



ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL

Available Online: <https://assajournal.com>

Vol. 05 No. 01. Jan-March 2026. Page#. 7019-7027

Print ISSN: [3006-2497](#) Online ISSN: [3006-2500](#)Platform & Workflow by: [Open Journal Systems](#)

Algorithmic Geopolitics: AI-Generated Deepfakes and Social Media Manipulation as Tools of Foreign Information Warfare

Kashaf Nadeem*

Department of Political Science & International Relations, University of Gujrat-50700, Punjab, Pakistan
22011587-006@uog.edu.pk, <https://orcid.org/0009-0009-4467-7148>

*Corresponding Author kashafnadeem197@gmail.com

Areeba Javed

Department of Political Science & International Relations, University of Gujrat-50700, Punjab, Pakistan
22011587-032@uog.edu.pk

Adil Zaman

Lecturer, Department of Political Science & International Relations, University of Gujrat-50700, Punjab, Pakistan

adil.zaman@uog.edu.pk

ABSTRACT

Generative AI has turned information warfare from a familiar tool of statecraft into something closer to a rebuilding of the international information environment itself. A state actor can now fabricate authoritative video, push false content across billions of social media feeds within hours. Moreover, it can turn platform recommendation algorithms into a force-multiplier for foreign influence operations, cheaply and largely without attribution. Drawing on structural Realism, Constructivist IR theory, and Copenhagen School securitization theory together, this paper examines how data, algorithms, and synthetic media have become instruments of power in an anarchic international system, attacking the intersubjective foundations. Two case studies: Russia's Internet Research Agency campaign in the 2016 U.S. presidential election, which reached an estimated 126 million Facebook users for roughly \$100,000, and the March 2022 Zelensky deepfake, the first confirmed use of synthetic video in active armed conflict, show that the real target of algorithmic geopolitics is not military capacity but the epistemic conditions of democratic political agency. It is a claim reinforced by experimental evidence that synthetic video erodes institutional trust even when audiences suspect manipulation. The paper identifies three governance failures: the attribution gap under the Tallinn Manual 2.0, the irreversibility of epistemic harm, and the asymmetric vulnerability of open societies, and proposes a multilateral synthetic-media treaty, mandatory platform accountability, and institutionalized pre-bunking as a response. A minimally reliable information environment is key to sovereignty, deterrence, and democratic legitimacy, and the structural transformation of this due to algorithmic warfare has undermined it all.

Keywords: *Algorithmic Geopolitics; AI-Generated Deepfakes; Social Media Manipulation; Information Warfare; Zelensky deepfake*

INTRODUCTION

The nature of power, conflict, and statecraft in the 21st Century has evolved. The previous geopolitical conflict was over territory, resources, and military equipment. But today's struggle is being fought over information landscapes, people who are building beliefs, institutional trust, and the political reality. This transformation has been sped up and reframed by the application of artificial intelligence on top of the many digital communication platforms. A state actor can now generate synthetic media of a foreign head of state, push it into billions of social media feeds within hours, and exploit recommendation-algorithm architecture to deepen social polarization, all without firing a shot. The consequences for sovereignty, democratic governance, and the stability of the liberal international order are significant, and so far poorly theorized and poorly governed.

Information has always served statecraft: propaganda, disinformation and wartime deception are all old practices (Rid,2020). Generative AI, large language models, neural voice synthesis, image diffusion, and deepfake video have introduced a qualitative discontinuity to an ancient tradition. Capabilities that once required state intelligence infrastructure are now cheaply available to state organs, non-state proxies, and well-resourced private actors alike. Combined with the virality built into social media platforms, this democratization of deception technology has turned information warfare into a central theatre of geopolitical competition rather than a supporting tool (Byman et al.,2023).

This shift is concretely illustrated by deepfakes, a type of synthetic media created by deep neural networks, such as cloning voices and creating fake text or face-swapping videos. The threat is highlighted by two recent incidents. A fake video emerged in March 2022 that appeared to show Ukrainian President Volodymyr Zelensky begging his soldiers to surrender to the Russians. The images didn't pass the trained eye; the head of the president was just a little bit too small, and his tone of voice was a little bit too flat. Within hours, Zelensky's office declared it to be a deepfake. They already had published warnings to the general public, and it was removed from the platforms of Meta & YouTube within hours (Byman et al.,2023). Two days before Slovakia's 2023 election, a poor-quality audio deepfake emerged presenting opposition leader Michal Simeck talking about vote-rigging. An election period media blackout prevented it from being publicly debunked before the polls opened (Bohacek,2024). In both cases, the synthetic media exploits legal and procedural loopholes that can come about when elections are not on schedule and synthetic media takes advantage of legal and procedural loopholes that can open up when elections are not on schedule.

Beyond electoral interference, deepfakes carry a broader menu of harms: non-consensual pornographic use that damages individual privacy, a general "truth decay" that corrodes public debate, and a "liar's dividend" that lets real wrongdoers dismiss authentic evidence as fabricated. At the level of international relations, deepfakes can be used to impersonate political or military leaders, manufacture false pretexts, and strain alliances (Chesney & Citron, 2019; Dobber et al., 2021; Goldstein et al., 2023).

Algorithmic geopolitics" is the name this paper gives to the resulting situation: in which digital information infrastructure itself is a space of strategic competition; and in which states compete over

the narrative environments and epistemic conditions of political judgment as well as over territory or resources. Social media platforms like Facebook, X (Twitter), TikTok and YouTube are engineered to engage, not to be accurate, so they are structurally designed to support this kind of competition (Bradshaw & Howard, 2019). International law has not followed suit: the state responsibility, non-intervention and sovereignty doctrines, which have shaped the past, must be reworked in a context where attribution is difficult (Schmitt, 2017).

LITERATURE REVIEW

2.1 Deepfakes as a Geopolitical Instrument

Since 2018, there has been a paradigm change in deepfake scholarship from technical description to political implications. Mirsky and Lee's survey describes the evolution of face-swap, voice-conversion and re-enactment technology to a stage where they can be used to produce fake media that cannot be easily recognized by the human eye alone, and identifies it as an opportunity for political leaders to exploit (Mirsky & Lee, 2021). Chesney and Citron codify the political threat in two ways: by directly creating a crisis and falsely assigning blame to officials, or by simply making the existence of deep fake tech a "liar's dividend" and allowing bad actors to simply shrug at the possibility of genuine incriminating evidence being fake (Chesney & Citron, 2019). Rini takes it one step further, arguing that deepfakes have the power not only to spread false beliefs, but to undermine the "epistemic backstop" that recorded media has long been used to create a democratic environment for deliberation (Rini, 2020). These theoretical arguments are backed by some experimental evidence: Vaccari and Chadwick validate that even when it comes to suspected deepfakes, uncertainty is measurably increased and trust is lowered in news sources (Vaccari & Chadwick, 2020). Dobber et al. show that microtargeted deepfakes produce statistically significant, and demographically concentrated, drops in support for the politicians they depict (Dobber et al., 2021). Read together, this body of work establishes that synthetic media's danger is epistemic as much as informational, a distinction central to how IR scholars should think about credibility and interstate signaling.

2.2 Computational Propaganda and Algorithmic Amplification

A second strand examines the infrastructure that carries synthetic content. Woolley and Howard define "computational propaganda" as the combination of platforms, bots, and data used to manipulate opinion, and document its use across dozens of countries even before generative AI entered the picture (Woolley & Howard, 2018). Howard's global survey found organized manipulation campaigns operating in 70 countries by 2019, up from 48 countries in 2018 and 28 countries in 2017. Facebook and Twitter attributed foreign influence operations to seven countries, including China, Iran, Russia, and Saudi Arabia, identified as sponsors of foreign-facing operations (Bradshaw & Howard, 2019). The structural mechanism enabling these operations is analyzed over 126,000 stories shared on Twitter across eleven years, they find that false news diffuses significantly farther, faster, and more broadly than true news (Goldstein et al., 2023).

2.3 IR Scholarship on Information Operations and Hybrid Warfare

The literature that directly relates to this is mainly placed into IR theory. As liberal societies are built on openness, digital-age political warfare is targeted at just that, according to Paterson and Hanley (Paterson & Hanley, 2020). Byman et al. go further in extending this concept of using deepfakes to

discredit enemy leadership, create evidence of atrocities, and demoralize their forces in the context of armed conflict (Byman et al., 2023).

THEORETICAL FRAMEWORK

The geopolitical ramifications of AI-generated deepfakes and algorithmic manipulation are highly complex and impossible to be captured by any single IR paradigm. This paper draws on structural Realism, Constructivism, and Copenhagen School securitization theory together, as they all provide analytical leverage that the others do not.

3.1 Structural Realism: Information Dominance as Power Maximization

According to the Structural Realism approach, the international system is anarchic and drives states to power self-help accumulation. So, when the cost of conventional military force proves too high or the tool too coarse, states adopt a different approach to warfare: hybrid warfare. The use of disinformation and propaganda as soft power, which have hard effects, and that takes advantage of the strategic vulnerability of the target societies, to break their strategic will and social consensus without an outbreak of conventional warfare (Filipec, 2019). Usefully expanded by the idea of cyber power, which is broken down into hard and soft cyber power, the disruptive attacks and the shaping of preferences through informational means, respectively (Nye, 2010). The Internet Research Agency is the prime example of the pattern in Russia. A low-cost campaign of fake persons and targeted social media ads. It was created not for any one kinetic goal, but to impact a competitor's democratic information environment from a systemic perspective (Mueller, 2019).

3.2 Constructivism: Narrative Power and the Social Construction of Political Reality

Constructivism holds that international structures are formed by means of intersubjective meaning, identity, and norms, not material capabilities alone. When state identities and interests are socially created, technologies that circulate and alter the informational environment in which they are produced are not only tactical dangers but on the ontological foundations of political reality (Wendt, 1992). Deepfakes are a tool to create authoritative-looking audiovisual "evidence" that can help increase a state's ability to manipulate target society's perception of its leaders and institutions. That people to view the damage to institutional trust as being caused by that synthetic video even if they suspect that it is manipulated (Vaccari & Chadwick, 2020). It proposes that the mechanism is not so much about inculcating false beliefs as disturbing the norm of a shared belief that records are reliable, which any policy response seeking to be effective must attempt to protect.

3.3 Securitization and Theoretical Synthesis

The Copenhagen School theory of securitization comes between the two, as security does not exist objectively but rather as a speech act. Security becomes a problem when an actor is able to make it into an existential threat that demands extraordinary measures (Buzan et al., 1998). This is how states and multilateral organizations are increasingly seeing algorithmic information manipulation, and it is the same way one might imagine that authoritarian states might view it, as a threat to democratic governance and sovereignty rather than a routine regulatory problem, albeit one open to a domestic turn for justifying domestic censorship, making it the politics of the contest. The three lenses together constitute one architecture: Realism describes the rationale behind states using the tools, Constructivism describes the extent of the damage they inflict, and securitization describes how

information integrity becomes a matter of great existential importance. Applied through this lens, the case studies that follow, namely Russia's IRA operations and Zelensky's deepfake, reveal a competitive power logic that is embedded in the narratives and securitized information environments, the latter of which neither the tradition of "narrative" nor the tradition of "securitized" information environments alone could predict.

CASE STUDY 1: Russia's Internet Research Agency (IRA) and the 2016 U.S. Presidential Election

The Internet Research Agency (IRA) is a Russian organization, based in St. Petersburg and backed by companies controlled by Russian billionaire Yevgeny Prigozhin. IRA was involved in a multi-year influence operation against the United States through media operations. It has been active in the U.S. since 2014, when it sent operatives for intelligence-gathering and merged all of its operations in the United States into one department. By the start of 2016, this "underminers" movement, which had spread to undermine the U.S. electoral system, had focused on promoting Donald Trump and denigrating Hillary Clinton. Staff was told to "take every chance to criticize" Clinton "and the rest" in an internal February 2016 memo.

The breadth of the operation, granted in sworn testimony before Congress and disclosed on platforms, was significant. In the last two years, IRA-controlled pages published roughly 80,000 posts, reaching an estimated 126 million people, using approximately 3,500 Facebook advertisements for about \$100,000. A parallel Instagram operation operated 170 Instagram accounts and approximately 120,000 pieces of content. On Twitter, 3,814 accounts affiliated with the IRA were retweeted by accounts such as the ones for Donald Trump Jr., Kellyanne Conway, Eric Trump, and Michael Flynn, among others, some gaining tens of thousands of followers. In addition to social media, IRA operatives wielded the guise of grassroots domestic organizers to facilitate actual political rallies in the U.S., including in November 2015, without any indications that any Trump campaign official would have known that he was engaging with foreign nationals. As the campaign progressed, the focus became more specific; by mid-2016, the messages were focused on African American voters and aimed to reduce turnout and focused on Hispanic communities and aimed to create a sense of distrust of U.S. institutions. Patterns include internal research into racial, religious, and partisan polarization, which surged at election debates, party conventions, and other high-salience political events, including a surge in April 2017, after the election itself.

The legal impact was large but limited: In February 2018, the U.S. Department of Justice indicted thirteen Russian nationals and three companies, including the IRA, for conspiracy to defraud the United States under 18 U.S.C. § 371. The best that prosecutors could do to provide legal clarity on the scope of the operation was the public document itself, though they admitted the realities of trying the Russians who are at present outside U.S. jurisdiction (Mueller, 2019).

CASE STUDY 2: The Zelensky Deepfake - March 2022

5.1 Historical Context: The First High-Profile Deepfake in Armed Conflict

On 16 March 2022, three weeks into Russia's full-scale invasion, a video appeared to show President Volodymyr Zelensky, in his now-familiar olive fatigues, instructing Ukrainian troops to surrender. It briefly circulated on the Ukraine 24 news website before spreading across VKontakte and Telegram and drawing international media attention. The forgery was imperfect: the head was subtly undersized, the

voice slightly flat. Zelensky's office promptly and publicly said it was a "deepfake," which it had warned about in the war. That warning matters analytically: it is treated here as an early instance of "pre-bunking," a defensive strategy this paper returns to as a policy recommendation. The incident is described as "the first high-profile use of a deepfake in an armed conflict" and defined as "a watershed moment in information operations". The framing, not just an incident, but a structural shift in the technology of warfare, is at the heart of the report's argument.

5.2 Technical Mechanisms: How the Deepfake Was Generated

The video was produced using a Generative Adversarial Network (GAN). It is a class of deep learning architecture built from two competing components: a Generator that attempts to produce convincing fake images or video, and a Discriminator trained to tell real media from fabricated media. The two train against each other iteratively; each time the Discriminator catches a fake, the Generator adjusts and produces a more convincing one. It is adjusted until the system reaches a stable point where neither component keeps improving relative to the other. Repeated over enough cycles, this adversarial process is what allows GANs to produce synthetic video realistic enough to pass as authentic footage of a named public figure.

What makes this capability geopolitically significant is how little it now takes to deploy. Research on systems such as TREAD (Terrorism Reduction with Artificial Intelligence Deepfakes) was developed at Northwestern University. It showed that someone with ordinary machine-learning competence can generate deepfake video at scale using computing hardware costing roughly \$10,000. The underlying GAN architectures are frequently released under open-source licenses, so the binding constraint is not technical know-how but training data, which a government can typically assemble within days, and modest computing power. That is, it was never a state secret and was not exotic. It was an easy-to-use and easy-to-cultivate technology; for this reason, it must be read as a model rather than just a single event.

5.3 Operational Analysis: Why Deepfakes Are Used in Armed Conflict

The Zelensky video fits into a known taxonomy of deepfake operations in conflict. The Zelensky video fits nicely into a taxonomy of the operations of deepfakes in conflict. The most obvious one is "falsifying orders": fake audio or video recordings of a commander giving instructions to the troops that they should surrender or withdraw or do something else that the enemy wants them to do. That was what the video had to say, and it clearly wasn't meant for the general public; it was for sowing doubt in the Ukrainian army at a time when they were being pressured by the Russian army to push hard for territory.

There's a related effect going the other way, too: when it's known deepfakes exist, then any legitimate order can be doubted and ignored, and vice versa, a wartime version of the "liar's dividend." A third one is to appeal to civilian morale, rather than directly to the command structure, with deepfakes of military forces committing atrocities, leaving their posts, or betraying the population that they are supposed to protect. The same line of reasoning was applied to the surrender video, a fake appeal from the one person whose personal refusal to leave Kyiv was meant to chip away at the civic resolve he had created. While the report is no doubt honest about the shortcomings in the video's operations, it dismisses the Zelensky deepfake as clunky and easy to believe. It notes that even good deepfakes may not have an immediate impact but does not say this is a sign of security. A race is taking place between detection

and generation. As new detectors come out, deepfakes can incorporate them into their Discriminator portion of a GAN and retrain their Generator to outsmart them. A dynamic compared here with that of malware evasion, and one that could possibly make reliable detection impossible at any point in the future. Another paradox is the other side of the coin: As viewers become skeptical of realistic video and audio, they also become skeptical of real communications. Furthermore, soldiers are dubious about what constitutes a real order, and the public is not sure if what a leader says is the real thing. It undermines diplomacy and military cooperation even if it's not a deepfake. The problem with the Zelensky incident, then, isn't that anyone believed the video, but that it turned those people to watch any Ukrainian leadership communication with a degree of suspicion they may not have had before.

5.4 Reading the Case Through Theory

The economics of the Zelensky deepfake matched the Realist logic outlined above virtually to a tee: a few thousand dollars of computer time and a handful of days of training data bought a strategic impact, military demoralization, a breakdown in command, and popular will pressure. Otherwise, it would have needed a real info op, real personnel, and real risk. In essence, it's the informational equivalent of missile proliferation- a capability that's made more widely available to any entity with the requisite resources. The Constructivist focus is on what was actually attacked. The emphasis on the forgers reproducing Zelensky's olive uniform was not tactical, since it had no military meaning, but rather symbolic: it was a created emblem of resistance and legitimate leadership, and the video was placed on the institutional website of Ukraine 24 to take the place of the authority of the media. Lastly, the framing of the incident as "a turning point in information operations". It's a kind of securitizing by itself; the language raises a single forged clip into an existential-threat narrative, the way the Copenhagen School talks about it, showing how the three theory lenses work together, in this case (Byman et al.,2023).

DISCUSSION AND SOLUTION

6.1 Why Existing Frameworks Are Failing

The fundamental problem with international law is attribution. Rules on non-intervention, and their extension to cyber operations, are addressed under the Tallinn Manual 2.0's 154 rules. It requires a victim state to establish clear attribution before it can lawfully respond with countermeasures or invoke collective self-defense. Deepfake operations are built to defeat exactly that requirement: proxy execution through troll farms, plausible deniability via third-party platforms, and the technical difficulty of tracing synthetic media back to its state of origin together produce a gap. Meanwhile, the harm is real, and the perpetrator may be known to intelligence services, yet legally unprovable by current evidentiary standards. That gap will remain exploitable until international law accepts technical provenance evidence the cryptographic watermarks, model fingerprints, and metadata forensics- as a basis for attribution (Schmitt, 2017).

A second failure is that most existing responses are reactive: platforms take down specific pieces of synthetic content after the fact, while the damage deepfakes cause is structural and outlives removal. The results of a representative sample of 2,005 UK adults showed that people were more uncertain than misled after encountering a deepfake. This uncertainty can actually have a discernable impact on trust in news, the researchers call "generalized indeterminacy and cynicism", that is, trust in authentic information is mitigated alongside that of fake information (Vaccari & Chadwick, 2020). Efforts to

remove a deepfake in its initial hours won't make up for the harm created if audiences already saw it, highlighting the need to focus on resilience in the policy fight, not just on moderating it later.

The third failure is structural asymmetry. While open environments can be accessed by outsiders, those who control their own information environment can filter and block content at home; it is the openness that characterizes liberal democracies that is what adversaries exploit. A governance framework that places identical obligations on every state would constrain democracies in practice while remaining unenforceable against the authoritarian actors it is meant to target, and it would do nothing to address platforms' own algorithmic amplification of synthetic content, which currently carries no meaningful legal liability (Byman et al., 2023).

6.2 Recommendations: A Multi-Level Governance Architecture

Closing these gaps calls for action at three levels together. First, a binding multilateral treaty on state use of synthetic media, modelled on the Chemical Weapons Convention and built around shared technical-attribution standards, or, short of that, agreed norms developed through the UN Group of Governmental Experts process. Second, mandatory platform accountability, anchored in the EU AI Act's Article 50 labelling and watermarking requirements and paired with a "Deepfakes Equities Process" for deliberate multi-agency oversight of any defensive use. Third, institutionalized pre-bunking, following Ukraine's own pre-emptive 2022 warning, since epistemic damage occurs before content spreads and cannot be undone by later takedowns. None of the three measures is individually effective (Byman et al., 2023; Schmitt, 2017).

CONCLUSION

This paper has argued that AI-generated deepfakes and algorithmic social media manipulation amount to more than a new tool of statecraft; they mark a structural change in the international information environment. There is one key asymmetry: Spreading convincing strategic deception is almost free, while proving the opposite is not. No single theoretical lens is enough; it is necessary to combine them. One of the reasons that it was obvious that cheap, deniable, high-leverage information tools would appeal to a state like Russia, whose IRA campaign reached an estimated 126 million on Facebook for about \$100,000, is that it makes sense to them. The deeper why is explained by constructivism: the intersubjective processes by which democratic publics build a collective political reality were attacked in the Zelensky video, which used his symbolic power against the country's will. In both instances, it was the political agency that was really being attacked, not military power.

Three governance failures follow from this analysis: the legal attribution gap, the irreversibility of epistemic harm, and the asymmetric vulnerability of open societies. They must be addressed in the context of the above treaty and platform accountability and pre-bunking measures, which must be done in tandem, and not in isolation. This is because the threat takes place at structural, discursive, and institutional levels. The overarching takeaway for IR scholarship is that all three of the key principles, sovereignty, deterrence, and democratic legitimacy and cohesion of the alliance, are contingent on a 'minimally reliable information environment'. Where that environment can be dismantled at near-zero cost, the discipline's foundational concepts need revision, not just extension. In the twenty-first century, truth itself has become contested terrain.

REFERENCES

- Bohacek, M. (2024). Slovakia as the precursor to deepfake-enabled election interference: Lessons learned and pathways forward. In *Workshop Proceedings of the 18th International AAAI Conference on Web and Social Media*. <https://doi.org/10.36190/2024.67>
- Bradshaw, S., & Howard, P. N. (2019). *The global disinformation order: 2019 global inventory of organised social media manipulation* (Working Paper 2019.2). Project on Computational Propaganda, Oxford Internet Institute, University of Oxford.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers. <https://doi.org/10.1515/9781685853808>
- Byman, D. L., Gao, C., Meserole, C., & Subrahmanian, V. S. (2023). *Deepfakes and international conflict*. Brookings Institution.
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107, 1753–1820.
- Dobber, T., Metoui, N., Trilling, D., Helberger, N., & de Vreese, C. (2021). Do (microtargeted) deepfakes have real effects on political attitudes? *The International Journal of Press/Politics*, 26(1), 69–91. <https://doi.org/10.1177/1940161220944364>
- Filipec, O. (2019). Hybrid warfare: Between realism, liberalism and constructivism. *Central European Journal of Politics*, 5(2), 52–71.
- Goldstein, J. A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., & Sedova, K. (2023). *Generative language models and automated influence operations: Emerging threats and potential mitigations*. arXiv. <https://doi.org/10.48550/arXiv.2301.04246>
- Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys*, 54(1), Article 7, 1–41. <https://doi.org/10.1145/3425780>
- Mueller, R. S., III. (2019). *Report on the investigation into Russian interference in the 2016 presidential election* (Vols. 1–2). U.S. Department of Justice.
- Nye, J. S., Jr. (2010). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School.
- Paterson, T., & Hanley, L. (2020). Political warfare in the digital age: Cyber subversion, information operations and ‘deep fakes.’ *Australian Journal of International Affairs*, 74(4), 439–454. <https://doi.org/10.1080/10357718.2020.1734772>
- Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
- Rini, R. (2020). Deepfakes and the epistemic backstop. *Philosophers’ Imprint*, 20(24), 1–16.
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press. <https://doi.org/10.1017/9781316822524>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society*, 6(1). <https://doi.org/10.1177/2056305120903408>
- Wendt, A. (1992). Anarchy is what states make of it: The social construction of power politics. *International Organization*, 46(2), 391–425. <https://doi.org/10.1017/S0020818300027764>
- Woolley, S. C., & Howard, P. N. (Eds.). (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford University Press. <https://doi.org/10.1093/oso/9780190931407.001.0001>