owned by a Chinese company, could present a national security threat, due the potential access the Chinese state might have to user data.[239] During an October 2020 U.S. Senate hearing, Senator Tammy Duckworth stated that, "social media companies cannot be trusted to put patriotism above profit," reflecting that while many platforms may be US-based, the prevailing perception is that these actors act in accordance with their own strategic interests.[240] Importantly, policy conversations surrounding influence operations have been grounded in a mistaken assumption that a singular set of policies will successfully remove a class of actors or content permanently from the environment. In reality, and as will be explored in this article, influence operations are responsive to this changing landscape. While constrained by new policies, states respond and adapt to avoid capture, better amplify content, and reach new audiences. Solutions will require an understanding of the levers of impact and ongoing, proactive policy implementation.

---

[237] See e.g., reporting on the November 2017 US congressional hearing in Mike Isaac and Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," *The New York Times,* October 30, 2017, https://www.nytimes. com/2017/10/30/technology/facebook-google-russia.html.

[238] Miles Parks, "Twitter Bans Ads From Russian State Media, Citing Election Interference Efforts," *NPR*, October 26, 2017, https://www.npr.org/2017/10/26/560199026/twitter-ends-russian-state-media-advertisements-citing-2016 -interference-efforts.

[239] Louise Matsakis, "Does TikTok Really Pose a Risk to US National Security?" *WIRED*, July 17, 2020, https://www. wired.com/story/tiktok-ban-us-national-security-risk/.

[240] "Social Media Content Moderation," C-SPAN Video, 3:36:21, October 28, 2020, https://www.c-span.org/video/ ?476686 -1/social-media-content-moderation#.

Nor is this thinking merely a reflection of a theoretical or potential impact. It is consistent with research showing that platform changes impact the online behavior of non-state actors, particularly Islamic State-linked groups and supporters, as well as ongoing research on the consequences of bans and deplatforming on extremist, alt-right groups in the West.[241] Further, the nascent literature on the impact of countermeasures against online disinformation points to the potential for platform actions to shape the efficacy of state influence operations.[242] This impact ranges from successfully rerouting established traffic away from influence campaign content to countering perceptional impact on users interacting with content.[243]

Private companies now have the power to influence the success, propagation, effectiveness, and population access of state-sponsored influence operations. They are, in effect, determining the landscape of strategic engagement through three key constraints: (1) *resource constraints*, i.e., how

---

241 See Tamar Mitts, "Countering Violent Extremism and Radical Rhetoric," *International Organization*, Vol. 76, Winter 2022, pp. 251-72; Tamar Mitts, "Banned: How Deplatforming Extremists Mobilizes Hate in Dark Corners of the Internet," (Working Paper), July 25, 2021; Morgan Meaker, "'Hate is Way More Interesting Than That': Why Algorithms Can't Stop Toxic Speech Online," *Pacific Standard Magazine*, February 28, 2019, https://psmag.com/ideas/neo-nazi-hate-speech- foiling-algorithms; Adrian Rauchfleisch, and Jonas Kaiser, "Deplatforming the far-right: An analysis of YouTube and BitChute," *Available at SSRN* (2021); Shiza Ali, Mohammad Hammas Saeed, Esraa Aldreabi, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini, "Understanding the Effect of Deplatforming on Social Networks," *In 13th ACM Web Science Conference 2021*, pp. 187-195; Rogers, Richard, "Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media," *European Journal of Communication,* Vol. 35, No. 3 (2020), pp. 213-229; Shagun Jhaver, Christian Boylston, Diyi Yang, and Amy Bruckman, "Evaluating the Effectiveness of Deplatforming as a Moderation Strategy on Twitter," *Proceedings of the ACM on Human Computer Interaction* (2021); Eshwar Chandrasekharan, Umashanthi Pavalanathan, Anirudh Srinivasan, Adam Glynn, Jacob Eisenstein, and Eric Gilbert, "You can't stay here: The efficacy of reddit's 2015 ban examined through hate speech," *Proceedings of the ACM on Human-Computer Interaction*, Vol. 1, No. CSCW (2017), pp. 1-22.

242 For a review of the literature base, see Laura Courchesne, Julia Ilhardt, and Jacob N. Shapiro, "Review of social science research on the impact of countermeasures against influence operations," *Harvard Kennedy School Misinformation Review,* (2021). On rerouting traffic away from influence campaign content see Sangyeon Kim, Omer F. Yalcin, Samuel E. Bestvater, Kevin Munger, Burt L. Monroe, and Bruce A. Desmarais, "The Effects of an Informational Intervention on Attention to Anti-Vaccination Content on YouTube," In *Proceedings of the International AAAI Conference on Web and Social Media* (2020), Vol. 14, pp. 949-953. On the use of warning labels see Jack Nassetta and Kimberly Gross, "State media warning labels can counteract the effects of foreign misinformation," *Harvard Kennedy School Misinformation Review*, (2020).

243 Sangyeon Kim, Omer F. Yalcin, Samuel E. Bestvater, Kevin Munger, Burt L. Monroe, and Bruce A. Desmarais, "The Effects of an Informational Intervention on Attention to Anti-Vaccination Content on YouTube," In *Proceedings of the International AAAI Conference on Web and Social Media* (2020), Vol. 14, pp. 949-953; Jack Nassetta and Kimberly Gross, "State media warning labels can counteract the effects of foreign misinformation," *Harvard Kennedy School Misinformation Review*, (2020).

expensive is it to upload and share content; (2) *content constraints*, i.e., what kind of content can be uploaded and shared; and (3) *audience constraints*, i.e., to whom can information be shared. For example, policies around account protection and verification impact how expensive it is to acquire accounts as part of an information operation, thereby contributing to the first constraint.[244] Policies which limit the type of information that can be propagated, such as algorithmic downranking of misleading information, contribute to the second constraint.[245] And changes that limit an influence operation's ability to get content to a targeted user base, such as WhatsApp's January 21, 2019 change which limited the number of people one could forward a message to, provide the third constraint.[246] Underlying this model and analysis, we introduce a dataset of 163 policies implemented by Facebook, Twitter, Instagram, YouTube, and WhatsApp from January 2016 through July 2021.

Despite evidence pointing to private control of the information landscape as a key feature of the current strategic environment, the field lacks a framework for thinking about the nature of private actors' influence and the ways in which policy decisions can change the environment. Many scholars have discussed how the landscape for inter-state competition and influence operations has changed (e.g., shifting online), but there has been minimal discussion on the attributes or nature of that landscape, let alone how those attributes (and the forces capable of changing them) impact state strategy and behavior.[247] Conceptualizing social media as an evolving, dynamic landscape for inter-state competition points to a need to understand how influence operations will respond to different

[244] Anita Joseph and Michele Paselli, "Verifying the Identity of People Behind High-Reach Profiles," Facebook, May 28, 2020, https://about.fb.com/news/2020/05/id-verification-high-reach-profiles/.
[245] Josh Constine, "Facebook will change algorithm to demote 'borderline content' that almost violates policies," *TechCrunch*, November 15, 2018, https://techcrunch.com/2018/11/15/facebook-borderline-content.
[246] WhatsApp Blog, "More Changes to Forwarding," WhatsApp, last modified January 21, 2019, https://blog.whatsapp.com/more-changes-to-forwarding.
[247] See for example Constance Duncombe, "Twitter and transformative diplomacy: social media and Iran-US relations," *International Affairs*, Vol. 93, No. 3 (2017), p. 545-562; Philip Seib, *Real-time diplomacy: Politics and power in the social media era* (Palgrave Macmillan, 2012); Tom Fletcher, "Naked diplomacy: power and statecraft in the digital age and the future of #diplomacy," *International Affairs*, Vol. 93, No. 4 (2017), p. 973-975.

types of changes. We introduce the first framework that accounts for the shifting nature of this landscape, how these changes impact state strategy and behavior, and support policy discussions around managing the online environment.

Doing so is important because platform changes that appear at first glance to be focused on other topics can have trickle-down effects on state competition and influence operations. The EU's privacy-focused General Data Protection Regulation (GDPR), for example, has reduced the ability of platforms and websites to track cybercrime and other malicious actors online and could inadvertently aid state influence campaigns in avoiding detection and removal.[248] And though Facebook's much-lauded early-2021 decision to ban Myanmar's military may have placed it "firmly on the side of the pro-democracy movement in Myanmar," it also remade the strategic information map for Myanmar's government.[249] Such shutting down of government accounts could, in principle, be done to any small country lacking a large enough market share to push back against platform decisions. One can envision the consequences this could have in places like Hong Kong.[250] While Facebook refused to provide the user data of suspected protestors to the Hong Kong authorities in July 2020, such pro-democratic behavior is not guaranteed.[251] Scholars and policymakers must recognize the strategic influence now in private hands.

---

248 Dustin Volz and Joseph Menn, "U.S. official warns of 'unintended consequences' of European data privacy law," *Reuters*, April 17, 2018, https://www.reuters.com/article/us-usa-cyber-nielsen/u-s-official-warns-of-unintended-consequences-of-european-data-privacy-law-idUSKBN1HO36J; Forbes Technology Council, "15 Consequences of GDPR," *Forbes*, August 15, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=2d1d226a94ad.

249 Billy Perrigo, "Facebook's Ban of Myanmar's Military Will Be a Test of the True Power of Social Media Platforms," *TIME Magazine*, March 1, 2021, https://time.com/5943151/facebook-myanmar-military-ban/.

250 Eric Cheung, "Why Facebook is losing friends in Hong Kong," *Rest of World*, February 28, 2021, https://restofworld.org/2021/why-facebook-is-losing-hongkong/; Holmes Chan, "How Hong Kong Became a Testing Ground for an 'Anti-Facebook' Movement," *VICE News*, December 18, 2020, https://www.vice.com/en/article/y3gnvk/how-hong-kong-became-a-testing-ground-for-an-anti-facebook-movement.

251 Hadas Gold, "Facebook, Google and Twitter won't give Hong Kong authorities user data for now," *CNN*, July 7, 2020, https://www.cnn.com/2020/07/06/tech/whatsapp-facebook-hong-kong/index.html.

We must also recognize the long-run consequences of state competition within this setting. The current consensus among both policymakers and the scholarly community is that autocratic governments, particularly Russia, gain an advantage in carrying out influence operations due to a lack of proactive regulation and content curation by the platforms.[252] In response, some have argued for more robust content moderation and account removal by social media companies, while others have called for governmental interventions.[253] However, state operations are adaptable, adjusting to new restrictions in much the same way as they would in a physical battlespace. Understanding of the new 'rules of the game,' including which algorithmic and policy levers impose more significant constraints, can help platforms and policymakers anticipate how state-sponsored efforts will respond. Conceptualizing social media as a novel landscape for inter-state competition allows for an arms race-like approach and prioritization of comparative rates of adaptation in developing countermeasures. If, as we argue, the online environment is a fundamentally new landscape for state competition, this also has implications for the international system and comparative state power.

Crucially, platforms, policy makers, and scholars of influence operations all lack a framework to think efficiently about the types of effects policy changes impose on influence operations. Calls for increased moderation with an intended goal to wholly eliminate influence operations online appear infeasible and impractical. Instead, long-term strategy should be aimed at containing the threat and reducing the effectiveness of these operations. Without explicit framing of the

252 Elizabeth Anne Bodine-Baron, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian social media influence*. (Santa Monica, CA: Rand Corporation, 2018.)
253 Bruce Schneier, "8 Ways to Stay Ahead of Influence Operations," *Foreign Policy*, August 12, 2019, https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/; T.S. Allen and Stephen Rodriguez, "To Protect Democracy, Protect the Internet," Foreign Policy, July 14, 2020, https://foreignpolicy.com/2020/07/14/united-states-election-interference-illegal-social-media/.

mechanisms of impact, proposing or crafting effective interventions remains a challenge. Our categorization model is useful for two reasons: (1) it categorizes policy along three levers of impact against influence operations, and (2) it helps to anticipate potential arenas for adaptation by influence operations.

The remainder of this article proceeds as follows: we begin by providing background on the importance of landscapes of engagement for understanding strategic constraints, the nature of historical influence operations, and state attempts to exert influence and control over the online environment. We then provide an overview of our model of strategic constraints. Next, we outline the relevance of this model in considering a range of politically oriented organizations operating online and adapting to these policy changes. Finally, we conclude with a discussion of the policy and research implications of the data and our model.

The Internet Landscape, Strategic Interaction, and Private Actors

In today's online information environment, private companies have unprecedented agency. This class of actors now has the power to control information flows and the fundamental terrain of the information environment. This section provides historical context for the current situation, outlines what is new, and discusses why states have limited agency compared to firms, at least so far.

Landscapes Impose Strategic Constraints

The landscape of engagement obviously matters for traditional inter-state strategic competition.[254] Such competition is arguably grounded in the goal of maintaining control and exerting power over

[254] Peter Andreas, "Redrawing the line: Borders and security in the twenty-first century," *International Security*, Vol. 28, No. 2 (2003), pp. 78-111.

territory and undermining the ability of other states to maintain control over their territory.[255] The very notion of the international system is predicated on actors behaving in a specific, well-defined landscape, the physical world in which this system exists. The landscape itself is not something states have historically had much control over, although with urbanization and the spread of major infrastructure some aspects of the landscape clearly reflect state decisions.[256] Topography, geography, the location of urban centers, and access to natural resources, among others, all impose strategic constraints. They limit or influence the ability of states to project power, as exemplified by Mearsheimer's (2001) discussion of 'the stopping power of water,' wherein the world's oceans naturally limit states from projecting and acquiring too much power.[257]

This centrality of the physical landscape is reiterated in the literature on civil wars and insurgencies. Fearon and Laitin (2003) identified 'rough terrain' as a key variable in predicting the onset of civil war, arguing that it allows insurgencies to operate successfully against comparatively stronger governmental forces.[258] Complex terrain, they argue, disadvantages state actors compared to rebels. Carter, Shaver, Wright (2019) expand on this analysis, showing with higher-resolution data that the landscape also has indirect effects in the context of civil war, with rugged terrain being partially responsible for the creation of distinct political groups alongside its previously recognized role in "complicating state repression."[259] Put simply, the landscape constrains state behavior, calculus, and capacity.

---

255 Robert Gilpin, *War and change in world politics*, (Cambridge University Press, 1981).
256 Antônio Sampaio, "Before and after urban warfare: Conflict prevention and transitions in cities." *International Review of the Red Cross,* Vol. 98, No. 901 (2016), pp. 71-95.
257 John J. Mearsheimer, *The tragedy of great power politics* (WW Norton & Company, 2001).
258 James D. Fearon and David D. Laitin, "Ethnicity, insurgency, and civil war," *American Political Science Review,* Vol. 97, No. 1 (2003), pp. 75-90.
259 David B. Carter, Andrew C. Shaver, and Austin L. Wright, "Places to hide: Terrain, ethnicity, and civil conflict," *The Journal of Politics,* Vol. 81, No. 4 (2019), pp. 1446-1465.

Physical geography also used to constrain information competition. Historically, there were three primary mechanisms through which states could seek to influence mass audiences: (1) mediated communication, wherein information is filtered through mass media (e.g., television, newspapers), (2) unmediated communication, wherein a state actor generates and promotes content themselves (e.g., dropping leaflets or radio broadcasts), and (3) indirect communication, wherein states leverage prominent figures and opinion leaders or disseminate information directly into tight-knit networks or communities.[260] All three were highly constrained by physical geography. Newspapers had to publish close to where they were read, television and radio required line-of-sight transmission, and leaflets had to be carried to their target region. Even elite networks operated on tightly defined geographies, albeit ones defined by social clubs and hotels rather than mountains and roads.

With the increasing migration of state activity online and into the realm of cyber, the landscape of information competition has become largely detached from the physical environment.[261] States can now move beyond those three traditional categories of information propagation. As others have observed, social media platforms, and the ability of users everywhere to access propaganda channels on the web, mean that state actors can directly target other states' political discussions at much lower cost than before, erasing the tyranny of distance and many of the access challenges that previously defined information competition.[262] But few have noticed that

---

[260] Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Q. Thurston, *Foundations of effective influence operations: A framework for enhancing army capabilities* (RAND Arroyo Center Santa Monica CA, 2009).

[261] Rhonda S. Zaharna "From propaganda to public diplomacy in the information age." *War, media and propaganda: A global perspective* (2004).

[262] David J. Betz and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyber-power* (Routledge, 2017).

these changes mean private actors can throttle up or down channels of influence through their own policy decisions.

What's New and What's Not

Historically, the information landscape had a strategic impact in the form of various competing influential actors, resource constraints, and audience access issues. But importantly, there were few entities which controlled transnational information flows, restricted access to the environment, or had potential to directly influence the form and content of influence campaigns as social media platforms do now. Baines and Jones (2018) in their review of historical foreign election interference highlight a variety of methods and technologies which supported operations, including a forged, incriminating letter leaked to the British press by Russia in 1924, the use of shortwave radio broadcasts by the U.S. to discredit the Italian Communist party in 1948, the British producing black propaganda for publication in Indonesian newspapers in the mid-1960s, and the U.S. funding propaganda campaigns broadcast through various mediums during the Chilean election in the mid-1960s.[263]

In historical conflicts, a state could successfully exert power and control over the information space by controlling access to the physical space inhabited by the target audience. Further, any constraints on influence operations, particularly accessing a target audience, were often predicated on physical access to the territory. For example, distributing leaflets often involved physically crossing into enemy territory and radio propaganda, which can be consequential,

263 Paul Baines and Nigel Jones, "Influence and interference in foreign elections: The evolution of its practice," *The RUSI Journal,* Vol. 163, No. 1 (2018), pp. 12-19.

depending on physical topography.[264] Thus, controlling an information space was often a reflection of state military power, highlighting how information operations were previously tethered to historical notions of kinetic control in a physical landscape. During the American Revolutionary War, for example, the Continental Army produced and strategically distributed handbills to encourage desertion among British fighters.[265] The new printing technology of the time enabled leaflets to be printed cheaply and in large numbers.[266] Propaganda leaflets were popular during WWI as a tool of psychological warfare and exerting influence over foreign populations.[267] Distribution occurred "through diverse instruments such as balloons, airplanes and artillery shells," and guided by a central strategy of maximizing the amount of leaflets distributed (over a billion).[268] During the Korean War, western forces also made use of airborne leaflets; with newspapers and radio eradicated, leaflets became the main source of information. As estimated 2.5 billion leaflets were dropped in Korea over three years.[269]

A U.S. CIA operation during the Cold War relied on radio, including Radio Free Europe, which broadcast to Eastern Europe, and Radio Liberty, which broadcast to the Soviet Union. The communist regime responded by jamming.[270] During the 2003 Iraq War, U.S. forces used leaflets and posters to campaign with Iraqi communities, as well as international coverage over mass media

264 A number of recent papers use the fact that physical geography limits radio reception to estimate the causal impact of propaganda. See for example Benjamin Barber IV and Charles Miller, "Propaganda and Combat Motivation: Radio Broadcasts and German Soldiers' Performance in World War II," *World Politics*, Vol. 71, No. 3 (2019), pp. 457-502; and Gagliarducci, Stefano, Massimiliano Gaetano Onorato, Francesco Sobbrio, and Guido Tabellini, "War of the Waves: Radio and Resistance during World War II," *American Economic Journal: Applied Economics*, Vol. 12, No. 4 (2020), pp. 1-38.
265 Carl Berger, *An introduction to wartime leaflets*, (Special Operations Research Office, the American University, 1959).
266 Carl Berger, *Broadsides and Bayonets*, (University of Pennsylvania Press, 2016).
267 Harold Dwight Lasswell, *Propaganda technique in world war I*, Vol. 170, MIT Press, 1971.
268 Seong Choul Hong, "Propaganda leaflets and Cold War frames during the Korean War," *Media, War & Conflict*, Vol. 11, No. 2 (2018), pp. 244-264.
269 Hong, "Propaganda leaflets and Cold War frames during the Korean War," pp. 244-264.
270 A. Ross Johnson, "Managing media influence operations: Lessons from radio free Europe/Radio liberty," *International Journal of Intelligence and Counterintelligence*, Vol. 31, No. 4 (2018), pp. 681-701.

channels to portray the validity of the war effort.[271] In more recent times, online media, such as Russian-controlled television network Russia Today, has weaponized op-eds, broadcasting of television reporting online, and 'useful idiots' to propagate messages abroad.[272] While modern forms of broadcast communication (e.g. radio and television) eased physical access requirements, states still possessed the power to interfere predicated on physical control (radio jamming, preventing access to certain television networks) over infrastructure.

Some would argue that private actors have always played a role in competition in the information environment. One can compare new trends in online disinformation and influence operations to historic 'yellow journalism', a form of sensationalist media of dubious veracity peddled for a profit-oriented motive.[273] One famous example is the claim that William Randolph Hearst and Joseph Pulitzer, owners of the largest domestic newspaper empires of the time, pushed the United States into war with Spain in 1898.[274] Though other scholars argue that the extent to which mass media was able to influence political decisions has been greatly exaggerated.[275]

Even if the 'yellow journalism' story is taken at face value, the scope of historical interference by traditional media is minimal compared with what social media companies can do.

---

[271] Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Q. Thurston, *Foundations of effective influence operations: A framework for enhancing army capabilities* (RAND Arroyo Center Santa Monica CA, 2009); Sean Aday, John Cluverius, and Steven Livingston, "As goes the statue, so goes the war: The emergence of the victory frame in television coverage of the Iraq War," *Journal of Broadcasting & Electronic Media*, Vol. 49, No. 3 (2005), pp. 314-331.

[272] Monika L. Richter, "The Kremlin's platform for 'useful idiots' in the West: An overview of RT's editorial strategy and evidence of impact," *European Values* (2017); Ilya Yablokov. "Conspiracy theories as a Russian public diplomacy tool: The case of Russia Today (RT)." *Politics,* Vol. 35, No. 3-4 (2015), pp. 301-315.

[273] Mark Balnaves, "A Return to the Good Old Days: Populism, Fake News, Yellow Journalism, and the Unparalleled Virtue of Business People," *The Palgrave Handbook of Management History* (2020), pp. 935-949.

[274] Craig Carey. "Breaking the News: Telegraphy and Yellow Journalism in the Spanish-American War." *American Periodicals: A Journal of History & Criticism*, Vol. 26, No. 2 (2016), pp. 130-148.

[275] W. Joseph Campbell, *Yellow journalism: Puncturing the myths, defining the legacies* (Greenwood Publishing Group, 2001).

While these mass media giants might have influenced state policy, they didn't determine a landscape of inter-state engagement. No company could introduce new features that radically changed the nature of public diplomatic work across the globe or suddenly favored specific governments.[276] Platforms create an information environment, rather than merely acting as a curator or publisher in an information environment.

And the broad reach that social media platforms exercise enables a much wider range of actions than previous technologies. Online, state actors can peddle information campaigns through official publishers who then promote the content on the platform (i.e., partisan media groups), self-publish content (i.e., using fake accounts or through official channels), and target specific groups, communities, and highly connected individuals to disseminate their content (i.e., targeting Facebook groups focused on specific topics or demographics). Even with its global reach, traditional mass media never held the same power over the global information ecosystem. And there was never such a concentration of power in the media industry. Today three companies, Facebook, Google, and Twitter, effectively control much of the information map. Not since the earliest days of the telegraph have a few actors had such control over global information flows.

States Are Limited in Their Ability to Shape the Landscape

The literature on internet governance has begun to account for the power of platforms.[277] DeNardis (2012) importantly notes that international relations scholarship is blinded to the potential impact of these actors due to its state and institution-centric approach. She states that the "focus on

[276] Jessica Brandt and Bret Schafer, "How China's 'wolf warrior' diplomats use and abuse Twitter."
Guy Schleffer and Benjamin Miller. "The Political Effects of Social Media Platforms on Different Regime Types (Summer 2021)." *Texas National Security Review*, (2021).
[277] Tarleton Gillespie, "Governance of and by platforms," *SAGE handbook of social media* (2017), pp. 254-278.

institutions, while important, sometimes misses core governance functions carried out via arrangements of technical architecture and through policy decisions of private industry. [...] Internet governance technologies not only embed political values in their design and operations but are increasingly being co-opted for political purposes irrelevant to their primary Internet governance function."[278] She highlights technologies' attributes as creating political and strategic ripple effects. DeNardis and Hackl (2015) argues that social media platforms play a "unique role as the intermediaries providing citizens with access to the digital public sphere" and are thus "central points of control on the Internet."[279] Gillespie (2015) emphasizes the variety of interventions taken by platforms which shape information flows in the online environment. And Gillespie (2017) argues that social media platforms perform governance functions, curating and placing restrictions on the type of speech users can engage in, in ways that can reflect an external state-driven regulatory environment but which are fundamentally the decisions of private actors.[280] However, a major gap in this literature is in considering the unique impacts of platform power beyond civilian users, to account for states' behavior and inter-state interaction in this new environment.[281]

The international community has grown increasingly concerned about the manipulation of the online environment by malicious actors and other ills attributed to social media. These concerns have manifested in calls for regulation and platform policy changes, and, in some cases, for the state to directly oversee aspects of platform operations.[282]

---

278 Laura DeNardis, "Hidden levers of Internet control: An infrastructure-based theory of Internet governance." *Information, Communication & Society*, Vol. 15, No. 5 (2012), pp. 720-738.

279 Laura DeNardis and Andrea M. Hackl, "Internet governance by social media platforms," *Telecommunications Policy*, Vol. 39, No. 9 (2015), pp. 761-770.

280 Tarleton Gillespie, "Governance of and by platforms," pp. 254-278.

281 Ibid.; Tarleton Gillespie, "Platforms are not intermediaries," *Georgetown Law Technology Review*, Vol. 2, No. 2 (2018), pp. 198-216.

282 Cecilia Kang and Adam Satariano, "Regulators Around the World Are Circling Facebook," *The New York Times*, April 25, 2019, https://www.nytimes.com/2019/04/25/technology/facebook-regulation-ftc-fine.html; Rebecca Heilweil, "At least one member of Congress thinks we need a government agency to regulate social media companies," *Vox*, March

Most regulatory actions taken by states against platforms lead to changes targeted at limited contexts. In the US, for example, the Federal Trade Commission imposed a $5 billion fine against Facebook relating to failures to secure user data.[283] The European Union and the United Kingdom have implemented several measures, including the General Data Protection Regulation (GDPR), which attempts to curb the amount of power and privileged access actors might have with and to social media user information.[284] Germany's anti-online hate speech law in 2017, called the Network Enforcement Act, introduced strict requirements for platforms to take action in removing online hate speech content within tight deadlines. This law was updated in June 2020, introducing the requirement that platforms report hate speech by Germans to German law enforcement.[285] France similarly attempted to introduce laws regarding platform moderation around hate speech and election-related content.[286] In February 2021, India called for platforms to introduce "grievance redressal mechanisms" for users with strictly set turnaround times.[287] Some countries have also explicitly introduced laws targeting 'fake news.' In October 2019, Singapore introduced an election-oriented content moderation law called the Protection of Online Falsehoods and Manipulation Bill (POFMA). It required platforms to remove content or "display prominent corrections at the

25, 2021, https://www.vox.com/recode/22351100/congress-peter-welch-facebook-twitter-google-youtube-social-media- agency; "Russia: Growing Internet Isolation, Control, Censorship: Authorities Regulate Infrastructure, Block Content," *Human Rights Watch*, June 18, 2020, https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control -censorship#.

283 Federal Trade Commission, "FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook," *Press Release* 24, FTC (2019).

284 Adam Satariano, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog" *The New York Times*, May 24, 2018, https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

285 Natasha Lomas, "Germany tightens online hate speech rules to make platforms send reports straight to the feds," *Tech Crunch*, June 19, 2020, https://techcrunch.com/2020/06/19/germany-tightens-online-hate-speech-rules-to-make-platforms-send-reports-straight-to-the-feds/.

286 David Morar and Bruna Martins dos Santos, "The push for content moderation legislation around the world," *Brookings Institution*, September 21, 2020, https://www.brookings.edu/blog/techtank/2020/09/21/the-push-for-content-moderation-legislation-around-the-world/.

287 Adi Robertson, "India sets stricter rules for social media giants," *The Verge*, February 25, 2021, https://www.theverge.com/2021/2/25/22300887/india-social-media-liability-rules-meity-facebook-whatsapp-twitter.

government's direction on their platforms, or face fines."[288] But all these changes are geographically limited and none of these actions have had the desired effects of hardening the information environment to malicious influence, or at least not obviously so.

One clear lever of influence on platform policy is global media attention to specific events and widespread condemnation of social media's role in them. Following clear evidence that it was being used by Russia to interfere in elections around the world, Twitter banned that country's state-owned media from posting advertisements on the platform.[289] When social media's role in the anti-Rohingya genocide in Myanmar came to light, Facebook banned several military-linked groups and increased content curation measures.[290] The Christchurch shooting in New Zealand, which was live streamed on Facebook, sparked increased efforts at moderating violent material online and a significant expansion of the Global Internet Forum to Counter Terrorism, an NGO-platform partnership to assist in the efficient identification and removal of terrorist content.[291]

Efforts to shape social media policy through coercive responses and threats amount to a recognition of social media's strategic importance and the centrality of company policies in determining how platforms shape political outcomes. Since 2015, Russia has attempted to levy fines against Facebook and Twitter for failing to adhere to a law requiring information sharing with the

---

[288] Amnesty International, "Singapore: Social media companies forced to cooperate with abusive fake news law," *Amnesty.org,* February 19, 2020, https://www.amnesty.org/en/latest/news/2020/02/singapore-social-media -abusive-fake-news-law/.

[289] Miles Parks, "Twitter Bans Ads From Russian State Media, Citing Election Interference Efforts," *NPR*, October 26, 2017, https://www.npr.org/2017/10/26/560199026/twitter-ends-russian-state-media-advertisements-citing-2016 -interference-efforts.

[290] Paul Mozur, "A Genocide Incited on Facebook, With Posts From Myanmar's Military," *The New York Times,* October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html; Rafael Frankel, "An Update on the Situation in Myanmar," *Facebook Newsroom*, February 11, 2020, https://about.fb.com/news/2021/02 /an-update-on-myanmar/.

[291] Verge Staff, "The response to the deadly mass shooting in Christchurch, New Zealand," *The Verge,* March 15, 2019, https://www.theverge.com/2019/3/16/18268907/christchurch-new-zealand-mass-shooting-tech-response-updates.

Russian state on Russian users.[292] In response to Facebook's ban on Russian-state advertising in 2017, a foreign ministry spokesperson stated that "retaliatory measures will naturally follow."[293] More recently, Russia has threatened that if Twitter fails to remove certain kinds of content, they will ban the platform domestically.[294] Early in March 2021, they restricted the speed of the platform as retaliation for failing to delete banned content.[295] This response by Russia is evidence that states view content curation performed by social media platforms as influencing their ability to get things done. India has similarly called on platforms to remove content on their behalf, asking Twitter in 2021 to block accounts of anti-government activists.[296] India has subsequently pursued restrictive and punitive legislation against platforms in response to this request not being met.

But the levers of state influence on platform policies appear limited.[297] While many state leaders recognize the great strategic importance of this landscape, as well as the need for exerting their own power and control over the space, few options seem to exist. The widespread availability of tools for countering attempts at controlling information flows (such as VPNs) means that even highly capable states such as China cannot keep their citizens off disfavored sites.[298] And Western governments have been no more effective. In 2017, U.S. Senator Lindsey Graham argued, "It's Russia today; it could be Iran and North Korea tomorrow. [...] What we need to do is sit down and

---

[292] AP, "Twitter, Facebook fined for not moving user data to Russia," *AP News*, February 13, 2020, https://apnews.com /article/a4fa655e946b9441b6e68ee3592a8f27.
[293] Miles Parks, "Twitter Bans Ads From Russian State Media, Citing Election Interference Efforts."
[294] Ivana Stradner, "Now Russia Has Its Own Ultimatum for Twitter," *Foreign Policy*, March 26, 2021, https:// foreignpolicy.com/2021/03/26/putin-twitter-ban-ultimatum-censorship-dissent/.
[295] Georgi Kantchev, "Russia Restricts Twitter Speed Over Banned Content," *The Wall Street Journal*, March 10, 2021, https://www.wsj.com/articles/russia-restricts-twitter-speed-over-banned-content-11615374130.
[296] Mitchell, Clark, "Twitter resists Indian government's orders to block protest accounts," *The Verge*, February 10, 2021, https://www.theverge.com/2021/2/10/22276479/twitter-free-speech-india-protests-government-block-orders.
[297] John Herrman, "What if Platforms Like Facebook Are Too Big to Regulate?" *The New York Times Magazine,* October 4, 2017, https://www.nytimes.com/2017/10/04/magazine/what-if-platforms-like-facebook-are-too-big-to-regulate .html.
[298] Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall*, (Princeton University Press, 2018).

find ways to bring some of the controls we have on over-the-air broadcast to social media to protect the consumer."[299] U.S, Senator Mark Warner's 2017 policy suggestions for regulation include increasing competition and data sharing between platforms as well as introducing measures for legal liability if the platforms fail to remove harmful content.[300] More recently, questions emerged regarding whether U.S, sanctions against Iran extended to prohibiting Iranian officials' use of Twitter.[301] Questions surrounding platforms' obligations to account for inter-state competition remain ongoing. So far, such efforts have largely failed.

These attempts to exert control over the information environment have taken three forms: (1) regulatory pressures and legislation which place restrictions on certain facets of platform activity in a particular country, which includes many of the data privacy laws, (2) retaliatory measures, including bans on specific platforms in-country when these companies fail to act in accordance with state demands; and (3) taking over platforms.

Regulatory pressures are relatively limited in their scope of influence on platform decisions. This is partly a product of geography and partly of civilian interest. States which can successfully introduce restrictions on platform behavior or induce changes are typically limited in altering the online landscape beyond their own physical (or ICT infrastructure-based) borders. This can be further circumvented when civilians travel abroad or use VPNs. Or, as was the case with Belgium in

299 Cecilia Kang, Nicholas Fandos, Mike Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill," *The New York Times,* October 31, 2017, https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html?smid=tw-share&_r=0.

300 Jamie Condliffe, "How to Fix Social Media's Big Problems? Lawmakers Have Ideas," The New York Times, July 30, 2018, https://www.nytimes.com/2018/07/30/business/dealbook/big-tech-regulation-ideas.html.

301 Michael Lipin, "Social Media Use by Iran's Sanctioned Officials Poses Dilemma for US," *VOA News*, September 10, 2019, https://www.voanews.com/middle-east/social-media-use-irans-sanctioned-officials-poses-dilemma-us; Miriam Berger and Adam Taylor, "Will Twitter ban Iran's supreme leader next?," *The Washington Post*, February 2, 2021, https://www.washingtonpost.com/world/2021/02/02/will-twitter-ban-irans-supreme-leader-next.

its attempt to force Facebook to introduce privacy protections of Belgian users, a platform can argue that another state has greater authority over a policy impacting a region.[302] Facebook argued for many years that because its EU headquarters was in Ireland, any EU-related policies would need to be enforced by the Irish Data Protection Commission.[303] Additionally, civilian interests often limit the ability of states to push for laws or legislation against platforms which directly address strategic competition. Domestic populations do not want the online space optimized for strategic influence, but rather features including privacy, secure transactions, freedom of expression, easy flow of money, etc.

Bans on platforms fail to work for two reasons: (1) platforms still own the online landscape outside of a state's borders, and (2) citizens now have many more options for circumventing these measures due to the ubiquity of ICT infrastructure. For example, the Syrian government's ban of messaging platform WhatsApp on national networks was easily overcome by citizens and rebel groups through the use of VPNs and neighboring telephone networks.[304] China's decision to block Instagram on national networks led millions of citizens to get VPNs in order to access a variety of censored platforms, including Twitter and Facebook.[305]

The only sure lever states have for retaking control is to buy firms, but even then, the impact on the landscape is limited. One example of the third approach is Russia's coercive purchase of the

---

302 David Meyer, "A Facebook case in Belgium could open the floodgates for GDPR privacy suits," *Fortune*, January 13, 2021, https://fortune.com/2021/01/13/facebook-belgium-ireland-privacy-tracking-cjeu-bobek-max-schrems/.
303 David Meyer, "In Facebook case, top EU court opens floodgates for more GDPR suits against Big Tech," *Fortune*, June 15, 2021, https://fortune.com/2021/06/15/cjeu-facebook-ireland-belgium-gdpr-lead-authority/.
304 Alessandria Masi, "Facebook's $19 Billion App Is Hugely Popular Among The Syrian Opposition," *Business Insider*, February 23, 2014, https://www.businessinsider.com/whatsapp-is-hugely-popular-among-syrian-rebels-and-activists - 2014-2.
305 William R. Hobbs and Margaret E. Roberts, "How sudden censorship can increase access to information," *American Political Science Review*, Vol. 112, No. 3 (2018), pp. 621-636.

platform VKontakte.[306] The drawbacks of this approach are the inherent difficulties of purchasing a private platform and placing it under government oversight, likely only possible under an authoritarian system. This is compounded by the fact that controlling a singular platform does not inherently mean controlling the information ecosystem. Importantly, while states can successfully acquire platforms through a forced sale, often users will migrate to other platforms. In the case of VKontakte, the purchase and public awareness of the Russian government's newfound influence over the platform led to bans in several countries, including Ukraine and China.[307]

Characterizing the Online Information Landscape

Policies impacting infrastructure, monetization, algorithmic curation, content moderation, and user engagement open and shut down opportunities for influence operations. Policy changes can influence states' approach to content and propagation, resource investment, and effectiveness of the campaign post-implementation. At a high-level, social media provides private actors with an unprecedented level of control and power over the landscape of engagement of influence operations. They can, for example, screen out entire categories of content, which can suddenly degrade the value of organizational investments. While a diverse range of actors, from civil society to supranational organizations, to academia, have actively advocated for increased moderation and policy interventions, recommendations lack a shared understanding of the mechanisms of impact.[308]

---

306 Amar Toor, "How Putin's cronies seized control of Russia's Facebook," *The Verge*, January 31, 2014, https://www.theverge.com/2014/1/31/5363990/how-putins-cronies-seized-control-over-russias-facebook-pavel-durov-vk.

307 "Ukraine bans its top social networks because they are Russian," *The Economist,* May 19, 2017, https://www.economist. com/europe/2017/05/19/ukraine-bans-its-top-social-networks-because-they-are-russian; "Russia's Media Watchdog Boasts It 'Convinced' China to Lift VKontakte Ban," *The Moscow Times,* February 15, 2018, https://www.themoscowtimes.com/2018/02/15/russia-media-watchdog-boasts-it-convinced-china-to-lift-vkontakte-ban-a60523.

308 Kamya Yadav, "Countering Influence Operations: A Review of Policy Proposals Since 2016," *Carnegie Endowment for International Peace, Partnership for Countering Influence Operations*, November 30, 2020, https://carnegieendowment.org/2020/11/30/countering-influence-operations-review-of-policy-proposals-since-2016-pub-83333.

Our model offers a starting point. It is meant to act as a guiding framework to isolate how policies introduced by private actors change the landscape and impose constraints on influence operations. In evaluating how platform policies shape the strategic environment it is helpful to focus on three key constraints they can impose: resource constraints, content constraints, and audience access constraints. Each reflects a core strategic question for information operations: (1) How hard is it to upload and share content? (2) What kinds of content can be uploaded and shared? (3) How effectively can you target audiences?

This section first describes each type of constraint, provides concrete examples, and then outlines the specific actions platforms have taken which contribute to each of the three kinds of constraints. We then use this framework to briefly analyze 163 policies implemented by Facebook, Twitter, Instagram, YouTube, and WhatsApp from January 2016 through July 2021. The constraints model introduced serves as an analytical tool for clarifying assumptions around mechanisms of impact and extending our understanding of potential countermeasures to include policies beyond those explicitly intended to target influence operations. This is aligned with work advocating the value of developing categorical variables and typologies to further research agendas (notably, Collier, LaPorte, Seawright (2008)).[309] The constraints model introduced serves as an analytical tool for clarifying assumptions around mechanisms of impact and extending our understanding of potential countermeasures to include policies beyond those explicitly intended to target influence operations.

[309] David Collier, Jody LaPorte, and Jason Seawright, "Putting typologies to work: Concept formation, measurement, and analytic rigor," *Political Research Quarterly*, Vol. 65, No. 1 (2012), pp. 217-232; David Collier, Jody LaPorte, and Jason Seawright, "Typologies: Forming concepts and creating categorical variables," in *The Oxford Handbooks of Political Methodology* (2008); Kenneth D. Bailey, *Typologies and taxonomies: An introduction to classification techniques* (Sage, 1994).

Resource Constraints.

Platform policies impact how expensive it is to run information operations at various stages of campaign development and implementation. They affect costs surrounding the acquisition of IO infrastructure, including the difficulty of creating fake accounts, the costs of purchasing accounts, and the associated material to build-out credible looking accounts. For example, this would include WhatsApp's February 4, 2019, introduction of a Touch ID or Face ID feature for logins.[310] These increases security standards when accessing accounts and makes it more difficult to steal for resale to influence operations. This type of policy may drive up the price of fake WhatsApp accounts. This would also include Facebook's December 19, 2017, introduction of a new feature alerting users when their photos are being used by others (e.g., fake profile pictures).[311] This type of policy may force states to invest in AI-generated photos in order to avoid detection or loss of accounts.

These policies may also impact the ability of influence operations to monetize content or rebuild infrastructure after a targeted ban. Another example would include Twitter's August 19, 2019, ban on platform advertising by state-controlled media entities.[312] This kind of policy limits the ability of states to promote influence operations through official and monetizable channels. In 2017, YouTube's advertising program permitted Russian state-affiliated news network RT to participate in its preferred news lineup program, which granted them "access to guaranteed revenue from premium advertisers. Those advertisers, in effect, subsidized Russia's international propaganda

310 WhatsApp Blog, "Introducing Touch ID & Face ID," *WhatsApp*, February 4, 2019, https://blog.whatsapp.com/introducing-touch-id-face-id.

311 Joaquin Quiñonero Candela, "Managing Your Identity on Facebook With Face Recognition Technology," *Facebook Newsroom*, last modified September 3, 2019, https://about.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/.

312 Twitter Inc., "Updating our advertising policies on state media," *Twitter Blog*, August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_media.html.

arm."[313] Since then, most platforms have imposed policy changes in an attempt to minimize revenue to influence operations. Policies and changes which improve detection of automated bots or fake accounts may also fall under this category, as they increase the resource investment needed to plausibly carry out a campaign. The following are possible subcategories for classifying policies imposing resource constraints:

1. ***Access to accounts (Creating accounts).*** Policies that introduce this constraint include account authentication measures, information requirements for account creation, and flags or limits on the number of accounts created by the same email address or phone number.
2. ***Access to credible-looking accounts (Buying or hacking accounts).*** This includes cybersecurity measures to prevent hacking or resale of stolen accounts. These policies also drive up the price of accounts on the online marketplace.
3. ***The repertoire of account behavior.*** This includes the range of actions available to users on a given platform, such as posting, commenting, messaging other users, repost or sharing content, creating groups, and the ability to promote links to external sites.
4. ***Cost of executing campaigns.*** This includes policies which impact the capacity of states to create and sustain numerous successful campaigns simultaneously. Policies or algorithmic curation measures influence how resource-intensive it is to run multiple accounts and in multiple settings. For example, content across accounts with similar wording is more likely to be flagged by specific platforms as part of an influence operation, but this is also a more efficient way for multiple analysts in an operation to push out a message.

[313] Daisuke Wakabayashi and Nicholas Confessore, "Russia's Favored Outlet Is an Online News Giant. YouTube Helped," *The New York Times,* October 23, 2017, https://www.nytimes.com/2017/10/23/technology/youtube-russia-rt.html.

5. ***Capacity to monetize IO content to support continued operations.*** This includes policies that limit the kind of content that can be advertised (both officially through platform resources and unofficially on a given account page). This also includes changes that place limits on the kind of content associated with advertisement, and limits on external links or promotion of branded content.
6. ***Capacity to avoid detection or removal.*** This includes changes to flagging policy or detection capacity of the platform. These policies fall under the 'Resource' category because influence operations can overcome this obstacle by investing more resources to either avoid detection or create new accounts.

Content Constraints.

Platform policies dictating the type of information that can be propagated in information operations. These policies can impact various stages of campaign development and implementation. This is likely a consideration in an influence operation's development of narratives and tactics, including key branding words identifying accounts as part of a broader movement, themes, and concepts. Ideally for states, the final narrative strategy helps avoid detection by moderators but is effectively promoted by the platform's algorithm. An example of this category of policy include WhatsApp's July 10, 2018 labeling of forwarded messages.[314] This also includes Facebook's September 13, 2018 fact-checking and labeling of videos and photos as either manipulated or fabricated, out of context or facing a text or audio claim.[315] Twitter similarly implemented an expanded rule on and labeling of

[314] WhatsApp Blog, "Labeling Forwarded Messages," *WhatsApp*, July 10, 2018, https://blog.whatsapp.com/labeling - forwarded-messages.
[315] Antonia Woodford, "Expanding Fact-Checking to Photos and Videos," *Facebook Newsroom*, last modified September 13, 2018, https://about.fb.com/news/2018/09/expanding-fact-checking/.

synthetic or manipulated media on March 5, 2020.[316] These labels may all prompt users to view labeled content with increased skepticism, undermining the potential effectiveness of a viral influence operations campaign. The following are possible subcategories for classifying policies imposing content constraints:

1. ***Limits on content exposure (Removal of content).*** Policies that prevent the use of specific key terms, phrases, images, sounds, videos.
2. ***Algorithm recommendations (Promotion and demotion of specific content).*** Although the type and format of content most likely to be promoted by the platform are not publicly available, all platforms possess an underlying algorithm that guides what kind of content is promoted more prolifically across users. This algorithm could include certain features and attributes of accounts, keywords, phrases, and initial engagement levels within a specific time window. For influence operations, the goal is to benefit from algorithm propagation without garnering attention from moderators who may flag the content as state linked.
3. ***Topic-focused curation (Labeling).*** Policies introducing human and algorithmic moderation of specific topics (i.e., COVID-19 and terrorism). Examples include content labeling, fact-checking, and redirection, which involves providing alternative, factual information that could undermine the IO content's message. This also includes labeling of state-sponsored media and state-affiliated accounts. These labels prompt users to view accounts with increased skepticism and effectively change the presentation of the content.

316 Yoel Roth and Ashita Achuthan, "Building rules in public: Our approach to synthetic & manipulated media," *Twitter Blog*, February 4, 2020, https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html.

Audience Access Constraints.

Platform changes that dictate, impact, or limit the reach of information operations. This impacts an influence operation's ability to propagate, including limiting or promoting interaction with a desired targeted user base and maximizing eyes on and engagement with content. An example of this type of policy includes WhatsApp's January 21, 2019, limit on the ability to forward a message to a maximum of five other people.[317] This introduces added friction to the rapid and widespread dissemination of an influence operation content. Facebook's June 14, 2019, update to the public comment ranking algorithm also imposes an audience access constraint. This update involved promoting comments more prominently on public posts when they have interactions from the Page or account that originally posted, or the comment is from a friend of the person who posted.[318] This policy devalues investments and may require additional effort or targeted strategies to overcome the demotion of campaign-associated accounts or content. Further, Instagram's October 31, 2017, update to include additional languages (Arabic, Hebrew, and Farsi) expands the scope of reach of state influence operations, enabling them to target populations which speak this language or access new users who join with the addition of these languages.[319] The following are possible subcategories for classifying policies imposing audience access constraints:

1. ***Targeted bans of or actions against state-sponsored accounts.*** This includes intentional and targeted actions to identify and remove suspicious accounts and content that appear

[317] WhatsApp Blog, "More Changes to Forwarding," *WhatsApp*, last modified January 21, 2019, https://blog.whatsapp.com/more-changes-to-forwarding

[318] Justine Shen, "Making Public Comments More Meaningful," *Facebook Newsroom*, June 14, 2019, https://about.fb.com/news/2019/06/making-public-comments-more-meaningful/.

[319] Instagram, "Introducing Instagram in Arabic, Hebrew and Farsi," *Instagram Blog*, October 31, 2017, https://about.instagram.com/blog/announcements/introducing-instagram-in-arabic-hebrew-and-farsi.

forensically linked to a state actor. This removal results in the loss of swathes of assets for the influence operation.

2. ***User ability to curate content.*** Policies which introduce or improve user ability to filter out particular accounts or content.
3. ***Algorithmic recommendations of accounts, pages, or communities.*** This includes methods such as redirection.
4. ***Capacity to generate novel interactions with the IO and have more eyes on content.*** This includes policies that limit the number of posts, comments, interactions, messages an individual account can make per day. This can also include platform formats for user interaction, such as limits on the size of online groups (as in the case of WhatsApp). These policies limit the frequency of content posting and daily behaviors as well as individual user exposure.
5. ***Capacity for IO content to be shared between users.*** This includes policies that limit message forwarding, such as Facebook and WhatsApp limit on the forwarding of messages, restrictions on messaging or tagging users in content without a prior connection (such as mutual followers or friends) to the IO account, or additional steps for users seeking to share labeled content.
6. ***Capacity to access and target particular demographics and geographic regions.*** Platform policies that impact the ease of implementing influence operations in a given geopolitical context. This can include platform policy changes made in specific countries or regions, both as part of platform phased roll-out of changes or in response to aforementioned domestic legislation. Although not yet studied, the western-centric approach of platforms, including their database of banned or objectionable keywords and actors, limits their experience and awareness of a given region's political and social context. Due to the

location of privately-owned platforms in the West, there are likely gaps or blind spots to categories of pernicious content and malicious users, as evidenced by Facebook's response in Myanmar. This could create opportunities or challenges for influence operations, depending on the context of operation.

Locating Platform Policy Changes in Constraint Space

To contextualize the rate and form of change occurring on social media platforms, we collected data on 163 publicly announced policies implemented by Facebook, Twitter, WhatsApp, Instagram, and YouTube from January 1, 2016, through July 15, 2021. Through review of public blog posts, we identified and categorized policies by the primary strategic constraint they introduced for influence operations. Our data included policies explicitly targeting disinformation, misinformation, and influence operations (including labels and fact-checking), policies which resulted in changes to algorithmic curation or demotion of specific content, policies which led to changes to account verification, and changes to high-level platform policy (including policies around permissible content and user behavior). We exclude changes to modes of interacting (including new emojis), business user specific policies, aesthetic changes to the platform, the introduction of or changes to available payments systems, the launch of new data or advertising resources, and new functionalities or features (i.e., WhatsApp's introduction of a Spanish language vaccine finder). We also excluded reported bans on IO-associated accounts because platforms typically do not provide a clear date for when the targeted removals began. Efforts including disinformation literacy and education tools were also excluded because while they may impact how users navigate social media (including perception or awareness), they do not affect the landscape itself. There may be other platform-related changes which don't fit strictly within a strategic constraints framework, including

WhatsApp's merger with Facebook which enables coordination between platforms regarding changes.

This analysis begins in 2016, as this is the year when most social media platforms began to consistently document policy changes through public announcements on their websites and blogs. These policies are global in scope, although implementation may not be consistent across all geographies.

Policy data was collected using public announcements by platforms. As such, there may be inconsistencies between the platform's public description of the policies and actual policies implemented. Further, each platform likely implemented back-end changes that they chose not to publicly disclose that are therefore inadvertently excluded. Policies that were discussed at a high-level without an implementation roll-out date(s) or concrete description of change are not included. It is important to note that the implementation date as recorded is the best proxy for global roll-out, the accuracy of this date in terms of scope and timing of implementation may vary from platform to platform. Most announcements explicitly say 'starting today' when discussing roll-out. A few policies, noted in the dataset, discuss a phased roll-out over the following weeks.

The goal of this data collection and analysis is threefold. First, it establishes one of the first datasets of social media policies. Scholarly study of online influence operations is relatively nascent and as such, no comprehensive dataset of platform policies has been created.[320] Further, social media companies have been reluctant to engage in transparency on the nature and scope of platform

[320] For a dataset of policies explicitly created to target influence operations, see Kamya Yadav, "Platform Interventions: How Social Media Counters Influence Operations."

changes.[321] While this dataset is far from comprehensive, excluding back-end changes and modifications to the platform that the company opts not to publicly announce, it is the first established dataset of publicly announced policies implemented by the most globally influential social media companies.

Second, this data has broader utility in supporting research on the efficacy of countermeasures and encouraging research on overlooked forms of impact on influence operations.[322] Courchesne et al. (2021) find that of 223 studies evaluating the impact of policy interventions on influence operations, 75% evaluated the impact of disinformation disclosure (when the platform "informs a user they have come in contact, shared, or interacted with disinformation"), 67 (30%) studied content labeling (when the platform includes a label attached to the content providing additional context or correcting the information), and 24 (11%) examined disinformation literacy (when the platform provides tools or games to educate users on disinformation identification). No studies examined the impact of changes such as introducing additional security and verification measures or engaging in content and account moderation. By highlighting the range of policies that could impact influence operations and providing a categorization of impact, this article seeks to encourage further research on alternative types of countermeasures.

And third, this analysis helps to describe and visualize the evolving nature of the landscape. It highlights the rate of new policies by year and the types of changes introduced. It also helps to

321 Heidi Tworek and Alicia Wanless, "Time for Transparency From Digital Platforms, But What Does That Really Mean?," *Lawfare*, January 20, 2022, https://www.lawfareblog.com/time-transparency-digital-platforms-what-does-really-mean.

322 Laura Courchesne, Julia Ilhardt, and Jacob N. Shapiro, "Review of social science research on the impact of countermeasures against influence operations," (Harvard Kennedy School Misinformation Review, 2021); Helen Innes and Martin Innes, "De-platforming disinformation: conspiracy theories and their control," *Information, Communication & Society*, (2021), pp. 1-19.

underscore the importance of the constraints classification system in making sense of policy changes.

Table 1 provides an overview of policies by platform and by constraint. Twitter publicly announced the highest number of policies during the period under review (totaling 55), with Facebook coming in close second (50). Policies introducing content constraints were the most common, accounting for 43%. Facebook introduced the highest number (32, or 45%) of policies imposing content constraints. Twitter introduced the highest number of policies imposing resource (20, or 40%) and audience access (17, or 40%) constraints.

Table 1. Policy Counts by Platform

	Resource	Audience Access	Content	Total
Facebook	9	9	32	50
Instagram	7	4	5	16
WhatsApp	3	5	3	11
Twitter	20	17	18	55
YouTube	11	7	13	31
Total	**50**	**42**	**71**	**163**

Figure 1 highlights policy counts by year by platform. It excludes 2021, as policies are unaccounted for after July 2021. Figure 1 illustrates that the number of new policies is increasing every year.

Figure 1. Policy Counts by Year by Platform, 2016 - 2020

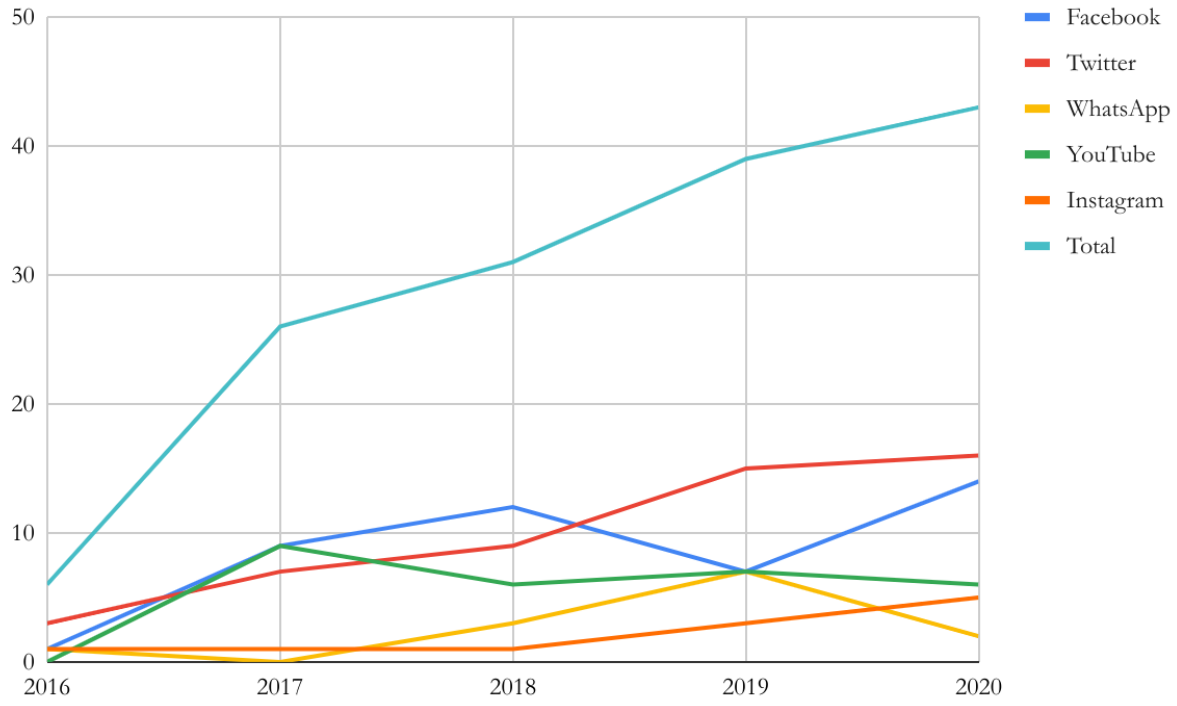


Table 2 provides a count of the constraints by year. Policies imposing content constraints have increased dramatically since 2016.

Table 2. Constraints by Year[323]

	Resource	Audience Access	Content	Total
2016	**5**	1	0	6
2017	9	7	**10**	26
2018	9	5	**17**	31
2019	**15**	14	10	39
2020	7	11	**25**	43
2021	5	4	**9**	18

[323] The row for 2021 only includes policies which met the inclusion criteria and were announced prior to July 16, 2021.

This data provides evidence of the following three trends in platform policy creation and implementation. First, as seen in Figure 1, the number of policies that could impact influence operations appears to be increasing yearly. This is in line with findings from other reviews of platform policy, highlighting the increasing rate of change of the online landscape.[324] Whether resulting from external pressure or internal changes, companies are seeking to implement (and publicize) an increasing number of policy changes. This has consequences for actors operating on these platforms, introducing a greater number of potential constraints on their behavior and additional obstacles to overcome in operating in the online environment. This data highlights how as a landscape, social media platforms are dynamic and evolving.

Second, as evidenced in Table 1 and 2, platform policies appear to most commonly impose content constraints on influence operations. This finding aligns existing research on platform policies and recommended countermeasures. Specifically, a review of 156 platform community standards used by 13 social media sites found that 117 (75%) directly place limits on "messages, narratives and subject matter" as compared to 20 (12%), which limit "reach of content and techniques used to expand reach."[325] A review of 104 influence operation-specific policies (as labeled by the platforms) similarly found an emphasis on content based countermeasures: 77 (74%) countermeasures principally involved targeting content, through redirection or content labeling.[326] Despite this emphasis on content constraints, there is no empirical basis for the idea that one specific form of countermeasures (and the constraints they impose) may be more or less effective in

[324] Kamya Yadav, "Platform Interventions: How Social Media Counters Influence Operations."
[325] Jon Bateman, Natalie Thompson, Victoria Smith, "How Social Media Platforms' Community Standards Address Influence Operations," *Carnegie Endowment for International Peace*, April 1, 2021, https://carnegieendowment.org/2021/04/01how-social-media-platforms-community-standards-address-influence-operations-pub-84201.
[326] Kamya Yadav, "Platform Interventions: How Social Media Counters Influence Operations."

undermining a state's ability to operate online.[327] Further, the impact of a given policy might vary, with certain policies imposing greater constraints on state-sponsored influence operations that rely on particular assets, infrastructure, or content. This data highlights the current emphasis on policies which impose content constraints and may suggest a need for policymakers to consider other potential mechanisms (including policies which deliberately impose audience access or resource constraints) for targeting influence operations.

Third, as seen in Table 1, this data showcases that there is variation among platforms in both the quantity of new policies introduced and the potential impact of these changes on influence operations. In conceptualizing the landscape as dynamic and evolving, with states adapting (or at a minimum, responding) to this change, uneven application of constraints across the online domain of operations may create opportunities for states. Although platforms are increasingly coordinating, uneven application of policies can result in cross-platform differences in the behaviors of influence operations. When faced with heavier constraints on one platform, states may opt to invest greater resources into developing assets and activity on another.

Platform Governance in the Real World

Emerging data and research suggest that many non-state organizations modify their online behavior and social media strategies in response to decisions made by the social media platforms.[328] These

---

327 Laura Courchesne, Julia Ilhardt, and Jacob N. Shapiro, "Review of social science research on the impact of countermeasures against influence operations."

328 See Tamar Mitts, "Countering Violent Extremism and Radical Rhetoric"; Tamar Mitts, "Banned: How Deplatforming Extremists Mobilizes Hate in Dark Corners of the Internet," (Working Paper), July 25, 2021; Morgan Meaker, "'Hate is Way More Interesting Than That': Why Algorithms Can't Stop Toxic Speech Online," *Pacific Standard Magazine*, February 28, 2019, https://psmag.com/ideas/neo-nazi-hate-speech- foiling-algorithms; Adrian Rauchfleisch, and Jonas Kaiser, "Deplatforming the far-right: An analysis of YouTube and BitChute," *Available at SSRN* (2021); Shiza Ali, Mohammad Hammas Saeed, Esraa Aldreabi, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini, "Understanding the Effect of Deplatforming on Social Networks," *In 13th ACM Web Science*

behavioral effects are also more than likely to apply to state influence operations on these same platforms. Analyses of influence operations captured and removed by the platforms indicate that state behavior online is adaptive and changes over time.[329] This section summarizes how different kinds of political organizations have responded to platform changes and the relevance of our model in capturing these effects. Case selection was partly driven by data availability, which introduces certain biases. Namely, the organizations analyzed are those which have had operations captured and publicly disclosed by the platforms for academic analysis. However, these cases serve to provide initial evidence regarding the responsive and adaptive nature of influence operations when faced with platform changes, rather than theory test which organizations may be more or less affected by these changes.

Islamic State and Non-State Armed Groups

The Islamic State has reacted to several stages of targeted policy measures and bans on various platforms over the last decade. In the early days of Twitter in 2014, the Islamic State and affiliated accounts responded to targeted bans by rejoining with slightly modified account names. This adaptation was aimed at avoiding initial algorithmic flagging while signaling their identity to their previous follower base. They included links in their Twitter bio to external and less moderated websites, such as WordPress and VKontakte, as backup options should they face another ban. They also modified their approach to content: rather than labeling themselves as Islamic State members,

Conference 2021, pp. 187-195; Rogers, Richard, "Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media," *European Journal of Communication,* Vol. 35, No. 3 (2020), pp. 213-229; Shagun Jhaver, Christian Boylston, Diyi Yang, and Amy Bruckman, "Evaluating the Effectiveness of Deplatforming as a Moderation Strategy on Twitter," *Proceedings of the ACM on Human-Computer Interaction* (2021); Eshwar Chandrasekharan, Umashanthi Pavalanathan, Anirudh Srinivasan, Adam Glynn, Jacob Eisenstein, and Eric Gilbert, "You can't stay here: The efficacy of reddit's 2015 ban examined through hate speech," *Proceedings of the ACM on Human-Computer Interaction*, Vol. 1, No. CSCW (2017), pp. 1-22.

329 Nathaniel Gleicher, Margarita Franklin, David Agranovich, Ben Nimmo, Olga Belogolova, Mike Torrey, "Threat Report: The State of Influence Operations 2017-2020," *Facebook Research*, May 20, 2021; Josh A. Goldstein and Shelby Grossman, "How disinformation evolved in 2020," *Brookings Institution*, January 4, 2021, https://www.brookings.edu /techstream/how-disinformation-evolved-in-2020/.

they would "offer an alibi in their profile — 'I'm not part of ISIS. I'm just posting news' — or set their accounts to private (which hid[..] their tweets and g[ave] them the ability to reject would-be followers)."[330] In the aftermath of publishing and publicizing the video of journalist James Foley's execution in August 2014, many "members of this group could be seen advising one another to temporarily deactivate their accounts to avoid scrutiny," representing their prediction of increased surveillance and action by social media platforms.[331]

In response to policy changes undertaken by Twitter beginning in mid-2015, which culminated in the removal of more than 125,000 accounts, Islamic State-linked accounts posted links to external websites, encouraging their audience to migrate to locations outside of mainstream platform control.[332] These alternative platforms subjected users to fewer curation measures. This included encrypted messaging apps (such as Telegram), Russian-owned platform VKontakte, and a small website called JustPaste.it, where the group uploaded "a large number of images of executions, beheadings and massacres, as well as more prosaic images of life – an essential part of the group's social media operation."[333] Mitts (2021), in her study of Islamic State supporters online, further documented that, "when the group began migrating to Telegram in the end of 2015, these users advertised the new platform to their followers, suggesting that they may have switched to Telegram to avoid detection."[334] In November 2019, a targeted removal operation of jihadist and Islamic State-linked accounts on Telegram led to another dispersal and movement to alternative platforms, where

330 Jacob Silverman, "Loose Tweets Sink Ships," *POLITICO*, August 28, 2014, https://www.politico.com/magazine/story/2014/08/islamic-state-twitter-110418/.
331 Ibid.
332 Twitter Inc., "Combating Violent Extremism," *Twitter Blog,* February 5, 2016, https://blog.twitter.com/en_us/a/2016/combating-violent-extremism.html.
333 Jacob Silverman, "Loose Tweets Sink Ships"; Carmen Fishwick, "How a Polish student's website became an ISIS propaganda tool," *The Guardian*, August 15, 2014, https://www.theguardian.com/world/2014/aug/15/-sp-polish -man-website-isis-propaganda-tool.
334 Tamar Mitts, "Countering Violent Extremism and Radical Rhetoric."

the group had pre-established accounts and could continue their dissemination of content.[335] These other platforms often engaged in less curation and overall fewer changes to the landscape's attributes. However, this migration offered a strategic tradeoff for the Islamic State: less mainstream platforms offered diminished audience access due to fewer baseline users and a more niche follower base.

Islamic State is not alone in adapting in this manner. Other large Islamist groups such as Hamas and Hezbollah also appear to have changed their social media strategy and content in response to actions taken by platforms, including the aforementioned changes (beginning in 2015) to improve detection of extremist content. Targeted bans on accounts and removal of content featuring violence or 'terroristic acts,' meant that these groups had to invest instead in affiliates to propagate their content and to disseminate content that would avert censorship.[336] Specifically, these groups opted to use community proxies, including media organizations and local charities, rather than official group-linked accounts to promote their activities. They are described as publishing "images and videos that deliver their message — but that do not set off the alarm bells of the social media platforms. Today, the groups mostly post images of festive parades and religious celebrations online, as well as videos of speeches by their leaders."[337] On Instagram, many videos and images promote Hamas under specific key hashtags rather than being uploaded by a centralized account.[338] These changes all appear to be in direct response to platform policies.

---

335 Meili Criezis, "Telegram's anti-IS Campaign: Effectiveness, Perspectives, and Policy Suggestions," *Global Network on Extremism and Technology*, July 30, 2020, https://gnet-research.org/2020/07/30/telegrams-anti-is-campaign-effectiveness-perspectives-and-policy-suggestions/; Flashpoint Analyst Team, "Jihadists Presence Online Decentralizes After Telegram Ban," *Intel Corporation*, January 17, 2020, https://www.flashpoint-intel.com/geopolitical-physical-security/jihadists-presence-online-decentralizes-after-telegram-ban/

336 Sheera Frenkel and Ben Hubbard, "After Social Media Bans, Militant Groups Found Ways to Remain," *The New York Times*, April 19, 2019, https://www.nytimes.com/2019/04/19/technology/terrorist-groups-social-media.html

337 Ibid.

338 Ibid.

Russia

Russia's response to policy changes point to a potential adaptive, or at least reactive, response by state operations to changes in the online environment, including platform detection and removal of campaign assets.

A 2020 Graphika report analyzing 300 assets removed by Facebook on September 24, 2020, points to a potential cross-platform response in account posting and creation.[339] The dataset includes Russian state-linked account accounts operating from 2013 - 2020. This campaign importantly exhibits a surge of accounts posting for the first time on Facebook in 2018, as compared to other years. This could be an operational response to Twitter's notification of user interaction with Russian accounts on January 31, 2018.[340] The Russian operation may have chosen to invest heavily in assets and operations on a different platform. While some of this activity perhaps reflected behavior relating to the 2018 U.S. election, very few accounts in this takedown posted about domestic US political content.

Platforms have also introduced changes that improved identification and flagging approaches, penalizing accounts using stolen or copied photos. In late December 2017, Facebook introduced an optional feature for users to know when other accounts were using their photos.[341] In October 2018, Twitter announced the roll-out of a new approach for fake account identification

339 Ben Nimmo, Camille Francois, C. Shawn Eib, Léa Ronzaud and Joseph Carter, "GRU and the Minions," *Graphika*, September 24, 2020, https://graphika.com/reports/gru-and-the-minions/.
340 Blair Guild, "Twitter notifies 1.4 million of interaction with Russian accounts," *CBS News*, January 31, 2018, https://www.cbsnews.com/news/twitter-notifies-1-4-million-of-interaction-with-russian-accounts/.
341 Joaquin Quiñonero Candela, "Managing Your Identity on Facebook With Face Recognition Technology," *Facebook Newsroom*, December 19, 2017, https://about.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/.

involving greater scrutiny towards accounts using stolen or stock photos as their profile avatar. [342] In response to these policy approaches, it seems that state influence operations broadly are investing in AI-generated profile pictures.[343] While this technology is relatively nascent, and use of this artificial imagery is often obvious, states appear to be investing in its improvement. A set of Russian-linked Facebook accounts and pages removed in September 2020 documented use of AI-generated profile pictures far more prolifically. [344]

An analysis from the Brennan Center, with accounts also verified and analyzed separately by Graphika, found two key differences in Russian-linked account behavior and strategy between 2016 and 2020. First, rather than creating accounts for fake groups or individuals, they increasingly mimicked real groups, organizations, and individuals. This mimicry included "subtle changes in the names or landing page addresses that are harder to notice."[345] Page transparency measures imposed by Facebook and Instagram are thought to be one reason for this change in tactics: these policies highlight account creation dates and previous names of Pages for users to better discern whether it is a credible account. This included a set of policies announced and rolled-out on Facebook impacting Page transparency between April and June of 2018.[346] Presumably, the logic behind co-opting the identities of existing and known organizations or individuals was to dissuade users from looking into these transparency metrics, relying on being mistaken for a real organization's Page.

---

342 Del Harvey and Yoel Roth, "An update on our elections integrity work," *Twitter Blog*, October 1, 2018, https://blog.twitter.com/en_us/topics/company/2018/an-update-on-our-elections-integrity-work.html.

343 Josh A. Goldstein and Shelby Grossman, "How disinformation evolved in 2020."

344 Ben Nimmo, Camille François, C Shawn Eib, Léa Ronzaud, "IRA Again: Unlucky Thirteen," Graphika, September 1, 2020, https://graphika.com/reports/ira-again-unlucky-thirteen/.

345 Young Mie Kim, "New Evidence Shows How Russia's Election Interference Has Gotten More Brazen," *Brennan Center for Justice*, March 5, 2020, https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows -how-russias-election-interference-has-gotten-more; Young Mie Kim, "Uncover: Strategies and Tactics of Russian Interference in US Elections," *Project DATA (Digital Ad Tracking & Analysis)*, (2018).

346 Facebook, "Introducing a New Info and Ads Section on Pages," *Facebook for Business*, June 28, 2018, https://www.facebook.com/business/news/introducing-a-new-info-and-ads-section-on-pages

Second, there is documented evidence of Russia outsourcing their content creation and account operation to increase the perceived credibility of accounts and produce more authentic-looking content. Starting in March 2020, one Russian-linked operation hired contributors and activists based in Ghana. Assets involved with this operation openly claimed to represent a Ghanian NGO, while posting about US-domestic issues.[347] This approach may reflect a range of policy decisions made by platforms that strengthened identity verification measures. In October 2018, Twitter updated its rules and flagging approaches to identify accounts using stolen or copied bios and those lying about user location in their profile.[348] In May 2020, Facebook introduced a policy requiring accounts and Pages to confirm the authenticity of their identity if a post went viral quickly.[349] In August 2020, Instagram introduced measures to force users to confirm their identity if flagged by the platform as participating in inauthentic activity.[350] These policies all make out-sourcing to real users a viable option to avoid identification and flagging. The Ghanian-based operation had a website linked to the NGO it claimed to represent to bolster its credibility. In the event that the Pages or accounts were forced to validate their identity in accordance with these new policies, they could either use the real identities of workers or more easily forge an accepted identification document.[351] Further, by using content created by real users working for the operation rather than copying or stealing existing language, they can avoid succumbing to new platform approaches targeting 'inauthentic' account behavior.

---

347 Ben Nimmo, Camille François, C. Shawn Eib, Léa Ronzaud, Melanie Smith, Thomas Lederer, Joseph A. Carter, Erin McAweeney, "IRA in Ghana," *Graphika*, March 12, 2020, https://public-assets.graphika.com/reports/graphika_report_ira_in_ghana_double_deceit.pdf.

348 Josh A. Goldstein and Shelby Grossman, "How disinformation evolved in 2020."

349 Anita Joseph and Michele Paselli, "Verifying the Identity of People Behind High-Reach Profiles," *Facebook Newsroom*, May 28, 2020, https://about.fb.com/news/2020/05/id-verification-high-reach-profiles/

350 Instagram, "Introducing New Authenticity Measures on Instagram," *Instagram Blog*, August 13, 2020, https://about.instagram.com/blog/announcements/introducing-new-authenticity-measures-on-instagram.

351 Facebook, "What Types of IDs does Facebook accept?" *Facebook Help Center*, last accessed September 2, 2021, https://www.facebook.com/help/159096464162185.

China

Finally, China's response to policy changes provides a very clear illustration of how state operations react and attempt to adapt to platform policies and decisions. A notable example is Graphika's reporting on a campaign termed 'Spamouflage' developed and administered by Chinese authorities beginning in 2018 through 2021.[352]

From 2018 through 2019, a Graphika investigation of Chinese-linked accounts found that the campaign operated across several platforms and used a mixture of spam-like posting and political posting in a bid to avoid detection. The campaign mainly centered around YouTube and video-based content, promoted on Twitter and Facebook. The infrastructure of this campaign, that is, the accounts utilized, "appear to have been taken over from genuine users and repurposed, no doubt in an attempt to evade the platforms' systems for identifying fake accounts."[353] These stolen or sold accounts were primarily of Bangladeshi origin. A small number were recorded to have been created by the campaign and built out. These accounts typically had foreign names and profile pictures (Western, Slavic, or Bangladeshi) but the content posted was in Chinese. The accounts could be divided into two groups by behavior; some accounts behaved as "primary posters," while others were "amplifiers" of the posted content.[354] The method of posting content is described as

[352] This account draws on four reports produced by network analysis firm Graphika with content dating back to 2018. The first Graphika report drew on data from Twitter, YouTube, and Facebook: Ben Nimmo, C. Shawn Eib, L. Tamora, "Cross-Platform Spam Network Targeted Hong Kong Protests," *Graphika*, September 25, 2019, https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf. Two other reports studied the same dataset of 936 Twitter accounts linked to the Chinese government: Kanishk Karan and Pepe Zhang, "Twitter's Hong Kong Archives: Chinese Commercial Bots at Work," *DFRLab*, September 4, 2019, https://medium.com/dfrlab/twitters-hong-kong-archives-chinese-commercial-bots-at-work-f4c7ae8eea64; Tom Uren, Elise Thomas, and Jacob Wallis, "Tweeting through the Great Firewall," *Australian Strategic Policy Institute*, September 3, 2019, https://www.aspi.org.au/report/tweeting- through-great-firewall?__cf_chl_jschl_tk__=pmd_9sBUUrJS8JJkBQMCUCOX9.lAqvG03lJMKITMVSpXhnE-1634695457-0-gqNtZGzNAjujcnBszQil.

[353] Ben Nimmo, C. Shawn Eib, L. Tamora, "Cross-Platform Spam Network Targeted Hong Kong Protests," *Graphika*, September 25, 2019, p., https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf.

[354] Ben Nimmo, Camille François, C. Shawn Eib, Léa Ronzaud, "Return of the (Spamouflage) Dragon," *Graphika*, April 24, 2020, https://public-assets.graphika.com/reports/Graphika_Report_Spamouflage_Returns.pdf.

follows: "they interspersed political content with unrelated spam, either video, text, or photographic; sometimes, different accounts posted the same content in the same order, suggesting that they were automated."[355]

In fall of 2019, multiple platforms (YouTube, Facebook, and Twitter) engaged in targeted removals of campaign assets. As a result, the campaign remained relatively dormant for the remainder of 2019, before resurfacing in late January and early February of 2020, around the time of the US travel ban on Chinese citizens. During this time, the campaign was "activating or acquiring a small number of dormant assets but using them to post at a far lower level and with a far lower proportion of political content." [356] This attempt to hide from the platforms is "reinforced by the way some of its assets changed their names. This is most easily discernible on Facebook, where the Page transparency feature allows viewers to see when pages shifted identity."[357] This change to Page transparency was publicly announced in June 2018.[358] Additionally, these Facebook page assets all "had a little under 5,000 followers, the level at which Facebook's page transparency setting automatically shows where a page is administered from."[359] This further appears as a deliberate choice by the campaign because each page had minimal engagement on any of their posts, despite the relatively high follower count. This likely points to a "a policy of purchasing enough followers to make the assets look authoritative, without obtaining so many that they triggered the transparency setting."[360]

---

355 Ibid., p. 2.
356 Ibid., p. 5.
357 Ibid., p. 12.
358 Rob Leathern and Emma Rodgers, "A New Level of Transparency for Ads and Pages," *Facebook Newsroom*, June 28, 2018, https://about.fb.com/news/2018/06/transparency-for-ads-and-pages/.
359 Ben Nimmo, Camille François, C. Shawn Eib, Léa Ronzaud, "Return of the (Spamouflage) Dragon," p. 15.
360 Ibid., p. 15.

In 2020, in the aftermath of platform enforcement actions in April, a new wave of the campaign was recorded in mid-June with an uptick in July and August. Major changes to the campaign included posting videos in English directed at critiquing the United States, a far higher volume of content being rapidly uploaded, and the use of AI-generated profile pictures. The videos promoted by this network were "commenting on recent U.S. official statements [and] created and uploaded in less than 36 hours."[361]

In 2021, the network exhibited two key changes in an effort to amplify its reach on the platform. These changes are likely both a product of platform action against the network and the relatively ineffectiveness of the campaign in garnering a real-life user audience from 2018 - 2020 (a product of algorithmic demotion, ineffective content and/or user targeting and amplification strategies). The first is that it began using "persona accounts which looked and behaved as though they were real people."[362] These accounts attempted to emulate real-life individual accounts including, a "Chinese mainland commentators known to support CCP rule over Hong Kong and Taiwan; an American businessman; a Latin American soap opera; and young women interested in geopolitics."[363] The second change is an alignment with official state propaganda; it has expanded the number of topics the accounts promote content about and "videos posted by the network closely tracked with Chinese official messaging."[364] This content, as of 2021, was also being amplified by official Chinese diplomat accounts across platforms.

---

[361] Ben Nimmo, Camille François, C. Shawn Eib, Léa Ronzaud, "Spamouflage Goes to America," *Graphika*, August 12, 2020, https://public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf, p. 2.
[362] Ben Nimmo, Ira Hubert, and Yang Cheng, "Spamouflage Breakout," *Graphika*, February 4, 2021, https://public-assets.graphika.com/reports/graphika_report_spamouflage_breakout.pdf, p.3.
[363] Ibid., p. 3.
[364] Ibid., p. 4.

Discussion and Policy Implications

Current regulatory conversations surrounding platform regulation advocate for policy changes without a clear articulation of intended impact. This article presented a conceptual framework and classification system for considering the impact of policy changes introduced by social media platforms on state-sponsored influence operations. Specifically, it argued that private actors control the online landscape, shaping the strategic calculus of states by implementing policies that introduce constraints on behavior and operations. It argues that policies introduce one of three constraints on influence operations: (1) resource constraints, (2) content constraints, (3) audience access constraints.

Engaging in a brief review of all policies announced by several major platforms (Facebook, Twitter, WhatsApp, YouTube, Instagram), we highlighted the applicability of the categorization schema for contextualizing the impacts of different policies and countermeasures on influence operations. We showed that the number of policy changes imposed by platforms are increasing, but that they most often induce content constraints on influence operations. The online landscape, and the changes made to it by private actors, is dynamic and evolving.

Through case studies, we highlighted how influence operations are responsive to platform changes, strengthening our argument that private actors shape the strategic calculus of states operating in the online landscape. For example, the Islamic State modified its content and account presentation to circumvent bans and algorithmic flags. Actions taken by the platform presented clear content and audience access constraints leading to an adaptation in their behavior and operations. When the landscapes of Facebook and Twitter became too hostile or too challenging to operate successfully on, in light of the numerous constraints imposed, they migrated elsewhere. These

alternative platforms offered operational landscapes that were more fixed, and as a result, they initially faced fewer constraints on their operations. However, this came at the cost of accessing a broader audience available on more mainstream social media platforms. For Russia, the resource constraint imposed by platforms' increased ability to detect stolen or copied photos led to an investment in and use of AI-generated profile photos. Russia also sought to rely on existing infrastructure, co-opting organizations in Ghana to propagate their campaign, in order to bypass increased measures evaluating account credibility. For China, the spam-like behavior of a recurring campaign illustrates the impact of content constraints; in an effort to avoid flagging by the platforms, the operation sought to disguise political messaging amidst the noise of spam content. Further, in an attempt to avoid transparency measures by Facebook, they artificially limited the number of followers on their Pages, thereby self-imposing an audience access constraint. China also faced resource constraints in creating credible-looking accounts associated with the operation, wherein they sought to mimic real-life profiles. While these policies are not the only thing that shapes state activity, they have a clear impact on the margins.

Our strategic constraints model generates a few key policy implications. First, platform policy development needs to account for its strategic impact and the secondary, downstream effects on state competition. This remains a critical gap in regulatory conversations and the types of changes pushed by states. To date these discussions have focused primarily on three key areas: data rights and protection, antitrust, and content regulation.[365] Regulatory conversations led by governments should involve experts who can highlight the secondary, downstream effects of such policies on state competition and influence operations. Some state policies which seek to regulate

[365] Siva Vaidyanathan, "What if Regulating Facebook Fails?" *WIRED,* July 2, 2021, https://www.wired.com/story/what-if-regulating-facebook-fails/.

social media platforms have problematic strategic implications for the landscape. As aforementioned, the EU's privacy-focused General Data Protection Regulation (GDPR), reduced the ability of platforms to track malicious actors, which could have inadvertent effects for state influence operations in avoiding detection and removal.[366] And, changes implemented by platforms can impact inter-state competition, in non-obvious ways, making it critical to account for strategic constraints.

Second, in formulating countermeasures against influence operations, platforms and policymakers must account for differences in impact among states, reflecting differences in organizational capacities, incentives, methods, and priorities. While some platform policy decisions will have a negligible impact on high-capacity states, such as Russia and China, low-capacity Western allies engaged in counter-campaigns may be disproportionately impacted in unintended ways.[367] Western governments need to develop mechanisms for sustained engagement with policy teams at platforms, to anticipate and understand the effects of policies which filter through to security competition.

Third, policymakers need to consider the impact of Western political pressure on platform policies can have for the Global South. The overwhelming majority of social media platforms are domiciled in the West and are influenced most by their host governments' regulations. And

366 Dustin Volz and Joseph Menn, "U.S. official warns of 'unintended consequences' of European data privacy law," *Reuters*, April 17, 2018, https://www.reuters.com/article/us-usa-cyber-nielsen/u-s-official-warns-of-unintended-consequences-of-european-data-privacy-law-idUSKBN1HO36J; Forbes Technology Council, "15 Consequences of GDPR," *Forbes*, August 15, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=2d1d226a94ad.

367 Relatively few states have developed capacities to monitor their information environments, let alone the analytical capacity to respond to platform changes which may shape their vulnerability to foreign influence. For a slightly dated summary of state capacities see Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation," *Computational Propaganda Research Project* (2019).

regulatory conversations in the West are largely devoid of any consideration of how changes may impact other states. Further, implementation may not be consistent across areas of the world due to language constraints and automation limitations. It is equally important to note the potential lack of intervention by platforms in non-Western settings and how this may create opportunities for misuse by and proliferation of malicious actors. For example, in 2020, Facebook spent 87% of its moderation time focused on U.S.-based content.[368]

Fourth, consideration of strategic constraints should be embedded in the types of changes platforms adopt. Government hearings and public calls for action have focused on greater regulation without in-depth consideration of the specific forms of regulation that are most effective. The logic behind most platform changes and recommendations appears to be grounded in targeting tactics (i.e., use of bot accounts, making it harder to use fake or stolen accounts, preventing certain kinds of content from being posted or shared), rather than addressing broader, long-term state strategies (i.e., understanding the evolution, adaptations and associated weak points of a campaign). Ideally, policy changes would target more than one constraint and integrate a holistic, strategic constraints mode of thinking into formulating new platform policies that can anticipate responsive and emergent behavior.

Platforms' current adaptive model for change is too slow and cumbersome. Conversations surrounding influence operations have been grounded in a mistaken assumption that a set of policies will successfully remove a class of actors or content permanently from the environment. The reality

368 Heidi Tworek, "Facebook's America-centrism Is Now Plain for All to See," *Center for International Governance Innovation*, October 4, 2021, https://www.cigionline.org/articles/facebooks-america-centrism-is-now-plain-for-all-to-see/; Justin Scheck, Newley Purnell, Jeff Horwitz, "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show," *Wall Street Journal*, September 16, 2021, https://www.wsj.com/articles/facebook -drug-cartels-human-traffickers-response-is-weak-documents-11631812953.

is that state influence campaigns operate on an ever-changing and dynamic system. They respond and adapt to avoid capture, better amplify content, and reach audiences. Instead, platforms must implement policies at a rate that exceeds the ability of states to adapt around them. Government approaches to the social media landscape must also reflect this adaptive process, including ongoing, continuous engagement with platforms and investing resources beyond pushing for a specific law or change. Policy conversations need to account for the two-way causal nature of this system: platforms respond to the behaviors of influence operations, but influence operations also adapt to platform changes. Both platforms and governments should implement policies and countermeasures reflecting the ongoing, adaptive nature of influence operations. To properly address the threats of this new landscape, states must make friends with the mapmakers.

Paper 3

Twitter and the Taliban: Patterns, Paradoxes, and the Power of Platforms

Introduction

On August 15, 2021, a spokesperson of the Islamic Emirate of Afghanistan, the Taliban's self-proclaimed state, declared on Twitter: "With the help of God, and the support of the nation, we are now in control of all parts of the country. We would like to congratulate our nation on this big achievement."[369] Written in English, this tweet was the culmination of the Taliban's two-decade long campaign - both online and on the battlefield - orchestrated to win the hearts, minds, and territories of Afghanistan. While global perception paints the Taliban as fundamentalist, regressive, and anti-modernist, the group has long recognized the power and importance of adopting the most advanced forms of information and communications technology (ICT) to promote their ideology and political goals. Over the last 20 years of conflict, the Taliban weaponized various forms of ICT to wage sophisticated, multimodal information warfare against U.S., NATO coalition, and Afghan government forces. The group's information campaign spanned radio, television, cell phones, organizational websites, and social media.[370] Across these technologies, the group deployed specific communication strategies and narratives to portray their success and benevolence while vilifying opponents.[371]

---

[369] Tweeted by Zabihullah Mujahid, official spokesman of the Islamic Emirate of Afghanistan (@Zabehullah_M33) on August 15, 2021; a screenshot of this tweet is documented on p. 29 of Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30," *Empirical Studies of Conflict Project* (2022).

[370] Tim Foxley, *The Taliban's propaganda activities: how well is the Afghan insurgency communicating and what is it saying?*, (SIPRI, 2007).

[371] Thomas H. Johnson, Matthew DuPee, and Wali Shaaker, *Taliban narratives: The use and power of stories in the Afghanistan conflict* (Oxford University Press, 2017); Peter Chroust, "Neo-Nazis and Taliban on-line: Anti-modern political movements and modern media," *Democratization*, Vol. 7, No. 1 (2000), pp. 102-118.

But since the Taliban's inception, the group has sought to weaponize the online environment. The group launched their first website, www.taliban.com, in 1998. By 2005, their official website, Al-Emarah, included content in five languages. The site would grow to include live streaming of their radio station, professionally produced videos of their exploits, blog-style updates, official statements from Taliban leadership, and links encouraging viewers to share their content on other online platforms. And eventually, they would branch out to mainstream social media platforms, creating accounts on Facebook, YouTube, and Twitter.[372]

By 2021, the Taliban's online activities evolved into a sophisticated information campaign on Twitter used to support the Taliban's takeover of Afghanistan in the wake of U.S. and NATO troop withdrawal. On Twitter, Taliban leaders, spokesmen, and avowed members live-tweeted military operations in real-time, leveraged specialized hashtags to expand the reach of their content, uploaded photos and videos to accuse American military forces of committing war crimes, and tagged the accounts of humanitarians, political organizations, and news agencies in their posts to prompt a response. Engaging in the most comprehensive quantitative analysis of Taliban-linked social media behavior to date, this article will explore two key questions of interest: How did the Taliban use Twitter to support military operations during the takeover of Afghanistan in 2021? And how did the Taliban leverage Twitter's features to promote their information campaign?

Critically, the Taliban have been using Twitter for more than ten years, throughout various phases of organizational strength and periods of the conflict. And yet, only three academic publications have attempted to document their behavior online and are limited in scope, with

[372] Sarah Atiq, "The Taliban embrace social media: 'We too want to change perceptions'," *BBC News*, September 6, 2021, https://www.bbc.com/news/world-asia-58466939.

analyses focused on English-language content from a limited set of Taliban accounts.[373] The Taliban's use of Twitter is also emblematic of forthcoming trends in non-state actor information behavior in conflict. Academic scholarship is increasingly documenting the role of modern ICT in reshaping political violence, including its use by non-state armed groups.[374] As a category of technology, ICT's ubiquity and global diffusion has impacts that both academics and policymakers alike have yet to fully discern. Importantly, smartphones with internet access are "more widely diffused than dynamite was and the AK-47 was and still is."[375] Social media companies are also beginning to consider the weaponization of their platforms by malicious actors, but their scope is often myopically focused on threats to the West, namely China, Russia, the Islamic State, and the alt-right movement.[376] And while academic literature exists on the social media use of certain non-state armed groups, we lack a clear model for understanding and predicting how non-state actors might weaponize the new online environment in different ways and what the primary barriers are to adoption (if any).[377]

---

[373] Vincent Bernatis, "The Taliban and Twitter: Tactical reporting and strategic messaging," *Perspectives on Terrorism*, Vol. 8, No. 6 (2014), pp. 25-35; Hazrat M. Bahar, "Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter," *Media Asia*, Vol. 47, No. 1-2 (2020), pp. 34-46; David Drissel, "Reframing the Taliban insurgency in Afghanistan: new communication and mobilization strategies for the Twitter generation," *Behavioral sciences of terrorism and political aggression*, Vol. 7, No. 2 (2015), pp. 97-128.

[374] See Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 401-413; Nils B. Weidmann, "Communication, technology, and political conflict: Introduction to the special issue," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 263-268; Barbara F. Walter, "The new new civil wars," *Annual Review of Political Science*, Vol. 20 (2017), pp. 469-486; Peter Warren Singer and Emerson T. Brooking, *LikeWar: The weaponization of social media* (Eamon Dolan Books, 2018).

[375] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford University Press, 2019).

[376] Laura Courchesne and Brian McQuinn, "After the Islamic State: Social Media and Armed Groups," *War on the Rocks,* April 9, 2021, https://warontherocks.com/2021/04/after-the-islamic-state-social-media-and-armed-groups/; Miles Parks, "Twitter Bans Ads From Russian State Media, Citing Election Interference Efforts," *NPR*, October 26, 2017, https://www.npr.org/2017/10/26/560199026/twitter-ends-russian-state-media-advertisements-citing-2016 - interference-efforts; Cecilia Kang, Nicholas Fandos, Mike Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill," *The New York Times,* October 31, 2017, https://www.nytimes.com /2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html?smid=tw-share&_r=0; Jamie Condliffe, "How to Fix Social Media's Big Problems? Lawmakers Have Ideas," The New York Times, July 30, 2018, https:// www.nytimes.com/2018/07/30/business/dealbook/big-tech-regulation-ideas.html.

[377] See Tamar Mitts, Gregoire Phillips, and Barbara F. Walter, "Studying the impact of ISIS propaganda campaigns," *The Journal of Politics*, Vol. 84, No. 2 (2022); Imran Awan, "Cyber-extremism: Isis and the power of social media," *Society*, Vol. 54, No. 2 (2017), pp. 138-149; Ken Menkhaus, "Al-Shabaab and social media: A double-edged sword," *Brown Journal of*

Analysis of the Taliban's adoption and use of social media also offers important lessons for international relations theory and policy discourse. As a case study, the Taliban is a theoretical puzzle: how did a seemingly inferior, under-resourced non-state armed group succeed in beating (or at the very least outlasting) a militarily superior force? While existing theories on asymmetric warfare offer insights, the cause(s) of the Taliban's success will be studied for years to come.[378] Part of this explanation must include understanding how the Taliban deployed technology. Taliban leaders understood the power of propaganda from the group's inception and used a wide range of ICT throughout the conflict to deploy their messaging. By 2021, as the Taliban took Afghanistan province by province, spokesmen and supporters updated social media with videos, images, and messages in real-time, preparing Afghans and the international community for their new regime.[379]

Employing a quantitative descriptive methods approach, this article will offer the most comprehensive review of the Taliban's use of social media to date, analyzing 112,354 tweets sourced from a network of 63 accounts linked to the Taliban's leadership, over a period of five and half months, April 1, 2021 to September 16, 2021. This article provides a detailed analysis of the Taliban's social media repertoire and tactics, preliminary documentation of the Taliban's use of

World Affairs, Vol. 20 (2013), p. 309; David Mair, "# Westgate: A case study–how Al-Shabaab used Twitter during an ongoing attack," In *Violent Extremism Online* (Routledge, 2016), pp. 65-86; Hyunjin Seo, "Visual propaganda in the age of social media: An empirical analysis of Twitter images during the 2012 Israeli–Hamas conflict," *Visual Communication Quarterly*, Vol. 21, No. 3 (2014), pp. 150-161; Gabriel Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," *New Media and Innovative Technologies,* Vol.22 (2008); Cyanne E. Loyle and Samuel E. Bestvater, "# rebel: Rebel communication strategies in the age of social media," *Conflict Management and Peace Science*, Vol. 36, No. 6 (2019, pp. 570-590.

[378] Andrew Mack, "Why big nations lose small wars: The politics of asymmetric conflict," *World politics*, Vol. 27, No. 2 (1975), pp. 175-200; Ivan Arreguin-Toft, *How the weak win wars: A theory of asymmetric conflict*, Vol. 99 (Cambridge University Press, 2005); Thazha Varkey Paul, *Asymmetric conflicts: war initiation by weaker powers*, No. 33 (Cambridge University Press, 1994).

[379] Charlie Winter, Abdullah Alrhmoun, Abdul Sayed, "The Taliban's vast propaganda machine has a new target," *WIRED*, August 28, 2021, https://www.wired.co.uk/article/taliban-propaganda-news-afghanistan.

social media to complement on-the-ground military operations, and introduces a novel dataset. It argues that during the summer takeover, the Taliban invested considerable time and organizational resources developing and amplifying a sophisticated online information campaign in real-time. It also argues that the Taliban made use Twitter's platform features to amplify their messaging and engage in both domestic and international outreach, including developing specialized hashtags to push specific propaganda narratives and leveraging mentions to attempt to garner a response from humanitarian organizations, key political players, and journalists. This analysis contributes to ongoing discourse on the role of social media in conflict, provides additional insight on how non-state armed groups approach weaponizing social media to further political and military goals, and offers a greater understanding of how the Taliban used the online environment during the 2021 takeover.

The remainder of this article proceeds as follows: it begins by providing background on the role of social media in modern political conflict, reviews the literature on non-state armed groups' use of social media, and summarizes existing research on the Taliban's social media and propaganda behavior. It then provides a brief history of the Taliban's use of ICT, particularly the internet, over the last twenty years of conflict. Next, it presents the findings of a quantitative analysis of over 100,000 tweets, including an overview of tweet frequency by week during the takeover, a comparison of locational data recorded on Taliban accounts with on-the-ground activity, discussion of key actors (including China, Russia and the U.S.) by Taliban-linked accounts, and a review of the most commonly used hashtags developed by the Taliban to amplify their messaging. Finally, the article concludes with a discussion of the policy and research implications of this quantitative analysis.

Non-State Armed Groups on Social Media

International relations is increasingly considering the role of emerging technologies in shaping political violence and conflict. In particular, research in the last decade has sought to evaluate how a range of political actors, from state militaries to terrorist organizations, have weaponized the internet and social media to promote their ideology, foment protests, recruit foreign fighters, and wage influence operations.[380] Zeitzoff (2017) has argued that social media has four key points of impact on conflict actors, including (1) reducing costs to communicate, (2) increasing the speed and scope of information sharing, (3) introducing strategic interaction and forcing competitive adaptation, and (4) supplying new sources of information. Critically, he argues that "social media's influence on conflict defies simplistic explanations that argue that it privileges incumbents or challengers."[381] Further, Walter (2017) argues that social media impacts the dynamics of civil wars and supports the activities of rebel groups. Social media enables non-state armed groups to facilitate coordination and recruitment, frame rebel ideology and aims in global terms to achieve international support, and increase the breadth of potential funding channels.[382]

Walter (2017) also emphasizes the massive increase in rebel group use of the internet, including the proliferation of terrorist-linked websites.[383] Terrorist organizations and non-state armed groups now leverage social media platforms to host content, access audiences, engage in secure communication, exert control over their brand, build and maintain community, generate financing,

[380] See Peter Warren Singer and Emerson T. Brooking, *LikeWar: The weaponization of social media*, (Eamon Dolan Books, 2018); Diego A. Martin, Jacob N. Shapiro, and Michelle Nedashkovskaya, "Recent trends in online foreign influence efforts." *Journal of Information Warfare*, Vol. 18, No. 3 (2019), pp. 15-48.
[381] Thomas Zeitzoff, "How social media is changing conflict," *Journal of Conflict Resolution,* Vol. 61, No. 9 (2017), pp. 1970-1991.
[382] Barbara F. Walter, "The new new civil wars," *Annual Review of Political Science*, Vol. 20, No. 1 (2017), pp. 469-86.
[383] Barbara F. Walter, "The new new civil wars."

and engage in information collection and curation.[384] A substantive literature base has emerged focused on the online activities of the Islamic State and its jihadist affiliates.[385] The Islamic State (IS) rose to global prominence in part due to its sophisticated use of the online environment, including accounts on popular social media platforms and the development of organizational websites, to promote a global brand and recruit foreign fighters. The success of the group's foreign recruitment has been partly attributed to its propaganda campaigns on social media.[386] Throughout its occupation of different territories of Syria and Iraq, the group turned to social media to share their messaging, including graphic videos encouraging violence, content appealing to grievances held by potential recruits, and blatant ideological propaganda highlighting the religious, material, and social benefits of supporting the group.[387] During their operations in Syria in 2015 and 2016, the Islamic State used Twitter as a "megaphone [...] to send out live updates of fighters tweeting about what it feels like to be in Syria."[388] A study of foreign fighters in Syria found that they leveraged Twitter "for purposes of recruitment and indoctrination, as well as to build a transnational community of violent extremism. It [was] also a means of psychological warfare directed at distant foes as well as local enemies—Kurds, competing rebel fighters, and regime forces."[389]

---

384 Brian Fishman, "Crossroads: Counter-terrorism and the Internet (February 2019)," *Texas National Security Review* (2019).

385 See Scott Gates and Sukanya Podder, "Social media, recruitment, allegiance and the Islamic State," *Perspectives on Terrorism*, Vol. 9, No. 4 (2015), pp. 107-116; Tamar Mitts, Gregoire Phillips, and Barbara F. Walter, "Studying the impact of ISIS propaganda campaigns," *The Journal of Politics*, Vol. 84, No. 2 (2022); Imran Awan, "Cyber-extremism: Isis and the power of social media," *Society*, Vol. 54, No. 2 (2017), pp. 138-149.

386 Antonia Ward, "ISIS's use of social media still poses a threat to stability in the Middle East and Africa," *Georgetown Security Studies Review* (2018).

387 Tamar Mitts, Gregoire Phillips, and Barbara F. Walter, "Studying the impact of ISIS propaganda campaigns," *The Journal of Politics*, Vol. 84, No. 2 (2022); Charlie Winter, "Apocalypse, later: a longitudinal study of the Islamic State brand," *Critical Studies in Media Communication*, Vol. 35, No. 1 (2018), pp. 103-121; Aaron Y. Zelin, "Picture or it didn't happen: A snapshot of the Islamic State's official media output," *Perspectives on Terrorism*, Vol. 9, No. 4 (2015), pp. 85-97; Charlie Winter, "Documenting the virtual 'caliphate'," *Quilliam Foundation*, Vol. 33, No. 1 (2015); Haroro J. Ingram, "An analysis of Islamic State's Dabiq magazine," *Australian Journal of Political Science*, Vol. 51, No. 3 (2016), pp. 458-477.

388 Imran Awan, "Cyber-extremism: Isis and the power of social media," *Society*, Vol. 54, No. 2 (2017), pp. 138-149.

389 Jytte Klausen, "Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq," *Studies in Conflict & Terrorism*, Vol. 38, No. 1 (2015), pp. 1-22.

Comparatively, a smaller set of studies have focused on a limited number of other prominent groups including Al-Shabaab, Hamas, and Hezbollah.[390] These studies tend to be narrowly focused, and generally explore how group ideology is promoted through social media messaging. For example, years prior to the Islamic State, militant group Al-Shabaab "effectively used Internet chat rooms, websites, and YouTube videos to recruit and fundraise internationally."[391] Famously, the group leveraged Twitter in September 2013, tweeting in real-time to take credit and provide updates on its terrorist attack on the Westgate Mall in Nairobi Kenya. This included tweets with images and videos taken from inside the mall during the attack, such as: "Here are 2 of the mujahideen inside the #Westgate Mall, unruffled and strolling around the Mall in such a sangfroid manner," and "A spectacular Al-Shabaab attack, with 50+ dead and guaranteed extended media coverage is finalized."[392] An analysis of 556 tweets made by 8 Al-Shabaab-linked accounts during the attack found that the overwhelming majority of tweets were in English. The group leveraged social media to propagate specific narratives about the attack aimed at Kenyans and the Kenyan government.[393]

A recent analysis of the social media presence of the nine most powerful armed groups in Myanmar found that online, these groups "act like states, using social media primarily to communicate with their constituents. [....] they also use social media as a tool of armed struggle, for command and

---

390 See Scott Gates and Sukanya Podder, "Social media, recruitment, allegiance and the Islamic State," *Perspectives on Terrorism*, Vol. 9, No. 4 (2015), pp. 107-116; Tamar Mitts, Gregoire Phillips, and Barbara F. Walter, "Studying the impact of ISIS propaganda campaigns," *The Journal of Politics*, Vol. 84, No. 2 (2022); Imran Awan, "Cyber-extremism: Isis and the power of social media," *Society*, Vol. 54, No. 2 (2017), pp. 138-149; Ken Menkhaus, "Al-Shabaab and social media: A double-edged sword," *Brown Journal of World Affairs*, Vol. 20 (2013); David Mair, "# Westgate: A case study–how Al-Shabaab used Twitter during an ongoing attack," In *Violent Extremism Online*, (Routledge, 2016), pp. 65-86; Hyunjin Seo, "Visual propaganda in the age of social media: An empirical analysis of Twitter images during the 2012 Israeli–Hamas conflict," *Visual Communication Quarterly*, Vol. 21, No. 3 (2014), pp. 150-161; Gabriel Weimann, "Hezbollah Dot Com: Hezbollah's Online Campaign," *New Media and Innovative Technologies,* Vol.22 (2008); Benjamin T. Jones and Eleonora Mattiacci, "A manifesto, in 140 characters or fewer: Social media as a tool of rebel diplomacy," *British Journal of Political Science*, Vol. 49, No. 2 (2019), pp. 739-76.

391 Ken Menkhaus, "Al-Shabaab and social media: A double-edged sword," *Brown Journal of World Affairs*, Vol. 20 (2013).

392 Ken Menkhaus, "Al-Shabaab and social media: A double-edged sword," *Brown Journal of World Affairs*, Vol. 20 (2013).

393 David Mair, "# Westgate: A case study–how Al-Shabaab used Twitter during an ongoing attack," In *Violent Extremism Online*, (Routledge, 2016), pp. 65-86.

control, intelligence, denunciation of traitors, and attacks against adversaries."[394] This study also found that these groups use social media for domestic and international outreach. In particular, these groups used Facebook to share content and leveraged hashtags to access specific audiences after official pages were removed by platform moderators.[395] An analysis of Hamas's online behavior during the 2012 Gaza conflict found that the group posted more than twice the number of propaganda images to Twitter than the Israel Defense Forces, sharing claims of civilian casualties caused by their opponent.[396]

In Libya, rebel groups have been documented using Facebook and Twitter as a tool for public diplomacy, coordinating with other groups and liaising with the domestic population.[397] Similarly, two rebel groups operating in the Sahel (National Movement for the Liberation of Azawad (MNLA) and Ansar Dine) both use social media "to engage in relations with foreign publics [...] including foreign elites, international organizations and civil society groups and individuals."[398] This approach to social media allows these groups to "redefine and expand their spheres of influence and the range of stakeholders in their conflicts"[399]

394 Stein Tønnesson, Min Zaw Oo, and Ne Lynn Aung. "Pretending to be States: The Use of Facebook by Armed Groups in Myanmar." *Journal of Contemporary Asia*, Vol. 52, No. 2 (2022), pp. 200-225.
395 Stein Tønnesson, Min Zaw Oo, and Ne Lynn Aung. "Pretending to be States: The Use of Facebook by Armed Groups in Myanmar." *Journal of Contemporary Asia*, Vol. 52, No. 2 (2022), pp. 200-225.
396 Hyunjin Seo, "Visual propaganda in the age of social media: An empirical analysis of Twitter images during the 2012 Israeli–Hamas conflict," *Visual Communication Quarterly*, Vol. 21, No. 3 (2014), pp. 150-161.
397 Benjamin T. Jones and Eleonora Mattiacci,"A manifesto, in 140 characters or fewer: Social media as a tool of rebel diplomacy," *British Journal of Political Science*, Vol. 49, No. 2 (2019), pp. 739-761; Laura Courchesne and Brian McQuinn, "After the Islamic State: Social Media and Armed Groups," *War on the Rocks*, April 9, 2021, https://warontherocks.com/2021/04/after-the-islamic- state-social-media-and- armed-groups/.
398 Michèle Bos and Jan Melissen, "Rebel diplomacy and digital communication: public diplomacy in the Sahel," *International Affairs*, Vol. 95, No. 6 (2019), pp.1331-1348.
399 Michèle Bos and Jan Melissen, "Rebel diplomacy and digital communication: public diplomacy in the Sahel," *International Affairs*, Vol. 95, No. 6 (2019), pp.1331-1348.

While these individual studies are important in furthering our understanding of non-state armed groups operating online, more research is needed. Loyle and Bestvater (2019) conducted one of the first comprehensive studies of non-state armed group use of social media, examining the behavior of 55 rebel groups on Twitter. The authors found that rebel groups typically use social media to spread messaging targeted at international audiences.[400] Expanding the literature on the social media use of armed groups is important for three primary reasons: (1) the current focus on the Islamic State's social media use potentially obscures the range of behaviors of armed groups operating online, (2) reviewing the social media activities of organizations involved in different conflicts allows for a clearer understanding of how online behaviors connect with and influence real-world events, and (3) mapping how different actors misuse social media platforms improves policy recommendations for regulation and moderation of online spaces.

The Taliban has operated on social media for over a decade, creating their first Twitter account in 2011. And yet, only three academic papers have sought to analyze the Taliban's behavior on social media. They are profoundly limited in scope, with analyses focused on the English-language content produced by only two Taliban accounts during narrow time intervals. Bernatis (2014) analyzed English language tweets from a single account, @alemarahweb, posted between May and September of 2012.[401] This analysis reviewed 349 tweets, only "coding tweets that reported on direct actions by insurgents or those which highlighted current events perceived by the Taliban to be beneficial to their cause (a protest against "American desecration of a Qur'an", for example)."[402] This research compared attack numbers and casualty counts as reported by the

[400] Cyanne E. Loyle and Samuel E. Bestvater, "# rebel: Rebel communication strategies in the age of social media," *Conflict Management and Peace Science*, Vol. 36, No. 6 (2019, pp. 570-590.
[401] Vincent Bernatis, "The Taliban and Twitter: Tactical reporting and strategic messaging," *Perspectives on Terrorism*, Vol. 8, No. 6 (2014), pp. 25-35.
[402] Ibid., p. 27.

Taliban's Twitter account with official statistics published by NATO's International Security Assistance Force (ISAF), a multinational military mission in Afghanistan. This research found that the Taliban used this Twitter account to engage in public relations aimed at foreign audiences. The research's primary finding was that the Taliban recorded a far higher number of attacks than the number disclosed by ISAF.

Bahar (2020) examined 502 tweets from a single Taliban Twitter account, that of its primary spokesperson (@Zabihullah_M33). These tweets were collected for three 11-day periods: January 20-31, February 20-28, and March 20-31 of 2018. This behavior was compared with the official Twitter account of the Afghan Ministry of Defense. This research found that the Taliban used Twitter to make claims of killing or wounding Afghan soldiers, share images of stolen equipment, and used targeted hashtag documenting allegations against their opponent (notably #WarCrimes). The primary finding was that both the Taliban and the Afghan Ministry of Defense used Twitter to highlight the success of specific operations and amplify claims of civilian deaths caused by their opponent.[403]

Drissel (2015) conducted qualitative rhetorical analysis of over 400 English-language tweets made by at least 3 different Taliban linked accounts between January - February 2012. He also includes analysis of content shared on the Taliban's English language website, shahamat-english.com.[404] This research found that these tweets aimed to "endeavored to frame (and re-frame) the movement in the globalized phraseology of militant Islamism – including Islamic jihad and the

[403] Hazrat M. Bahar, "Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter," *Media Asia*, Vol. 47, No. 1-2 (2020), pp. 34-46.
[404] David Drissel, "Reframing the Taliban insurgency in Afghanistan: new communication and mobilization strategies for the Twitter generation," *Behavioral sciences of terrorism and political aggression*, Vol. 7, No. 2 (2015), pp. 97-128.

Muslim ummah."[405] Additionally, these tweets served to further propaganda aimed at Western audiences, including "narrative frameworks of justice globalism, including anti-imperialism, universal human rights, and national self-determination, appeared to be intended [...] to garner sympathy and generate political pressure on the US government (and NATO) to exit the country precipitously."[406]

While these studies offer a useful starting point, they fail to provide insight as to the scope and scale of the Taliban's presence on social media, as well as the group's approach to social media during key periods in the conflict. To address this gap, this article will provide the most comprehensive quantitative analysis of the Taliban's social media to date. This article also provides a valuable baseline understanding of the online activity and repertoire during a crucial period: the Taliban's 2021 takeover of Afghanistan. The analysis conducted in this article is necessary and important, both for understanding the Taliban and the conflict dynamics at play during the summer of 2021 and in furthering the field's understanding of how armed groups operate online and use social media during major military operations.

ICT and the Taliban

The Taliban emerged in 1994 during the Afghan civil war. Many of the group's founding members were mujahideen, who fought Soviet forces during the Soviet-Afghan war during the 1980s. From their inception, the group sought to instate a government in Afghanistan reflecting their Islamist ideology that enforced a strict interpretation of Sharia law. In 1996, the group took control of the capital city of Kabul and established the Islamic Emirate of Afghanistan, with Mullah Mohammed

[405] Ibid., p. 122.
[406] Ibid., p. 123.

Omar leading their new government.[407] By 1998, they had gained control of 90% of the country. However, owing to their human rights abuses, most members of the international community did not recognize the Taliban as the country's official government. The Taliban's refusal to surrender Al Qaeda leader, Osama Bin Laden, exacerbated their pariah status. After terrorist attacks on U.S. embassies in Kenya and Tanzania in 1998, the U.S. launched airstrikes on Al Qaeda sites in Afghanistan and imposed sanctions on the country.[408]

During the Taliban's rule over Afghanistan, it prohibited the use of a wide range of information and media technologies. The group banned "the internet and confiscated or destroyed television sets, cameras, and video tapes."[409] Consequences for violating these bans involved violent punishments including public lashings.[410] During this period, Mullah Omar, founder of the Taliban and then leader of the newly established Islamic Emirate of Afghanistan, "famously refused to be photographed."[411] While some ICT-based infrastructure existed in Afghanistan, it was primarily used by the Taliban's senior leaders. For example, the Afghan Wireless Communications Company (AWCC), described as a "rudimentary analog mobile telephone system," enabled Taliban commanders to coordinate and make international calls.[412] In 2001, Afghanistan had "between 10,000 and 20,000 fixed lines [operational telephones], and mobile telecommunications were

[407] S. Yaqub Ibrahimi. "The Taliban's Islamic Emirate of Afghanistan (1996–2001): War-Making and State-Making as an Insurgency Strategy." *Small Wars & Insurgencies* Vol. 28, No. 6 (2017), pp. 947-972.
[408] S. Yaqub Ibrahimi. "The Taliban's Islamic Emirate of Afghanistan (1996–2001): War-Making and State-Making as an Insurgency Strategy." *Small Wars & Insurgencies* Vol. 28, No. 6 (2017), pp. 947-972.
[409] Sarah Atiq, "The Taliban embrace social media: 'We too want to change perceptions'."
[410] Thomas H. Johnson, Matthew DuPee, and Wali Shaaker, *Taliban narratives: The use and power of stories in the Afghanistan conflict*, p. 89.
[411] Gavin Butler, "How Social Media Helped 'Taliban 2.0' Take Control of Afghanistan," *Vice News*, August 19, 2021, https://www.vice.com/en/article/z3x5we/social-media-helped-taliban-control-afghanistan.
[412] Thomas H. Johnson, Matthew DuPee, and Wali Shaaker, *Taliban narratives: The use and power of stories in the Afghanistan conflict*.

virtually nonexistent."[413] Throughout this period, Afghans lacked international connectivity and were forced to cross borders to make international phone calls.[414]

Despite enforcing an ideology hostile to technology for Afghans, the Taliban actively adopted advanced ICT. In 1998, they launched their first website, www.taliban.com. Prior to the U.S. invasion, there were only an estimated 2,000 internet users in Afghanistan and in August of 2001, the Taliban issued a ban on internet use.[415] Thus, the goal of this online initiative was presumably to project a positive image of their regime to foreign audiences.[416] They also permitted foreign journalists to film Taliban fighters for documentaries and international reporting, although members of leadership were not featured.[417] Instead, for domestic audiences they developed "jihadist songs (without musical accompaniment)." These would later become a feature of videos they produced and distributed as propaganda.[418]

In the aftermath of Al Qaeda's 9/11 attacks, U.S.-led forces invaded the country and removed the Taliban from power.[419] Throughout November 2001, the Taliban faced repeated losses in key cities, including Kabul. NATO's coalition force, dedicated to supporting the security efforts of a new Afghan government, was created in December of 2001, titled the International Security

---

413 Sheldon Himelfarb and Cecilia Paradi-Guilford, "Can You Help Me Now? Mobile Phones and Peacebuilding in Afghanistan," *United States Institute for Peace*, November 15, 2010, https://www.usip.org/publications/2010/11/can-you-help-me-now.

414 "From Transition to Transformation: The Role of the ICT Sector in Afghanistan," World Bank, May 2013, https://www.infodev.org/infodev-files/final_afghanistan_ict_role_web.pdf.

415 Thomas H. Johnson, Matthew DuPee, and Wali Shaaker, *Taliban narratives: The use and power of stories in the Afghanistan conflict*, p. 89; "Taliban orders Afghan ban on access to Internet," *The Irish Times*, August 25, 2001, https://www.irishtimes.com/news/taliban-orders-afghan-ban-on-access-to-internet-1.394327

416 Neil Krishan Aggarwal, *The Taliban's Virtual Emirate: The Culture and Psychology of an Online Militant Community* (Columbia University Press, 2016).

417 Antonio Giustozzi, *Koran, Kalashnikov, and Laptop: The Neo-Taliban Insurgency in Afghanistan 2002-2007* (Columbia University Press, 2008), p. 13.

418 Antonio Giustozzi, *Koran, Kalashnikov, and Laptop: The Neo-Taliban Insurgency in Afghanistan 2002-2007*, p. 12.

419 Abdulkader H. Sinno, *Organizations at war in Afghanistan and beyond* (Cornell University Press, 2011).

Assistance Force (ISAF).[420] On December 5, the Bonn Agreement, negotiated with Northern Alliance and other Afghan factions, was signed and installed Hamid Karzai as the country's interim leader. On December 9, Taliban forces surrendered Kandahar, with Mullah Omar and other members of leadership fleeing to Pakistan.[421] An estimated 20% of the Taliban's fighting force had been killed by early 2002. During their exile, the Taliban formed a governing council called the Quetta Shura.[422]

After the group's exodus, some Taliban fighters and associated insurgent groups remained in Afghanistan. Those with explicit Taliban affiliation operated as an underground movement, organizing actions and attacks without direct instructions from leadership. These activities also included promoting propaganda and recruiting from local populations.[423] Other groups and factions, including the Haqqani Network, the Peshawar (or Ijraya) Shura, and the Miran Shah Shura, also carried out attacks before eventually aligning themselves with the Quetta Shura council of the Taliban.[424] From an organizational standpoint, the Taliban primarily operated in a decentralized manner, with a gradual adaptation towards centralized control and structure as the conflict progressed. The Quetta Shura leadership council oversaw various commissions that performed specialized functions for the organization. These included political, military, judicial, health and information commissions, described as "administrative organs through which the Taliban operate a

420 Thomas H. Johnson, Matthew DuPee, and Wali Shaaker, *Taliban narratives: The use and power of stories in the Afghanistan conflict* (Oxford University Press, 2017), pp. 217 - 264.
421 "The U.S. War in Afghanistan: 1999 – 2021," *Council on Foreign Relations*, https://www.cfr.org/timeline/us-war-afghanistan.
422 Antonio Giustozzi, *The Taliban at War: 2001-2018* (Oxford University Press, USA, 2019), p. 18.
423 Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 20.
424 Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 106.

shadow government."[425] The information commission oversaw "the Taliban's ever growing media outlets."[426]

While sporadic conflict continued with disparate contingents of Taliban forces, by November of 2003, U.S. Secretary of Defense Donald Rumsfeld had declared an "end to major combat."[427] During the summer of 2003, Taliban fighters reportedly used satellite phones in large numbers and had motorcycles fitted with phone chargers.[428] In 2004, the new Afghan constitution established freedom of speech and permitted the establishment of private media, thereby promoting the growth of an ICT sector in Afghanistan.[429] From 2003 through 2006, during a brief lull in the conflict, foreign-owned telecom companies built mobile phone towers across the country.[430]

With U.S. military focus turning to Iraq, the Taliban resurfaced with new combat tactics, operating as a large-scale insurgency scale in the summer of 2006. The Taliban deployed improvised explosive devices (IEDs), suicide bombers, and engaged in targeted assassinations.[431] By 2006, the Taliban began to use field radios and cell phones to coordinate among fighters.[432] These technologies enabled the group to improve intelligence collection and remotely detonate IEDs. Taliban supporters used these same communication channels to notify the group of coalition

---

425 Lindsay Maizland, "The Taliban in Afghanistan," *Council on Foreign Relations*, September 15, 2021, https://www.cfr.org /backgrounder/taliban-afghanistan; Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 60.
426 Thomas H. Johnson, "Taliban adaptations and innovations."
427 "The U.S. War in Afghanistan: 1999 – 2021," *Council on Foreign Relations*, https://www.cfr.org/timeline/us-war-afghanistan.
428 Antonio Giustozzi, *Koran, Kalashnikov, and Laptop: The Neo-Taliban Insurgency in Afghanistan 2002-2007*, p. 152.
429 Hazrat M. Bahar, "Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter," *Media Asia* Vol. 47, No. 1-2 (2020), pp. 34-46.
430 Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat," *The Wall Street Journal,* March 22, 2010, https://www.wsj.com/articles/SB10001424052748704117304575137541465235972.
431 Thomas H. Johnson, "Taliban adaptations and innovations," *Small Wars & Insurgencies*, Vol. 24, No. 1 (2013), pp. 3-27; Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 133.
432 Gilles Dorronsoro, *The Taliban's winning strategy in Afghanistan*.

movements.[433] However, the use of both radio and cell phones introduced strategic trade-offs for the Taliban. Coalition forces were able to track their movements through their unsecured usage. The Taliban gradually became aware of their vulnerability to communication monitoring. To mitigate this risk, the Taliban would occasionally revert to using "coded messages or even dropping radios in favor of low-technology techniques like torch-signaling."[434] Cell phone use by individual fighters also began to create problems and risks for the group. Beginning in 2008, the Taliban attempted to introduce and enforce stricter mobile phone discipline among their fighters.[435] By May 2011, the Taliban issued an order for forces to limit their use of mobile phones, with "only one or two people, or just the commander" carrying them.[436] An interview with a Taliban member in 2012 highlights this concern: "We know British forces have the technology to hear our mobiles and radios. We knew this before and that's why we change our numbers very often and most of the time keep our mobiles off. Mostly we use Thuraya [a specific brand of satellite phone] phones or satellite phones for communication, [as] British troops and Americans don't have the ability to listen to the satellite phones."[437] In reality, British and American troops were still able to track these satellite phones.[438] Meanwhile, American troops hoped to take advantage of the Afghan populace's increasing connectivity. U.S. forces painted "phone tip-line signs on walls outside U.S. bases," encouraging civilians to call with intelligence about the Taliban.[439] These tips were typically provided at night when informers were less likely to be spotted by the Taliban or their supporters.

433 Gilles Dorronsoro, *The Taliban's winning strategy in Afghanistan*.
434 Antonio Giustozzi, *Koran, Kalashnikov, and Laptop: The Neo-Taliban Insurgency in Afghanistan 2002-2007*, p. 152.
435 Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 151.
436 Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 151.
437 Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 151.
438 Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 151.
439 Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat."

The Taliban also sought to control the information environment of Afghanistan through cell phone networks. Beginning in 2008, the group destroyed hundreds of cell towers and coerced (often foreign-owned) companies into selectively providing service during key hours, with the goal of preventing intelligence gathering and controlling civilian communication. The Taliban also began to coerce cell tower providers into nightly shutdowns in an effort to prevent intelligence collection by opposing military forces. When providers failed to adhere to their demands, the Taliban responded by attacking and destroying towers.[440] In February and early March of 2008, they attacked cell towers in Kandahar and Helmand provinces.[441] In the fall of that same year, they threatened mobile phone operators to shut down service during the day in Ghazni province.[442] In October, the Taliban announced that the "trial phase" of cell service shutdowns had shown to be successful, and that they planned to pursue national bans on night-time service, citing that these actions were "to protect the Afghan people."[443]As articulated by one U.S. army psychological operations officer, the Taliban deployed and controlled this infrastructure "as a weapons system. If you control the communications of a population, you can control their thoughts." [444]

By 2008, Taliban-produced videos were also spreading among the civilian population through cell phones.[445] By 2009, 52% of Afghans were reported to have access to a cell phone.[446] At

[440] Jacob N. Shapiro and David A. Siegel, "Coordination and security: How mobile communications affect insurgency." *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 312-322.; Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat."
[441] Norias Nori, "Afghanistan: Mobile-Phone Towers Are Taliban's New Target," *Radio Free Europe / Radio Free Liberty,* March 3, 2008, https://www.rferl.org/a/1079578.html.
[442] Reuters Staff, "Taliban orders mobile shutdown in Afghan province," *Reuters*, October 21, 2008, https://www.reuters.com/article/us-afghan-mobiles/taliban-orders-mobile-shutdown-in-afghan-province-idUSTRE49K2HS20081021.
[443] Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat."
[444] Indira A.R. Lakshmanan, "Fighting the Taliban with cell phones," *The New York Times*, March 23, 2010, https://www.nytimes.com/2010/03/24/world/asia/24iht-letter.html.
[445] Gilles Dorronsoro, *The Taliban's winning strategy in Afghanistan*.
[446] Andira A.R. Lakshmanan, "Fighting the Taliban with cell phones."

this time, targeting cell towers had "become a central part of the Taliban campaign."[447] In the lead up to the 2009 presidential elections, the Taliban enforced nighttime shutdowns, largely focused on the southern provinces.[448] The Taliban also charged protection fees to cell tower providers. If companies failed to pay, the Taliban would destroy their towers and network rigs.[449] Around the election, the Taliban destroyed 18 towers owned by Roshan, one of the primary telecom providers in Afghanistan, after they refused to pay the Taliban protection fines.[450]

By 2010, more companies adhered to the Taliban's shutdown demands. According to reporting, at least three telecom companies "strictly abide by Taliban hours in several provinces, going off air precisely at 5 p.m. and going back on at 6.30 a.m."[451] Telecom company Roshan turned off all of its towers in Helmand Province in 2010. At this time, it was reported that an informal agreement existed among all cell phone carriers in Afghanistan to "shut down their networks at night in areas where the insurgents are active."[452]

In spite of these shutdowns, analysts remarked on the "increasing use of mobile phone videos distributed by the Taliban."[453] In 2010, the U.S. special envoy to Afghanistan, Richard Holbrooke, stated, "We found that Afghans in the most-troubled, insurgent-held areas lived in information wastelands dominated by militant propaganda."[454] In an interview that same year,

---

447 Jacob N. Shapiro and David A. Siegel, "Coordination and security: How mobile communications affect insurgency"; Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat."

448 Robert M. Gonzalez, "Cell phone access and election fraud: evidence from a spatial regression discontinuity design in Afghanistan, *American Economic Journal: Applied Economics,* Vol. 13, No. 2 (2021), pp. 1-51.

449 Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 74.

450 Sheldon Himelfarb, "Can You Help Me Now?: Mobile Phones and Peacebuilding in Afghanistan," United States Institute for Peace, November 15, 2010, https://www.usip.org/publications/2010/11/can-you-help-me-now.

451 Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat."

452 Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat."

453 Sheldon Himelfarb, "Can You Help Me Now?: Mobile Phones and Peacebuilding in Afghanistan."

454 Andira A.R. Lakshmanan, "Fighting the Taliban with cell phones."

Zabihullah Mujahid, a Taliban spokesperson, emphasized the importance of ICT access for Afghans: "We believe that whatever benefits our people is in the interest of the Islamic Emirate. We won't prevent any mobile company from building new towers, because we know that the more the operators expand their networks, the more access our people will have to telecommunications services."[455] In 2010, the International Security Assistance Force (ISAF) spokesperson stated that, "cellphones are a powerful tool for the Taliban: They offer a cheap and effective means to direct insurgent activities or pass intelligence. At the same time, we are seeing Taliban attempts to deny regular Afghans access to this technology as a means of social control and operational protection."[456]

In March 2011, the Taliban ordered a two-week shutdown in cellular coverage in Helmand Province to prevent civilians from providing intelligence to NATO forces about their movements. This shutdown was respected by all of the private cellular network operators in Afghanistan.[457] A Taliban spokesman provided a rationale to international media, stating, "The leadership has decided to ban all telephone networks and this move is better for all residents of Helmand. Their spies provide information by cell phones which lead to civilian deaths." [458] This illustrates the careful balance the Taliban sought to strike with cell tower infrastructure: they needed to limit access, but totally eliminating the technology appeared too detrimental to other information needs and the relationship they had with the civilian population. As articulated by Dafoe and Lyall (2015), the Taliban also exhibited significant spatial variation in their approach to cell phones. Specifically, "In some cases, local Taliban have destroyed cell phone towers, either out of security considerations or

455 Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat."
456 Yaroslav Trofimov, "Cell Carriers Bow to Taliban Threat."
457 Associated Press, "Taliban turn cell phones back on in Afghan south, " *CTV News*, April 5, 2011, https://www.ctvnews.ca/taliban-turn-cell-phones-back-on-in-afghan-south-1.627627.
458 Ismail Sameem, "Taliban stop cell phone signals in key Afghan province," *Reuters,* March 24, 2011, https://www.reuters.com/article/afghanistan-taliban-phones/taliban-stop-cell-phone-signals-in-key-afghan-province-idUSL3E7EO12O20110324

from economic motives such as efforts to coerce telecommunications companies. In other regions, the Taliban have moderated their stance, allowing cell phone towers to operate during the day if they are turned off nightly. [....] In still other locations, the Taliban do not interfere with these towers at all. Instead, they have struck local bargains with these companies to receive funds – often in the guise of grants, work programs, or 'protection money' – in exchange for their cooperation in leaving the transmitters alone."[459] This approach likely reflects both the strategic costs and advantages of the technology and the semi-decentralized organizational structure of the Taliban at this time.

Beginning in 2009, in the face of the Taliban's growing violence and success, the U.S. sent additional troops to Afghanistan as part of a surge effort. The Taliban performed poorly during the surge, resulting in intra-organizational splintering. Consequently, the Taliban suffered losses in the following years: "of the first generation of Taliban commanders, few were still alive in 2014, even those in the northern province who had come late to the insurgency."[460] In 2015, the Taliban announced the death of leader Mullah Omar, months after it was publicly confirmed by Afghan security services.[461] His death, and the Taliban's cover up, resulted in a wave of desertions and exacerbated internal divisions.

However, by 2016, the Taliban had resumed and expanded their efforts. By 2018, the Taliban's attacks could be described as a "war of attrition, punctuated by assaults against cities, meant to demonstrate the Taliban's military proficiency even to the most distracted observers."[462] Negotiations between Taliban, U.S., and Afghan forces occurred throughout 2018 and 2019. On

[459] Allan Dafoe and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda."
[460] Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 121.
[461] Antonio Giustozzi, *The Taliban at War: 2001-2018*, p. 203.
[462] Thomas H. Johnson, "Taliban adaptations and innovations,"pp. 255-6.

February 29, 2020, the U.S. and the Taliban signed an agreement committing to U.S. force withdrawal from the country in 2021.[463] On April 14, 2021, U.S. president Joe Biden announced that the withdrawal would be completed by September 2021.[464]

The Taliban understood the power of ICT early on in their history, although its usage centered on bolstering their legitimacy to the international community. Instead, domestically they opted to control the information environment by eliminating the Afghan population's access to ICT, mirroring the strategies of other state actors.[465] As the conflict progressed, the Taliban integrated information operations and military activities, increasing the success of both. As described by one observer, "the more territory [the Taliban] captured or troops that surrendered, the more fodder it had for its propagandists; the more fodder it had for its propagandists, the more it could triumph on the battlefield before even firing a bullet."[466]

The Taliban Online

By 2005, many Taliban leaders "from the ranks of district commander upwards [were] equipped with laptops even when operating inside Afghanistan, where access to electricity [was] rare."[467] The same year, the Taliban launched an updated website, entitled Al-Emarah, a reference to the state they were seeking to reimpose, the Islamic Emirate of Afghanistan. This website was active

463 Thomas Clayton, "Afghanistan: Background and US Policy in Brief," *Congressional Research Service,* (2022).
464 Missy Ryan and Karen DeYoung, "Biden will withdraw all U.S. forces from Afghanistan by Sept. 11, 2021," *Washington Post*, April 13, 2021, https://www.washingtonpost.com/national-security/biden-us-troop-withdrawal-afghanistan/2021/ 04/13/918c3cae-9beb-11eb-8a83-3bc1fa69c2e8_story.html.
465 Simon Denyer, "China's scary lesson to the world: Censoring the Internet works," *Washington Post*, May 23, 2016, https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html; Adam Satariano and Valerie Hopkins, "Russia, Blocked From the Global Internet, Plunges Into Digital Isolation," *New York Times*, March 7, 2022, https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html.
466 Charlie Winter, Abdullah Alrhmoun, Abdul Sayed, "The Taliban's vast propaganda machine has a new target."
467 Antonio Giustozzi, *Koran, Kalashnikov, and Laptop: The Neo-Taliban Insurgency in Afghanistan 2002-2007*, p. 13.

throughout the takeover in 2021, offering content in five different languages: English, Arabic, Pashto, Dari and Urdu.[468] This website offered the Taliban an additional platform for propaganda, where they disputed casualty counts and claimed victories over NATO and U.S. forces.[469] The website was "divided into sections that include Islam, news, commentary, statements, poetry, taranas [chants], articles, books, magazines, and a link for the online Taliban Radio, Shar'iaht Voice."[470]

By 2008, the online environment began to more intensely supplement the Taliban's military operations, as the group regularly posted text updates and videos documenting (and often exaggerating) their successes. This included uploading content to Al-Emarah, where they "regularly post[ed] news updates from the field of battle with a decidedly pro-Taliban bias."[471]

In 2009, the Taliban's use of the internet became more sophisticated. The Taliban accused U.S. and NATO forces of peddling disinformation and encouraged the development of "Mujahedeen Support Groups" to counter the messaging and information campaign of Western forces.[472] They also created a YouTube account, entitled Istiqlal Media. This channel uploaded videos including "narrated montages of car bombings and gun battles set to music."[473] They also began to embed YouTube videos on their official Al-Emarah website(s) for the first time. The decision to use YouTube appears to reflect technical constraints, because "standard formats -- RMVB, AVI, MPEG -- have simply overloaded their web servers and exhausted their bandwidth [...]

---

468 Sarah Atiq, "The Taliban embrace social media: 'We too want to change perceptions'."
469 Emmerson Brooking, "Before the Taliban took Afghanistan, it took the internet."
470 Thomas H. Johnson, Matthew DuPee, and Wali Shaaker., *Taliban narratives: The use and power of stories in the Afghanistan conflict*, p. 85.
471 David Drissel, "Reframing the Taliban insurgency in Afghanistan: new communication and mobilization strategies for the Twitter generation."
472 Emmerson Brooking, "Before the Taliban took Afghanistan, it took the internet."
473 Joshua Keating, "The Taliban's YouTube channel," *Foreign Policy*, October 13, 2009, https://foreignpolicy.com/2009/ 10/13/the-talibans-youtube-channel/.

By turning to YouTube, the Taliban gain a free, highly-reliable video broadcast service with the potential to reel in a vast, viral audience."[474] At this time, the Al-Emarah website made use of a "complete multimedia package of voice, video and text."[475] They also added a share to Facebook feature on their website to encourage viewers to propagate their content to new platforms.[476]

In both 2011 and 2012, hackers targeted the Al-Emarah website. A Taliban spokesperson characterized the hack as an attack by enemies and foreign intelligence services: "The enemy tries to push its propaganda. The enemy is worried by what gets published on our webpage. It's confusing for them, so they try to react."[477] One hack involved replacing images on its website with videos of Taliban's atrocities. The Taliban appeared to have resolved these hacks relatively quickly.

By 2011, the Taliban had joined Twitter, publicly feuding with NATO public affairs officials on the platform.[478] This included personal attacks, including an incident where Taliban accounts made public mention of a NATO commander's mistress.[479] In 2011, the most active Taliban-linked Twitter account was that of their official website (@alemarahweb), which would primarily post English-language tweets.[480] By September of 2011, the account had 5,487 followers and had tweeted 1,700 times. The account followed only four other accounts, including @alsomood, which provided

474 Adam Rawnsley, "Taliban Steps Boldly in 2007, Invades YouTube," *WIRED,* October 13, 2009, https://www.wired. com/2009/10/taliban-steps-boldy-in-2007-invades-youtube/.
475 Ibid.
476 Emmerson Brooking, "Before the Taliban took Afghanistan, it took the internet."
477 Rob Taylor, "Taliban website hacked as Afghan cyber war heats up," *Reuters*, April 27, 2012, https://www.reuters .com/article/afghanistan-taliban-hacking/taliban-website-hacked-as-afghan-cyber-war-heats-up-idUSL3E8FR3X820120427.
478 Justin Hendrix, "Social Media and the Future of the Taliban," *Tech Policy Press*, August 20, 2021, https://techpolicy. press/social-media-and-the-future-of-the-taliban/.
479 Peter Warren Singer and Emerson T. Brooking, *LikeWar: The weaponization of social media*, (Eamon Dolan Books, 2018), p. 201.
480 Bashir Ahmad Gwakh, "The Taliban's Internet Strategy," *Radio Free Europe / Radio Liberty*, September 9, 2011, https://www.rferl.org/a/the_talibans_internet_strategy/24323901.html; Brooking, "Before the Taliban took Afghanistan, it took the internet."

updates on the Taliban's activities in Arabic. This account was linked to the personal Facebook account of Abdul Sattar Maiwandi, the web editor of a Taliban website. His public Facebook account would frequently post updates about suicide bombings and attacks on coalition forces. He also appeared to run a Facebook fan page for Mullah Omar, the leader of the Taliban.[481] The Taliban reportedly used social media to communicate with funders, sister organizations, and supporters. Due to the relatively limited use of the internet by Afghans at this time, the primary audience of public postings appeared to be the international community.

Throughout 2012, the group used Twitter to promote propaganda and relay information about military actions on the ground. From February to June, the Taliban tweeted to take "responsibility for IED strikes, sniper attacks, and grenade-based ambushes on both coalition forces and the Afghan Army in particular."[482] Their Twitter presence totaled at least 9 different accounts. These accounts also followed "the accounts of major news organizations, Afghan charities, the ANA, and even individual American and British soldiers."[483] From May to September 2012, the group engaged in English language messaging on Twitter, aimed at demoralizing Western audiences. Their messaging included propaganda and explicit disinformation, describing the "damage inflicted on ISAF forces" and using "terms like 'invader,' 'puppet,' or 'minion' to categorize individuals opposed to the Taliban."[484]

---

481 Ibid.
482 David Drissel, "Reframing the Taliban insurgency in Afghanistan: new communication and mobilization strategies for the Twitter generation," p. 114.
483 Ibid.
484 Vincent Bernatis, "The Taliban and Twitter: Tactical reporting and strategic messaging," *Perspectives on Terrorism*, Vol. 8, No. 6 (2014), pp. 25-35.

By 2013, the video quality of social media content improved significantly, including footage of active combat filmed by drones.[485] In 2014, several Taliban social media profiles appeared to have been removed by the platforms. These targeted removals and bans coincided with a period of external pressure facing platforms, including Facebook, YouTube, and Twitter, to remove content uploaded by another jihadist group, the Islamic State.[486] During attacks on the city of Kunduz in 2015 and 2016, Taliban fighters brought their cellphones to battle, sharing selfies on social media in the aftermath. Meanwhile, official Taliban accounts shared videos on Twitter as proof of their success, contradicting claims made by ISAF and Afghan forces downplaying the intensity of the attacks.[487]

The Taliban are documented to have first joined WhatsApp and Telegram in 2015.[488] In 2016, the Taliban launched a Pashto-language Android app, which was almost immediately deleted from Google Play store.[489] On November 1, 2017, the Afghan government banned Telegram and WhatsApp in the country citing security risks. This ban lasted for 20 days but failed in part due to public backlash resulting from the impact this ban had on civilians.[490]

Throughout 2018, both Taliban forces and the Afghan government used social media to advance messaging about the state of the conflict. The Taliban-created 'Islamic State of Afghanistan'

485 Emmerson Brooking, "Before the Taliban took Afghanistan, it took the internet."
486 Ibid.
487 Ibid.
488 Justin Hendrix, "Social Media and the Future of the Taliban" ; Mohammad Zahid, "Taliban selfies: Why militants posed for photos in Kunduz," *BBC*, September 30, 2015, https://www.bbc.com/news/world-asia-34387854.
489 Emmerson Brooking, "Before the Taliban took Afghanistan, it took the internet."
490 Ibid.; Ezzatullah Mehrdad, "How Citizen Uproar Halted Afghanistan's Ban on WhatsApp," *Fast Company,* November 21, 2017, https://www.fastcompany.com/40498985/after-citizen-uproar-afghanistan-ends-a-ban-on-whatsapp-and-telegram; Mozilla, "Resisting a WhatsApp and Telegram ban in Afghanistan," I*nternet Health Report*, April 2018, https://internethealthreport.org/2018/resisting-a-whatsapp-and-telegram-ban-in-afghanistan/.

Facebook page was reported to have received over 2,000 likes before being removed by the platform. Separately, individual Facebook accounts of Taliban members and supporters were active, sharing pro-Taliban messaging with "hundreds of friends" on the platform. These profiles were "loaded with hundreds of Taliban videos, photos, and narratives."[491] The Afghan government, recognizing the importance of social media, announced a 2018 ceasefire using Facebook. Meanwhile, during the spring offensive, Al Khandaq, a hashtag trended on Twitter highlighting Taliban actions and peaked the day prior to the October 2018 parliamentary elections.[492] A comparative analysis of Twitter activity from January to March, found that the Taliban tweeted at a higher rate and in more languages than Afghan Ministry of Defense accounts. Both sides made exaggerated claims of conflict-related damage inflicted on the other and posted "information that [was] not matched with or confirmed by mainstream media."[493] The Taliban also "categorically and stubbornly denied civilian casualties."[494]

Throughout 2019 and 2020, the Taliban made frequent use of Twitter to provide updates about battles, involving infographics and video clips.[495] The Taliban's Twitter presence also expanded to include more accounts: at least 50 Taliban-linked accounts were created in August and September of 2019.[496] During the 2019 election, the Taliban promoted specific hashtags and posted the same message across multiple Taliban-branded accounts. A DFR Lab investigation documented

[491] Thomas H. Johnson, Matthew DuPee, and Wali Shaaker, *Taliban narratives: The use and power of stories in the Afghanistan conflict*, p. 89.
[492] DFR Lab, "Suspicious Twitter accounts boosted Taliban hashtag prior to Afghan election," *Medium*, November 1, 2019, https://medium.com/dfrlab/suspicious-twitter-accounts-boosted-taliban-hashtag-prior-to-afghan-election-c303561713cf.
[493] Hazrat M. Bahar, "Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter."
[494] Ibid.
[495] Emmerson Brooking, "Before the Taliban took Afghanistan, it took the internet."
[496] DFR Lab, "Suspicious Twitter accounts boosted Taliban hashtag prior to Afghan election."

67 active Taliban accounts that tweeted amidst violent attacks leading up to the election on September 28, 2019. These tweets included hashtags included #AlFath, a reference to Al Fath Jihadi Operations, an offensive targeting Afghan governmental and military forces that began in April of 2018. The hashtag was used in association with tweets promoting false claims of Taliban victory in contested territories, including "parts of Khost, Jowzjan, Faryab, Paktika, Ghazni, Kunduz, Kapisa, Logar, Farah, Takhar, and Baghlan. Such location-specific hashtags seemed to reinforce the threat of Taliban control over places where its control is in fact weaker."[497] The English transliteration version of the hashtag was shared and used by Taliban accounts at a much higher rate than the Arabic version, which was primarily associated with Pashto language Tweets. This is a likely indicator that this information campaign was aimed at foreign audiences.

By November 2019, the Taliban's most successful Twitter account was that of its chief spokesperson and the editor-in-chief of the daily news bulletin, Zabiullah Mujahid (@Zabehulah_M33). At this time, he had tweeted over 81,400 times.[498] As described by a Taliban member, the process for developing tweets was fairly sophisticated, reportedly involving a:

> "team of writers to cross-check facts shared by some of the hardline Islamist groups fighters, who double as reporters in the 34 provinces across the country. The writers prepare press statements in five languages and gather footage and photographs shot on smartphones. The editor-in-chief then approves final drafts of the reports - highlighting the group's claimed

[497] Ibid.
[498] DFR Lab, "Suspicious Twitter accounts boosted Taliban hashtag prior to Afghan election."

victories in its war aimed at toppling the U.S.-backed Afghan government - before they are published by IT specialists based outside the country."[499]

By 2019, the Taliban published "six magazines in Pashto, Dari, Urdu and Arabic, and post [...] news reports on 10 websites in five languages, as well as operating smaller websites that offer theological guidance, videos, and war poetry written by fighters."[500] The reported annual cost of their information operations was 25 million Afghanis, roughly $323,000 USD, in 2019. Designated spokesmen were tasked with international media engagement, reportedly responding to news correspondents over WhatsApp within an hour.[501]

By 2020, the Taliban's information campaigning was led by a specialized media and communications wing. This group was reportedly led by Qari Saeed Khosty. Khosty has a personal Twitter account, created in 2015, which as of February 2022 had amassed close to 190,000 followers. His Twitter biography included a link to a personal website, qarisaeed.com. The media wing's efforts were also supported by Zabihullah Mujahid. As of February 2022, Mujahid has amassed close to half a million followers. Both accounts publish photos and videos glorifying the Taliban and attacking their opponents. This leadership team oversees "audio, video and written content" propagated on behalf of the Taliban across mediums and technologies. This division is staffed by a "dedicated team of volunteers promoting the Taliban's ideology online."[502] The team also engages in direct oversight on the type of content that can be shared by supporters; this included a set of specific

499 Abdul Qadir Sediqi, "Taliban fighters double as reporters to wage Afghan digital war," *Reuters,* May 10, 2019, https://www.reuters.com/article/us-afghanistan-taliban-media/taliban-fighters-double-as-reporters-to-wage-afghan-digital-war-idUSKCN1SH035.
500 Ibid.
501 Ibid.
502 Sarah Atiq, "The Taliban embrace social media: 'We too want to change perceptions'."

guidelines, "not to comment on the foreign policy issues of neighboring countries that would constrain our relations with them."[503] As of 2021, this team reportedly paid 1,000 Afghanis ($11.51 USD) per month for online data access, and possesses "four fully equipped multimedia studios that are used for generating audio, video content and digital branding." [504] This allowed the group to upload high-quality videos to their YouTube channels and the group's website, Al-Emarah.[505]

Quantitative Analysis: Twitter Activity During the 2021 Takeover

In the months prior to the Taliban's takeover of Afghanistan in 2021, the group weaponized a variety of social media platforms to propagate their messaging. These platforms included WhatsApp, Facebook, and Twitter. The Taliban's websites also remained active throughout the takeover. The group's primary website, Al-Emarah, and its multi-language versions, were supported by an American website security and infrastructure provider, CloudFlare, who only revoked access after public backlash in the aftermath of the takeover in August.[506] The Taliban's information campaign at this time involved training and equipping "soldiers with microphones and smartphones to report from the front lines as their forces swept into new territory."[507] The messaging itself emphasized the inevitability of victory and the group's utopian vision of life under their rule.

503 Ibid.
504 Ibid.
505 Ibid.
506 April Glaser, Kevin Collier and Cyrus Farivar, "Some Taliban websites go offline amid broader tech crackdown," *NBC News*, August 20, 2021, https://www.nbcnews.com/tech/tech-news/taliban-websites-go-offline-broader-tech-crackdown-rcna1735; Craig Timberg, "Taliban websites operating in five languages go dark," *The Washington Post*, August 20, 2021, https://www.washingtonpost.com/technology/2021/08/20/taliban-internet-websites-twitter-facebook/.
507 Paul Mozur and Zia ur-Rehman, "How the Taliban Turned Social Media Into a Tool for Control," *The New York Times*, August 20, 2021, https://www.nytimes.com/2021/08/20/technology/afghanistan-taliban-social-media.html.

Beginning in May, Taliban accounts pushed out specific hashtags on Twitter, including "#kabulregimecrimes (attached to tweets accusing the Afghan government of war crimes); #westandwithTaliban (an attempt to drive grassroots support) and #نَصْرٌ_مِّنَ_اللهِ_وَفَتْحٌ_قَرِيب (help from God and victory is near)."[508] The Taliban's primary spokesman, Zabiullah Mujahid (@Zabehulah_M33), tweeted an average of 21 times per day between March and August 2021. Analysis of this account also provided evidence of the Taliban using Twitter to shape the information environment before, during, and after key battles. For example, Zabiullah tweeted warnings that the Taliban were rapidly advancing on the city of Mazar-i-Sharif beginning on August 9. The city was eventually captured on August 14. The account also highlighted the group's capture of other cities on the way to Kabul, including Pul-e-alam and Maidan Wardak.[509] Recognizing the potential impact of this influence campaign, Afghan Vice President Amrullah Saleh "warned his forces and the public not to fall for false claims of Taliban victories on social media, and called on people to avoid sharing details of military operations that could compromise security." [510] Taliban messaging was also amplified by a supportive ecosystem using the tactic of "copypasta," wherein other accounts copy and tweet identical messages. One such tweet was posted on August 15, stating "everyone in Kabul, including foreigners and diplomatic mission personnel, were safe and that the Taliban would maintain peace."[511]

[508] Sarah Atiq, "The Taliban embrace social media: 'We too want to change perceptions'."
[509] DFR Lab, "As the Taliban offensive gained momentum, so did its Twitter propaganda campaign," *Medium*, August 19, 2021, https://medium.com/dfrlab/as-the-taliban-offensive-gained-momentum-so-did-its-twitter-propaganda-campaign-75021ba3082.
[510] Sarah Atiq, "The Taliban embrace social media: 'We too want to change perceptions.'"
[511] DFR Lab, "As the Taliban offensive gained momentum, so did its Twitter propaganda campaign," *Medium*, August 19, 2021, https://medium.com/dfrlab/as-the-taliban-offensive-gained-momentum-so-did-its-twitter-propaganda-campaign-75021ba3082.

Crucially, Twitter was one of the only mainstream social media companies that permitted the group to operate on their platform. Whereas Facebook, WhatsApp, YouTube, took explicit stances that any Taliban-affiliated account would be removed, Twitter stated that they would only take action against content posted by the Taliban in violation of existing policies.[512] This decision proved consequential, as the Taliban had invested considerable focus and resources in developing an information campaign on Twitter. In speaking with BBC reporters, a member of the Taliban's social media team stated, "Most Afghans don't understand English, but the leaders of the Kabul regime actively communicated in English on Twitter - because their audience is not Afghans but the international community. The Taliban wanted to counter their propaganda and that's why we too focused ourselves on Twitter."[513]

After the takeover on August 15, 2021, Taliban leaders "put out messages in English and livestreamed press events," in a bid to gain legitimacy and acceptance among foreign audiences.[514] They also relied on an encrypted messaging platform, WhatsApp, to communicate with Afghan civilians, each other and journalists. They reportedly set up specific numbers for a complaints commission, where civilians could report issues after takeover.[515] They used Twitter to disseminate a positive vision of their governance that included: "images and videos of [Taliban] leaders posing with Ismail Khan, a well-known local commander and Taliban opponent, showing him unrestrained

[512] BBC, "Afghanistan: Facebook Continues Ban of Taliban-Related Content," *BBC*, August 17, 2021, https://www.bbc.com/news/business-58239786; Bhaskar Chakravorti, "Facebook's Taliban Ban Will Prove Costly for Afghans," *Foreign Policy,* August 26, 2021. https://foreignpolicy.com/2021/08/26/taliban-facebook-ban-social-media-afghanistan/; Elizabeth Culliford, "YouTube Says It Does Not Allow Taliban-Affiliated Accounts," *Reuters*, August 17, 2021, https://www.reuters.com/technology/youtube-says-it-bans-accounts-believed-be -owned-by-taliban-2021-08-17/; Shirin Ghaffary, "How Facebook, Twitter, and YouTube Are Handling the Taliban." *Vox*, August 18, 2021, https://www.vox.com/recode/22630869/facebook-youtube-twitter-taliban-ban-social-media-afghanistan; Naomi Nix and Bloomberg, "Facebook and Twitter Weigh Giving a Social-Media Megaphone to the Taliban," *Fortune*, August 21, 2021, https://fortune.com/2021/08/21/facebook-twitter-social-media-taliban/.

[513] Sarah Atiq, "The Taliban embrace social media: 'We too want to change perceptions.'"

[514] Paul Mozur and Zia ur-Rehman, "How the Taliban Turned Social Media Into a Tool for Control."

[515] Gavin Butler, "How Social Media Helped 'Taliban 2.0' Take Control of Afghanistan."

and appearing at ease," and a video of a young boy discussing how happy he is in an interview with a Taliban 'reporter' holding a microphone with the group's logo.[516] News outlets across the globe stressed the role of social media in supporting the Taliban's operations during this period.[517]

Building on this preliminary documentation conducted by journalists and policy analysts, this research intends to provide a more robust analysis of the scope and scale of the Taliban's use of Twitter during the 2021 takeover.

Methods

This research pursues an actor-based approach to social media analytics, engaging in both content and trend analysis of the Taliban's content.[518] Using Twitter's academic research application programming interface (API), tweets from a core set of 63 Taliban-linked Twitter accounts were downloaded. From April 1 to September 16, 2021, these accounts produced 112,354 tweets, including retweets. These accounts also posted content in four languages: English, Pashto, Dari, Urdu.[519] This timeline was selected to provide a baseline activity prior to the U.S. president's announcement of military withdrawal on April 14, as well as data on their activity after the takeover on August 15. Accounts qualified for inclusion in the core network if they met at least one of the following inclusion criteria: (1) the account bio explicitly stated the individual's affiliation with

---

516 Paul Mozur and Zia ur-Rehman, "How the Taliban Turned Social Media Into a Tool for Control."

517 Gavin Butler, "How Social Media Helped 'Taliban 2.0' Take Control of Afghanistan," *VICE News*, August 19, 2021, https://www.vice.com/en/article/z3x5we/social-media-helped-taliban-control-afghanistan; Paul Mozur and Zia ur-Rehman, "How the Taliban Turned Social Media Into a Tool for Control," *The New York Times*, August 20, 2021. https://www.nytimes.com/2021/08/20/technology/afghanistan-taliban-social-media.html.

518 Stefan Stieglitz and Linh Dang-Xuan, "Social media and political communication: a social media analytics framework," Social network Analysis and Mining, Vol. 3, No. 4 (2013), pp. 1277-1291. For research with similar methods, see Alexandra A. Siegel and Joshua A. Tucker. "The Islamic State's information warfare: Measuring the success of ISIS's online strategy." Journal of language and politics 17, no. 2 (2018): 258-280.

519 This data was also published as a working paper, see Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30," *Empirical Studies of Conflict Project* (2022).

and/or role within the Taliban (or the Islamic Emirate of Afghanistan), (2) the profile image or banner included images of the Taliban's flag, logo, or photos of high-ranking members, (3) the account included a link to the Al-Emarah website in their profile bio (this was a common feature of accounts claiming to be 'journalists,' despite exclusively writing content for the Taliban's website), and/or (4) repeatedly and primarily posted pro-Taliban content, including insider videos and messages on behalf of the group. By September 2021, this network of 63 accounts had cumulatively amassed more than two million followers on Twitter.

While the Taliban used other social media platforms and websites, analyzing their Twitter behavior is important for four reasons: (1) Twitter explicitly permitted the Taliban to operate openly on their platform during this period.[520] This contrasts policy and moderation decisions made by Facebook and Google to target and remove Taliban-associated content and accounts. (2) Members of the Taliban's social media team have stated in interviews with journalists that the group intentionally invested in developing a Twitter presence to develop an international audience.[521] (3) Initial evidence suggests Twitter acted as the Taliban's primary online platform during the takeover, with the average Taliban Twitter account producing 23 times more content than the average Taliban Facebook page.[522] And (4) from a data collection standpoint, Twitter's academic research application

520 BBC, "Afghanistan: Facebook Continues Ban of Taliban-Related Content," *BBC*, August 17, 2021, https://www.bbc.com/news/business-58239786; Bhaskar Chakravorti, "Facebook's Taliban Ban Will Prove Costly for Afghans," *Foreign Policy,* August 26, 2021. https://foreignpolicy.com/2021/08/26/taliban-facebook-ban-social-media-afghanistan/; Elizabeth Culliford, "YouTube Says It Does Not Allow Taliban-Affiliated Accounts," *Reuters*, August 17, 2021, https://www.reuters.com/technology/youtube-says-it-bans-accounts-believed-be -owned-by-taliban-2021-08-17/; Shirin Ghaffary, "How Facebook, Twitter, and YouTube Are Handling the Taliban." *Vox*, August 18, 2021, https://www.vox.com/recode/22630869/facebook-youtube-twitter-taliban-ban-social-media-afghanistan; Naomi Nix and Bloomberg, "Facebook and Twitter Weigh Giving a Social-Media Megaphone to the Taliban," *Fortune*, August 21, 2021, https://fortune.com/2021/08/21/facebook-twitter-social-media-taliban/.

521 Sarah Atiq, "The Taliban embrace social media: 'We too want to change perceptions.'"

522 Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30," *Empirical Studies of Conflict Project* (2022).

programming interface (API) allows for the collection and analysis of data from individual Taliban accounts in ways that are not currently possible on other platforms such as Facebook or YouTube.

The goal of this analysis is to provide initial insight into the ways in which the Taliban weaponized Twitter (and its platform features) to advance its messaging throughout their military takeover of Afghanistan. To achieve this, I analyzed this data to observe frequency of tweeting over time, engagement with Taliban content over time, the accounts mentioned in Taliban tweets, the hashtags used by the Taliban to amplify content, the geographic locations specified in Taliban tweets with comparison to on-the-ground activity, and Taliban discussion of major powers (namely, the U.S., Russia, and China). This analysis primarily pursues a descriptive approach because it is the first step in establishing the scope and scale of the Taliban's online behavior and how it might connect with military action in the real world. Existing studies on the Taliban's online presence (and most other studies of non-state armed groups on social media) predominantly engage in rhetorical analysis, focusing on narratives and messaging.[523] They fail to establish a sense of the group's strategies in using and deploying the technology. While discussion of the specific narrative frames promoted by the Taliban is included (see Appendix 1 for additional analysis of the Taliban's English-language rhetoric surrounding U.S. forces), this analysis principally focuses how the Taliban leveraged the platform's infrastructure to amplify their content, the intensity of the information campaign throughout the takeover, the online record of the group's military operations during the summer.

[523] See Vincent Bernatis, "The Taliban and Twitter: Tactical reporting and strategic messaging";
Hazrat M. Bahar, "Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter"; David Drissel, "Reframing the Taliban insurgency in Afghanistan: new communication and mobilization strategies for the Twitter generation."

Results

Between April 1 and September 16, 2021, the 63 Taliban-linked accounts produced 112,354 tweets, of which 66,736 were original posts. The remaining tweets consisted of retweets, replies, or quote tweets. These 63 Taliban-linked accounts produced an average of 4,494 tweets per week. Unsurprisingly, the Taliban produced the highest number of tweets during the week of August 15, when the group took Afghanistan's capital of Kabul. During this week, the group produced more than twice the average, totaling 10,201 tweets.

Table 1 provides a brief overview of key dates leading up to the Taliban's takeover of Afghanistan, beginning with U.S. President Biden's announcement of the timeline of U.S. troop withdrawal on April 14 and ending with the Taliban's conquest of Kabul on August 15.

Table 1. Timeline of 2021 Taliban Takeover of Afghanistan[524]

Key Dates	Event
April 14	President Biden announces troop withdrawal
May 2	Taliban launch major offensive against Afghan forces in Helmand province
May 11	Taliban capture Nerkh District in Wardak Province
June 7	Taliban capture Dawlat Abad District in Faryab Province
June 8	Attacks and fights in Nangarhar, Khost, Maidan Wardak, Logar, Faryab, Pakita, Ghor, Sar-e-Pul, Badghis, Ghazni, Uruzgan, Baghlan, Kunduz and Helmand Provinces
June 13	Taliban attacked a security outpost in Shulgara district in Balkh Province. Launched large-scale attack on security checkpoints in Baharak, Namak-e-Ab, Darqad and Yingi Districts of Takhar Province.

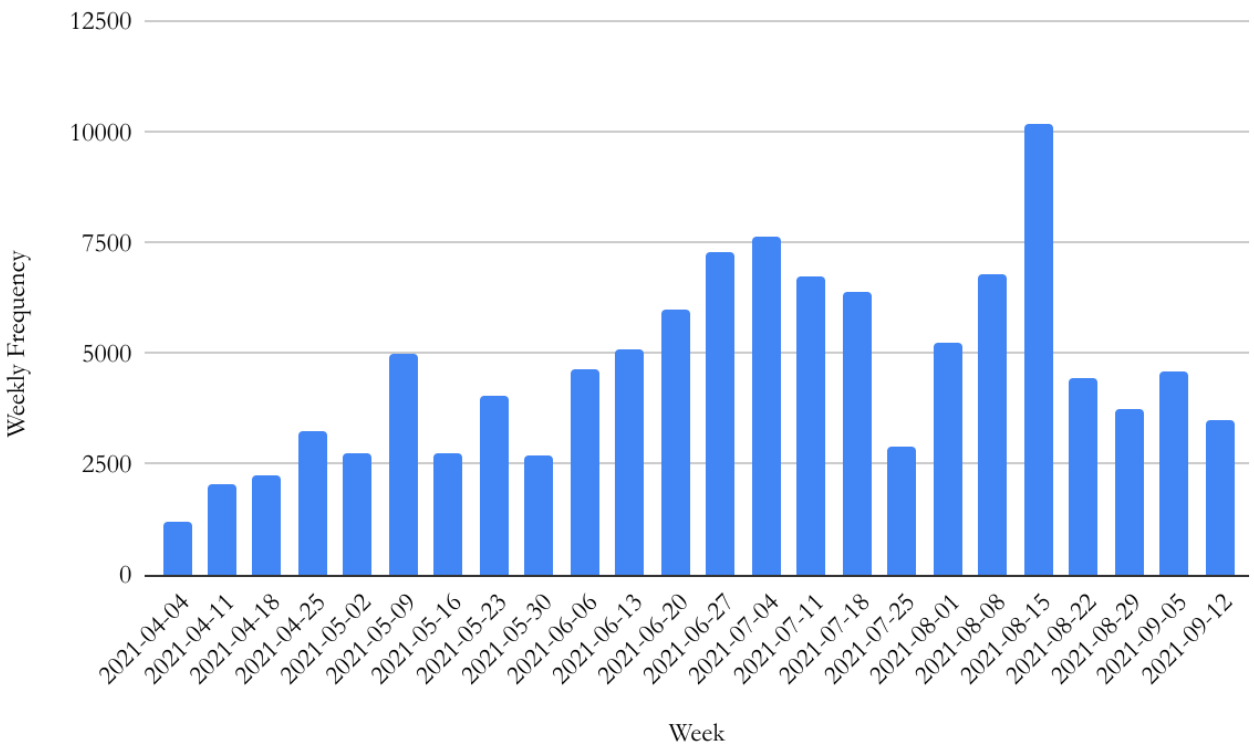
[524] See Reuters, "Timeline: The Taliban's rapid advance across Afghanistan," *Reuters*, August 15, 2021, https://www.reuters.com/world/timeline-talibans-rapid-advance-across-afghanistan-2021-08-15/; "Afghanistan: Incidents and Statements involving Taliban : 2021," South Asia Intelligence Review, https://www.satp.org/terrorist-incident-text/afghanistan/taliban_Aug-2021.

June 14	Taliban capture Anar Dara District in Farah Province, Khas Uruzgan District in Uruzgan Province, and Gosfandi and Sayyad Districts in Sar-e-Pul Province. Total captured districts now at 33.
June 18	Taliban capture Dahana-i-Ghori District in Baghlan Province, Awba District in Herat Province and Shireen Tagab District in Faryab Province.
June 19	Taliban take 17 districts in eight provinces.
June 21	Taliban take 13 districts in eight provinces.
June 24	Taliban take Khost Firing and Guzargah-e-Noor districts in Baghlan Province. They also captured the centers of seven Districts in Faryab, Baghlan, Uruzgan, Logar and Ghazni Provinces/
June 25	Taliban capture Dolina District in Ghor Province.
June 26	Taliban captured five districts: Shor Tapa in Balkh Province, Chak and Sayed Abad in Maidan Wardak Province, Rustaq in Takhar Province and Arghistan in Kandahar Province.
June 27	Taliban captured the centers of four districts in Ghazni and Paktika provinces.
June 28	Key Taliban commander killed in Helmand province. Two districts, Khakriz in Kandahar and Baraki Barak in Logar, were captured.
June 29	Taliban capture the centers of four districts in four provinces.
June 30	Taliban capture the center of Tagab District in Kapisa Province.
July 2	U.S. forces leave Bagram Air Base. Taliban capture 13 districts in four provinces.
July 3	Taliban capture the centers of 9 districts in four provinces.
July 4	Taliban captured 11 districts in three provinces.
July 8 - 16	Major clashes between Afghan government and Taliban forces, resulting in high Taliban casualties. Taliban captures Taiwara and Pasaband Districts in Ghor Province.
July 22	Taliban capture Ghazi Abad District in Kunar Province.
July 25 - 27	Major clashes between Afghan government and Taliban forces, resulting in high Taliban casualties.
July 27 - 28	Taliban delegation visits China.
July 28 - 31	Major clashes between Afghan government and Taliban forces, resulting in high Taliban casualties.
August 1 - 5	Major clashes between Afghan government and Taliban forces.

August 6	Taliban took provincial capital Zaranj
August 7	Taliban capture Sheberghan city, the provincial capital of Jawzjan Province.
August 8	Taliban capture Sar-e-Pul city, the provincial capital of Sar-e-Pul province and Kunduz city, the provincial capital of Kunduz Province.
August 9	Taliban capture Taloqan city, the provincial capital of Takhar Province.
August 12 - 13	Taliban takeover four provincial capitals, including Kandahar
August 14	Taliban take northern city of Mazar-i-Sharif and Pul-e-Alam, capital of Logar province
August 15	Taliban take Jalalabad and enter Kabul

Figure 1 provides an overview of the Taliban's weekly activity levels on Twitter throughout the period under review.

Figure 1. Weekly Tweet Count by Taliban-Linked Accounts (April 1 - September 16)[525]



[525] This data was also published as a working paper, see Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30." Data from April 1 - 3 have been lumped in with the week of April 4. The week of

As illustrated in Figure 1 and Table 1, the Taliban's online activity appears to have some correlation with key events during the takeover. In comparing Figure 1 with the key dates outlined in Table 1, the data has several notable peaks. These peaks include:

1. A small peak during the week of April 25, likely reflecting discussion of the U.S.'s failure to meet the previously established May 1 deadline for total withdrawal.[526] Further evidence of this specific narrative can be found in Appendix 1.
2. Another peak occurs during the week of May 9. This correlates with the Taliban's major ongoing offensive in Helmand and the group's capture of their first district, Nerkh in Wardak Province.
3. The weeks of July 4 and June 27 had the second and third highest tweet counts, respectively. These weeks mark an uptick in the scope and intensity of the conflict between Taliban and Afghan military forces during the takeover. At the end of June, Taliban forces had quickly captured critical cities in several provinces.
4. The week of August 15 final capture of the country, and arrival in Kabul); highest peak on August 15.

Figure 1 additionally highlights differences in online activity levels before, during, and after the Taliban's military operations during the summer takeover. The average weekly tweet volume from April 1 to May 1 was 2,189. From the start of major clashes in early May through the capture of Kabul on August 15, Taliban accounts tweeted an average of 5,385 times per week (closer to 5,000 if the week of August 15 is excluded). Once the Taliban took power, the group's Twitter activity decreased, averaging 4,069 tweets per week from August 22 through September 16. This

526 Fatima Faizi, Fahim Abed and Najim Rahim, "Afghan War Casualty Report: May 2021," *The New York Times*, June 3, 2021, https://www.nytimes.com/2021/05/06/world/asia/afghan-war-casualty-report-may-2021.html.

may provide some indication of the kind of content the Taliban believed was most important to emphasize and propagate.

Table 2 and Figure 2 highlights the level of engagement the Taliban received on their content. Taliban tweets received close to 7 million likes and over 350,000 replies during the period under review. These tweets were retweeted close to 1 million times and quote tweeted (reshared to a user's account with added commentary) over 90,000 times. In August of 2021, over 2 million users followed these 63 accounts. Establishing the Taliban's engagement is a first step in understanding the efficacy of the campaign. The Taliban's Twitter content appeared to enjoy considerable engagement by its audience. For context, Twitter identified 3,841 Russian-linked accounts that sought to amplify an incendiary influence campaign during the 2016 U.S. presidential election. Content produced by these accounts received comparatively less engagement than the Taliban by their target audience: a total of 1.4 million U.S. users were notified by Twitter for having liked, retweeted, replied to, mentioned or followed these Russian linked accounts.[527] Excluding followers, the Taliban received over 8.3 million interactions during the period under review.

Table 2. Summary Statistics - Engagement with Taliban Tweets (April 1, 2021 - September 16, 2021)[528]

Form of Engagement	Count
Quote Tweets	93,937
Replies	387,184

[527] Ashley Gold, "Twitter: More than 677,000 U.S. users engaged with Russian troll accounts," *Politico*, January 19, 2018, https://www.politico.com/story/2018/01/19/twitter-users-russian-trolls-437247; Twitter Public Policy, "Update on Twitter's review of the 2016 US election," *Twitter Blog*, January 19, 2018, https://blog.twitter.com/official/en_us/topics/ company/2018/2016-election-update.html.

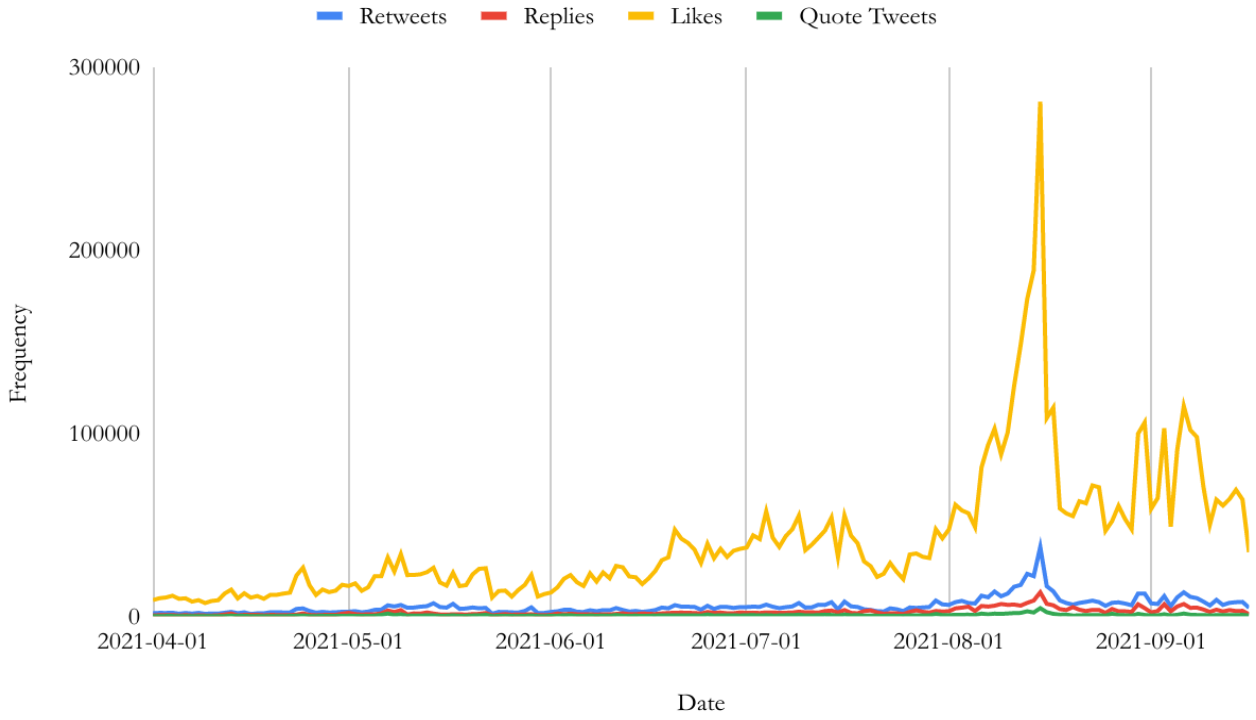
[528] This data was also published as a working paper, see Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30."

Retweets	940,688
Likes	6,928,223

Engagement with the 63 Taliban-controlled accounts saw a steady increase between April and early August 2021, before a massive spike in mid-August, which corresponded to the takeover of Kabul (see Figure 5). Unsurprisingly, the group received the highest number of likes on August 15 (280,906), followed by August 14 (188,790), August 13 (173,199), and August 12 (148,133). Across forms of engagement, the Taliban received the highest level of engagement during the group's final military push towards Kabul. Interestingly, average daily engagement became much higher in the aftermath of the takeover. For instance, from April 1 through August 14 the average daily retweet count was 4,635 and the average daily like count was 32,118. After the takeover on August 15, from August 16 through September 16, the average daily retweet count was 8,518 and the average daily like count was 71, 228. This massive increase in engagement may be due to the permissibility of openly supporting the Taliban when they became the governing authority of Afghanistan. Another possible explanation may be Afghan sentiment that the Taliban were monitoring their online activity. Fearing reprisals, many Afghans began to remove old tweets or delete their social media presence altogether after the group took power.[529]

[529] Khudai Noor Nasar, "Afghanistan: Social media users delete profiles over fear of attack," *BBC*, September 27, 2021, https://www.bbc.com/news/world-asia-58710194; Chris Stokel-Walker, "Afghans are racing to erase their online lives," *WIRED*, August 17, 2021, https://www.wired.co.uk/article/afghanistan -social-media-delete.

Figure 2. Daily Engagement on Taliban-Linked Tweets (April 1 - September 16)[530]



In addition to likes and replies, Figure 3 highlights mentions of Taliban accounts and retweets of Taliban content. The yellow line (labeled Taliban-authored) highlights when accounts within the 63 core account dataset retweeted or mentioned other accounts within this network, highlighting a potential content amplification tactic.. Engagement over those four months involved 1,508,701 mentions of Taliban accounts. Mentions are a good indicator of the degree to which Taliban messaging was seen by users who were not following the core network of Taliban accounts. While not all mentions necessarily represent support (for example, a user may mention a Taliban account in a tweet criticizing their behavior or ideology), 62% (939,529) of them were retweets, all of which directly amplified Taliban messaging. Engagement peaked on August 15, with 57,159

[530] This data was also published as a working paper, see Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30."

mentions of Taliban accounts, 37,753 of which were retweets. Mentions followed a similar pattern to likes and replies, with mentions peaking on August 15 and remaining high for the following weeks through September.

Figure 3. Mentions of the Taliban and Taliban-Authored Tweets (April 1 - September 16)[531]

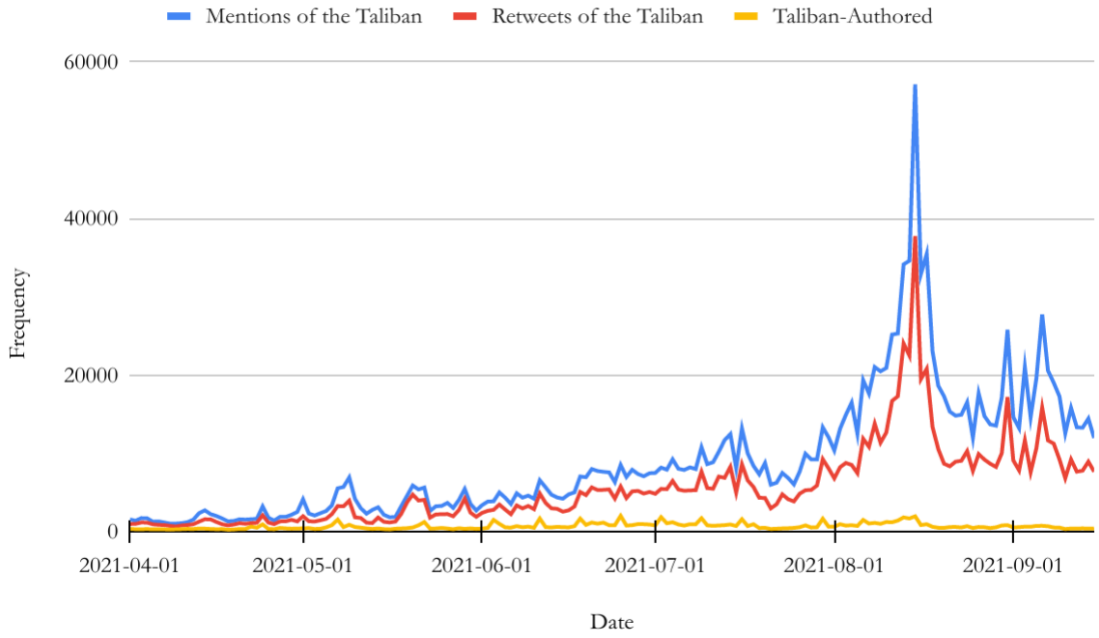


Figure 4 highlights the account creation dates of the 63 Taliban-linked accounts. This figure highlights that during the takeover, the Taliban primarily relied on pre-existing accounts that had been created long before this military operation. 52 (82%) Taliban accounts were created and actively tweeting content on behalf of the group before 2021. This helps to provide insight on how Taliban content has been moderated by Twitter and the group's investment in developing assets on Twitter prior to the takeover. From this data, it appears that the group did not need to build new assets in preparation for their use during the summer takeover, but rather they could rely on existing accounts with pre-built followings. In line with other reports, the Taliban has been active on Twitter

[531] This data was also published as a working paper, see Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30."

since at least 2011 and interestingly, many (40%) had been active on Twitter for at least two years prior to the takeover. The longevity of these accounts on the platform is important to underscore and presents a key question: given recent efforts to target jihadist-linked groups operating online (such as the Islamic State), how were the Taliban able to operate in the open for so many years?

Figure 4. Creation Dates of Taliban Accounts[532]

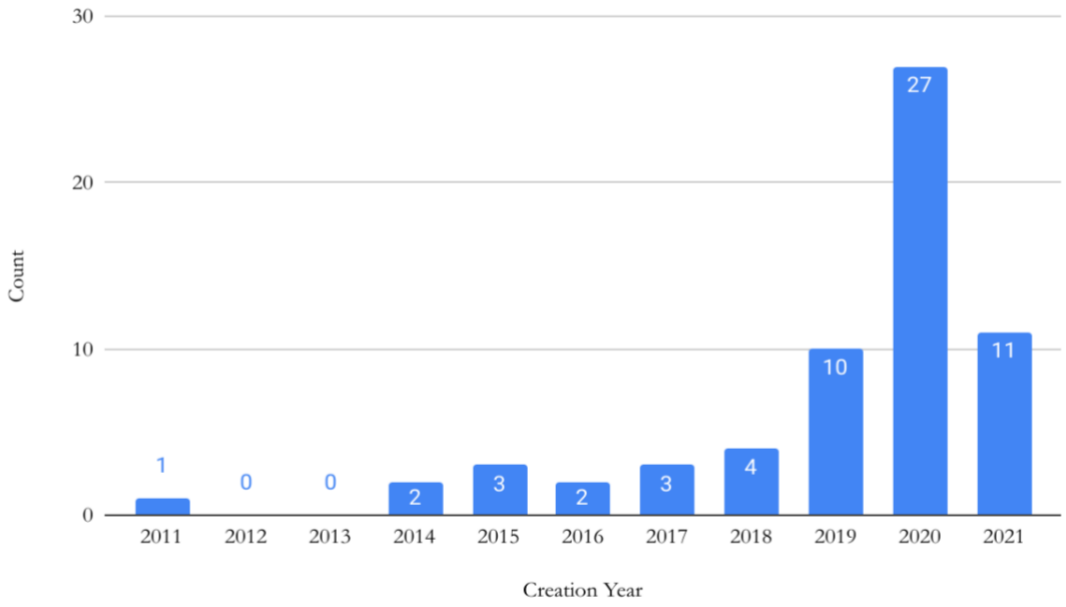


Table 3 provides an overview of the top 25 hashtags used by Taliban-linked accounts. Hashtags help to promote content on the platform, allowing users to search content from different accounts labeled under a particular hashtag. This is an important tool for amplification of Taliban accounts beyond their immediate network of followers. Within the dataset, hashtags were used 48,826 times. The Taliban created and used 4,128 distinct hashtags on their posts. Almost half (44%) of the most commonly used hashtags were in English. The most common hashtag was #الفتح, a Pashto word that means victory. An English transliteration of this word, Al-Fath, was used previously as a hashtag, designating the name of a Taliban offensive in 2019.[533] Other common

[532] This data was also published as a working paper, see Laura Courchesne, Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30."
[533] DFR Lab, "Suspicious Twitter accounts boosted Taliban hashtag prior to Afghan election."

hashtags included #KabulRegimeCrimes, which were used in tweets highlight accusations of American, NATO, and Afghan forces engaging in war crimes and human rights abuses, #WLC2DeceivedSoldier, which was used in tweets encouraging Afghan soldiers to defect and join the Taliban and #Helmand Massacre, referencing an apparent attack on civilians by Afghan and American forces. Taliban hashtags can be categorized by function, amplifying and connecting content that shared a similar rhetorical goal: villainizing their opponents (#kabulregimecrimes, #helmandmassacre), promoting positive depictions of the Taliban and their proposed regime (#talibanourguardians, #lifeundrcontroloftaliban, #westandwithtaliban), and highlighting military victories ((Victory) #الفتح , (Our soldiers are blessed by God) #عسکرو_خدای_مو_راوله, (Victory is near and from God) #نَصْرٌ_مِّنَ_اللهِ_وَفَتْحٌ_قَرِيب, #successesoftaliban). For hashtags included in tweets focused on U.S. forces and English-speaking audiences, see Appendix 1.

Table 3. Hashtags Used by Taliban Accounts (Top 25)

Hashtag	Frequency in Taliban Tweets	English Translation
#الفتح	4673	"Al-Fath; victory"
#kabulregimecrimes	3163	
#wlc2deceivedsoldier	1814	
#helmandmassacre	1798	
#طالبان	1677	"Taliban"
#talibanourguardians	1456	
#wewantislamicsystem	1331	
#shaheedameerulmomineen	1160	Shaheed is the English transliteration of an Arabic word that means martyr. Amir al-Mu'minin is the Arabic title for the supreme leader of an Islamic community. Associated with posts about Akhtar Mansoor, second leader of the Taliban, killed

		in 2016.
#عسکرو_خدای_مو_راوله	1096	“Our soldiers are blessed by God”
#عاجل	1079	“Urgent”
#taliban	1054	
#lifeundrcontroloftaliban	1043	
#شهیدامیرالمؤمنین	961	"Martyr Amir al-Mu'minin." Amir al-Mu'minin is the Arabic title for the supreme leader of an Islamic community. Associated with posts about Akhtar Mansoor, second leader of the Taliban, killed in 2016.
#تازه	820	“Latest/New/Fresh”
#talibanleadermessage	744	
#successesoftaliban	732	
#westandwithtaliban	692	
#afghanistan	594	
#جنایت	560	“Crime”
#ویډیو	474	“Video”
#أفغانستان	468	“Afghanistan”
#نَصْرٌ_مِّنَ_اللهِ_وَفَتْحٌ_قَرِيب	466	“Victory is near and from God”
#نن_د_عفوې_ورځ_ده	292	“Pardons today”
#هلمند	269	“Helmand”
#jihadisttraining	266	

Table 4 provides a list of the top twenty-five most commonly mentioned accounts in Taliban tweets. Mentions are another tool for amplification of content. Accounts that are mentioned in

Taliban tweets are effectively tagged in the post and typically receive a notification that prompts them to view the tweet. Users searching for content associated with a mentioned account are also exposed to these tweets. 6,593 accounts were mentioned in Taliban tweets and mentions were used 51,828 times. Mentions appeared to serve four key functions: (1) to tag other key Taliban accounts of senior leaders or avid supporters, who then retweeted and amplified the content, (2) to tag key members of the Afghan government, including President Ashraf Ghani and senior members of his team, (3) to tag news organizations, such as TOLOnews and Al Jazeera, in hopes that they would report on the content the Taliban shared, and (4) to tag humanitarian organizations, including the Human Rights Watch, to call attention to what they deemed to be 'war crimes' perpetrated by U.S. and Afghan forces. Beyond the top 25, other commonly mentioned accounts included that of the U.S. President, BBC News, the New York Times, CNN, ABC News, and the International Criminal Court. For mentions included in tweets focused on U.S. forces and English-speaking audiences, see Appendix 1.

Table 4. Accounts Mentioned in Taliban Tweets (Top 25)

Mentioned Username	Frequency of Account Mention in Taliban Tweets	Account Description
@zabehulah_m33	2608	Official Twitter Account of the Spokesman of Islamic Emirate of Afghanistan, Zabihullah Mujahid
@ieaoffice	845	Spokesman of the Political Office of the Islamic Emirate of Afghanistan
@saeedkhosty	780	Taliban spokesman, Qari Saeed Khosty
@ashrafghani	475	President of the Islamic Republic of Afghanistan, Ashraf Ghani
@qyahmadi21	448	Taliban spokesman, Qari Yousaf Ahmadi
@akhundzada111	411	Taliban member and supporter

@wasiqahmadullah	385	Ahmadullah Wasiq, member of Taliban's media team and host of a show on Al Emarah website. Now he is Deputy Head of the Cultural Commission.
@tariq__mashal	376	Taliban member and supporter
@hrw	340	Official account for the Human Rights Watch
@shamshadnetwork	336	Official account of Shamshad Radio & Television Network, popular Pashto-language network in Afghanistan
@suhailshaheen1	336	Member of the Taliban's negotiation team and head of the political office, Suhail Shaheen.
@ajabreaking	335	Official account Al Jazeera's breaking news in Arabic
@tolonews	333	Official account for TOLOnews, a large news organization in Afghanistan
@bilalkarimi21	315	Taliban spokesman, Bilal Karimi
@habibzada1988	313	Taliban member and supporter
@hafghan8	309	Taliban member and supporter
@a_jahid_jalal	305	Taliban member and supporter
@murtazawi3	305	Shahussain Murtazawi, senior adviser and spokesperson for Ashraf Ghani
@shafioriakhil	292	Senior Taliban member, Shafiullah Azam
@govfidai	280	Mohammad Halim Fidai, former governor of Paktia Province
@anashaqqani313	278	Anas Haqqani, senior leader of the Taliban
@nunnasia	269	Online news site, Nunn.Asia
@ahmadsaeed101	256	Taliban member and supporter
@vqvyvrhrvcase9c	256	Taliban member and supporter
@mobeenkhan1231	249	Taliban member and supporter

This research also sought to capture whether and how often the Taliban mentioned specific locations relevant to their ongoing military operations throughout the summer. To accomplish this, I reviewed the data for the discussion of any of Afghanistan's 34 provinces in English, Pashto, Urdu

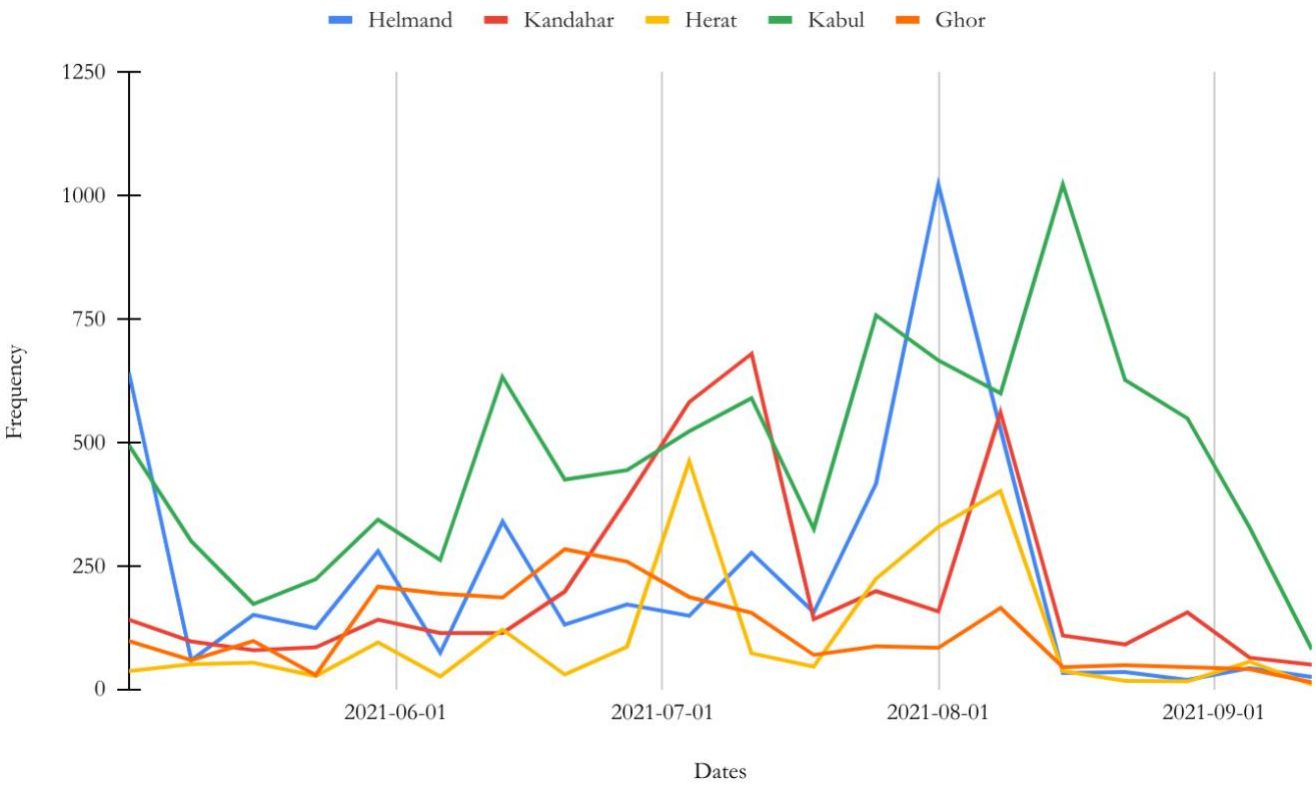
and Dari from the start of major military operations during the week of May 1 through September 16. During this period, Taliban tweets discussed Afghan provinces 42,863 times. As highlighted in Table 5, the five most discussed provinces were Kabul (9,246), Helmand (4,664), Kandahar (4,147), Ghor (2,342), and Herat (2,181). The frequency of the Taliban's discussion of Kabul is not surprising, given the importance of the province and capital city of the same name. The number is likely inflated in part due to the Taliban's use of 'Kabul regime' to refer to the Afghan government. Similarly, in early May, the Taliban frequently made use of the hashtag #HelmandMassacre, accusing Afghan forces of harming civilians, increasing the count of Helmand mentions in the dataset.

Table 5. Frequency of Taliban Discussion of Afghanistan's 34 Provinces

Province	Count	Province	Count
Kabul	9246	Laghman	847
Helmand	4664	Zabul	843
Kandahar	4147	Paktia	817
Ghor	2342	Nimruz	637
Herat	2181	Badghis	578
Baghlan	1479	Sar-e-Pul	570
Badakhshan	1401	Samangan	483
Mazar-e-Sharif	1319	Paktika	452
Takhar	1295	Ghazni	435
Kunduz	1067	Parwan	401
Panjshir	1039	Kapisa	268
Logar	1012	Nuristan	213
Wardak	926	Kunar	213
Faryab	885	Bamyan	212
Farah	871	Oruzgan	142
Khost	871	Nangarhar	103
Jawzjan	858	Daikundi	46

In reviewing a comparison of weekly discussions of the five most discussed provinces, pictured in Figure 5, interesting trends emerge. Specifically, peaks in activity discussing each province appear to correlate with key moments in the Taliban's military operation, suggesting that the group sought to document and amplify their activities online in real-time, with a high degree of granularity, tweeting updates in each province about their activities. For additional figures of Twitter activity discussing all 34 provinces, see Appendix 2.

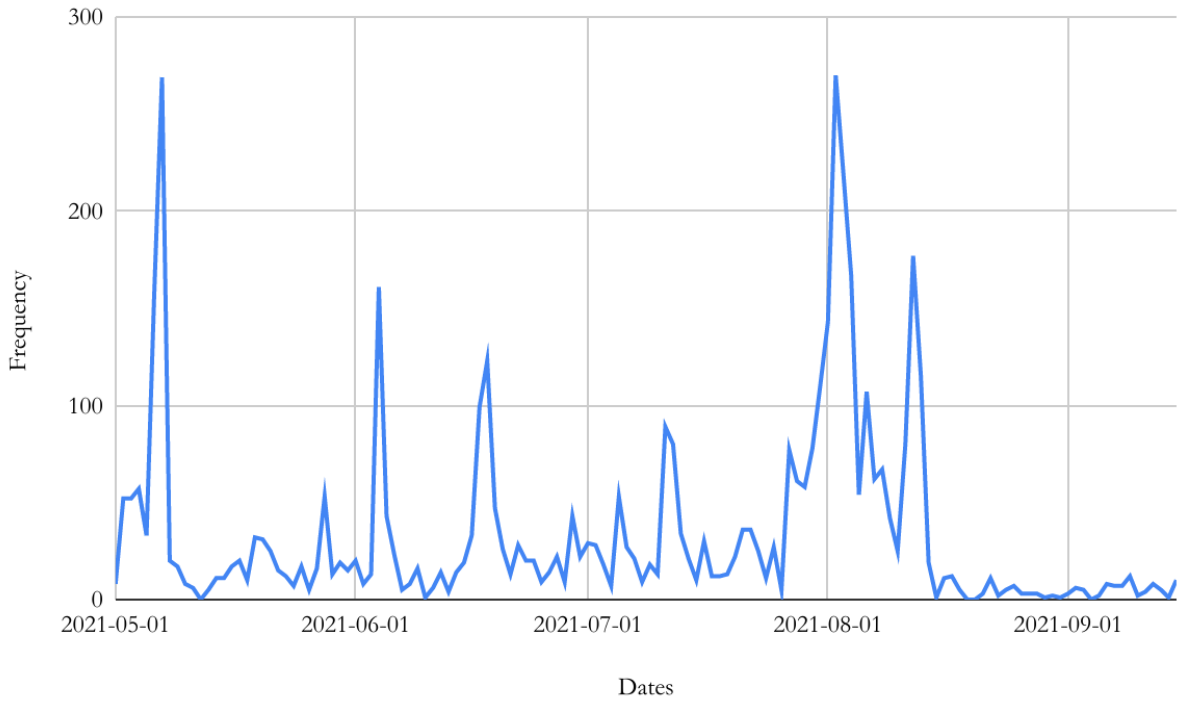
Figure 5. Weekly Discussion of Kabul, Helmand, Kandahar, Ghor and Herat Province by Taliban Accounts (May 1 - September 16)



As seen in Figure 5 and 6, discussion of Helmand Province peaked during the first two weeks of August, with its highest peak in tweet counts during the week of August 1 (publishing 1022

tweets). This corresponds with a period of intense fighting when the Taliban began its attempt to take Helmand's provincial capital of Lashkar Gah. On August 1, Taliban forces had entered the city and came within meters of the governor's office.[534] At this point during the conflict, the Taliban had yet to take over a provincial capital and were aggressively pursuing this accomplishment. The second highest week of Twitter activity related to Helmand was that of August 8. Lashkar Gah was captured on August 13.[535]

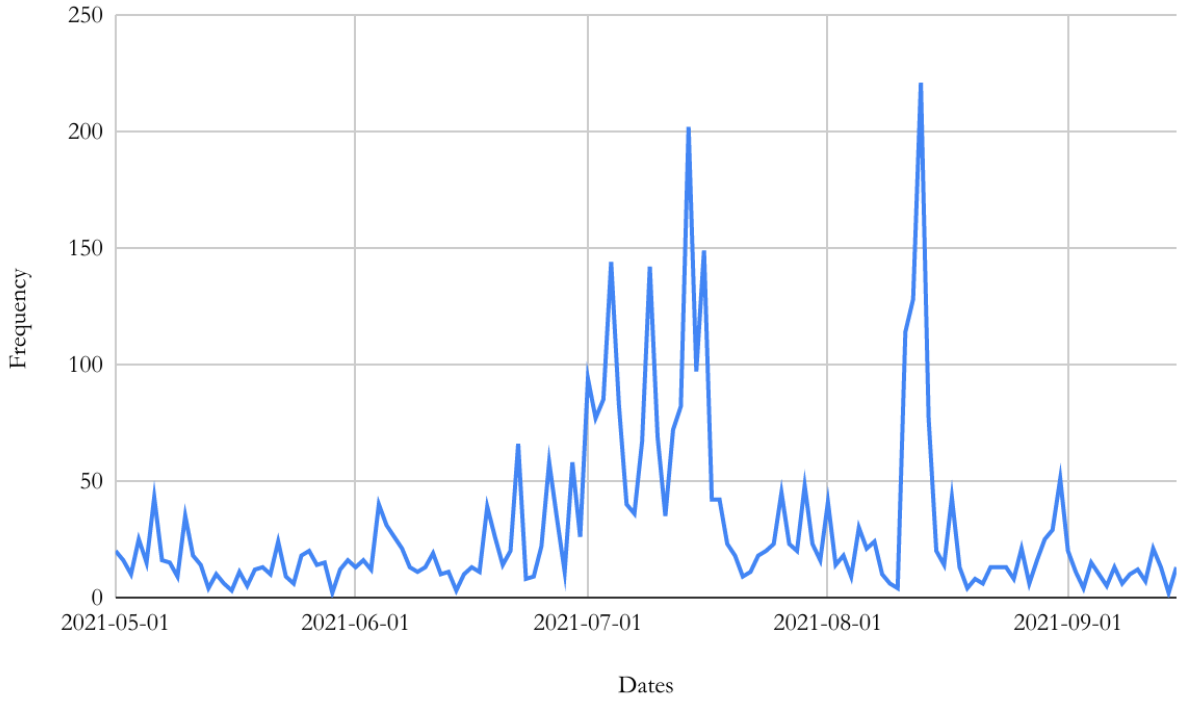
Figure 6. Daily Discussion of Helmand Province by Taliban Accounts (May 1 - Sep 16)



[534] BBC, "Afghanistan: Taliban continue attacks on three major cities," *BBC*, August 1, 2021, https://www.bbc.com/news/world-asia-58040141; BBC, "Afghanistan: Street fighting rages as Taliban attack key city," *BBC,* August 3, 2021, https://www.bbc.com/news/world-asia-58051481.
[535] Al Jazeera, "Timeline: Afghanistan provincial capitals captured by Taliban," *Al Jazeera News,* August 11, 2021, https://www.aljazeera.com/news/2021/8/11/afghanistan-taliban-provincial-capitals-cities-timeline.

Kandahar had two major peaks, the week of July 11 (publishing 679 tweets) and the week of August 8 (560 tweets). During the weeks of July 4 (the second highest week, with 581 tweets) and July 11, the Taliban were embroiled in heavy fighting in Kandahar city, entering the city on July 9.[536] On August 12, the Taliban had taken over Kandahar's provincial capital.[537]

Figure 7. Daily Discussion of Kandahar Province by Taliban Accounts (May 1 - Sep 16)

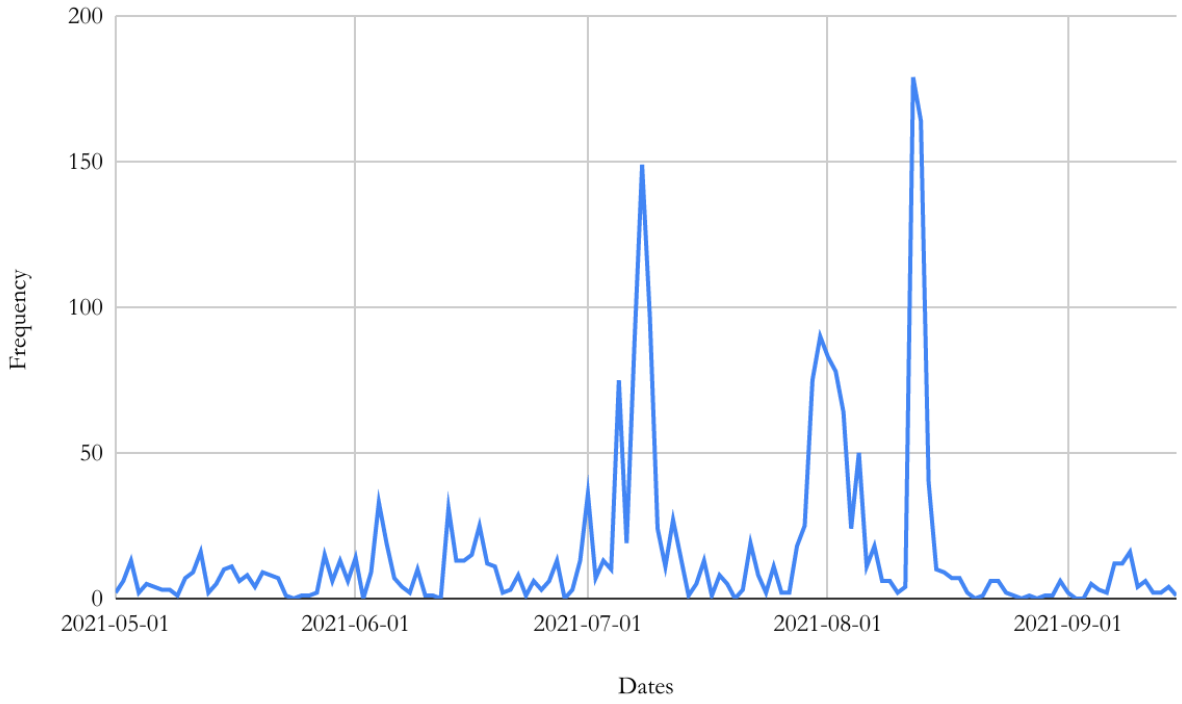


As seen in Figure 5, Herat also has two primary peaks, the week July 4 and the three weeks leading up to the capture of Herat city (July 25 - August 14). During the week of July 4, the Taliban

[536] Adam Nossiter, "Taliban Enter Kandahar City and Seize Border Posts," *The New York Times*, July 9, 2021, https://www.nytimes.com/2021/07/09/world/asia/taliban-kandahar-afghanistan.html.
[537] Bill Roggio and Andrew Tobbin, "Kandahar City falls to the Taliban," *Long War Journal*, August 12, 2021, https://www.longwarjournal.org/archives/2021/08/kandahar-city-falls-to-the-taliban.php.

successfully captured eight districts and two important border towns in Herat province.[538] Then, beginning on July 28, the Taliban began its assault on Herat city, eventually succeeding in capturing the city on August 12, noted as a peak in Figure 8.[539]

Figure 8. Daily Discussion of Herat Province by Taliban Accounts (May 1 - Sep 16)

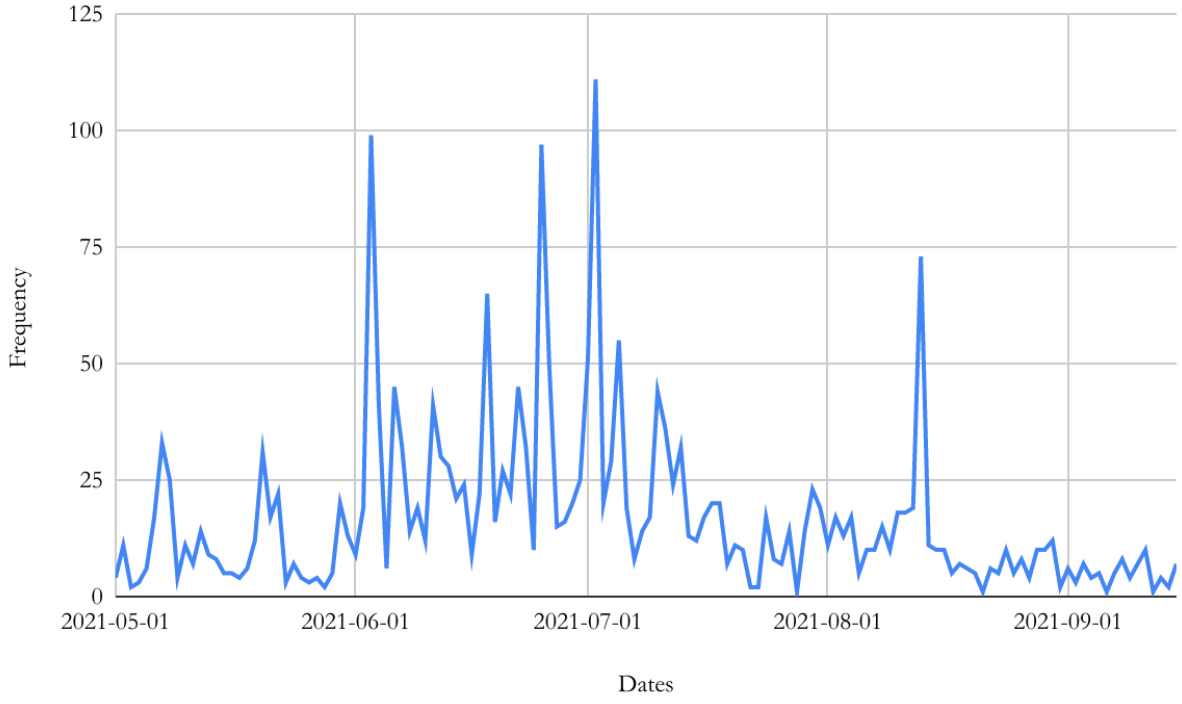


[538] Naseer Ahmad Salehi, "Ismail Khan Mobilizes Hundreds in Herat to Crush Taliban," *TOLONews*, July 9, 2021, https://tolonews.com/afghanistan-173398.

[539] Al Jazeera, "Timeline: Afghanistan provincial capitals captured by Taliban"; Ali M. Latifi, "Afghanistan's Herat under pressure amid ongoing Taliban assault," Al Jazeera, July 31, 2021, https://www.aljazeera.com/news/2021/7/31/afghanistans-herat-under-pressure-amid-ongoing-taliban-assault.

Ghor's activity pattern appears to reflect conflict intensity in the region. Highest tweet counts occur during the month of June, before experiencing another uptick during the week of August 8. In June, the Taliban took over key districts in the province, including Tolak and Dollina.[540] On August 13, the provincial capital of Ghor, Feruz Koh was taken by the Taliban.

Figure 9. Daily Discussion of Ghor Province by Taliban Accounts (May 1 - Sep 16)

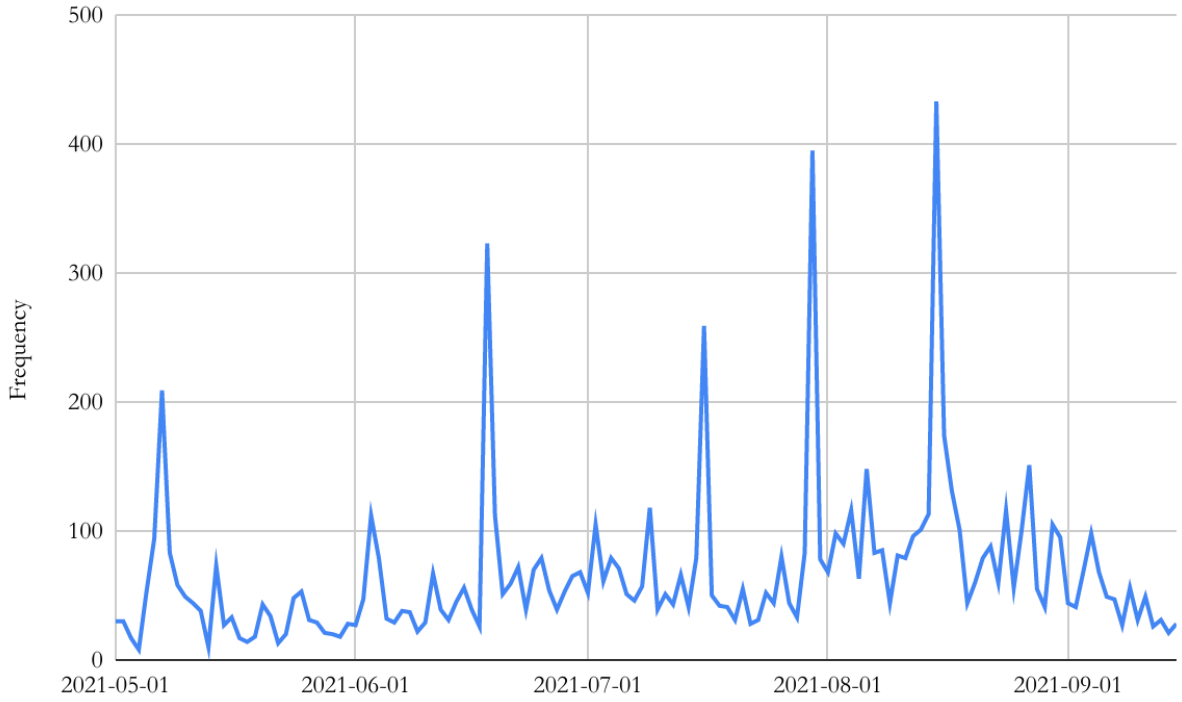


Kabul province activity pattern is quite sporadic and appears unlinked to on-the-ground activity, likely a reflection of the Taliban's use of 'Kabul regime' to refer to the Afghan government. However, it did reach its highest peak on August 15, when the group took Afghanistan's capital. An

[540] Giriraj Bhattacharjee, "Afghanistan: The final battle," *South Asia Monitor*, June 29, 2021, https://www.southasiamonitor.org/afghanistan/afghanistan-final-battle; TOLONews, "District in Ghor Falls to Taliban after 'Heavy Clashes,'" *TOLONews*, June 12, 2021, https://tolonews.com/afghanistan-172783.

important question to consider for the data moving forward is how to isolate discussion of Kabul as a location as opposed to references to the government.

Figure 10. Daily Discussion of Kabul Province by Taliban Accounts (May 1 - Sep 16)

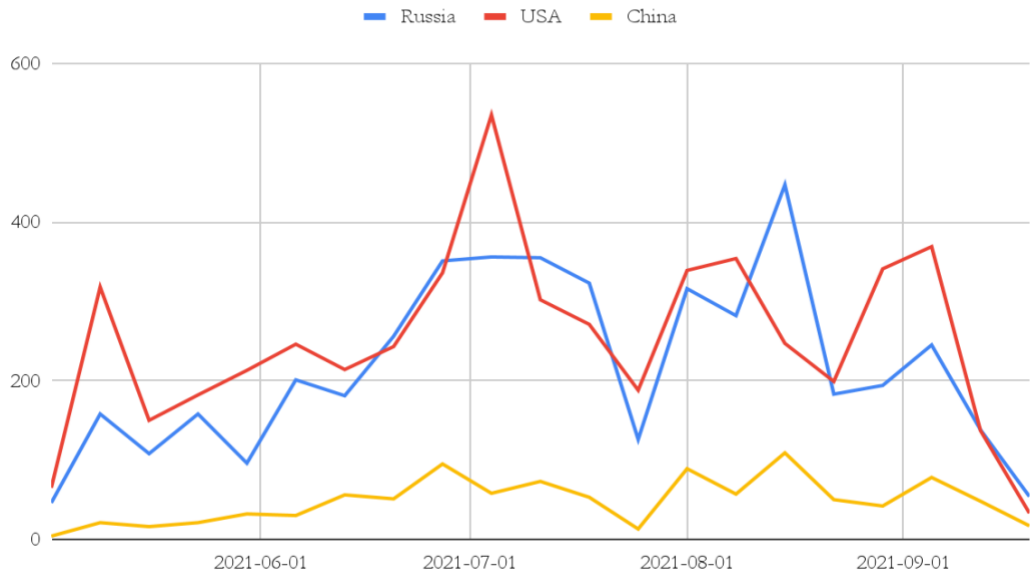


This research also reviewed mentions of major state actors by Taliban accounts in English, Pashto, Dari, and Urdu. The goal of this analysis was to gain insight as to how the group might be positioning themselves globally, in anticipation of the new government they sought to install. However, discussion of foreign actors composed a small percentage of the Taliban's overall information campaign. The Taliban produced 4,574 tweets that mentioned Russia, 5,282 tweets that mentioned the U.S., and 1,013 tweets mentioning China. Interestingly, Taliban content that included mention of the U.S. peaked during the week of July 4. During this week (July 8), U.S. President Biden made a public speech at the White House reaffirming his decision for the continued

withdrawal of U.S. troops from Afghanistan.[541] Further analysis is needed to determine why discussion of the U.S. may have been elevated during this period. Fascinatingly, the highest week for tweets concerning Russia as that of August 15. During this week, the Taliban mentioned Russia at almost twice the rate of the U.S. Russia was quick to create a diplomatic relationship with the Taliban once they took power; Ambassador Dmitry Zhirnov met with Taliban leaders within 48 hours of the group's conquest of Kabul.[542] Further research is needed to identify the specific narratives the Taliban propagated about Russia. Both Russia and the U.S. are mentioned at a comparable volume among Taliban tweets, despite the potential assumption that U.S. withdrawal would be a key topic among Taliban accounts. As compared to Russia and the U.S., China is not discussed as often in the data. A Taliban delegation visited China on July 27 and 28, but this does not correspond to an increase in activity.[543]

[541] David E. Sanger and Aishvarya Kavi, "Biden makes his case on U.S. withdrawal from Afghanistan as the Taliban gain ground," *The New York Times*, July 8, 2021, https://www.nytimes.com/2021/07/08/us/politics/biden-afghanistan-speech-taliban.html.
[542] Petr Kozlov & Anna Rynda, "Afghan crisis: Russia plans for new era with Taliban rule," *BBC*, August 21, 2021, https://www.bbc.com/news/world-europe-58265934.
[543] Reuters Staff, "China says Taliban expected to play 'important' Afghan peace role," *Reuters*, July 28, 2021, https://www.reuters.com/world/china/taliban-delegation-visits-china-taliban-spokesperson-2021-07-28/.

Figure 11. Weekly Discussion of Russia, U.S., and China by the Taliban (May 1 - Sep. 16)



Discussion

This research sought to engage in analysis of the Taliban's social media data to provide answers to two key questions of interest: How did the Taliban use Twitter to support their military operations during the takeover of Afghanistan? And how did the Taliban leverage Twitter's features to promote their information campaign?

In response to this first question, the data analysis highlighted that the Taliban used Twitter in conjunction with on-the-ground activity. Results are indicative of two key trends: (1) the frequency and intensity of the Taliban's Twitter activity appears to correlate with pivotal events in the conflict, and (2) the Taliban documented their movements as they took the country and moved toward Kabul. As highlighted by Figure 1, spikes in tweet frequency roughly correlated with key moments in the conflict, with the highest level of activity taking place during the week of August 15. It also highlighted how the Taliban's Twitter activity changed dramatically during major military

operations, increasing by more than twofold from its baseline levels in April, marking a shift in the Taliban's online behavior and investment in the platform.

Table 2 and Figures 2 and 3 reviewed the level of engagement these Taliban accounts received, establishing that the Taliban's content was moderately "successful" in garnering engagement. While more research would be necessary to establish the percentage of engagement that excluded Taliban members (or the presence of fake accounts), this engagement is significant, arguably on par with that of influence operations developed by state actors. The efficacy of the Taliban's campaign in successfully reshaping perceptions or influence behavior remains an open question, as it does for other state-sponsored influence operations.[544] However, what is clear is that the Taliban received considerable attention online, both domestically and internationally.

Table 5 and Figures 5 through 10, highlight the Taliban's discussion of strategic locations on Twitter and its relationship to on-the-ground activity. This data supports the notion that the group documented their military operations with a high-level of detail, sharing their exploits in real-time. In particular, Figures 6 through 10 show how upticks in discussion of five provinces track with Taliban operations in those locations. This data helps to establish that the Taliban invested considerable time and organizational resources developing and amplifying a sophisticated, coordinated online information campaign. The volume and real-time nature of these Twitter posts points to Taliban perception that social media was an important tool to advance their military and political goals. While further research is needed, this analysis provides an important baseline assessment of the level

[544] Bateman, Jon, Elonnai Hickok, Laura Courchesne, Isra Thange, and Jacob N. Shapiro, "Measuring the Effects of Influence Operations: Key Findings and Gaps from Empirical Research," *Carnegie Endowment for International Peace,* June 28, 2021, https://carnegieendowment.org/2021/06/28/measuring-effects-of-influence-operations-key-findings -and-gaps-from-empirical-research-pub-84824.

of online activity. Building on this, future research should seek to analyze the specific narratives shared before, during, and after consequential conflict events, including when the group intentionally sought to spread disinformation and how they framed victories (and losses).

In responding to the second question, the data highlighted that the Taliban used Twitter's features and lack of moderation to amplify their messaging. The group used the platform to engage domestic and international audiences, including developing specialized hashtags to push specific propaganda narratives and leveraging mentions to attempt to garner a response from humanitarian organizations, key political players, and journalists. As shown in Table 3, the Taliban created hashtags to promote and connect content across accounts that furthered specific narratives. This included hashtags tied to content that accused the Afghan government of war crimes, encouraged Afghan soldiers to defect, promoted the benefits of Taliban governance, and highlighted their victories during the summer months.

In Table 4, the account handles of commonly mentioned accounts were reviewed. Use of these mentions appeared to serve one of four purposes (1) to encourage amplification of content by other Taliban members or the group's online support network, (2) to garner a response from key members of the Afghan government, (3) to gain attention from mainstream news organizations, or (4) to portray American and Afghan forces as engaging in war crimes warranting a response from the humanitarian community. Both mentions and hashtags served as content amplification tools while helping the group to further specific narratives.

Further, Figure 4 highlighted that the Taliban relied on existing accounts on the platform, with a significant majority of accounts established before 2021. This allowed the group to rely on

pre-existing communities of followers to amplify content at the beginning of the summer. This data also provokes a question regarding platform policy: the Taliban's ability to use their accounts without interruption for years potentially points to a lack of active moderation by Twitter.

Finally, Figure 11 provides an initial indication of how the Taliban might have used Twitter for public diplomacy. The data highlighted that the Taliban accounts engaged in ongoing discussion about Russia, China, and the U.S. throughout the summer. Discussion of China was fairly consistent across the weeks under review, although mentioned at lower levels than Russia and the U.S. An interesting trend that bears repeating is the frequency with which Taliban accounts discussed Russia, almost on par with the U.S, despite the backdrop of U.S. withdrawal from Afghanistan as a key impetus for the Taliban's takeover of the county. Further research is needed to ascertain the specific narratives the Taliban promoted regarding each county.

The results of this analysis prompt additional questions and future research. First, what were the real-world effects of the Taliban's social media activity? For example, did the Taliban's promotion of content encouraging defections and discussing pardons (such as the content included under the hashtag, #wlc2decievedsoldiers) translate to an increase in Afghan soldiers joining the Taliban? Did the promotion of content highlighting the positive aspects of Taliban rule change the opinions of Afghans? And did the Taliban's documentation of the group's mounting victories make the international community and Afghans feel that the Taliban victory was inevitable?

Second, is social media data a valuable and informative record of this conflict? Given the detail with which the Taliban documented its activities, further analysis is needed to determine whether the group shared additional details of specific clashes and its daily operational activities (for

example, what kind of content fell under the label of hashtag #jihadisttraining?), when the group promoted disinformation, and which battles the Taliban chose to highlight or underplay. The social media activity of other key Afghan, NATO, and U.S. leaders and organizations should also be compared to understand how different voices shaped perception of the conflict online.

Conclusion

The paper provided compelling evidence of social media's important role during the Taliban's 2021 takeover of Afghanistan. The paper included a novel analysis of 112,354 tweets from 63 Twitter accounts run by Taliban senior leaders, spokesmen, and avowed members. To the author's knowledge, this is the most comprehensive analysis of the Taliban's social media activity to date. This research established the scope and scale of the Taliban's use of social media during the takeover and the ways in which the Taliban aimed to leverage Twitter to complement their military operations. The volume of tweets, combined with high engagement and frequency of incendiary content (see Appendix 1), demonstrates that the Taliban were left largely unchecked on Twitter.

This paper generates several key policy implications. First, social media highlights how future technologies might reduce the ability of armed groups to coerce private actors. Earlier in their organizational history, the Taliban were able to gain information control over several regions of Afghanistan by coercing cell service providers into limiting access. This strategy succeeded in part because the physical infrastructure supporting the technology was located within the bounds of the conflict setting. If a company failed to comply, the Taliban would destroy their towers. However, newer technologies, especially social media, are partly divorced from the physical landscape of a conflict. For example, when the Taliban was targeted by Facebook moderators, it had few methods

for recourse. The group's only option was to circumvent bans, make public complaints, or eliminate the technology from its arsenal. In fact, there is evidence from the broader Twitter dataset that the Taliban seemingly called out the former CEO of Twitter, Jack Dorsey, for interfering with Taliban propaganda, tweeting, "To the owner of @Twitter! We are not robots but humans If these atrocities could take place in your country now you would be many times more than us trying to spread the voice of your oppression to the world.@jack #HelmandMassacre." However, there is no evidence of a response from the platform.

Second, there are reasons to doubt that platforms are doing an effective job of moderating armed groups. The Taliban's proliferation and persistence on a mainstream social media platform owned by a U.S. company raises important questions including, how many other non-state armed groups are weaponizing social media? And how are existing policies enabling social media's continued misuse by malicious actors, despite public overtures that platforms are focused on problems of violence and extremism online?

And third, the Taliban's reliance on publicly available infrastructure, built and owned by an American company, offered an opportunity for U.S. forces to effectively engage in counter-information operations. In identifying these accounts, the U.S. government could have partnered with Twitter to have them removed or placed targeted ads and counter-narratives on the account pages. In addition, Twitter is an American company. Therefore the U.S. military and intelligence services might have had additional levers through which to influence the company to target the Taliban's online operations. From the platform side, existing counter-radicalization policies (including the redirect method, which involves redirecting users to alternative content when they

search for terms associated with extremism) could also be applied in this case.[545] Twitter could have deployed a range of approaches beyond removals, such as labeling the account (as they do with Russian and Chinese state media accounts) or placing labels on incendiary content (as they do with COVID and election disinformation).[546]

Appendix 1

Analysis of a Subset of Taliban Activity: English-Language Tweets Discussing U.S. Forces

[545] Ryan Greer and Vidhya Ramalingam, "The Search for Extremism: Deploying the Redirect Method," *The Washington Institute for Near East Policy*, February 27, 2020, https://www.washingtoninstitute.org/policy-analysis/search-extremism - deploying-redirect-method.

[546] Twitter Support, "New labels for government and state-affiliated media accounts," *Twitter Blog*, August 6, 2020, https://blog.twitter.com/en_us/topics/product/2020/new-labels-for-government-and-state-affiliated-media-accounts; "COVID-19 misleading information policy," *Twitter Help Center*, https://help.twitter.com/en/rules-and-policies/ medical-misinformation-policy; "Civic integrity policy," Twitter Help Center, https://help.twitter.com/en/rules- and-policies/election-integrity-policy.

Using Twitter's academic research application programming interface (API), tweets from a core set of 57[547] Taliban-linked Twitter accounts were downloaded. Accounts labeled as Taliban-linked met at least one of the following inclusion criteria: (1) the account bio explicitly stated their affiliation with and/or role within the Taliban (or the Islamic Emirate of Afghanistan), (2) the profile image or banner included images of the Taliban's flag, logo, or photos of high-ranking members, (3) the account included a link to the Al-Emarah website in their profile bio (this was a common feature of accounts claiming to be 'journalists,' despite exclusively writing content for the Taliban's website), and/or (4) repeatedly and primarily posted pro-Taliban content, including insider videos and messages on behalf of the group. By September 2021, this network of 57 accounts had cumulatively amassed more than two million followers on Twitter. From April 1 to September 16, 2021, they produced 103,789 tweets, including retweets.[548] This timeline was selected to provide a baseline activity prior to the U.S. president's announcement of military withdrawal on April 14, as well as data on the month after the takeover on August 15.

For the purposes of this paper, I examined a small subset of Taliban tweets from this broader dataset. Tweets qualified for inclusion if they were in English and made explicit reference to either "U.S.," "US," "USA," "America," or "American." While some tweets made reference to American forces, including mentions of former U.S. president George W. Bush or references to "foreign marauders," they were excluded from this initial dataset unless they directly mentioned the key terms. English language use is leveraged as a proxy for Taliban information campaigning targeting international audiences, as the average Afghan would not be able to read English. I analyzed this data to observe frequency of tweeting over time, engagement with Taliban content

[547] This analysis was conducted before an additional 6 accounts were added to the dataset; this is the reason for the discrepancy between the 63 accounts reviewed in the article as compared to the 57 in this appendix analysis.
[548] See comment above.

over time, the accounts mentioned in Taliban tweets, the hashtags used by the Taliban to amplify content, and the links shared in Taliban tweets. The goal of this analysis is to provide initial insight into the ways in which the Taliban weaponized Twitter (and its platform features) to advance its messaging about U.S. forces to the international community in the lead up to the takeover.

Results

Table 6: Summary Statistics of Taliban Tweets (April 1, 2021 - September 16, 2021)

Total Tweets	251
Quote Tweets	140
Replies to Tweets	233
Retweets of Tweets	891
Likes of Tweets	3713

The 57 Taliban-linked accounts produced 251 English language tweets featuring U.S.-oriented descriptors between April 1 and September 16, 2021. These tweets received 3,713 likes and 233 replies. These tweets were retweeted 891 times and quote tweeted (reshared to a user's account with added commentary) 140 times. The Taliban-linked accounts averaged 8.9 English language tweets per week discussing the U.S. As illustrated in Figure 12, the week with the highest tweet production (May 2 - 8) coincides with the resurgence of Taliban attacks and the beginning of the takeover, following U.S. failure to meet the previously established May 1 deadline for total withdrawal.[549] Criticism of the withdrawal's pushback is among the common themes of the dataset.

Figure 12: Tweet Count by Taliban-Linked Accounts by Week (April 1 - September 16)

[549] Fatima Faizi, Fahim Abed and Najim Rahim, "Afghan War Casualty Report: May 2021," *The New York Times*, June 3, 2021, https://www.nytimes.com/2021/05/06/world/asia/afghan-war-casualty-report-may-2021.html.

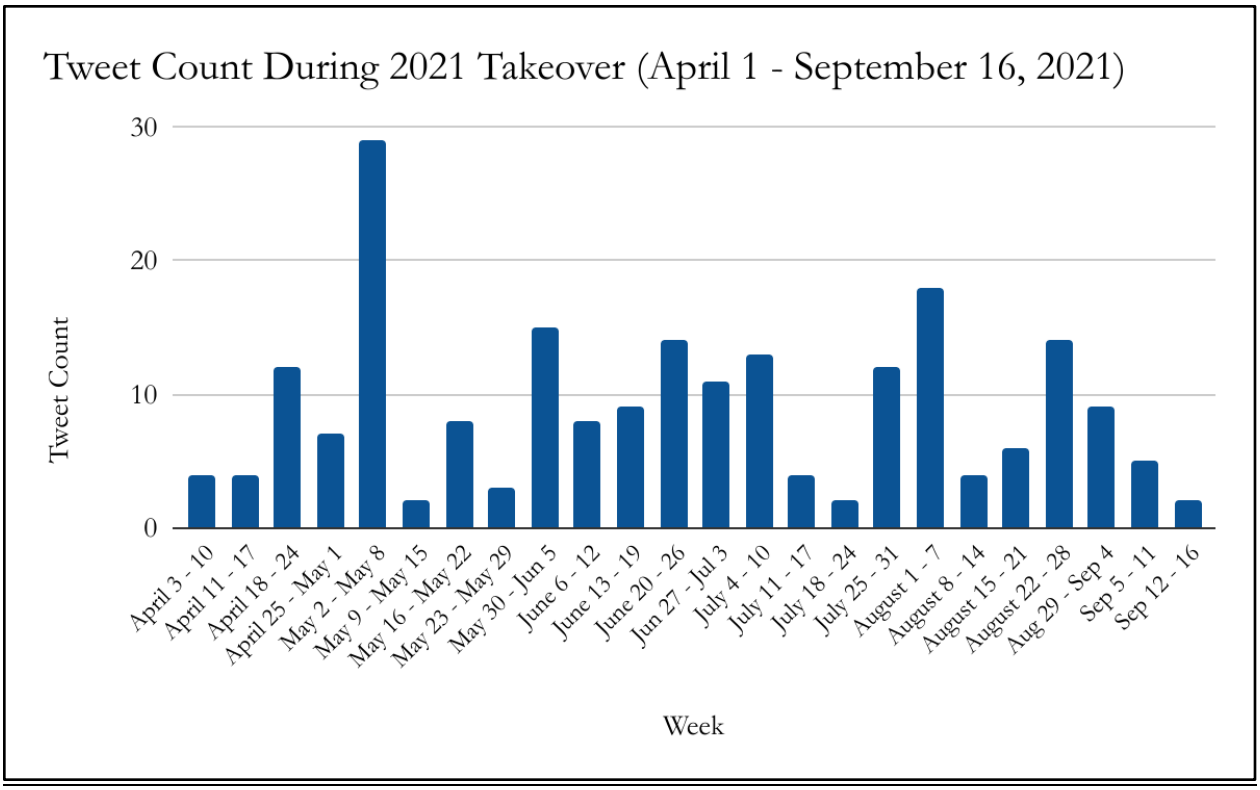


Figure 13 outlines the number of likes tweets received by week during the period under review. The most liked tweet occurred in September of 2021, receiving 753 likes.

Figure 13: Like Count on Taliban-Linked Tweets by Week (April 1 - September 16)

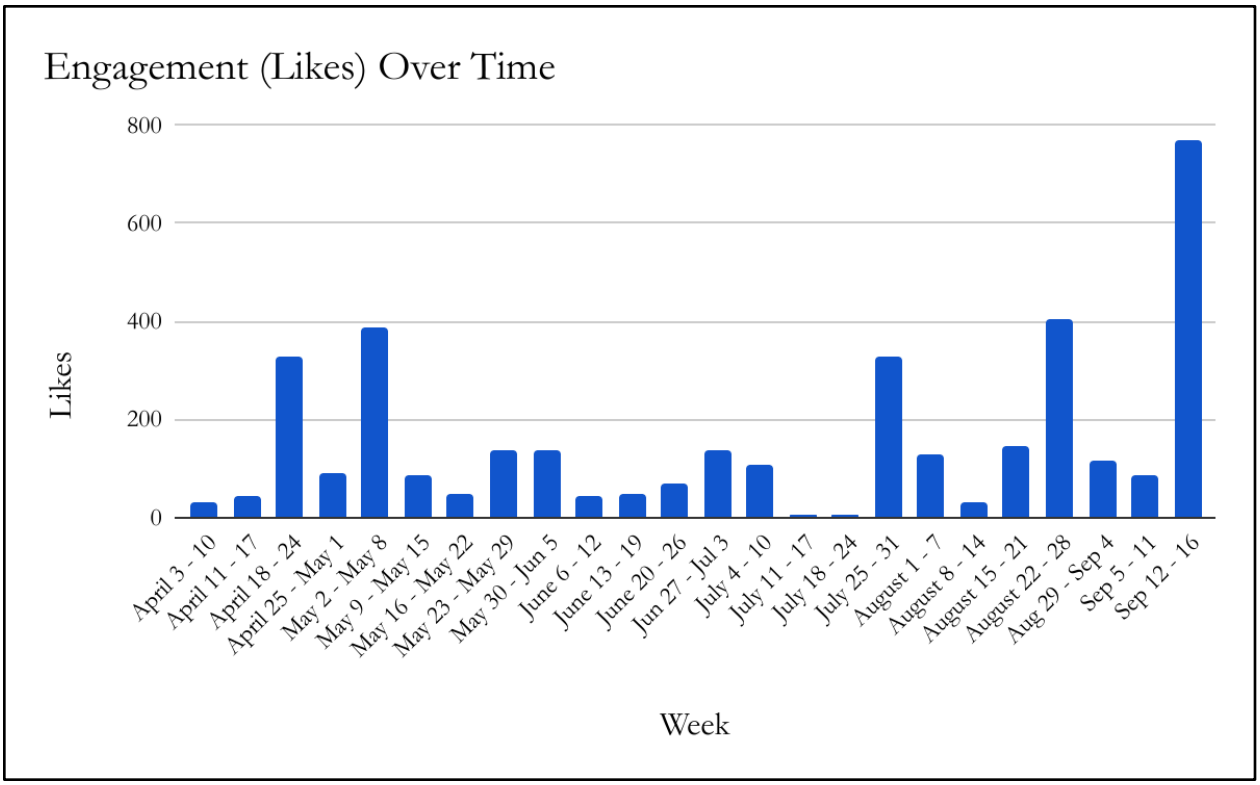


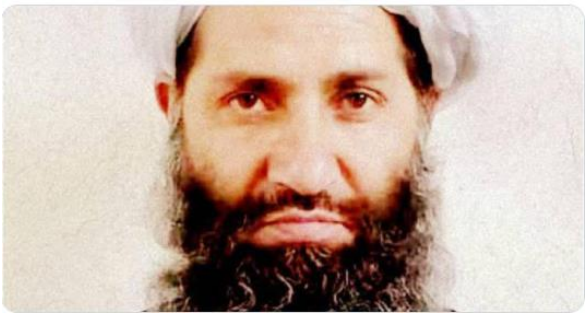
Table 7 includes the top ten most liked tweets within the dataset, including the date the tweet was posted, the content of the tweet, and accompanying media. These tweets include (1) an image of the American flag being used to cover trash, (2) an official statement from the Taliban including a link to their official website, (3) a video from the Kabul airport after the takeover, (4) a video of a dead body lying next to a tank coupled with accusations of American war crimes, (5) praise of Mullah Omar and his sacrifices in the fight against the U.S., (6) a threat from a Taliban leader of repercussions for U.S. forces, (7) a claim that had the Taliban cooperated with the Americans they would have lost in a similar fashion to Iraqi president Saddam Hussein and Libyan leader Muammar Gaddafi, (8) a video of men desecrating bodies of dead Taliban members, accusing Americans of supporting war crimes, (9) a claim that Afghan soldiers were surrendering and handing over American weapons to the Taliban and (10) a video of a man shot in the chest, accompanied by text

accusing Americans engaging in war crimes. It is also important to note that three of these tweets featured videos containing graphic violence in violation of Twitter's stated policies.

Table 7: Top 10 Most Liked Tweets

Date Posted	Tweet	Like	Linked Content
2021-09-13	American flag used as a garbage tools for Afghan fruits in Lashkar Gah of Helmand	753	
2021-05-27	Statement of Islamic Emirate regarding reports about establishment of American bases in the region	121	alemarahenglish.net/?p=46222 

2021-08-25	Badri 313 battalion and US Soldiers Face to Face in Kabul Airport.	112	
2021-07-30	O Americans! Your cruel officers have trained these savages. You support the most oppressive and corrupt government in the world You pay your taxes to them So you are all complicit in these crimes Shame on you #KabulRegimeCrimes	91	Video of dead body lying by a tank
2021-04-24	This is the place where Mullah Umar spend last years of his life, he commanded war against US invasion for 12 years from these mud huts. Success doesn't lie in having modern warfares, lavish lifestyle or wealth indeed it is in obedience of Allah and his prophet SAW.	89	

2021-05-09	#Taliban leader Hebatullah Akhundzada warns US to abstain from further provocations and violations of Doha deal. "If America again fails to live up to its commitments, then the world must bear witness and hold America accountable for all the consequences."	84	
2021-04-24	Americans used 2 give warnings 2 the leaders of 3 Islamic countries to comply with their demands. Saddam & Gaddafi agreed 2 their demands, bt Mullah Omar didn't. Both of them were finished but the friends of Mullah Omar hv made NATO withdraw from Afghanistan. #TheLegendaryLeader	72	
2021-07-30	Only American savages can train such savages No one else can train such savages #KabulRegimeCrimes	58	Video of dead bodies hanging from a tree, being beaten by individuals with clubs.
2021-06-28	#Breaking: Kabul regime's commandos handover American weapons To #Taliban in Qarabagh district of #Ghazni province.	57	Link was unavailable; date of removal unclear.

2021-07-30	O savage and uncivilized Americans Check out your trained soldiers #KabulRegimeCrimes	55	Video of a dead body; shot in the chest.

Interestingly, one of the tweets features a highly stylized image of Mullah Omar, surrounded by flower designs featuring the Twitter handle of a Taliban-affiliated graphic designer. It is unclear whether this image was part of a larger campaign.

Figure 14 outlines the number of retweets tweets received by week during the period under review. These accounts received the highest number of retweets during the week of July 25.

Figure 14: Retweet Count on Taliban-Linked Tweets by Week (April 1 - September 16)

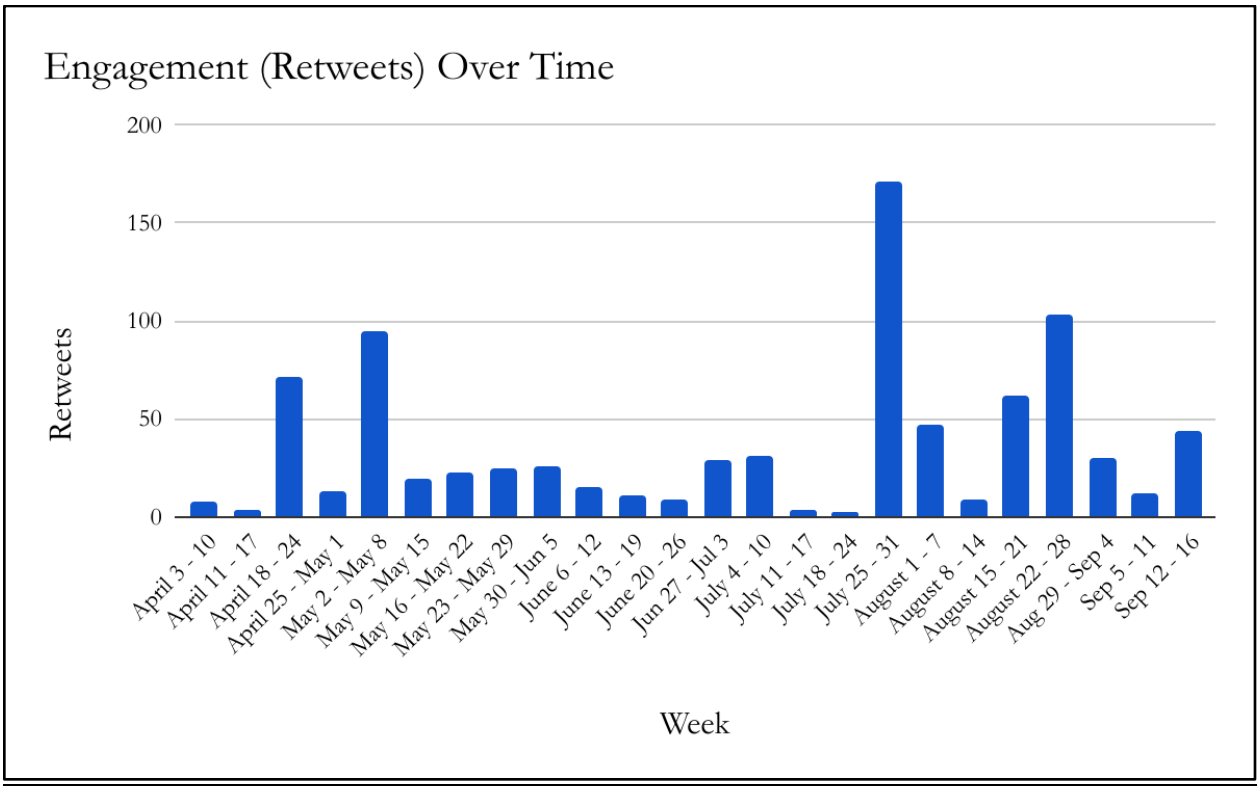


Table 8 provides an overview of the top twenty most common hashtags used by Taliban-linked accounts. Hashtags help to promote content on the platform, allowing users to search tweets labeled under a particular hashtag. Within the dataset, 127 (50.5%) tweets used hashtags. 41 distinct hashtags were used. Hashtags which had similar meaning or function were classified together in Table 3. The most common hashtags included #KabulRegimeCrimes, which were used in tweets highlight accusations of American, NATO and Afghan forces engaging in war crimes and human rights abuses, and #Helmand Massacre, referencing an apparent attack on civilians by Afghan and American forces (the veracity of this attack could not be corroborated). The #WLC2DeceivedSoldier was used for tweets encouraging Afghan soldiers to defect and join the Taliban.

Table 8: Hashtag Usage (Top 20)

Hashtag	Count
#KabulRegimeCrimes	22
#HelmandMassacre	19
#Afghanistan	13
#WLC2DeceivedSoldier	11
#Taliban	10
#TalibanOurGuardians	8
#Breaking; #BREAKING; #BREAKING_NEWS; #Justnow	7
#ShaheedAmeerulMomineen	7
#warcrimes; #WarCrime	7
#LegendaryLeader; #TheLegendaryLeader	6
#Helmand	6
#WeWantIslamicSystem	6
#LifeUndrControlOfTaliban	5
#US	4

#Ashraf; #Ghazni	4
#KabulAirport; #EvacuateKabulAirport; #Kabul_Airport; #Kabul_airport	4
#Afghans; #Afghan	3
#American	3
#TalibansLeaderMessage	2
#Bagram	2

Table 9 provides a list of the top twenty-five most commonly mentioned accounts in Taliban tweets. 54 tweets (21.5%) included a mention. The top three accounts include: the Human Rights Watch (most often used in tweets accusing U.S. forces of war crimes), the president of the Islamic Republic of Afghanistan, and the president of the United States.

Table 9: Mentions in Taliban Tweets (Top 25)

Account	Account Description	Frequency
@hrw	Human Rights Watch	15
@ashrafghani	Ashraf Ghani, President of the Islamic Republic of Afghanistan	11
@POTUS	Joe Biden, President of the United States	6
@NATOscr	No account currently exists; references NATO Senior Civilian Representative in Afghanistan	6
@UN_HRC	UN Human Rights Council	5
@UNHumanRights	UN Human Rights Office	5
@bbclysedoucet; @bbcpashto; @BBCHARDtalk; @BBCNews; @BBCBreaking	BBC News	5

@IeaOffice	Spokesman of the Political Office of the Islamic Emirate of Afghanistan	4
@VOANews	Voice of America News Organization	4
@US4AfghanPeace	U.S. Special Representative for Afghanistan	4
@ScottMorrisonMP	Scott Morrison, Prime Minister of Australia	4
@dfat	Australian Department of Foreign Affairs and Trade	4
@cnn; @cnnbrk; @cnni	CNN News	4
@USArmy	United States Army	3
@NYTimes; @nytimes	New York Times	3
@DrabdullahCE	Dr. Abdullah Abdullah, Chairman of the High Council for National Reconciliation	3
@Commander_RS	General Scott Miller, Commander of NATO	3
@IntlCrimCourt	International Criminal Court (ICC)	2
@suhailshaheen1	Taliban Member	2
@Zabehulah_M33	Taliban Member, lead spokesman	2
@GeneralKenneth8	General Kenneth F. McKenzie Jr., U.S. Marine Corps General	2
@NATO	NATO	2
@abcnews; @ABC	ABC News	2
@StateDeptPM	Political-Military Affairs, US Department of State	1
@USEmbassyKabul	U.S. Embassy in Afghanistan	1

Table 10 provides a list of the links shared by Taliban-linked accounts during this period. Links to the Taliban's official website, Al Emarah, were shared three times. The accounts shared articles from

a variety of reputable news organizations, including ABC News, BBC, CNN, Reuters and the New York Times.

Table 10: Links Shared

Source	Title	Date Shared
ABC News	Afghan President Ashraf Ghani says 'sudden' withdrawal of US troops opened the door for Taliban to target major cities	2021-08-12
Al Emarah Website	Taliban official website; no longer available	2021-05-26; 2021-05-27; 2021-08-04
Al Jazeera	Taliban expect US withdrawal in May; vow to restore Islamic rule	2021-04-11; 2021-05-03
Al Jazeera	Afghanistan's president says will step aside if election is held	2021-04-15
Al Jazeera	UK in talks with Taliban to evacuate British citizens, Afghans	2021-09-01
Al Jazeera	Qatar jet carrying technical team lands in Kabul: Live	2021-09-03
Axios	Trump officials back away from 2020 Taliban peace deal after withdrawal chaos	2021-08-02
BBC	Afghanistan: All foreign troops must leave by deadline - Taliban	2021-07-06
BBC	Afghanistan: US investigates civilian deaths in Kabul strike	2021-09-02
BBC	Beaten and humiliated by Hindu mobs for being a Muslim in India	2021-09-03
Center for European Policy Analysis	Afghanistan's End Portends a Darker U.S. future	2021-08-25
CNBC	U.S. will conduct airstrikes in Afghanistan against the Taliban as foreign forces withdraw	2021-07-28; 2021-07-29
CNN	Biden and world leaders meet at 2021 NATO summit	2021-06-15

CNN	Talks with Taliban are making 'very little progress' as militant group gains momentum, says Afghan official	2021-07-02
Foreign Policy	America Loves Excusing Its War Criminals	2021-08-04
France 24	Afghan soldiers execute a villager suspected of aiding the Taliban by IED	2021-08-04
Hindustan Times	In a huge shift, India opens channels with Afghan Taliban factions and leaders	2021-06-08
Human Rights Watch	Afghanistan: CIA-Backed Forces Commit Atrocities, Disband All Irregular Paramilitary Forces, Cooperate with Independent Investigations	2021-08-11
Just Security	How US-Funded Abuses Led to Failure in Afghanistan	2021-08-02
New York Times	'We Will Not Forgive,' Biden Says, Vowing Retaliation for Kabul Attack	2021-08-27
New York Times	Restoration of Kabul's Closed Airport Begins as Some Afghan Aid Resumes	2021-09-05
Reuters	Taliban enter Afghan capital as US diplomats evacuate by chopper	2021-08-15
The Conversation	US punishes International Criminal Court for investigating potential war crimes in Afghanistan	2021-08-06
The Guardian	Mullah Omar - in his own words	2021-07-05
U.S. Embassy in Afghanistan	Security Alert U.S. Embassy Kabul, Afghanistan (August 7, 2021)	2021-08-07
Wall Street Journal	In Kabul, Private Rescue Efforts Grow Desperate as Time to Evacuate Afghans Runs Out	2021-08-02
Washington Post	Biden will withdraw all U.S. forces from Afghanistan by Sept. 11, 2021	2021-04-13

Washington Post	As the last American forces prepare to leave Afghanistan, Biden says the country's fate is in its own hands	2021-06-26

Customizing Twitter to Advance Informational Aims

The Taliban weaponized a variety of features available on the Twitter platform to craft and propagate compelling information campaigning. Among the dataset of 251 English-language, U.S.-oriented tweets, Taliban messaging centered around six key themes:

(1) **Accusing the American military of war crimes and human rights abuses**. This included repeatedly referring to U.S. forces as savages, using the hashtags #KabulRegimeCrimes and #HelmandMassacre to amplify their messaging. An example tweet includes: "In 2001 when US backed militias took thousands of our fighters (Taliban) as prisoners of war, they stuffed them alive in containers and burnt them. In 2021, regime militia surrendering to us (Taliban) are received with hugs & smiles."

(2) **Highlighting civilian casualties and attributing them to U.S. and Afghan forces, especially in Helmand and at the Kabul airport.** An example tweet includes: "@NYTimes IEA gave & advanced warnings to foreign forces that these attacks were imminent. Why did the US continue to remain at the airport? ThE US presence was the reason why DAESH attacked the Airport killing MORE Afghans! @IeaOffice @cnn"

(3) **Providing descriptions of Taliban victory over U.S. and Afghan forces.** An example tweet includes: "Taliban have overrun a military base in Sar-e-pul, seizing the following items as booty:- 300 American military gun M16- 50 Ranger cars- 20 MB (Badass Military) vehicles - 40 KAMAZ trucks."

(4) **Threatening military action if the U.S. failed to meet the pre-established deadline for withdrawal of May 1.** An example tweet includes: "NOTHING in Afghanistan happens to schedule. It is understandable that the US withdrawal may run over 1st May deadline. However, the US must remember that once this deadline is passed, the truce will cease and their troops will come under attack."

(5) **Bragging about the Taliban's supremacy over American forces.** An example tweet includes: "O Stupid Americans. We will destroy your precious tanks for less than $ 100. Our Mujahideen do not have a salary. They are fighting only for God and the freedom of the country. Stay for another hundred years. In the end, you run away frustrated and ashamed. Get out sooner"

(6) **Critiques of U.S. foreign policy, arguing that Americans are deceitful and renege on promises.** An example tweet includes: "History tells that when the Americans left Vietnam, they didn't help those who had sided by them. Those American supporters were left alone to the mercy Vietnamese freedom fighters.#WLC2DeceivedSoldier" and "Americans used 2 give warnings 2 the leaders of 3 Islamic countries to comply with their demands. Saddam & Gaddafi agreed 2 their demands, bt Mullah Omar didn't. Both of them were finished but the friends of Mullah Omar hv made NATO withdraw from Afghanistan. #TheLegendaryLeader"

In examining the links shared by Taliban accounts, it is important to highlight that the overwhelming majority were articles and reports from reputable, well-recognized, and primarily Western organizations. These links were shared either to bolster Taliban claims, or as a means to refute the arguments of Western journalists against the Taliban. Of note, while they did link three times to the Taliban's official website, they did not share links to any overt disinformation or to

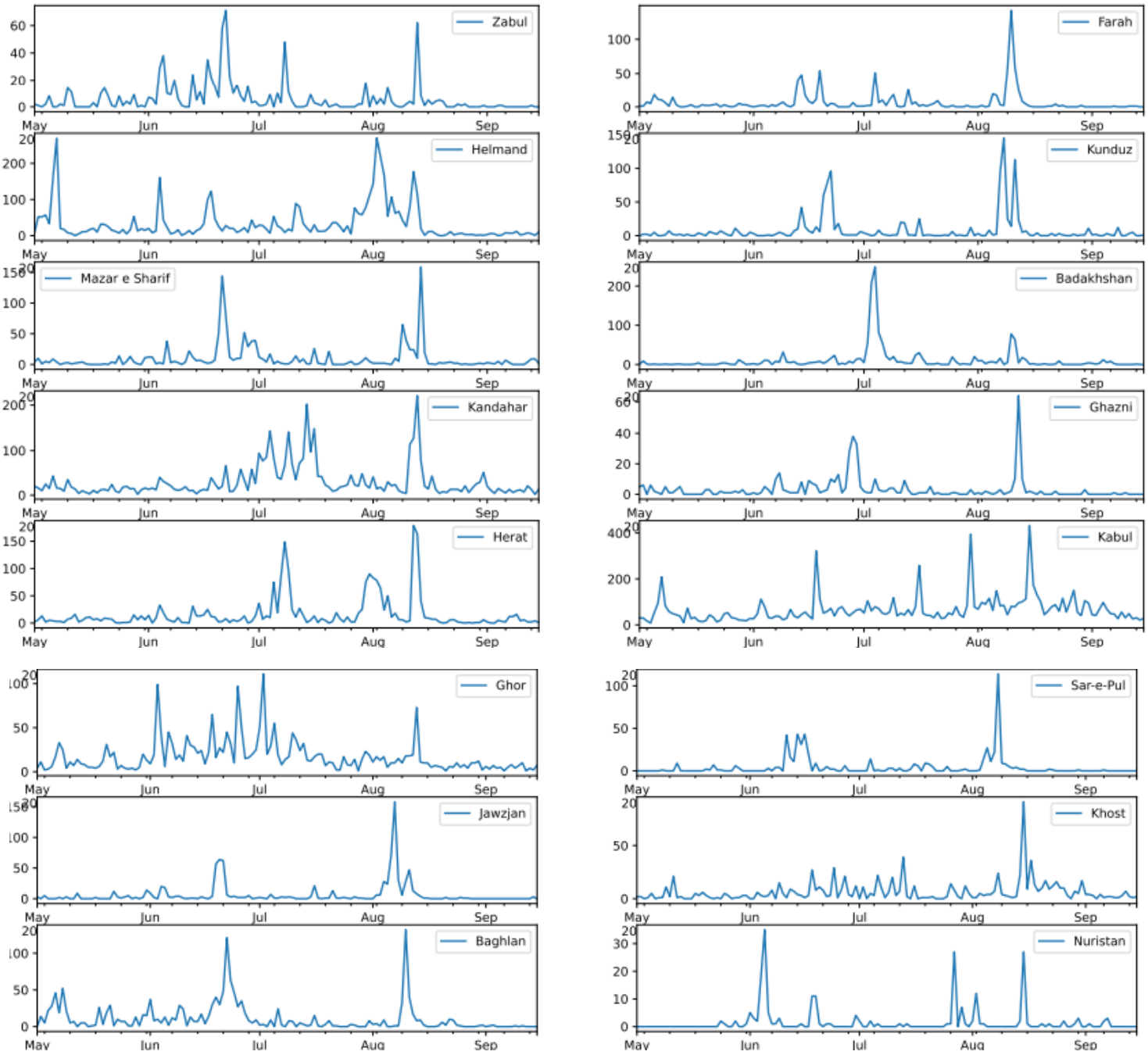
content made by Taliban supporters. They appeared to use this Twitter feature to help enhance the credibility of the information they shared. Rather than overt lies, they opted to amplify inconvenient truths.

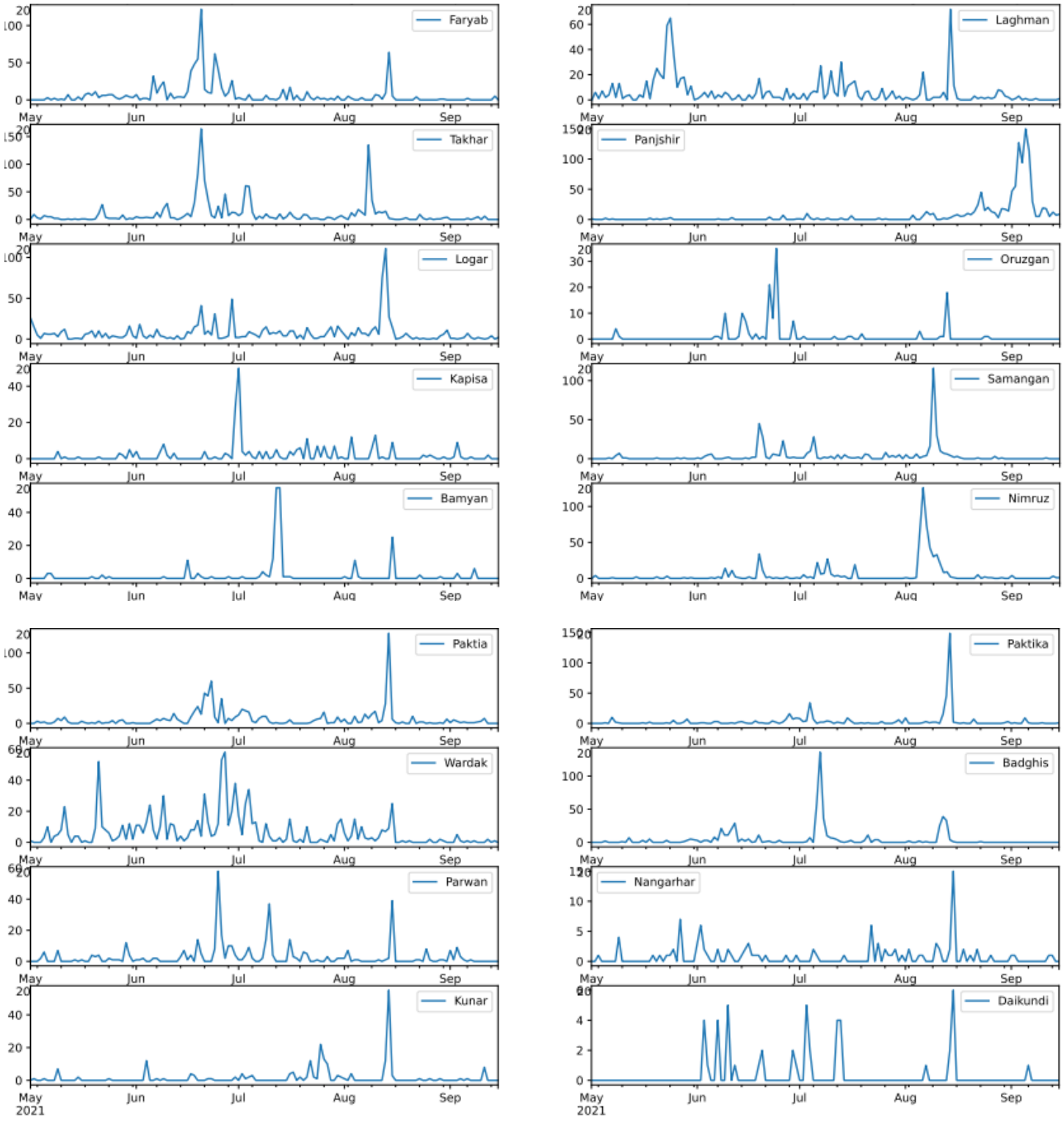
The Taliban's use of mentions signals an understanding of the different key players in the conflict, with a wide range of military leadership, foreign diplomats, and journalists tagged in Taliban tweets. It is unclear whether the use of mentions was intended to gain a response from the tagged account. The Taliban's also used hashtags to label and amplify content. Some of these hashtags can be categorized as geographic, including #Kabul, #Bagram, and #Helmand. The more general labels allowed Taliban content to be viewed by non-supporter Twitter users if they searched for content pertaining to #Afghanistan or the #KabulAirport. The pro-Taliban labels, including #LifeUndrControlOfTaliban and #TalibanOurGuardians, allowed users to view Taliban content across a wide range of Taliban-linked accounts.

This dataset included a total of 31 videos and 60 photos, allowing their audience to view media which persuasively supported their claims, including videos of dead bodies being brutalized and a woman being pushed by American soldiers. While not tested in this analysis, there also appears to be some connection between on-the-ground events and tweets by Taliban accounts, with a documented increase in Twitter activity at the beginning of their military operations in May and tweets including real-time updates from battles. From examining this dataset of tweets, a set of sophisticated and well-orchestrated communication strategies emerge, underscoring that documenting whether an armed organization adopts and uses a technology fails to tell a complete story of military advantage when it comes to ICT.

Appendix 2

Taliban Discussion of Afghanistan's 34 Provinces (May 1 - September 16)




Faryab
Laghman
Takhar
Panjshir
Logar
Oruzgan
Kapisa
Samangan
Bamyan
Nimruz
Paktia
Paktika
Wardak
Badghis
Parwan
Nangarhar
Kunar
Daikundi
May
Jun
Jul
Aug
Sep
2021

Conclusion

What explains variation in the adoption and use of information and communications technology (ICT) by armed organizations in modern conflicts? In presenting disruptive attribute theory, this project argues that four factors, reflecting attributes of ICT when deployed as a military technology, are critical: first, ICT introduces distinct and strategic interaction effects resulting from shared use of common infrastructure; second, ICT increases the role and importance of private sector actors who are now responsible for controlling access to technologies; third, the ubiquity of ICT creates different modes of technology acquisition, including passive or unintentional adoption, reflecting the diffusion of technology in non-military settings, and; fourth, ICT allows for customization and novel applications of technology, privileging sophisticated and adaptive usage strategies.

All three papers argued that while existing organizationally oriented models are important, analysis must also include an examination of the role of technological attributes. The first paper, *The Armed CTO: Towards a Theory of ICT Adoption,* introduced the disruptive attribute theory investigating the relevance of four intervening variables in shaping ICT adoption outcomes and behaviors by state militaries and non-state armed groups. Using adoption-capacity theory (the widely accepted model for technology adoption by organizations) as the baseline model, four attributes of ICT were argued to increase or decrease demands on organizational capacity, resulting in a broader range of adoption outcomes than currently predicted. Currently, adoption-capacity theory posits that the ubiquity and low cost of modern ICT lowers the required financial intensity needed by organizations, thereby increasing the rate of adoption. But this explanation fails to account for seemingly counterintuitive

adoption behaviors related to ICT, such as lack of adoption despite financial means, regression to less advanced forms of ICT, and intentional destruction of ICT infrastructure. Further, the paper argued that in understanding ICT adoption, technological imitation or innovation in the direction of the more technologically complex is neither inevitable nor inherently advantageous. The more technologically advanced forms of ICT will not necessarily be adopted by groups, even when controlling for resource limitations.

The second paper, *What's New about the New Information Environment? How Private Firms Shape the Landscape for Strategic Competition*, honed in on disruptive attribute framework's second variable: the role of private actors. It argued that the degree of control platforms have in shaping the landscape is unprecedented. This control is exacerbated by the limited levers of influence states have on private platforms. This paper also presented a categorization schema for contextualizing the impacts of different policies and countermeasures on influence operations. Using three qualitative case studies, the paper showed that influence operations are responsive to platform changes. The paper also highlighted that policy changes imposed by platforms are increasing, but that they most often induce content constraints on influence operations. The paper argued that platform policy development must account for strategic impact and the secondary, downstream effects of changes on state competition. Further, consideration of strategic constraints should be embedded in the types of changes platforms adopt. Importantly, and as was then highlighted by the findings of the third paper, more attention must be paid to how policies impact (or fail to impact) the Global South.

The third paper, *Twitter and the Taliban: Pattern Paradoxes, and the Power of Platforms*, engaged in a comprehensive quantitative analysis of the Taliban's social media behavior during the 2021 takeover, establishing the scope and scale of the Taliban's presence on Twitter and the tactics the

group deployed in using the platform. This analysis highlighted the group's sophisticated use of platform features to amplify inconvenient truths and position itself as a morally and militarily superior force, in preparation for its intended role as the new government of Afghanistan. Overall, it establishes that the Taliban invested considerable time and organizational resources developing and amplifying a sophisticated and coordinated campaign in real-time. Open questions remain, including how instrumental social media was in the Taliban's summer takeover, but the implications are clear.

Evidence provided by this paper suggested that platforms are seemingly ignoring how certain politically motivated actors misuse their platforms. The Taliban's unchecked activity on Twitter may be indicative of broader trends of non-state armed groups permitted to proliferate and organize online, which could have dramatic consequences for other conflict contexts. Further, the possible singular exception to the argument of limited levers of state influence presented in Paper 2 is the United States. Most of the globally popular social media companies have American founders and have headquarters physically located within the U.S. And yet, in the case of the Taliban, the U.S. did not seek to exercise any kind of regulatory or coercive influence to limit their opponent's access.

Evidence presented across all three papers confer several common and policy relevant implications. First, they all stress how achieving total information control is difficult in modern conflict settings. Doing so is highly resource intensive and even then, there are ways to circumvent it. Paper 1 features multiple attempts by state actors to target the communications capacities of non-states: Syria's ban on WhatsApp on national networks (in response the rebels used Jordan's networks and alternative communication devices), the Nepalese government shutdown of cell service (in response the CPN-M reverted to satellite phones), and the Mexican government's targeting of cartel communications (in response Los Zetas built a national radio network). Paper 3

highlights the adaptive behaviors and strategies of the Taliban as they faced a changing information environment. During the group's rule over Afghanistan in the 1990s, the Taliban prevented the development of an ICT sector, enabling them to be the primary source of information for all Afghans. Once they morphed into an insurgency, with no oversight of the growth of the domestic technology sector, the Taliban knew that to compete in a new information environment, the group would need to adopt new technologies and develop tailored and adaptive usage strategies.

Second, the project highlights the growing importance of private actors and the limited ability of states to push back in the new information environment. Paper 2 asserts that there are two primary mechanisms through which states can attempt to influence social media companies: pass legislation (which can limit content or reduce the ability of platforms to collect user data) or enact total bans. However, the scope of impact of these approaches is limited to the geographical bounds of the state. Paper 1 also highlights the Russian government's acquisition of social media platform VKontakte. However, owning or banning a platform doesn't guarantee total control: in the recent crackdown on domestic information flows, Russian civilians are finding ways to access outside information. Paper 3 similarly highlights this challenge: while the Taliban were able to effectively coerce cell phone providers to access the technology, they lacked the same mechanism of influence with social media platform Facebook, forcing them to turn to Twitter. Usual avenues of influence, such as threats of violence or destruction of infrastructure, were irrelevant because the platforms are not physically based in the conflict environment.

Finally, the information landscape is changing, but it may not impact all actors equally. Paper 2 specifically argues that social media platforms are creating a new landscape, with a digital topography under their control. This paper provides an important caveat that application of these

policies may be uneven, depending on the actor or country. Demonstrable evidence of this is found in Paper 3's quantitative section, which highlights a small subset of the Taliban's proliferation on Twitter prior to the takeover. It is abundantly clear that the platform took minimal to no action against their content. This is especially highlighted by Table 7 in Appendix 1, which includes descriptions of videos in clear violation of Twitter's stated sensitive media policies preventing the posting of gore and overt violence.[550] These videos are still available on the platform (as of April 14, 2022). While platforms continue to improve their capacities, the case of the Taliban on Twitter may foreshadow the advantages that smaller groups and non-state actors may have in this new environment.

Collectively, these papers help to develop valuable theory, while also introducing two new datasets for use in future studies. However, they are not without limitations. First, they principally engage in theory building. Additional studies will be required to test the strength and full explanatory power of disruptive attribute theory presented in Paper 1. This same criticism applies to the approach taken in Paper 2: robust, quantitative analysis pinpointing the effects of a specific policy on state (and non-state) influence operations is required before confident, predictive claims can be made about the impact of a given platform policy. Finally, while Paper 3 identified important patterns in the Taliban's social media adoption and usage behaviors, the next step is to understand how this online effort translates to supporting real-world activities, such as military effectiveness.

Second, there are inherent biases in the cases and data used by all three papers. In Paper 1, the case studies featured involve comparatively well-resourced actors, on both the state and non-state side. Further research must be conducted to identify the interplay of the factors described by

550 "Sensitive Media Policy," *Twitter Help Center,* https://help.twitter.com/en/rules-and-policies/media-policy.

disruptive attribute theory with an organization's level of and type of funding. In Paper 2, case studies of social media use by armed organizations privilege those that have been caught by researchers or the platform. Only a select group of states and non-states have documented and extensive records of their online exploits. In turning to the data on platform policies, social media companies are not fully transparent about all changes made to social media platforms and do not always apply changes consistently in all contexts. Therefore, a policy which is theorized to impose a content constraint may be recorded as impacting a Chinese influence operation but not one from Venezuela. This difference in impact could be the of an uneven application of platform policy, due to organizational constraints faced by the platform such as a lack of resources devoted to content in a particular language or a cultural understanding of specific terms. The model takes policy descriptions and company statements at face value, an assumption made in order to isolate important mechanisms of impact. Much of the value of the model presented in Paper 2 is in simplifying in order to present a way of understanding both intended and unintended changes to the online landscape on the behaviors and capacities of politically motivated actors. However, it is important to note the online landscape has additional layers of complexity and change (i.e., the obscured nature of algorithmic recommendations on a given platform) that are beyond the scope of Paper 2. For Paper 3, it may be that there are some Taliban accounts that evaded identification and are thus excluded from this analysis.

Additionally, the project provoked several additional avenues for future inquiry. These include:

Adaptation. How do states and non-state actively adapt to challenges of ICT usage during conflict? Research is beginning to document how influence operations adapt. But the field lacks a sense of adaptation time and comparative rates of adaptation. In theory, social media offers a

valuable testing ground: it grants a time-stamped method of calculating the resurgence of new accounts associated with a state influence operation or a rebel group after a ban**.** Despite targeted removals and bans, both state and non-state armed organizations have persisted online in various forms, continually experimenting with new evasion tactics, platforms, and modes of propagating content. The research base lacks a conceptual framework for capturing this technological adaptation, often a byproduct of the decisions made by private actors rather than an opponent.

Privatization of the ICT sector. In civil wars, do states with publicly owned ICT infrastructure have an information advantage? In Paper 1, the Nepalese government was able to institute a national shutdown of cell networks because this infrastructure was all government owned**.** Both Russia and China have an iron grip on their domestic information environments, blocking online access to specific content and filtering global media. But Paper 1 also highlights how when Syria banned WhatsApp on national networks, rebels and civilians switched to using Jordanian cell networks. With the growth of VPNs and the development of a global ICT market, this perceived advantage may be lessened.

Timing of ICT introduction into a conflict setting. How does the timing and form of ICT diffusion shape conflict outcomes and the behaviors of conflict actors? As highlighted briefly in Paper 3, the onset of the conflict marked the beginnings of an ICT sector in Afghanistan. The Taliban were forced to cope with a set of ICT-based challenges prompted by massive foreign investment into developing national infrastructure. But for the cases highlighted in Paper 1, in other conflicts, armed groups grapple with preexisting ICT. How might this lead to differences in strategy, adoption, and use? There is some speculation that Russian forces in Ukraine are also avoiding the destruction of infrastructure because, in the event of success, this infrastructure would be relied

upon to establish governance functions. The timing of ICT introduction into a conflict setting also warrants further research. While a robust research base correlates rates of violence with access to phone service, it is important to investigate how individual actors grapple with the introduction of new technologies into a conflict space.

Social media platforms treat actors differently. How does the uneven application of policies shape strategies and innovations of states versus non-states in the online environment? When the Taliban took power, there was discourse around whether their newfound status as a state meant that they should be allowed access to social media. But, as highlighted in Paper 3, this discussion was largely irrelevant for Twitter, which had allowed the group to proliferate on their platform prior to the takeover. Paper 2 argues for the power of platforms in shaping the landscaping of strategic interaction. It presents compelling evidence of the Islamic State, Russia, and China responding to changes to platform policies. However, these policies (and the constraints they impose) appear to be applied inconsistently. Policies may be a forcing mechanism for adaptation and innovation that only certain actors are forced to deal with.

Understanding ICT adoption and usage patterns is increasingly essential, as the online information age presents new opportunities and challenges for organizations at war. The forms of information that can be collected, promoted, and controlled have changed and increased dramatically with the introduction of new forms of technology. The nature of ICT's global diffusion, dual-use function, relatively low-costs, and ease of adoption rather uniquely empowers lesser forces in challenging powerful states, including both civilians and non-state armed groups, leading to important consequences for the international system. The increasing relevance of social media to modern conflicts also emphasizes the need for focused attention on ICT's role in supporting the

success of armed organizations. Disruptive attribute theory underscores the need to think holistically about the organizational limitations and opportunities imposed by ICT on armed actors, from states to non-state armed groups, to begin building a better picture of how ICT will shape the future of conflict.

Bibliography

Abdelkader, Rima, and Emmanuelle Saliba, "Syrians Trapped in Aleppo Using WhatsApp to Post Cries for Help," *NBC News*, December 14, 2016, https://www.nbcnews.com/storyline/aleppos-children/syrian-dispatches-call-help-n696166.

Ackerman, Gary A., ""Designing Danger" Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue," *Journal of Strategic Security,* Vol. 9, No. 1 (2016), pp. 1-11.

Ackerman, Spencer, "Radio Zeta: How Drug Cartels Stayed Networked," *WIRED,* December 27, 2011, https:// www.wired.com/2011/12/cartel-radio-mexico/.

Aday, Sean, John Cluverius, and Steven Livingston, "As goes the statue, so goes the war: The emergence of the victory frame in television coverage of the Iraq War," *Journal of Broadcasting & Electronic Media*, Vol. 49, No. 3 (2005), pp. 314-331.

Adena, Maja, Ruben Enikolopov, Maria Petrova, Veronica Santarosa, and Ekaterina Zhuravskaya, "Radio and the Rise of the Nazis in Prewar Germany," *The Quarterly Journal of Economics*, Vol. 130, No. 4 (2015), pp. 1885-1939.

AFP, "Russia Bans Media Outlets From Using Words 'War,' 'Invasion'," *The Moscow Times*, https://www. themoscowtimes.com/2022/02/26/russia-bans-media-outlets-from- using-words-war-invasion-a76605.

Aggarwal, Neil Krishan, *The Taliban's Virtual Emirate: The Culture and Psychology of an Online Militant Community*, (Columbia University Press, 2016).

Al Jazeera, "Timeline: Afghanistan provincial capitals captured by Taliban," *Al Jazeera*, August 11, 2021, https://www.aljazeera.com/news/2021/8/11/afghanistan-taliban-provincial-capitals -cities-timeline.

Ali, Shiza, Mohammad Hammas Saeed, Esraa Aldreabi, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini, "Understanding the Effect of Deplatforming on Social Networks," In *13th ACM Web Science Conference* (2021).

Allen, Greg, and Taniel Chan, *Artificial intelligence and national security*, (Cambridge, MA: Belfer Center for Science and International Affairs, 2017).

Allen, T.S., and Stephen Rodriguez, "To Protect Democracy, Protect the Internet," *Foreign Policy*, July 14, 2020, https://foreignpolicy.com/2020/07/14/united-states-election-interference-illegal -social-media/.

Allyn, Bobby, "Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn," *NPR*, March 16, 2022, https://www.npr.org/2022/03/16/1087062648/deepfake-video -zelenskyy-experts- war-manipulation-ukraine-russia.

Amnesty International, "Singapore: Social media companies forced to cooperate with abusive fake news law," *Amnesty.org*, February 19, 2020, https://www.amnesty.org/en/latest/news/2020/02/singapore-social -media-abusive-fake-news-law/.

Andreas, Peter, "Redrawing the line: Borders and security in the twenty-first century," *International Security*, Vol. 28, No. 2 (2003), pp. 78-111.

Ang, Peng Hwa, Shyam Tekwani, and Guozhen Wang, "Shutting down the mobile phone and the downfall of Nepalese society, economy and politics," *Pacific Affairs*, Vol. 85, No. 3 (2012), pp. 547-561.

Angst, Corey M., Ritu Agarwal, Vallabh Sambamurthy, and Ken Kelley, "Social contagion and information technology diffusion: The adoption of electronic medical records in US hospitals," *Management Science*, Vol. 56, No. 8 (2010), pp. 1219-1241.

AP, "Twitter, Facebook fined for not moving user data to Russia," *AP News*, February 13, 2020, https:// apnews.com/article/a4fa655e946b9441b6e68ee3592a8f27.

Armand, Alex, Paul Atwell, and Joseph F. Gomes, "The reach of radio: Ending civil conflict through rebel demobilization," *American Economic Review*, Vol. 110, No. 5 (2020), pp. 1395-1429.

Arreguin-Toft, Ivan, *How the weak win wars: A theory of asymmetric conflict*, Vol. 99 (Cambridge University Press, 2005)

Associated Press, "Taliban turn cell phones back on in Afghan south," *CTV News*, April 5, 2011, https:// www.ctvnews.ca/taliban-turn-cell-phones-back-on-in-afghan-south-1.627627.

Atiq, Sarah, "The Taliban embrace social media: 'We too want to change perceptions'," *BBC News*, September 6, 2021, https://www.bbc.com/news/world-asia-58466939.

Awan, Imran, "Cyber-extremism: Isis and the power of social media," Society, Vol. 54, No. 2 (2017), pp. 138-149.

Bahar, Hazrat M., "Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter," *Media Asia,* Vol. 47, No. 1-2 (2020), pp. 34-46.

Bailard, Catie Snow, "Ethnic conflict goes mobile: Mobile technology's effect on the opportunities and motivations for violent collective action," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 323-337.

Bailey, Kenneth D., *Typologies and taxonomies: An introduction to classification techniques* (Sage, 1994).

Baines, Paul, and Nigel Jones, "Influence and interference in foreign elections: The evolution of its practice," *The RUSI Journal*, Vol. 163, No. 1 (2018), pp. 12-19.

Balnaves, Mark, "A Return to the Good Old Days: Populism, Fake News, Yellow Journalism, and the Unparalleled Virtue of Business People," *The Palgrave Handbook of Management History* (2020), pp. 935-949.

Barber, Benjamin, and Charles Miller, "Propaganda and Combat Motivation: Radio Broadcasts and German Soldiers' Performance in World War II," *World Politics*, Vol. 71, No. 3 (2019), pp. 457-502.

Bateman, Jon, Elonnai Hickok, Laura Courchesne, Isra Thange, and Jacob N. Shapiro, "Measuring the Effects of Influence Operations: Key Findings and Gaps from Empirical Research," *Carnegie Endowment for International Peace,* June 28, 2021, https://carnegieendowment.org /2021/06/28/measuring-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research-pub-84824.

Bateman, Jon, Natalie Thompson, Victoria Smith, "How Social Media Platforms' Community Standards Address Influence Operations," *Carnegie Endowment for International Peace,* April 1, 2021, https://carnegieendowment.org/2021/04/01how-social-media-platforms - community-standards-address-influence-operations-pub-84201.

Bay, Sebastian, Giorgio Bertolin, Nora Biteniece, Edward H. Christie, Anton Dek, R. Fredheim, J. Gallacher, Kateryna Kononova, and Tetiana Marchenko. "Responding to Cognitive Security Challenges." *NATO STRATCOM Centre of Excellence* (2019).

BBC, "Afghanistan: Facebook Continues Ban of Taliban-Related Content," *BBC*, August 17, 2021, https://www.bbc.com/news/business-58239786.

BBC, "Afghanistan: Street fighting rages as Taliban attack key city," *BBC*, August 3, 2021, https://www.bbc.com/news/world-asia-58051481.

BBC, "Afghanistan: Taliban continue attacks on three major cities," *BBC*, August 1, 2021, https://www.bbc.com/news/world-asia-58040141.

Becker, Jo, and Steven Lee Myers, "Russian Groups Crowdfund the War in Ukraine," *The New York Times*, June 11, 2015, https://www.nytimes.com/2015/06/12/world/europe/russian - groups-crowdfund-the-war- in-ukraine.html.

Berger, Carl, *An introduction to wartime leaflets* (Special Operations Research Office, the American University, 1959).

Berger, Carl, *Broadsides and Bayonets* (University of Pennsylvania Press, 2016).

Berger, Miriam, and Adam Taylor, "Will Twitter ban Iran's supreme leader next?" *The Washington Post*, February 2, 2021, https://www.washingtonpost.com/world/2021/02/02/will-twitter-ban -irans-supreme-leader -next.

Berman, Eli, Joseph H. Felter, and Jacob N. Shapiro, *Small Wars, Big Data* (Princeton University Press, 2018).

Bernatis, Vincent, "The Taliban and Twitter: Tactical reporting and strategic messaging," *Perspectives on Terrorism*, Vol. 8, No. 6 (2014), pp. 25-35.

Berti, Benedetta, "What's in a name? Re-conceptualizing non-state armed groups in the Middle East," *Palgrave Communications*, Vol. 2, No. 1 (2016), pp. 1-8.

Betz, David J., and Tim Stevens, *Cyberspace and the State: Towards a Strategy for Cyber-power* (Routledge, 2017).

Bhattacharjee, Giriraj, "Afghanistan: The final battle," *South Asia Monitor*, June 29, 2021, https://www.southasiamonitor.org/afghanistan/afghanistan-final-battle.

Bitektine, Alex, "Prospective case study design: qualitative method for deductive theory testing," *Organizational research methods*, Vol. 11, No. 1 (2008), pp. 160-180.

Bodine-Baron, Elizabeth Anne, Todd C. Helmus, Andrew Radin, and Elina Treyger, *Countering Russian social media influence*, (Santa Monica, CA: Rand Corporation, 2018).

Bond, Shannon, and Bobby Allyn, "Russia is restricting social media. Here's what we know," *NPR*, March 21, 2022, https://www.npr.org/2022/03/07/1085025672/russia-social-media-ban.

Bos, Michèle, and Jan Melissen, "Rebel diplomacy and digital communication: public diplomacy in the Sahel," *International Affairs*, Vol. 95, No. 6 (2019) pp. 1331-1348.

Bradshaw, Samantha, and Philip N. Howard, "The global organization of social media disinformation campaigns," *Journal of International Affairs*, Vol. 71, No. 1.5 (2018), pp. 23-32.

Bradshaw, Samantha, and Philip N. Howard, "The Global Disinformation Disorder: 2019 Global Inventory of Organised Social Media Manipulation," Working Paper (Oxford, UK), *Project on Computational Propaganda* (2019).

Brandt, Jessica, and Bret Schafer, "How China's 'wolf warrior' diplomats use and abuse Twitter," *Brookings Institution,* October 28, 2020, https://www.brookings.edu/techstream/how-chinas -wolf-warrior- diplomats-use-and-abuse-twitter/.

Brandt, Jessica, Valerie Wirtschafter, and Adya Danaditya, "Popular podcasters spread Russian disinformation about Ukraine biolabs," *Brookings Institution*, March 23, 2022, https://www. brookings.edu/techstream/popular-podcasters-spread-russian-disinformation-about-ukraine- biolabs/.

Brooking, Emmerson T.,"Before the Taliban took Afghanistan, it took the internet," *The Atlantic Council*, (2021).

Brownstone, Andy, "Meet the Libyan rebels on the front line," *BBC Newsbeat*, May 24, 2011, http://www.bbc. co.uk/newsbeat/13505340.

Bruton, Elizabeth, "Communication Technology," *International Encyclopedia of the First World War*, last updated December 9, 2014, https://encyclopedia.1914-1918-online.net/article/ communication_technology.

Bunker, Robert J., "Mexican Cartel Operational Note No. 1: Mexican Military Operations against Los Zetas Communications Networks," *Small Wars Journal* (2011).

Bunker, Robert J., and Alma Keshavarz, "Narco Radio C2 and CCTV Networks Reader," *Small Wars Journal -- El Centro eBook* (2019).

Butler, Gavin,"How Social Media Helped 'Taliban 2.0' Take Control of Afghanistan," *Vice News*, August 19, 2021, https://www.vice.com/en/article/z3x5we/social-media-helped-taliban -control-afghanistan.

Campbell, Donald T., "III."Degrees of freedom" and the case study," *Comparative political studies*, Vol. 8, No. 2 (1975), pp. 178-193.

Campbell, Donald T., "Pattern matching as an essential in distal knowing," In *The psychology of Egon Brunswik* (1966), pp. 81-106.

Campbell, W. Joseph, *Yellow journalism: Puncturing the myths, defining the legacies* (Greenwood Publishing Group, 2001).

Candela, Joaquin Quiñonero, "Managing Your Identity on Facebook with Face Recognition Technology," *Facebook Newsroom*, December 19, 2017, https://about.fb.com/news/2017/12/ managing-your-identity -on-facebook-with-face -recognition-technology/.

Carey, Craig, "Breaking the News: Telegraphy and Yellow Journalism in the Spanish-American War," *American Periodicals: A Journal of History & Criticism*, Vol. 26, No. 2 (2016), pp. 130-148.

Carter, A., and Erin McAweeney, "IRA in Ghana," *Graphika*, March 12, 2020, https://public-assets .graphika.com/reports/graphika_report_ira_in_ghana_double_deceit.pdf.

Carter, David B., Carter, Andrew C. Shaver, and Austin L. Wright, "Places to hide: Terrain, ethnicity, and civil conflict," *The Journal of Politics*, Vol. 81, No. 4 (2019), pp. 1446-1465.

Chakravorti, Bhaskar, "Facebook's Taliban Ban Will Prove Costly for Afghans," *Foreign Policy*, August 26, 2021. https://foreignpolicy.com/2021/08/26/taliban-facebook-ban-social -media-afghanistan/.

Chan, Holmes, "How Hong Kong Became a Testing Ground for an 'Anti-Facebook' Movement," *VICE News*, December 18, 2020, https://www.vice.com/en/article/y3gnvk/how-hong-kong-became-a-testing- ground-for-an-anti-facebook-movement.

Chandrasekharan, Eshwar, Umashanthi Pavalanathan, Anirudh Srinivasan, Adam Glynn, Jacob Eisenstein, and Eric Gilbert, "You can't stay here: The efficacy of reddit's 2015 ban examined through hate speech," *Proceedings of the ACM on Human-Computer Interaction*, Vol. 1, No. CSCW (2017), pp. 1-22.

Cheung, Eric, "Why Facebook is losing friends in Hong Kong," *Rest of World*, February 28, 2021, https://restofworld .org/2021/why-facebook-is-losing-hongkong/.

Chroust, Peter, "Neo-Nazis and Taliban on-line: Anti-modern political movements and modern media," *Democratization*, Vol. 7, No. 1 (2000), pp. 102-118.

Clark, Mitchell, "Twitter resists Indian government's orders to block protest accounts," *The Verge*, February 10, 2021, https://www.theverge.com/2021/2/10/22276479/twitter-free-speech - india-protests- government-block-orders.

"Civic integrity policy," *Twitter Help Center*, https://help.twitter.com/en/rules-and-policies /election-integrity-policy.

Clayton, Thomas, "Afghanistan: Background and US Policy in Brief," *Congressional Research Service* (2022).

Clements, Sam, "Los Zetas Drug Cartel Has Their Own Radio Network," *VICE*, January 2, 2013, http://www. vice.com/read/the-los-zetas-drug-cartel-have-theirown-radio-network.

Cohen, Eliot A., "Change and transformation in military affairs," *Journal of Strategic Studies*, Vol. 27, No. 3 (2004), pp. 395-407.

Collier, David, Jody LaPorte, and Jason Seawright, "Putting typologies to work: Concept formation, measurement, and analytic rigor," *Political Research Quarterly*, Vol. 65, No. 1 (2012), pp. 217-232.

Collier, David, Jody LaPorte, and Jason Seawright, "Typologies: Forming concepts and creating categorical variables," in *The Oxford Handbook of Political Methodology* (2008).

Condliffe, Jamie, "How to Fix Social Media's Big Problems? Lawmakers Have Ideas," *The New York Times*, July 30, 2018, https://www.nytimes.com/2018/07/30/business/dealbook/big-tech -regulation-ideas.html.

Constine, Josh, "Facebook will change algorithm to demote 'borderline content' that almost violates policies," *TechCrunch*, November 15, 2018, https://techcrunch.com/2018/11/15/facebook-borderline-content.

Courchesne, Laura Bahar Rasikh, Brian McQuinn, and Cody Buntain, "Powered by Twitter? The Taliban's Takeover of Afghanistan, Working Paper No. 30," *Empirical Studies of Conflict Project*, (2022).

Courchesne, Laura, and Brian McQuinn, "After the Islamic State: Social Media and Armed Groups," *War on the Rock*s, April 9, 2021, https://warontherocks.com/2021/04/after-the-islamic- state-social-media-and- armed-groups/.

Courchesne, Laura, Julia Ilhardt, and Jacob N. Shapiro, "Review of social science research on the impact of countermeasures against influence operations," *Harvard Kennedy School Misinformation Review*, (2021).

"COVID-19 misleading information policy," *Twitter Help Center*, https://help.twitter.com/en/rules -and-policies/medical-misinformation-policy.

Criezis, Meili, "Telegram's anti-IS Campaign: Effectiveness, Perspectives, and Policy Suggestions," *Global Network on Extremism and Technology*, July 30, 2020, https://gnet-research.org/2020/07/30/telegrams-anti-is-campaign-effectiveness-perspectives-and-policy-suggestions/

Crisp, Wil, and Suadad al-Salhy, "Exclusive: Inside Hizbollah's fake news training camps sowing instability across the Middle East," *The Telegraph*, August 2, 2020, https://www.telegraph.co.uk/news/2020/08/02/exclusive-inside-hezbollahs-fake-news-training-camps-sowing/.

Cronin, Audrey Kurth, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford University Press, 2019).

Culliford, Elizabeth, "Facebook removes Russian Network that Targeted Influencers to Peddle Anti-Vax Message," *Reuters*, August 10, 2021, https://www.reuters.com/technology/facebook-removes-russian- network-that-targeted- influencers-peddle-anti-vax-2021-08-10/.

Culliford, Elizabeth, "YouTube Says It Does Not Allow Taliban-Affiliated Accounts." *Reuters*, August 17, 2021, https://www.reuters.com/technology/youtube-says-it-bans-accounts-believed-be -owned-by-taliban-2021-08-17/.

Dafoe, Allan and Jason Lyall, "From cell phones to conflict? Reflections on the emerging ICT–political conflict research agenda," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 401-413.

Davis, Paul K., Eric V. Larson, Zachary Haldeman, Mustafa Oguz, and Yashodhara Rana, *Understanding and influencing public support for insurgency and terrorism* (Santa Monica, CA: RAND National Defense Research Institute, 2012).

Davis, Wynne, "Ukraine appears to have stalled Russia's advance. Here's what that could mean," *NPR*, March 18, 2022, https://www.npr.org/2022/03/18/1087314355/russia-ukraine -invasion-latest-analysis.

DeNardis, Laura, "Hidden levers of Internet control: An infrastructure-based theory of Internet governance." *Information, Communication & Society,* Vol. 15, No. 5 (2012), pp. 720-738.

DeNardis, Laura, and Andrea M. Hackl, "Internet governance by social media platforms," *Telecommunications Policy*, Vol. 39, No. 9 (2015), pp. 761-770.

Denyer, Simon, "China's scary lesson to the world: Censoring the Internet works," *The Washington Post*, May 23, 2016, https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html.

Detsch, Jack and Amy Mackinnon, ""The Ukrainians Are Listening': Russia's Military Radios Are Getting Owned," *Foreign Policy*, March 22, 2022, https://foreignpolicy.com/2022/03/22/ukraine-russia-military-radio/.

DFR Lab, "As the Taliban offensive gained momentum, so did its Twitter propaganda campaign," *Medium*, August 19, 2021, https://medium.com/dfrlab/as-the-taliban-offensive-gained -momentum -so-did-its- twitter-propaganda -campaign-75021ba3082.

DFR Lab, "Suspicious Twitter accounts boosted Taliban hashtag prior to Afghan election," *Medium*, November 1, 2019, https://medium.com/dfrlab/suspicious-twitter-accounts-boosted- taliban-hashtag-prior-to- afghan-election-c 303561713cf.

Dixit, Kunda, "Keep in touch: Satellite phones may be the only way to communicate in the event of a natural disaster," *Nepali Times*, March 26, 2010, http://archive.nepalitimes.com/news.php? id=16929#.YKPRR jsZ7q8.

Dorronsoro, Gilles, *The Taliban's winning strategy in Afghanistan*, Carnegie Endowment for International Peace, Vol. 29 (2009).

Drissel, David, "Reframing the Taliban insurgency in Afghanistan: new communication and mobilization strategies for the Twitter generation," *Behavioral sciences of terrorism and political aggression*, Vol. 7, No. 2 (2015), pp. 97-128.

Duncombe, Constance, "Twitter and transformative diplomacy: social media and Iran-US relations," *International Affairs*, Vol. 93, No. 3 (2017), pp. 545-562.

Duvanova, Dinissa, Alexander Semenov, and Alexander Nikolaev, "Do social networks bridge political divides? The analysis of VKontakte social network communication in Ukraine," *Post-Soviet Affairs,* Vol. 31, No. 3 (2015), pp. 224-249.

Eckstein, Harry, "Case study and theory in political science," *Case Study Method* (2000), pp. 119-164.

Eckstein, Harry, *Regarding politics: Essays on political theory, stability, and change*, (University of California Press, 1992).

Erlanger, Steven, "How Volodymyr Zelensky rallied Ukrainians, and the world, against Putin," *The New York Times*, February 27, 2022, https://www.nytimes.com/2022/02/27/world/europe/volodymyr-zelensky -ukraine -russia.html.

Evangelista, Matthew, *Innovation and the arms race* (Cornell University Press, 2019).

Facebook, "Introducing a New Info and Ads Section on Pages," *Facebook for Business*, June 28, 2018, https://www.facebook.com/business/news/introducing-a-new-info-and-ads-section-on-pages

Facebook, "What Types of IDs does Facebook accept?," *Facebook Help Center*, last accessed September 2, 2021, https://www.facebook.com/help/159096464162185.

Faizi, Fatima, Fahim Abed and Najim Rahim, "Afghan War Casualty Report: May 2021," *The New York Times*, June 3, 2021, https://www.nytimes.com/2021/05/06/world/asia/afghan-war-casualty-report-may- 2021.html

Fearon, James D., and David D. Laitin, "Ethnicity, insurgency, and civil war," *American Political Science Review*, Vol. 97, No. 1 (2003), pp. 75-90.

Federal Trade Commission, "FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook," Press Release 24, *FTC* (2019).

Feldstein, Steven, "The road to digital unfreedom: How artificial intelligence is reshaping repression," *Journal of Democracy*, Vol. 30, No. 1 (2019), pp. 40-52.

Feldstein, Steven, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, (Oxford University Press, 2021).

Fischer, Sarah, "Internet becomes battleground in Russia's Ukraine invasion," *Axios*, February 27, 2022, https://www.axios.com/internet-key-battleground-russia-ukraine-b39b49a2-79ff-4fdf-af15-1dee5 217c867.html.

Fishman, Brian, "Crossroads: Counter-terrorism and the Internet (February 2019)," *Texas National Security Review* (2019).

Fishwick, Carmen, "How a Polish student's website became an ISIS propaganda tool," *The Guardian*, August 15, 2014, https://www.theguardian.com/world/2014/aug/15/-sp-polish-man- website-isis-propaganda- tool.

Flashpoint Analyst Team, "Jihadists Presence Online Decentralizes After Telegram Ban," *Intel Corporation*, January 17, 2020, https://www.flashpoint-intel.com/geopolitical-physical-security/jihadists-presence -online-decentralizes-after-telegram-ban/

Fletcher, Tom, "Naked diplomacy: power and statecraft in the digital age and the future of #diplomacy," *International Affairs*, Vol. 93, No. 4 (2017), p. 973-975.

Forbes Technology Council, "15 Consequences of GDPR," *Forbes*, August 15, 2018, https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=2d1d226a94ad.

Foxley, Tim, The Taliban's propaganda activities: how well is the Afghan insurgency communicating and what is it saying? (SIPRI, 2007).

Frankel, Rafael, "An Update on the Situation in Myanmar," *Facebook Newsroom*, February 11, 2020, https://about.fb.com/news/2021/02 /an-update-on-myanmar/.

Frenkel, Sheera, and Ben Decker, "Taliban Ramp Up on Social Media, Defying Bans by the Platforms," *The New York Times*, August 18, 2021. https://www.nytimes.com/2021/08/18/technology/taliban-social-media-bans.html.

Frenkel, Sheera, and Ben Hubbard, "After Social Media Bans, Militant Groups Found Ways to Remain," *The New York Times*, April 19, 2019, https://www.nytimes.com/2019/04/19/technology/terrorist-groups- social-media.html.

"From Transition to Transformation: The Role of the ICT Sector in Afghanistan," *World Bank*, May 2013, https://www.infodev.org/infodev-files/final_afghanistan_ict_role_web.pdf.

Fuhrmann, Matthew, and Michael C. Horowitz, "Droning on: Explaining the proliferation of unmanned aerial vehicles," *International Organization*, Vol. 71, No. 2 (2017), pp. 397- 418.

Gagliarducci, Stefano, Massimiliano Gaetano Onorato, Francesco Sobbrio, and Guido Tabellini, "War of the waves: Radio and resistance during World War II," *American Economic Journal: Applied Economics*, Vol. 12, No. 4 (2020), pp. 1-38.

Gates, Scott, and Sukanya Podder, "Social media, recruitment, allegiance and the Islamic State," *Perspectives on Terrorism*, Vol. 9, No. 4 (2015), pp. 107-116.

Gebeily, Maya, "Secret Syria network warns of air raids over WhatsApp," *The Times of Israel*, January 21, 2016, https://www.timesofisrael.com/secret-syria-network-warns-of-air-raids-over- whatsapp/.

George, Alexander L. and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (MIT Press, 2005).

Gerring, John, "Case selection for case-study analysis: Qualitative and quantitative techniques," In *The Oxford Handbook of Political Methodology*, (2008).

Gerring, John, "Qualitative methods," *Annual Review of Political Science*, Vol. 20 (2017), pp. 15-36.

Gerring, John, "What is a case study and what is it good for?," *American Political Science Review*, Vol. 98, No. 2 (2004), p. 341-354.

Gerschenkron, Alexander, *Economic Backwardness in Historical Perspective: A Book of Essays* (Cambridge, Mass.: Belknap, 1962).

Ghaffary, Shirin, "How Facebook, Twitter, and YouTube Are Handling the Taliban," *Vox*, August 18, 2021, https://www.vox.com/recode/22630869/facebook-youtube-twitter-taliban-ban - social-media-afghanistan.

Gill, Paul, "Tactical innovation and the provisional Irish Republican Army," *Studies in Conflict & Terrorism*, Vol.40, No. 7 (2017), pp. 573-585.

Gillespie, Tarleton, "Governance of and by platforms," *SAGE handbook of social media* (2017), pp. 254-278.

Gillespie, Tarleton, "Platforms are not intermediaries," *Georgetown Law Technology Review*, Vol. 2, No. 2 (2018), pp. 198-216.

Gilli, Andrea and Mauro Gilli, "Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage," *International Security*, Vol. 43, No. 3 (2018), pp. 141 - 189.

Gilpin, Robert, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1981)

Giustozzi, Antonio, *Koran, Kalashnikov, and Laptop: The Neo-Taliban Insurgency in Afghanistan 2002-2007* (Columbia University Press, 2008).

Giustozzi, Antonio, *The Taliban at War: 2001-2018* (Oxford University Press, USA, 2019).

Glaser, April, Kevin Collier and Cyrus Farivar, "Some Taliban websites go offline amid broader tech crackdown," *NBC News*, August 20, 2021, https://www.nbcnews.com/tech/tech-news/ taliban-websites-go-offline-broader-tech -crackdown-rcna1735.

Gleicher, Nathaniel, Margarita Franklin, David Agranovich, Ben Nimmo, Olga Belogolova, Mike Torrey, "Threat Report: The State of Influence Operations 2017-2020," *Facebook Research*, May 20, 2021.

Gohdes, Anita R., "Pulling the plug: Network disruptions and violence in civil conflict," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 352-367.

Gohdes, Anita R., "Studying the Internet and Violent conflict," *Conflict Management and Peace Science*, Vol. 35, No. 1 (2018), pp. 89-106.

Gold, Ashley, "Twitter: More than 677,000 U.S. users engaged with Russian troll accounts," *Politico*, January 19, 2018, https://www.politico.com/story/2018/01/19/twitter-users-russian-trolls -437247.

Gold, Hadas, "Facebook, Google and Twitter won't give Hong Kong authorities user data for now," *CNN*, July 7, 2020, https://www.cnn.com/2020/07/06/tech/whatsapp-facebook-hong -kong/index.html.

Goldman, Emily O., "Cultural foundations of military diffusion," *Review of International Studies*, Vol. 32, No. 1 (2006), pp. 69-91.

Goldman, Emily O., "Receptivity to revolution: Carrier air Power in Peace and War," *The Diffusion of Military Technology and Ideas* (2003).

Goldstein, Josh A., and Shelby Grossman, "How disinformation evolved in 2020," *Brookings Institution*, January 4, 2021, https://www.brookings.edu/techstream/how-disinformation-evolved-in-2020/.

Gonzalez, Robert M., "Cell phone access and election fraud: evidence from a spatial regression discontinuity design in Afghanistan," *American Economic Journal: Applied Economics*, Vol. 13, No. 2 (2021), pp. 1-51.

Greenberg, Julia, "Why Facebook and Twitter Can't Just Wipe Out ISIS Online," *WIRED,* November 21, 2015, https://www.wired.com/2015/11/facebook-and-twitter-face-tough - choices-as-isis-exploits-social-media/.

Greenburg, Andy, "Google's New YouTube Analysis App Crowdsources War Reporting," *WIRED*, April 20, 2016, https://www.wired.com/2016/04/googles-youtube-montage-crowdsources- war-reporting/.

Greer, Ryan, and Vidhya Ramalingam, "The Search for Extremism: Deploying the Redirect Method," *The Washington Institute for Near East Policy,* February 27, 2020, https://www. washingtoninstitute.org/policy-analysis/search-extremism-deploying-redirect-method.

Grossman, Shelby, Katie Jonsson, Nicholas Lyon, and Lydia Sizer, "Slanted Narratives, Social Media, and Foreign Influence in Libya," *Journal of Quantitative Description: Digital Media*, Vol. 1 (2022) pp. 1-57.

Grove, Thomas, "Russian Social Media Seen as Threat to Ukraine and to Cybersecurity," *The Wall Street Journal*, May 29, 2017, https://www.wsj.com/articles/russian-social-media-seen-as-threat-to-ukraine-and-to- cybersecurity-1496055 606.

Guild, Blair, "Twitter notifies 1.4 million of interaction with Russian accounts," *CBS News*, January 31, 2018, https://www.cbsnews.com/news/twitter-notifies-1-4-million-of-interaction-with - russian-accounts/.

Gwakh, Bashir Ahmad, "The Taliban's Internet Strategy," *Radio Free Europe / Radio Liberty*, September 9, 2011, https://www.rferl.org/a/the_talibans_internet_strategy/24323901.html.

Hachhethu, Krishna, "Maoist insurgency in Nepal: An overview," *The Naxal Challenge: Causes, Linkages and Policy Option* (2008) pp. 136-52.

Hachhethu, Krishna, "The Communist Party of Nepal (Maoist): Transformation from an insurgency group to a competitive political party," *European Bulletin of Himalayan Research*, Vol. 33, No. 34 (2009), pp. 39-71.

Halverson, James, "Los Zetas and proprietary radio network development," *Journal of Strategic Security*, Vol. 9, No. 1 (2016), pp. 70-83.

Hargittai, Eszter, "Weaving the Western Web: Explaining differences in Internet connectivity among OECD countries," *Telecommunications policy,* Vol. 23, No. 10-11 (1999), pp. 701-718.

Harvey, Del, and Yoel Roth, "An update on our elections integrity work," *Twitter Blog*, October 1, 2018, https://blog.twitter.com/en_us/topics/company/2018/an-update-on-our-elections - integrity-work.html.

Heilweil, Rebecca, "At least one member of Congress thinks we need a government agency to regulate social media companies," *Vox*, March 25, 2021, https://www.vox.com/recode/ 22351100/congress-peter-welch-facebook-twitter-google-youtube-social-media- agency.

Heller, Sam, "The Syrian Ceasefire Is Held Together by an Unlikely Group of Frenemies — and WhatsApp," *VICE*, March 16, 2016, https://www.vice.com/en/article/xw3kvw/the-americans-russians-and-the-un-are-keeping-syrias-shaky-ceasefire-afloat-with-whatsapp-text-messages.

Hendrix, Justin, "Social Media and the Future of the Taliban," *Tech Policy Press*, August 20, 2021, https://techpolicy.press/social-media-and-the-future-of-the-taliban/.

Herbert, Matt, "Libya's War Becomes a Tech Battleground," *Institute for Security Studies*, October 8, 2019, https://issafrica .org/iss-today/libyas-war-becomes-a-tech-battleground.

Herrman, John, "What if Platforms Like Facebook Are Too Big to Regulate?" *The New York Times Magazine*, October 4, 2017,https://www.nytimes.com/2017/10/04/magazine/what-if-platforms-like-facebook- are-too-big-to-regulate .html.

Higgins, Eliot, "These are the Cluster Munitions Documented by Ukrainian Civilians," *Bellingcat,* March 11, 2022, https://www.bellingcat.com/news/rest-of-world/2022/03/11/these- are-the-cluster-munitions -documented-by-ukrainian-civilians/.

Himelfarb, Sheldon, and Cecilia Paradi-Guilford, "Can You Help Me Now?: Mobile Phones and Peacebuilding in Afghanistan," *United States Institute for Peace,* November 15, 2010, https://www.usip.org/publications/ 2010/11/can-you-help-me-now.

Hobbs, William R., and Margaret E. Roberts. "How sudden censorship can increase access to information," *American Political Science Review*, Vol. 112, No. 3 (2018), pp. 621-636.

Holman, Timothy, "'Gonna Get Myself Connected' The Role of Facilitation in Foreign Fighter Mobilizations," *Perspectives on Terrorism*, Vol. 10, No. 2 (2016), pp. 2-23.

Hong, Seong Choul, "Propaganda leaflets and Cold War frames during the Korean War," *Media, War & Conflict*, Vol. 11, No. 2 (2018), pp. 244-264.

Horowitz, Michael C., "Artificial intelligence, international competition, and the balance of power," *Texas National Security Review*, Vol. 1, Issue 3 (2018).

Horowitz, Michael C., "Do emerging military technologies matter for international politics?," *Annual Review of Political Science*, Vol. 23 (2020), pp. 385-400.

Horowitz, Michael C., "Nonstate actors and the diffusion of innovations: The case of suicide terrorism," *International Organization*, Vol. 64, No. 1 (2010), pp. 33-64.

Horowitz, Michael C., "Nonstate actors and the diffusion of innovations: The case of suicide terrorism," *International Organization*, Vol. 64, No. 1 (2010), pp. 33-64l.

Horowitz, Michael C., Shahryar Pasandideh, Andrea Gilli, and Mauro Gilli, "Correspondence: Military-Technological Imitation and Rising Powers," *International Security*, Vol. 44, No. 2 (2019), pp. 185-192.

Horowitz, Michael C., *The diffusion of military power: Causes and consequences for international politics,* (Harvard University, 2007).

Horton, Alex and Shane Harris, "Russian troops' tendency to talk on unsecured lines is proving costly," *The Washington Post*, March 27, 2022, https://www.washingtonpost.com/national-security/2022/03/27 /russian-military-unsecured- communications/.

Howard, Philip N., Aiden Duffy, Deen Freelon, Muzammil M. Hussain, Will Mari, and Marwa Maziad, "Opening closed regimes: what was the role of social media during the Arab Spring?," *Available at SSRN 2595096* (2011).

Huang, Aaron, "Combatting and Defeating Chinese Propaganda and Disinformation," *HKS Belfer Center for Science and International Affairs* (July 2020).

Hudson, Valerie M., *Artificial intelligence and international politics* (Routledge, 2019).

Ibrahimi, S. Yaqub, "The Taliban's Islamic Emirate of Afghanistan (1996–2001): War-Making and State-Making as an Insurgency Strategy," *Small Wars & Insurgencies*, Vol. 28, No. 6 (2017), pp. 947-972.

Ingram, David, "Facebook says it is taking down more material about ISIS, al-Qaeda," *Reuters*, April 23, 2018, https://www.reuters.com/article/facebook-extremism-int/facebook- says-it-is- taking-down-more-material-about-isis-al-qaeda-idUSKBN1HU2PY.

Ingram, Haroro J., "An analysis of Islamic State's Dabiq magazine," *Australian Journal of Political Science* Vol. 51, No. 3 (2016), pp. 458-477.

Innes, Helen, and Martin Innes, "De-platforming disinformation: conspiracy theories and their control," *Information, Communication & Society,* (2021), pp. 1-19.

Instagram, "Introducing Instagram in Arabic, Hebrew and Farsi," *Instagram Blog*, October 31, 2017, https://about.instagram.com/blog/announcements/introducing-instagram-in-arabic-hebrew-and-farsi.

Instagram, "Introducing New Authenticity Measures on Instagram," *Instagram Blog,* August 13, 2020, https://about.instagram.com/blog/announcements/introducing-new-authenticity-measures-on-instagram.

International Crisis Group, "Nepal's Maoists: Their Aims, Structure and Strategy," *Asia Report, No. 104* (2005).

Isaac, Mike, and Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," *The New York Times,* October 30, 2017, https://www.nytimes.com/2017 /10/30/ technology/facebook- google-russia.html.

Ives, Mike, "Satellite internet terminals, sent by Elon Musk, arrive in Ukraine," *The New York Times*, March 1, 2022, https://www.nytimes.com/2022/02/28/world/europe/elon-musk-satellite-internet-ukraine. html.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness, "Fancy bears and digital trolls: Cyber strategy with a Russian twist," *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), pp. 212-234.

Jervis, Robert, *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon* (Cornell University Press, 1989).

Jhaver, Shagun, Christian Boylston, Diyi Yang, and Amy Bruckman, "Evaluating the Effectiveness of Deplatforming as a Moderation Strategy on Twitter," *Proceedings of the ACM on Human-Computer Interaction* (2021).

Johnson, A. Ross, "Managing media influence operations: Lessons from radio free Europe/Radio liberty," *International Journal of Intelligence and Counterintelligence*, Vol. 31, No. 4 (2018), pp. 681-701.

Johnson, Dominic D.P., and Dominic Tierney, "Bad world: The negativity bias in international politics," *International Security*, Vol. 43, No. 3 (2018), pp. 96-140.

Johnson, James, "Artificial intelligence & future warfare: implications for international security," *Defense & Security Analysis*, Vol. 35, No. 2 (2019), pp. 147-169.

Johnson, Thomas H., "Taliban adaptations and innovations," *Small Wars & Insurgencies,* Vol. 24, No. 1 (2013), pp. 3-27.

Johnson, Thomas H., "The Taliban insurgency and an analysis of Shabnamah (Night Letters)," *Small Wars & Insurgencies*, Vol. 18, No. 3 (2007), pp. 317-344.

Johnson, Thomas H., Matthew DuPee, and Wali Shaaker, *Taliban narratives: The use and power of stories in the Afghanistan conflict* (Oxford University Press, 2017).

Jones, Benjamin T., and Eleonora Mattiacci, "A manifesto, in 140 characters or fewer: Social media as a tool of rebel diplomacy," *British Journal of Political Science*, Vol. 49, No. 2 (2019), pp. 739-76.

Jones, Seth G., *In the graveyard of empires: America's war in Afghanistan*, (WW Norton & Company, 2010).

Joseph, Anita and Michele Paselli, "Verifying the Identity of People Behind High-Reach Profiles," *Facebook Newsroom*, May 28, 2020, https://about.fb.com/news/2020/05/id-verification-high-reach-profiles/

Juniper, Dean, "The First World War and Radio Development," *The RUSI Journal*, Vol. 148, No. 1 (2003), pp. 84-89.

Kalyvas, Stathis N., *The landscape of political violence* (New York: Oxford University Press, 2019).

Kang, Cecilia, and Adam Satariano, "Regulators Around the World Are Circling Facebook," *The New York Times,* April 25, 2019, https://www.nytimes.com/2019/04/25/technology/facebook -regulation-ftc-fine.html.

Kang, Cecilia, Nicholas Fandos, Mike Isaac, "Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill," *The New York Times*, October 31, 2017,

https://www.nytimes.com/2017/10/31/us/politics/facebook-twitter-google-hearings-congress.html?smid=tw-share&_r=0.

Kantchev, Georgi, "Russia Restricts Twitter Speed Over Banned Content," *The Wall Street Journal*, March 10, 2021, https://www.wsj.com/articles/russia-restricts-twitter-speed-over-banned -content-11615374130.

Karan, Kanishk, and Pepe Zhang, "Twitter's Hong Kong Archives: Chinese Commercial Bots at Work," *Medium*, September 4, 2019, https://medium.com/dfrlab/twitters-hong-kong-archives-chinese-commercial-bots-at-work-f4c7ae8eea64.

Kaylan, Melik, "Syria's War Viewed Almost in Real Time," The Wall Street Journal, September 27, 2013, https://www.wsj.com/articles/syria8217s-war-viewed-almost-in-real-time-138030 5826.

Keating, Joshua, "Firing mortars? There's an app for that," *Slate*, September 18, 2013, https://slate. com/news-and-politics/2013/09/video-of-free-syrian-army-using-an-ipad -to-aim-mortars.html.

Keating, Joshua, "The Taliban's YouTube channel," *Foreign Policy,* October 13, 2009, https://foreign policy.com/2009/10/13/the-talibans-youtube-channel/.

Keefe, Patrick Radden, "Cocaine Incorporated," *The New York Times*, June 15, 2012, http://www. nytimes.com/2012/06/17/magazine/how-a-mexican-drugcartel-makes-its-billions.html.

Kellow, Christine L., and H. Leslie Steeves, "The role of radio in the Rwandan genocide," *Journal of communication*, Vol. 48, No. 3 (1998), pp. 107-128.

Kemp, Simon, "Digital 2021: Afghanistan," *Data Reportal*, February 11, 2021, https://datareportal .com/reports/digital -2021-afghanistan.

Kern, Rebecca, Mark Scott, Clothilde Goujard, "Social media platforms on the defensive as Russian-based disinformation about Ukraine spreads," *POLITICO,* March 24, 2022,

https://www.politico.com/news/2022/02/24/social-media-platforms-russia-ukraine-disinformation-00011559.

Kiiski, Sampsa and Matti Pohjola, "Cross-country diffusion of the Internet," *Information Economics and Policy*, Vol. 14, No. 2 (2002), pp. 297-310.

Kim, Sangyeon, Omer F. Yalcin, Samuel E. Bestvater, Kevin Munger, Burt L. Monroe, and Bruce A. Desmarais, "The Effects of an Informational Intervention on Attention to Anti-Vaccination Content on YouTube," In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 14, (2020) pp. 949-953.

Kim, Young Mie, "Uncover: Strategies and Tactics of Russian Interference in US Elections," *Project DATA (Digital Ad Tracking & Analysis*), (2018).

Kim, Young Mie, "New Evidence Shows How Russia's Election Interference Has Gotten More Brazen," *Brennan Center for Justice*, March 5, 2020, https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more.

Klausen, Jytte, "Tweeting the Jihad: Social media networks of Western foreign fighters in Syria and Iraq," *Studies in Conflict & Terrorism*, Vol. 38, No. 1 (2015), pp. 1-22.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, and Jenny Oberholtzer, *Lessons from Russia's operations in Crimea and Eastern Ukraine,* (Rand Corporation, 2017).

Kononov, Nickolay, "The Kremlin's Social Media Takeover," *The New York Times*, March 10, 2014, https://www. nytimes.com/2014/03/11/opinion/the-kremlins-social-media-takeover.html.

Kozlov, Petr and Anna Rynda, "Afghan crisis: Russia plans for new era with Taliban rule," *BBC*, August 21, 2021, https://www.bbc.com/news/world-europe-58265934.

Lakshmanan, Indira A.R., "Fighting the Taliban with cell phones," *The New York Times*, March 23, 2010, https://www.nytimes.com/2010/03/24/world/asia/24iht-letter.html.

Larson, Eric V., Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Q. Thurston, *Foundations of effective influence operations: A framework for enhancing army capabilities* (RAND Arroyo Center Santa Monica CA, 2009).

Lasswell, Harold Dwight, *Propaganda technique in world war I,* Vol. 170, MIT Press, 1971.

Latifi, Ali M., "Afghanistan's Herat under pressure amid ongoing Taliban assault," *Al Jazeera*, July 31, 2021, https://www.aljazeera.com/news/2021/7/31/afghanistans-herat-under-pressure-amid-ongoing-taliban-assault.

Lawoti, Mahendra, "Evolution and growth of the Maoist insurgency in Nepal," In *The Maoist Insurgency in Nepal*, (Routledge, 2009), pp. 25-50.

Leathern, Rob, and Emma Rodgers, "A New Level of Transparency for Ads and Pages," *Facebook Newsroom*, June 28, 2018, https://about.fb.com/news/2018/06/transparency-for-ads -and-pages/.

Li, Darryl, "Echoes of violence: Considerations on radio and genocide in Rwanda," *Journal of Genocide Research*, Vol. 6, No. 1 (2004), pp.9-27.

Lin, Herbert, "The existential threat from cyber-enabled information warfare," *Bulletin of the Atomic Scientists*, Vol. 75, No. 4 (2019), pp. 187-196.

Lindsay, Jon R., *Information technology and military power,* (Cornell University Press, 2020).

Lipin, Michael, "Social Media Use by Iran's Sanctioned Officials Poses Dilemma for US," *VOA News*, September 10, 2019, https://www.voanews.com/middle-east/social-media-use-irans -sanctioned-officials-poses-dilemma-us.

Lisa J. Campbell, "Los Zetas: operational assessment," *Small Wars & Insurgencies*, Vol. 21, No. 1 (2010), pp. 55-80.

Lomas, Natasha, "Germany tightens online hate speech rules to make platforms send reports straight to the feds," *Tech Crunch*, June 19, 2020, https://techcrunch.com/2020/06/19/

germany-tightens-online-hate-speech-rules-to-make-platforms-send-reports-straight-to-the-feds/.

Loyle, Cyanne E., and Samuel E. Bestvater, "#rebel: Rebel communication strategies in the age of social media," *Conflict Management and Peace Science*, Vol. 36, No. 6 (2019), pp. 570-590.

Macías-Medellín, Martín, and Laura H Atuesta, "Constraints and military coordination: How ICTs shape the intensity of rebel violence," *International Interactions*, Vol. 47, No. 4 (2021), pp. 692-719.

Mack, Andrew, "Why big nations lose small wars: The politics of asymmetric conflict," *World Politics*, Vol. 27, No. 2 (1975), pp. 175-200.

Mahnken, Thomas G., Joseph Maiolo, and David Stevenson, *Arms races in international politics: from the nineteenth to the twenty-first century* (Oxford University Press, 2016).

Mair, David, "# Westgate: A case study–how Al-Shabaab used Twitter during an ongoing attack," In *Violent Extremism Online* (Routledge, 2016), pp. 65-86.

Maisland, Lindsay, "China's Modernizing Military," *Council on Foreign Relations*, February 5, 2020, https://www. cfr.org/backgrounder/chinas-modernizing-military.

Maisland, Lindsay, "The Taliban in Afghanistan," *Council on Foreign Relations*, September 15, 2021, https://www. cfr.org/backgrounder/taliban-afghanistan

Maisland, Lindsay, "Why China-Taiwan Relations Are So Tense," *Council on Foreign Relations*, May 10, 2021, https://www.cfr.org/backgrounder/china-taiwan-relations-tension-us-policy.

Makhortykh, Mykola, and Maryna Sydorova, "Social media and visual framing of the conflict in Eastern Ukraine," *Media, War & Conflict,* Vol. 10, No. 3 (2017), pp. 359-381.

Manacorda, Marco, and Andrea Tesei, "Liberation technology: Mobile phones and political mobilization in Africa," *Econometrica,* Vol. 88, No. 2 (2020), pp. 533-567.

Mansell, Robin, Chrisanthi Avgerou, Roger Silverstone, and Danny Quah, *The Oxford handbook of information and communication technologies*, (Oxford Handbooks, 2007).

Mansfield, Edwin, "Technical change and the rate of imitation," *Econometrica: Journal of the Econometric Society* (1961), pp. 741-766.

Martin, Diego A., Jacob N. Shapiro, and Julia G. Ilhardt, "Version 2.0: Recent trends in online foreign influence efforts," August 5, 2020, https://scholar.princeton.edu/sites/default/files/jns/files/trends_in_online_influence_efforts_v2.0_aug_5_2020.pdf.

Martin, Diego A., Jacob N. Shapiro, and Michelle Nedashkovskaya, "Recent trends in online foreign influence efforts," *Journal of Information Warfare*, Vol. 18, No. 3 (2019), pp. 15-48.

Masi, Alessandra, "Facebook's $19 Billion App Is Hugely Popular Among the Syrian Opposition," *Business Insider*, February 23, 2014, https://www.businessinsider.com/whatsapp-is-hugely-popular-among-syrian-rebels-and-activists-2014-2.

Matsakis, Louise, "Does TikTok Really Pose a Risk to US National Security?" *WIRED,* July 17, 2020, https://www.wired.com/story/tiktok-ban-us-national-security-risk/.

Mayzelle, Megan, Maria-Paz Santibañez, Jessica Schweiger, and Courtney Jallo, "Assessment of Information and Communication Technologies in Afghan Agricultural Extension," (2015).

Mazarr, Michael J., Ryan M. Bauer, Abigail Casey, Sarah A. Heintz, and Luke J. Matthews, *The emerging risk of virtual societal warfare: Social manipulation in a changing information environment* (RAND Corporation, 2019).

Meaker, Morgan, "'Hate is Way More Interesting Than That': Why Algorithms Can't Stop Toxic Speech Online," *Pacific Standard Magazine*, February 28, 2019, https://psmag.com/ideas/neo-nazi-hate-speech-foiling-algorithms.

Mearsheimer, John J., *The tragedy of great power politics*, (WW Norton & Company, 2001).

Mehrdad, Ezzatullah, "How Citizen Uproar Halted Afghanistan's Ban on WhatsApp," *Fast Company*, November 21, 2017, https://www.fastcompany.com/40498985/after-citizen-uproar- afghanistan-ends-a-ban-on- whatsapp-and-telegram.

Menkhaus, Ken,"Al-Shabaab and social media: A double-edged sword," *Brown Journal of World Affairs*, Vol. 20 (2013).

Merrin, William, *Digital war: A critical introduction* (Routledge, 2018).

Meyer, David, "A Facebook case in Belgium could open the floodgates for GDPR privacy suits," Fortune, January 13, 2021, https://fortune.com/2021/01/13/facebook-belgium-ireland-privacy-tracking-cjeu -bobek-max-schrems/.

Meyer, David, "In Facebook case, top EU court opens floodgates for more GDPR suits against Big Tech," *Fortune*, June 15, 2021, https://fortune.com/2021/06/15/cjeu-facebook-ireland -belgium-gdpr-lead -authority/.

Midlarsky, Manus I., Martha Crenshaw, and Fumihiko Yoshida, "Why violence spreads: The contagion of international terrorism," *International Studies Quarterly*, Vol. 24, No. 2 (1980), pp. 262-298.

Miller, Elhanan, "Syrian opposition uses home-made rockets and Google technology, video reveals," *The Times of Israel*, August 20, 2012, http://www.timesofisrael.com/ syrianopposition-uses- home-made-rockets-google-technology-new video-reveals/.

Mitts, Tamar, "Countering Violent Extremism and Radical Rhetoric," *International Organization*, Vol. 76, Winter 2022, pp. 251–72.

Mitts, Tamar, "Banned: How Deplatforming Extremists Mobilizes Hate in Dark Corners of the Internet," (Working Paper), July 25, 2021.

Mitts, Tamar, Gregoire Phillips, and Barbara F. Walter, "Studying the impact of ISIS propaganda campaigns," *The Journal of Politics*, Vol. 84, No. 2 (2022).

Molina, Brett, "Ukraine confirms arrival of Starlink satellite internet hardware after plea to Elon Musk," *USA Today*, March 1, 2022, https://www.usatoday.com/story/tech/2022/03/01/ starlink-ukraine-elon-musk -satellite-internet/ 9328753002/.

Monaco, Nick, Melanie Smith, and Amy Studdart, "Detecting Digital Fingerprints: Tracing Chinese Disinformation in Taiwan," *Graphika*, August 25, 2020, https://graphika.com/ reports/ detecting-digital-fingerprints-tracing -chinese-disinformation-in-taiwan/.

Montgomery, Evan Braden, "Signals of strength: Capability demonstrations and perceptions of military power," *Journal of Strategic Studies*, Vol. 43, No. 2 (2020), pp. 309-330.

Morar, David, and Bruna Martins dos Santos, "The push for content moderation legislation around the world," *Brookings Institution*, September 21, 2020, https://www.brookings.edu/blog/tech tank/2020/09/21/the-push-for-content-moderation-legislation-around-the-world/.

Mozilla, "Resisting a WhatsApp and Telegram ban in Afghanistan," *Internet Health Report*, April 2018, https://internethealthreport.org/2018/resisting-a-whatsapp-and-telegram-ban-in -afghanistan/.

Mozur, Paul, "A Genocide Incited on Facebook, With Posts From Myanmar's Military," *The New York Times*, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/ myanmar-facebook-genocide .html.

Mozur, Paul, and Zia ur-Rehman, "How the Taliban Turned Social Media Into a Tool for Control," *The New York Times*, August 20, 2021, https://www.nytimes.com/2021/08/20/ technology/afghanistan-taliban-social-media.html.

Mozur, Paul, Mike Isaac, David E. Sanger, and Richard C. Paddock, "Facebook Takes a Side, Barring Myanmar Military After Coup," *The New York Times*, February 24, 2021, https://www. nytimes.com/2021/02/24/ technology/facebook -myanmar-ban.html.

Myre, Greg, "From Wristwatches To Radio, How World War I Ushered In The Modern World," *NPR*, April 2, 2017, https://www.npr.org/sections/parallels/2017/04/02/521792062/ from-wristwatches-to-radio- how-world-war-i-ushered-in-the-modern-world.

Nasar, Khudai Noor, "Afghanistan: Social media users delete profiles over fear of attack," *BBC*, September 27, 2021, https://www.bbc.com/news/world-asia-58710194.

Nassetta, Jack, and Kimberly Gross, "State media warning labels can counteract the effects of foreign misinformation," *Harvard Kennedy School Misinformation Review* (2020).

Nimmo, Ben, C. Shawn Eib, L. Tamora, "Cross-Platform Spam Network Targeted Hong Kong Protests," *Graphika*, September 25, 2019, https://public-assets.graphika.com/reports/ graphika_report_ spamouflage.pdf.

Nimmo, Ben, Camille François, C Shawn Eib, Léa Ronzaud, "IRA Again: Unlucky Thirteen," *Graphika*, September 1, 2020, https://graphika.com/reports/ira-again-unlucky-thirteen/.

Nimmo, Ben, Camille Francois, C. Shawn Eib, Léa Ronzaud and Joseph Carter, "GRU and the Minions," *Graphika*, September 24, 2020, https://graphika.com/reports/gru-and-the - minions/.

Nimmo, Ben, Camille François, C. Shawn Eib, Léa Ronzaud, "Return of the (Spamouflage) Dragon," *Graphika*, April 24, 2020, https://public-assets.graphika.com/reports/Graphika _Report_Spamouflage_Returns. pdf.

Nimmo, Ben, Camille François, C. Shawn Eib, Léa Ronzaud, "Spamouflage Goes to America," *Graphika*, August 12, 2020, https://public-assets.graphika.com/reports/graphika_report_ spamouflage_goes_to _america.pdf.

Nimmo, Ben, Camille François, C. Shawn Eib, Léa Ronzaud, Melanie Smith, Thomas Lederer, Joseph A. Carter, Erin McAweeney, "IRA in Ghana: Double Deceit," *Graphika*, March 12, 2020, https://www. graphika.com/reports/ira-in-ghana-double-deceit/.

Nimmo, Ben, Ira Hubert, and Yang Cheng, "Spamouflage Breakout," *Graphika*, February 4, 2021, https:// public-assets.graphika.com/reports/graphika_report_spamouflage_breakout.pdf.

Nix, Naomi, and Bloomberg, "Facebook and Twitter Weigh Giving a Social-Media Megaphone to the Taliban," *Fortune*, August 21, 2021, https://fortune.com/2021/08/21/facebook-twitter -social-media-taliban/.

Nossiter, Adam, "Taliban Enter Kandahar City and Seize Border Posts," *The New York Times*, July 9, 2021, https://www.nytimes.com/2021/07/09/world/asia/taliban-kandahar-afghanistan.html.

Nori, Norias, "Afghanistan: Mobile-Phone Towers Are Taliban's New Target," *Radio Free Europe / Radio Free Liberty*, March 3, 2008, https://www.rferl.org/a/1079578.html.

O'Connor, Sarah, Fergus Hanson, Emilia Currey, and Tracy Beattie, "Cyber-enabled foreign interference in elections and referendums," *Australian Strategic Policy Institute* (2020).

Ogura, Kiyoko, "Seeking state power: The communist party of Nepal (Maoist)," *Berghof Transitions Series,* No. 3 (2008).

Pancevski, Bojan, "Using a New Cyber Tool, Westerners Have Been Texting Russians About the War in Ukraine," *The Wall Street Journal*, March 22, 2022, https://www.wsj.com/articles/using-a-new-cyber-tool-westerners-have-been-texting-russians-about-the-war-in-ukraine-11647100803.

Parks, Miles, "Twitter Bans Ads From Russian State Media, Citing Election Interference Efforts," *NPR*, October 26, 2017, https://www.npr.org/2017/10/26/560199026/twitter-ends-russian -state-media -advertisements-citing-2016 -interference-efforts.

Paul, Thazha Varkey, *Asymmetric conflicts: war initiation by weaker powers* (Cambridge University Press, 1994).

Payne, Kenneth, "Artificial intelligence: a revolution in strategic affairs?," *Survival*, Vol. 60, No. 5 (2018), pp. 7-32.

Perrigo, Billy, "Facebook's Ban of Myanmar's Military Will Be a Test of the True Power of Social Media Platforms," *TIME Magazine*, March 1, 2021, https://time.com/5943151/facebook-myanmar-military- ban/.

Pfeffer, Anshel, "Russian forcing occupied Ukrainians to use its mobile network," *Haaretz*, March 28, 2022, https://www.haaretz.com/world-news/europe/premium-occupiers-forcing - ukrainians-to-switch-to-russian-cell-phone-networks-1.10703781.

Pierskalla, Jan H., and Florian M. Hollenbach, "Technology and collective action: The effect of cell phone coverage on political violence in Africa," *American Political Science Review*, Vol. 107, No. 2 (2013), pp. 207-224.

Pollpeter, Kevin, "Toward an Integrative C4ISR System: Informationization and Joint Operations in the People's Liberation Army," In *The PLA at Home and Abroad: Assessing the Operational Capabilities of China's Military* (Carlisle: Strategic Studies Institute, 2010).

Posen, Barry R., *The Sources of Military Doctrine: France, Britain, and Germany between the World Wars* (Ithaca NY: Cornell University Press, 1984).

Radin, Andrew, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, *The Future of the Russian Military: Russia's ground combat capabilities and implications for US-Russia competition* (RAND Corporation Santa Monica United States, 2019).

Ranstorp, Magnus, and Magnus Normark, *Unconventional Weapons and International Terrorism* (Abingdon, UK: Routledge, 2009).

Ranstorp, Magnus, and Magnus Normark, *Understanding Terrorism Innovation and Learning* (Oxon: Routledge, 2015).

Rauchfleisch, Adrian and Jonas Kaiser, "Deplatforming the far-right: An analysis of YouTube and BitChute," *Available at SSRN* (2021).

Rawnsley, Adam, "Taliban Steps Boldly in 2007, Invades YouTube," *WIRED,* October 13, 2009, https://www. wired.com/2009/10/taliban-steps-boldy-in-2007-invades-youtube/.

Reuters Staff, "Taliban orders mobile shutdown in Afghan province," *Reuters*, October 21, 2008, https://www.reuters.com/article/us-afghan-mobiles/taliban-orders-mobile-shutdown-in-afghan-province-idUSTRE49K2HS20081021.

Reuters Staff, "Timeline: The Taliban's rapid advance across Afghanistan," *Reuters*, August 15, 2021,https://www.reuters.com/world/timeline-talibans-rapid-advance-across-afghanistan-2021-08-15/.

Richter, Monika L., "The Kremlin's platform for 'useful idiots' in the West: An overview of RT's editorial strategy and evidence of impact," *European Values* (2017).

Rider, Toby J., "Understanding arms race onset: Rivalry, threat, and territorial competition," *The Journal of Politics*, Vol. 71, No. 2 (2009), pp. 693-703.

Roberts, Margaret E., *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton University Press, 2018).

Robertson, Adi, "India sets stricter rules for social media giants," *The Verge*, February 25, 2021, https://www.theverge.com/2021/2/25/22300887/india-social-media-liability-rules-meity-facebook-whatsapp-twitter

Rød, Espen Geelmuyden, and Nils B. Weidmann, "Empowering activists or autocrats? The Internet in authoritarian regimes," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 338-351.

Rogers, Richard, "Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media," *European Journal of Communication*, Vol. 35, No. 3 (2020), pp. 213-229.

Roggio, Bill and Andrew Tobbin, "Kandahar City falls to the Taliban," *Long War Journal*, August 12, 2021, https://www.longwarjournal.org/archives/2021/08/kandahar-city-falls-to-the-taliban.php.

Romano, Aja, "Reckoning with the war meme in wartime," *Vox*, February 25, 2022, https://www.vox.com/culture/2022/2/25/22950655/ukrainian-invasion-memes-political-cartoons-controversy.

Rose, Sunniva, "Syrians worry about regime proposal to ban WhatsApp calls," *The National*, October 18, 2018, https://www.thenationalnews.com/world/mena/syrians-worry-about-regime- proposal-to-ban-whatsapp-calls-1.782118.

Rosen, Stephen P., *Winning the Next War: Innovation in the Modern Military* (Ithaca, NY: Cornell University Press, 1991).

Roth, Yoel, and Ashita Achuthan, "Building rules in public: Our approach to synthetic & manipulated media," Twitter Blog, February 4, 2020, https://blog.twitter.com/en_us/topics /company/2020/new-approach -to-synthetic-and- manipulated-media.html.

"Russia: Growing Internet Isolation, Control, Censorship: Authorities Regulate Infrastructure, Block Content," *Human Rights Watch*, June 18, 2020, https://www.hrw.org/news/2020/06/18/ russia-growing-internet -isolation-control -censorship#.

"Russia's Media Watchdog Boasts It 'Convinced' China to Lift VKontakte Ban," *The Moscow Times*, February 15, 2018, https://www.themoscowtimes.com/2018/02/15/russia-media -watchdog-boasts-it-convinced -china-to-lift-vkontakte-ban-a60523.

"Russian soldiers face ban on selfies and blog posts," *BBC*, October 5, 2017, https://www. bbc.com /news/ world -europe-41510592.

Ryan, Missy, and Karen DeYoung, "Biden will withdraw all U.S. forces from Afghanistan by Sept. 11, 2021," *The Washington Post*, April 13, 2021, https://www.washingtonpost.com/national-security/biden-us-troop-withdrawal-afghanistan/2021/04/13/918c3cae-9beb-11eb-8a83-3bc1fa69c2e8_story.html.

Sabin, Sam, and Laurens Cerulus, "3 reasons Moscow isn't taking down Ukraine's cell networks," *POLITICO*, March 7, 2022, https://www.politico.com/news/2022/03/07/ukraine-phones - internet-still-work- 00014487.

Sagan, Scott D., "Why do states build nuclear weapons?: Three models in search of a bomb," *International Security*, Vol. 21, No. 3 (1996), pp. 54-86.

Said-Morehouse, Lauren, "How Syrian activists use WhatsApp to tell the world their stories," *CNN*, September 28, 2016, https://www.cnn.com/2016/09/28/middleeast/whatsapp-syria-aleppo -activists/index.html.

Salehi, Naseer Ahmad, "Ismail Khan Mobilizes Hundreds in Herat to Crush Taliban," *TOLONews*, July 9, 2021, https://tolonews.com/afghanistan-173398.

Sameem, Ismail, "Taliban stop cell phone signals in key Afghan province," *Reuters,* March 24, 2011, https://www.reuters.com/article/afghanistan-taliban-phones/taliban-stop-cell-phone-signals-in-key-afghan-province-idUSL3E7EO12O20110324

Sampaio, Antônio, "Before and after urban warfare: Conflict prevention and transitions in cities," *International Review of the Red Cross*, Vol. 98, No. 901 (2016), pp. 71-95.

Sanger, David E. and Aishvarya Kavi, "Biden makes his case on U.S. withdrawal from Afghanistan as the Taliban gain ground," *The New York Times*, July 8, 2021, https://www.nytimes.com/ 2021/07/08/us/politics/biden-afghanistan -speech-taliban.html.

Satariano, Adam and Valerie Hopkins, "Russia, Blocked From the Global Internet, Plunges Into Digital Isolation," *The New York Times*, March 7, 2022, https://www.nytimes.com/2022/03/07/technology/ russia-ukraine-internet-isolation.html.

Satariano, Adam, "G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog," *The New York Times*, May 24, 2018, https://www.nytimes.com/2018/05/24/technology/ europe-gdpr-privacy. html.

Satariano, Adam, "Russia Intensifies Censorship Campaign, Pressuring Tech Giants," *The New York Times*, February 26, 2022, https://www.nytimes.com/2022/02/26/technology/russia-censorship-tech.html.

Sauer, Pjotr, "Russia bans Facebook and Instagram under 'extremism' law," *The Guardian*, March 21, 2022, https://www.theguardian.com/world/2022/mar/21/russia-bans-facebook-and -instagram-under-extremism-law.

Scheck, Justin, Newley Purnell, Jeff Horwitz, "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show," *The Wall Street Journal*, September 16, 2021, https://www.wsj.com/articles/facebook-drug-cartels-human-traffickers -response-is-weak-documents-11631812953.

Schleffer, Guy, and Benjamin Miller, "The Political Effects of Social Media Platforms on Different Regime Types (Summer 2021)," *Texas National Security Review* (2021).

Schmid, Jon, and Jonathan Huang, "State adoption of transformative technology: Early railroad adoption in China and Japan," *International Studies Quarterly*, Vol. 61, No. 3 (2017), pp. 570-583.

Schneier, Bruce, "8 Ways to Stay Ahead of Influence Operations," *Foreign Policy,* August 12, 2019, https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/.

Sediqi, Abdul Qadir, "Taliban fighters double as reporters to wage Afghan digital war," *Reuters*, May 10, 2019, https://www.reuters.com/article/us-afghanistan-taliban-media/taliban-fighters -double-as-reporters-to-wage-afghan-digital-war-idUSKCN1SH035.

Seib, Philip, *Real-time diplomacy: Politics and power in the social media era* (Palgrave Macmillan, 2012).

"Sensitive Media Policy," *Twitter Help Center*, https://help.twitter.com/en/rules-and-policies/media-policy.

Seo, Hyunjin, "Visual propaganda in the age of social media: An empirical analysis of Twitter images during the 2012 Israeli–Hamas conflict," *Visual Communication Quarterly*, Vol. 21, No. 3 (2014), pp. 150-161.

Sessa, Maria Giovanna, "Ukraine conflict disinformation: worldwide narratives and trends," *EU Disinfo Lab*, https://www.disinfo.eu/publications/ukraine-conflict-disinformation-world wide-narratives-and-trends/.

Shapiro, Jacob N., and David A. Siegel, "Coordination and security: How mobile communications affect insurgency," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 312-322.

Shapiro, Jacob N., and Nils B. Weidmann, "Is the phone mightier than the sword? Cellphones and insurgent violence in Iraq," *International Organization,* Vol. 69, No. 2 (2015), pp. 247-274.

Shapiro, Jacob N., and Nils B. Weidmann, "Talking about killing: Cell phones, collective action, and insurgent violence in Iraq," *Collective Action and Insurgent Violence in Iraq* (2011).

Sharma, Gopal, "Nepal frees top leader, restores some mobile phones," *Reuters*, May 2, 2005, https://reliefweb. int/report/nepal/nepal-frees-top-leader-restores-some-mobile-phones.

Sheetz, Michael, "Elon Musk's SpaceX sent thousands of Starlink satellite internet dishes to Ukraine, company's president says," *CNBC*, March 22, 2022, https://www.cnbc.com/2022/03/22/ elon-musk-spacex -thousands-of-starlink-satellite- dishes-sent-to-ukraine.html.

Shen, Justine, "Making Public Comments More Meaningful," *Facebook Newsroom*, June 14, 2019, https://about. fb.com/news/2019/06/making-public-comments-more-meaningful/.

Shirazi, Farid, Ojelanki Ngwenyama, and Olga Morawczynski, "ICT expansion and the digital divide in democratic freedoms: An analysis of the impact of ICT expansion, education and ICT filtering on democracy," *Telematics and Informatics*, Vol. 27, No. 1 (2010), pp. 21-31.

Siegel, Alexandra A., and Joshua A. Tucker, "The Islamic State's information warfare: Measuring the success of ISIS's online strategy," Journal of Language and Politics, Vol. 17, No. 2 (2018), pp. 258-280.

Silverman, Jacob, "Loose Tweets Sink Ships," *POLITICO*, August 28, 2014, https://www.politico .com/magazine/story/2014/08/islamic-state-twitter-110418/.

Simonite, Tom, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," *WIRED*, March 17, 2022, https://www.wired.com/story/zelensky-deepfake-facebook - twitter-playbook/.

Singer, Peter W., "Winning the war of words: Information warfare in Afghanistan," *Brookings Institution* (2001).

Singer, Peter W., and Emerson T. Brooking, *LikeWar: The weaponization of social media* (Eamon Dolan Books, 2018).

Sinno, Abdulkader H., *Organizations at war in Afghanistan and beyond* (Cornell University Press, 2011).

Sinpeng, Aim, "State Repression in Cyberspace: The Case of Thailand," *Asian Politics & Policy*, Vol. 5, No. 3 (2013), pp. 421-440.

Sly, Liz, "U.S. soldiers are revealing sensitive and dangerous information by jogging," *The Washington Post*, January 29, 2018, https://www.washingtonpost.com/world/a-map-showing-the-users -of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html.

Sopko, John F., *Afghanistan's Information and Communications Technology Sector: US Agencies Obligated Over $2.6 Billion to the Sector, but the Full Scope of US Efforts is Unknown, Special Inspector General for Afghanistan Reconstruction* (Arlington United States, 2016).

"Social Media Content Moderation," *C-SPAN Video*, 3:36:21, October 28, 2020, https://www.c-span.org /video/ ?476686 -1/social-media-content-moderation#.

"Social Media Stats Afghanistan," *statcounter: GlobalStats,* accessed on April 1, 2022, https://gs.statcounter.com/social-media-stats/all/afghanistan/#monthly-202001-202109.

South Asia Terrorism Portal, "Afghanistan: Incidents and Statements involving Taliban: 2021," *South Asia Intelligence Review*, https://www.satp.org/terrorist-incident-text/afghanistan /taliban_Aug-2021.

Stack, Liam, "Watching Syria's War," *The New York Times*, last accessed September 8, 2021, https://www .nytimes.com/ interactive/projects/watching-syrias-war.

Stokel-Walker, Chris, "Afghans are racing to erase their online lives," *WIRED*, August 17, 2021, https://www.wired.co.uk/article/afghanistan-social-media-delete.

Stradner, Ivana, "Now Russia Has Its Own Ultimatum for Twitter," *Foreign Policy*, March 26, 2021, https:// foreignpolicy.com/2021/03/26/putin-twitter-ban-ultimatum-censorship-dissent/.

Straus, Scott, "What is the relationship between hate radio and violence? Rethinking Rwanda's "Radio Machete,"" *Politics & Society*, Vol. 35, No. 4 (2007), pp. 609-637.

Stieglitz, Stefan, and Linh Dang-Xuan, "Social media and political communication: a social media analytics framework," Social Network Analysis and Mining, Vol. 3, No. 4 (2013), pp.1277-1291.

Sundberg, Ralph, Kristine Eck, and Joakim Kreutz, "Introducing the UCDP non-state conflict dataset," *Journal of Peace Research*, Vol. 49, No. 2 (2012), pp. 351-362.

Susarla, Anjana, "Why Zelenskyy's 'selfie videos' are helping Ukraine win the PR war against Russia," *The Conversation*, March 1, 2022, https://theconversation.com/why-zelenskyys-selfie- videos-are-helping- ukraine-win-the-pr-war-against-russia-178117.

Sweeney, Michael S., *Secrets of victory: The Office of Censorship and the American press and radio in World War II* (University of North Carolina Press, 2001).

Tabor, Damon, "Radio Tecnico: How the Zetas Cartel Took Over Mexico with WalkieTalkies," *Popular Science*, March 25, 2014, http://www.popsci.com/article/technology/radio-tecnico - how-zetas-cartel-took- overmexico-walkie-talkies.

"Taliban orders Afghan ban on access to Internet," *The Irish Times*, August 25, 2001, https://www.irishtimes.com/news/taliban-orders-afghan-ban-on-access-to-internet-1.394327

Tau, Byron, "Premise Mobile-Phone App Suspends Ukraine Activities After Accusations Fly," *The Wall Street Journal*, February 26, 2022, https://www.wsj.com/livecoverage/russia-ukraine - latest-news-2022-02-26/card/premise-mobile-phone-app-suspends-ukraine-activities-after-accusations-fly-8FDnhZe9raunaIJ4HV66.

Taylor, Rob, "Taliban website hacked as Afghan cyber war heats up," *Reuters*, April 27, 2012, https://www.reuters.com/article/afghanistan-taliban-hacking/taliban-website-hacked-as-afghan-cyber-war-heats-up-idUSL3E8FR3X820120427.

Thapa, Deepak, "Understanding the Maoist movement of Nepal, Vol. 10," *Centre for Social Research and Development* (2003).

"The U.S. War in Afghanistan: 1999 – 2021," *Council on Foreign Relations*, https://www.cfr.org/ timeline/us-war- afghanistan.

Thompson, George Raynor, "Military Communication," *Britannica Encyclopedia*, last updated April 25, 2018, https://www.britannica.com/technology/military-communication/.

Tiezzi, Shannon, "It's Official: China's Military Has 5 New Theater Commands," *The Diplomat*, February 2, 2016, https://thediplomat.com/2016/02/its-official-chinas-military-has-5- new-theater-commands/.

Timberg, Craig, "Taliban websites operating in five languages go dark," *The Washington Post,* August 20, 2021, https://www.washingtonpost.com/technology/2021/08/20/taliban-internet -websites-twitter-facebook

Timberg, Craig, and Drew Harwell, "Social media fuels new type of 'fog of war' in Ukraine conflict," *The Washington Post*, February 24, 2022, https://www.washingtonpost.com/ technology/ 2022/02/24/ukraine-russia-war-twitter-social-media.

"Timeline: The events leading up to Russia's invasion of Ukraine," *Reuters*, March 1, 2022, https://www.reuters.com/world/europe/events-leading-up-russias-invasion-ukraine-2022-02-28/.

Tishler, Nicole A., "Trends in terrorists' weapons adoption and the study thereof," *International Studies Review*, Vol. 20, No. 3 (2018), pp. 368-394.

Todd, Brian, "How Zelensky is using social media to dominate the information war," *CNN Situation Room*, March 9, 2022, https://www.cnn.com/videos/media/2022/03/09/volodymyr -zelensky-social-media -ukraine-todd-dnt-intl-tsr-vpx.cnn.

TOLONews, "District in Ghor Falls to Taliban after 'Heavy Clashes,'" *TOLONews*, June 12, 2021, https://tolonews.com/afghanistan-172783.

Tønnesson, Stein, Min Zaw Oo, and Ne Lynn Aung, "Pretending to be States: The Use of Facebook by Armed Groups in Myanmar," *Journal of Contemporary Asia*, Vol. 52, No. 2 (2022), pp. 200-225.

Toor, Amar, "How Putin's cronies seized control of Russia's Facebook," *The Verge*, January 31, 2014, https://www.theverge.com/2014/1/31/5363990/how-putins-cronies-seized-control -over-russias-facebook-pavel-durov-vk.

Trochim, William MK., "Outcome pattern matching and program theory," *Evaluation and program planning*, Vol. 12, No. 4 (1989), pp. 355-366.

Trochim, William MK., "Pattern matching, validity, and conceptualization in program evaluation," *Evaluation review*, Vol. 9, No. 5 (1985), pp. 575-604.

Trofimov, Yaroslav, "Cell Carriers Bow to Taliban Threat," *The Wall Street Journal*, March 22, 2010, https://www.wsj.com/articles/SB10001424052748704117304575137541465235972.

Twitter Inc., "Combating Violent Extremism," *Twitter Blog*, February 5, 2016, https://blog.twitter .com/en_us/ a/2016/combating-violent-extremism.html.

Twitter Inc., "Updating our advertising policies on state media," *Twitter Blog,* August 19, 2019, https://blog.twitter.com/en_us/topics/company/2019/advertising_policies_on_state_medi a.html.

Twitter Public Policy, "Update on Twitter's review of the 2016 US election," *Twitter Blog*, January 19, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/2016-election -update.html.

Twitter Support, "New labels for government and state-affiliated media accounts," *Twitter Blog*, August 6, 2020, https://blog.twitter.com/en_us/topics/product/2020/new-labels-for-government-and-state-affiliated-media-accounts.

Tworek, Heidi, "Facebook's America-centrism Is Now Plain for All to See," *Center for International Governance Innovation*, October 4, 2021, https://www.cigionline.org/articles/facebooks -america-centrism-is-now -plain-for-all-to-see/.

Tworek, Heidi and Alicia Wanless, "Time for Transparency From Digital Platforms, But What Does That Really Mean?," *Lawfare*, January 20, 2022, https://www.lawfareblog.com/time-transparency-digital-platforms-what-does-really-mean.

"Ukraine bans its top social networks because they are Russian," *The Economist*, May 19, 2017, https://www.economist.com/europe/2017/05/19/ukraine-bans-its-top-social-networks-because-they-are-russian.

United States Department of State, *U.S. Department of State Country Report on Human Rights Practices 2005 - Nepal,* March 8, 2006, https://www.refworld.org/docid/441821a829.html.

Uren, Tom, Elise Thomas, and Jacob Wallis, "Tweeting through the Great Firewall," *Australian Strategic Policy Institute*, September 3, 2019, https://www.aspi.org.au/report/tweeting-through greatfirewall?__cf_chl_jschl_tk__=pmd_9sBUUrJS8JJkBQMCUCOX9.lAqvG03lJMKITM VSpXhnE-1634695457-0-gqNtZGzNAjujcnBszQil.

Vaidyanathan, Siva, "What if Regulating Facebook Fails?" *WIRED*, July 2, 2021, https://www.wired. com/story/ what-if-regulating-facebook-fails/.

Van Creveld, Martin, *Technology and war: From 2000 BC to the present* (Simon and Schuster, 2010).

Vargas-Bianchi, Lizardo, "Qualitative theory testing by deductive design and pattern matching analysis," *SocArxiv* (2020), https://doi.org/10.31235/osf.io/w4gxe.

Verge Staff, "The response to the deadly mass shooting in Christchurch, New Zealand," *The Verge*, March 15, 2019, https://www.theverge.com/2019/3/16/18268907/christchurch-new-zealand-mass-shooting -tech-response-updates.

Vinokour, Maya, "Russia's Media Is Now Totally in Putin's Hands," *Foreign Policy*, April 1, 2022, https://foreignpolicy.com/2022/04/05/russia-media-independence-putin/

Volchek, Dmitry, and Claire Bigg, "Ukrainian bloggers use social media to track Russian soldiers fighting in east," *The Guardian*, June 3, 2015, https://www.theguardian.com/world/2015/jun/03/bloggers-social- media-russian-soldiers-fighting-in-ukraine.

Volz, Dustin, and Joseph Menn, "U.S. official warns of 'unintended consequences' of European data privacy law," *Reuters*, April 17, 2018, https://www.reuters.com/article/us-usa-cyber-nielsen/ u-s-official-warns-of-unintended-consequences-of-european-data-privacy-law-idUSKBN1HO36J.

Wakabayashi, Daisuke, and Nicholas Confessore, "Russia's Favored Outlet Is an Online News Giant. YouTube Helped," *The New York Times*, October 23, 2017, https://www.nytimes.com/ 2017/10/23/technology/youtube-russia-rt.html.

Wall, Melissa, and Sahar El Zahed, "Syrian citizen journalism: A pop-up news ecology in an authoritarian space," *Digital Journalism*, Vol. 3, No. 5 (2015), pp. 720-736.

Walter, Barbara F., "The new civil wars," *Annual Review of Political Science*, Vol. 20 (2017), pp. 469-486.

Waltz, Kenneth N., *Theory of International Politics* (New York: McGraw-Hill, 1979).

Ward, Antonia, "ISIS's use of social media still poses a threat to stability in the Middle East and Africa," *Georgetown Security Studies Review* (2018).

Warren, T. Camber, "Explosive connections? Mass media, social media, and the geography of collective violence in African states," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 297-311.

Warrick, Joby, "Private money pours into Syrian conflict as rich donors pick sides," *The Washington Post*, June 15, 2013, https://www.washingtonpost.com/world/national-security/private-money-pours-into-syrian-conflict-as-rich-donors-pick-sides/2013/06/15/67841656-cf8a-11e2-8845-d970ccb04497_story.html.

Weidmann, Nils B., "Communication, technology, and political conflict: Introduction to the special issue," *Journal of Peace Research*, Vol. 52, No. 3 (2015), pp. 263-268.

Weimann, Gabriel, "Hezbollah Dot Com: Hezbollah's Online Campaign," *New Media and Innovative Technologies*, Vol. 22 (2008).

Weissenstein, Michael, "Mexico's cartels build own national radio system," *Associated Press*, December 26, 2011, https://www.seattletimes.com/nation-world/mexicos-cartels-build-own-national -radio-system/.

Wejnert, Barbara, "Integrating models of diffusion of innovations: A conceptual framework," *Annual review of sociology*, Vol. 28, No. 1 (2002), pp. 297-326.

WhatsApp Blog, "Introducing Touch ID & Face ID," *WhatsApp,* February 4, 2019, https://blog. whatsapp.com / introducing-touch-id-face-id.

WhatsApp Blog, "Labeling Forwarded Messages," *WhatsApp*, July 10, 2018, https://blog.whatsapp. com/labeling -forwarded-messages.

WhatsApp Blog, "More Changes to Forwarding," *WhatsApp*, last modified January 21, 2019, https://blog. whatsapp.com/more-changes-to-forwarding

"Why Russian radios in Ukraine are getting spammed with heavy metal," *The Economist*, March 28, 2022, https://www.economist.com/the-economist-explains/2022/03/28/why-russian-radios-ukraine-war-intercepted-heavy-metal.

Winter, Charlie. "Apocalypse, later: a longitudinal study of the Islamic State brand." Critical Studies in Media Communication 35, no. 1 (2018): 103-121.

Winter, Charlie, "Documenting the virtual 'caliphate,'" *Quilliam Foundation*, Vol. 33, No. 1 (2015).

Winter, Charlie, Abdullah Alrhmoun, Abdul Sayed, "The Taliban's vast propaganda machine has a new target," *WIRED*, August 28, 2021, https://www.wired.co.uk/article/taliban-propaganda-news-afghanistan.

Wolfsfeld, Gadi, Elad Segev, and Tamir Sheafer, "Social media and the Arab Spring: Politics comes first," *The International Journal of Press/Politics*, Vol. 18, No. 2 (2013), pp. 115-137.

Woodford, Antonia, "Expanding Fact-Checking to Photos and Videos," Facebook Newsroom, last modified September 13, 2018, https://about.fb.com/news/2018/09/expanding-fact-checking/.

Wuthnow, Joel, and Phillip Charles Saunders, *Chinese military reform in the age of Xi Jinping: Drivers, challenges, and Implications* (Government Printing Office, 2017).

Yablokov, Ilya, "Conspiracy theories as a Russian public diplomacy tool: The case of Russia Today (RT)," *Politics*, Vol. 35, No. 3-4 (2015), pp. 301-315.

Yadav, Kamya, "Countering Influence Operations: A Review of Policy Proposals Since 2016," *Carnegie Endowment for International Peace, Partnership for Countering Influence Operations*, November 30, 2020, https://carnegieendowment.org/2020/11/30/countering-influence-operations-review-of-policy-proposals-since-2016-pub-83333.

Yadav, Kamya, "Platform Interventions: How Social Media Counters Influence Operations," *Carnegie Endowment for International Peace, Partnership for Countering Influence Operations*, January 25, 2021, https://carnegieendowment.org/2021/01/25/platform-interventions-how-social-media-counters-influence-operations-pub-83698.

Yin, Robert K., *Case study research and applications* (Sage, 2018).

Yuan, Li, "Why the Chinese Internet Is Cheering Russia's Invasion," *The New York Times*, February 27, 2022, https://www.nytimes.com/2022/02/27/business/china-russia-ukraine-invasion.html.

Zaharna, Rhonda S., "From propaganda to public diplomacy in the information age," *War, media and propaganda: A global perspective* (2004).

Zahid, Mohammad, "Taliban selfies: Why militants posed for photos in Kunduz," *BBC*, September 30, 2015, https://www.bbc.com/news/world-asia-34387854.

Zeitzoff, Thomas, "Does social media influence conflict? Evidence from the 2012 Gaza conflict," *Journal of Conflict Resolution*, Vol. 62, No. 1 (2018), pp. 29-63.

Zeitzoff, Thomas, "How social media is changing conflict," *Journal of Conflict Resolution*, Vol. 61, No. 9 (2017), pp. 1970-1991.

Zeitzoff, Thomas, "Using social media to measure conflict dynamics: An application to the 2008–2009 Gaza conflict," *Journal of Conflict Resolution*, Vol. 55, No. 6 (2011), pp. 938-969.

Zelin, Aaron Y., "Picture or it didn't happen: A snapshot of the Islamic State's official media output," *Perspectives on Terrorism*, Vol. 9, No. 4 (2015), pp. 85-97.

Zisk, Kimberly Marten, *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955 - 1991* (Princeton University Press, 1993).