Critical Studies in Media Communication

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcsm20

Defending the state from digital Deceit: the reflexive securitization of deepfake

Bryan C. Taylor

To cite this article: Bryan C. Taylor (2021) Defending the state from digital Deceit: the reflexive securitization of deepfake, Critical Studies in Media Communication, 38:1, 1-17, DOI: 10.1080/15295036.2020.1833058

To link to this article: https://doi.org/10.1080/15295036.2020.1833058

Published online: 21 Oct 2020.

CRITICAL STUDIES IN MEDIA COMMUNICATION
2021, VOL. 38, NO. 1, 1–17
https://doi.org/10.1080/15295036.2020.1833058

Defending the state from digital Deceit: the reflexive securitization of deepfake

Bryan C. Taylor

Department of Communication, University of Colorado-Boulder, Boulder

ABSTRACT

Recent revelation of disinformation campaigns conducted by external adversaries on social media platforms has triggered anxiety among western liberal democracies. One focus of this anxiety has been the emerging technology known as *deepfake*. In examining related controversy, I use the theoretical lens of *securitization* to establish how *communicative reflexivity* shapes the attribution of threat to digital media. Next, focusing on the case of the U.S. government, I critique deepfake's securitization by applying two theories of media and state (in-) security. I argue that deepfake sustains the liberal state's conventional dread of *mimetic* threats posed to its *ontological security*. I then challenge this narrative by exploring *satire* as an alternate configuration of deepfake's capabilities. I conclude by summarizing the implications of this case for ongoing study of digital media, conflict, and politics.

ARTICLE HISTORY
Received 20 February 2020
Accepted 30 September 2020

KEYWORDS
Digital media; securitization; mimesis; ontological security; satire

Introduction: information warfare and the reflexive securitization of digital media

Early in the new millennium, the dominant paradigm of Internet connectivity emphasized inequality among global populations. Neoliberal speakers framed the primary challenge for international security as linking people to "the vast circuits of information which organize life on an increasingly global scale" (Reid, 2009, p. 608). However, this utopian vision suffered from a dubious assumption – that Internet audiences will necessarily engage new sources of information for beneficial purposes such as learning and growth.

The crises of Internet-based disinformation and authoritarian populism currently afflicting the western liberal democracies suggest otherwise (Bradshaw & Howard, 2019). In post 2016 hindsight, we see that the projects of networked politics were not restricted to globalization, public diplomacy, or protest movement organization. Instead, security officials failed to anticipate four converging trends in international conflict and social media development (Singer & Brooking, 2018). First, companies such as Facebook deliberately prioritized user engagement and revenue generation in their platform designs. Second, powerful states such as Russia refined their use of

CONTACT Bryan C. Taylor ✉ bryan.taylor@colorado.edu 🖃 Department of Communication, University of Colorado-Boulder, UCB 270, Boulder, CO, 80309-0270

cyber- and conventional operations to foment confusion and paralysis among international targets. Third, the popularity of social media platforms stimulated problematic psychological conditions among their users, such as homophily and confirmation bias. Finally, domestic political campaigns and international adversaries exploited these dynamics through strategic use of memes, sock puppets, and bots to promote viral circulation of divisive disinformation.

Numerous studies and reports conclude that these developments have created a novel and disorienting condition of insecurity (Horowitz et al., 2018; Sayler, 2019). Alternately known as "hybrid warfare" and "gray zone conflict" (Hicks et al., 2019), and associated with regimes of "post-" democracy and truth, this condition has blurred distinctions that conventionally organize security logics. Examples include those between *domestic* and *international* politics; *political* and *military* spheres; *civilian, proxy*, and *official* actors; and *peace* and *war*. While liberal states have long provoked citizens' mistrust through their domestic use of propaganda (Taylor, 2007), this current situation is extreme. Its development has outpaced not only traditional mechanisms of democratic governance, but also those of communication scholarship (Karpf, 2017).

In this essay, I address a central implication of this condition: *the reflexive securitization of digital media*. By this phrase, I associate two dimensions of digital media. The first arises from the familiar observation that such media enable the performance *of* communication, and the collection and analysis of data *about* that performance. Increasingly, however, these capabilities stimulate the intervention of corporate and state regimes seeking to exploit related benefits and minimize risks for valued interests (Meinrath & Vitka, 2014; Mirghani, 2011). In some cases, this process leads to the designation of digital media as *security threats*.

The second dimension of this phrase acknowledges that, while such outcomes may seem obvious or automatic, they are not so. As scholars of "securitization" remind us (Vuori, 2017), threatening objects do not *inherently* possess that status. Instead, they *assume* it *discursively* in political contexts such as policy deliberation. Here, speakers creatively solicit audiences to authorize the use of extreme measures to manage seeming threat. Securitization subsequently transforms the moral and political status of its objects, removing them from conventional protection by legal and human rights. Potentially, securitized objects are relegated to "zones of exception," in which sovereigns exercise discretion in deciding whether and how they may continue to exist.

Considered together, these two dimensions suggest how the securitization of digital media encourages speakers to *reflexively* engage its communicative status. Here, those actors *discursively* attribute and problematize a technology's *communicative* affordances – for example, in characterizing user practices and their consequences. As a result, such securitization is *meta-communicative*, and its critique requires acute sensitivity to communication concerns.

In this essay, I explore this implication by critiquing recent securitization of the digital technology known as "deepfake." Briefly, this term refers to recent innovation configuring the capabilities of computing, artificial intelligence, multi-media editing software, and archived digital records (Hao, 2018). Deepfake users pit machine-learning algorithms against each other in "generative-adversarial networks" (GAN's) to produce, test, and refine audio-visual texts. Potentially, these texts plausibly simulate the appearance and activities of existing figures, and synthesize depictions of artificial figures. These depictions may then be presented to audiences in either marked (e.g. as parody) or unmarked fashion (e.g. as disinformation). In responding to the appearance of deepfake, numerous speakers have publicly declared its fearful qualities. In this process, they have frequently associated deepfake with the sphere of "national security" – for example, by noting the threat posed to election integrity by faked videos discrediting political candidates. The U.S. government has responded by mobilizing its considerable resources to manage the apparent deepfake threat.

In the sections that follow, I critique this response as a case of reflexive securitization of digital media. I begin by reviewing distinctive conditions that influence this type of event, and proposing a critical agenda that challenges its potential to prematurely foreclose media evolution. I next review recent controversy surrounding the emergence of deepfake. I then apply two sets of theoretical traditions well-suited for exploring its reflexive securitization. The first tradition, *mimesis*, emphasizes the transgressive capability of media for creating uncanny imitation – one that frequently provokes allegations of nefarious deception. Deepfake's mimetic power subsequently threatens the *ontological security* of liberal state actors, triggering their defensive securitization. I argue that while this effort usefully defends vulnerable groups and cherished institutions, it also distorts consideration of deepfake's potential for *critically* transforming security politics. I illustrate that argument by considering deepfake's capability for *security satire*. I conclude by discussing the implications of this case for ongoing critique of digital media and securitization.

Critiquing the reflexive securitization of digital media: an overview

Securitization theory was originally developed by European scholars in the field of security studies (Waever, 1995). It has subsequently been used by communication scholars to study the evolving relationship between media, politics and conflict (Hasian et al., 2015; Vultee, 2010; Walsh & Barbara, 2006) – particularly how military and political officials, mainstream news outlets, and online publics have influenced post 9/11 audiences concerning the global war on terrorism. In this study, I draw from existing work depicting the securitization of digital media (Andersen, 2017; Hart et al., 2014; Lacy & Prince, 2018; Lawson, 2014). Space does not permit review of the state's ongoing mobilization of artificial intelligence, biometric, cybersecurity, and surveillance technologies. Instead, I briefly focus on communicative affordances of digital media that provoke securitization campaigns. Here, it is important to acknowledge the wide-ranging and fluid politics of those campaigns. Typically, they are initiated by security elites, but regular citizens may demand state regulation of an emerging technology. Citizens may also protest the state's use of technology, seeking modification or termination of particular security policies (Glass, 1993). In some cases, these popular campaigns are endorsed by security elites. In all cases, however, securitization speakers are concerned with technological affordances enabling "bad actors" to create undesirable states of insecurity for valued groups and their interests (Ekblom, 2012). Viewed in this light, digital media offer eight communicative capabilities that are particularly likely to stimulate securitization claims (Potzsch, 2017).

First, the *digital* formatting of data may permit the unacknowledged creation and circulation of copied files by hackers and whistleblowers. Second, the *increasing volume and* *rate* of online communication may overwhelm popular and official audiences, degrading their critical reception and decision-making capabilities. Third, the digital *convergence* of media formats may permit bad actors to blur content genres, and expose private activities through the creation and circulation of information-rich recordings. Fourth, advances in *data compression* potentially enable institutions to unilaterally collect users' personal information, and store it in massive archives vulnerable to breach and exploitation. Fifth, growing system capabilities for *interactivity* may increase user risk of exposure to identity deception, covert surveillance, and misappropriation of recorded data. Sixth, *networked* connectivity reduces centralization and control of security actors, and may encourage their unauthorized diffusion of deceptive and damaging influence. Seventh, layers of embedded programs *automate* online communication, potentially subjecting users to misdirection and constraint by unauthorized controllers. Finally, online *algorithms* that pre-emptively assess and exploit user value commonly display design bias, which cultivates misrecognition and injustice.

Collectively, these characteristics of digital media constitute risky affordances of communication that are likely to figure in their reflexive securitization. To date, related studies have emphasized themes such as the irrational and opportunistic inflation of "cyber-threat" by politicians (Hartnett, 2011) and defense experts (Lawson & Middleton, 2019); evolving efforts by military officials to regulate the use of digital media among deployed troops (Silvestri, 2015); the abuse of internet memes by alt-right political campaigns as vehicles of vicious rhetoric (Woods & Hahner, 2019); online campaigns by post-9/11 liberal states to counter violent extremism (Braddock, 2019); related usage of speech-violence metaphors (e.g. "information bomb") to criminalize online discourse (Stahl, 2016) and finally, the role of material–semiotic relationships in shaping attributions of digital media's authorship, significance, and effects (Andersen, 2017). Collectively, these findings offer handholds for critics seeking to advance understanding of the reflexive securitization of digital media.

But what is a suitable purpose of that critique? Here, I argue that by attributing the nature and consequences of an emerging technology, securitization may essentialize and stigmatize its identity. This effect may in turn undermine ethical reflection and democratic deliberation surrounding its development. This claim references familiar scholarly debate concerning the ontology and etiology of technology. Social constructionists, for example, emphasize the "interpretive flexibility" displayed by developing technologies, as various groups interact to influence their form, function, and significance (Bijker, 2008). Similarly, theorists of "assemblage" (Slack & Wise, 2005) depict technology as constituted by indeterminate relationships between its material and symbolic components. The possibilities for these relationships are typically "fixed" by influences manifest in specific contexts. Frequently, contingent articulations of technology are institutionalized, and misrecognized as static objects with inherent causality. Nonetheless, these articulations remain (in theory) open to reconfiguration. While they possess important differences, these traditions share an image of technology as an unfolding site of contest between motivated groups, seeking to resolve its ethical and political "ambivalence" (Feenberg, 2002). The implication for this study is that reflexive securitization of digital media may prematurely foreclose the becoming of *both* technology *and* communication. As a result, we do well to practice critical vigilance.

A brief history of deepfake

Initially, Deepfake emerged during 2017 among a subreddit community, whose members developed software enabling them to insert facial images from one video source onto figures depicted in another, and subsequently released those modified texts online. While some of these experiments were humorous, most repurposed pornographic video recordings to exploit the *personae* of popular female actors. Between 2018 and 2019, a growing number of amateurs, professional *auteurs*, and formal organizations adopted deepfake technology to release thousands of multimedia texts on platforms such as YouTube, some of which achieved significant publicity (Ajder et al., 2019). To create these spectacles, users engaged in at least three types of technical operation. The first category involved *manipulating components of a single existing text*. The second involved *remixing components of multiple existing texts*. The third category involved *synthesizing "new" texts*. During this period, the source materials remediated in deepfake texts expanded beyond entertainment programming to include recordings of public figures engaged in conventional, role-related conduct (e.g. U.S. Presidents Barrack Obama and Donald Trump). During this period, the term "deepfake" was increasingly reserved for texts occupying the third category (i.e. in contrast to "cheapfake" videos occupying the first category).

During this period, crowds of regular online users, and a chorus of professional journalists, academics, and technologists responded to deepfake developments. While a few of these professionals cautioned against premature and "hysterical" overreaction (Brandom, 2019; Feldman et al., 2019; "Deepfakes are dangerous,", 2019), their collective discourse converged to attribute controversial – if not dangerous – status to deepfake. It did so by expressing speakers' surprise, curiosity, and alarm concerning the "immense" threats (Beavers, 2019) deepfake posed to allegedly vulnerable targets. These depictions emphasized a "perfect storm" of "weaponized" technology (Hsu, 2019) and "computational propaganda" (Parkin, 2019) that had been "unleashed" (Beavers, 2019) to create a "wormhole of darkness" ("A reason to despair,", 2019). Because these "terrifying" and "uncanny" (Kearns, 2019) technologies would prove irresistible to unethical actors, their use seemed inevitable. The rapid, viral spread of deepfake texts – likened to "a zombie horde" (Warner, 2019) – would be hard to detect (e.g. among private, encrypted networks), and would likely sow widespread confusion, division, and "civil unrest" (Brown, 2019). In elaborating these claims, elite speakers developed four primary themes.

First, because deepfake typically misled online users about the ontological status of its depicted figures, it constituted *a toxic source of deception*. In particular, deepfake threatened to erode – if not fully eradicate – public confidence in visual media as a reliable source of evidence for verifying the actuality of reported events (Wright, 2019). Second, speakers emphasized that deepfake *exacerbated a growing epistemological crisis* in liberal democratic societies, spawned by the Internet's proliferation of dubious information and extremist opinion (Paris & Donovan, 2019). By crippling the development of consensus and civility required for democratic governance, deepfake could thus "undo much of the last century's progress toward peace, stability and prosperity" (Parkin, 2019), and "spiral [societies] . . . headlong into a dystopian acid trip of a world" (Parkinson, 2019). Third, speakers depicted deepfake as *perpetuating a destructive trend of covert interference* in domestic elections by external adversaries. Those figures had harnessed online resources such as "fake news" and trolling to compromise the democratic ideals of citizen education and deliberation. Speakers thus emphasized the urgency of these threats for the impending cycle of national elections – particularly the 2020 U.S. Presidential campaign (Metz, 2019). Finally, speakers emphasized *facilitating conditions* that hastened the manifestation of deepfake threats. Trends cited here included *declining barriers* to the production of plausible deepfakes, including time, cost, and users' skill-level (Stankiewicz, 2019). Alternately, the availability and sophistication of related software had *dramatically increased* (Foley, 2019), allowing users to transpose images of entire heads to permit "full control of another person" (Summerville, 2019).

Rapidly, this wave of popular and professional discourse stimulated official securitization. Here, various speakers rose to narrate threats posed by deepfake to *U.S. national security*. The following list of scenarios (Chesney & Citron, 2018, pp. 20–21) illustrates the range of envisioned concerns:

- Fake videos could feature public officials taking bribes, uttering racial epithets, or engaging in adultery.
- Soldiers could be shown murdering innocent civilians in a war zone, precipitating waves of violence and even strategic harms to a war effort.
- False audio might convincingly depict U.S. officials privately "admitting" a plan to commit this or that outrage overseas, exquisitely timed to disrupt an important diplomatic initiative.
- A fake video might depict emergency officials "announcing" an impending missile strike on Los Angeles or an emergent pandemic in New York, provoking panic and worse.

Other speakers elaborated these initial threat scenarios. One military blogger (Littell, 2019) imagined the blackmailing of spies and diplomats, using artificial depictions of their bodies, *en flagrante delicto*: "*Marcus looks down at the phone and sees a video of a man embracing a woman for a kiss. He's the man in the video. But the woman is not his wife*" (emphasis added). Other fearful visions included a repetition of the 2012 attack on the U.S. consulate in Benghazi, Libya: "Local citizens could be mobilized or recruited by extremist groups through the circulation of a fabricated video for a comparable attack" (Littell, 2019). Elsewhere, journalists reported the emergence of fake member profiles on social media networks, apparently intended for the seduction and recruitment of security professionals (Satter, 2019), and the haunting projection by one scientist of deepfake deception triggering the international use of nuclear weapons (Christian, 2018).

In response to these and other calls, federal actors mobilized to assess and respond to deepfake threats. Support agencies such as the Congressional Research Service (Sayler & Harris, 2019) prepared briefs explaining existing Department of Defense programs devoted to the detection of malicious artificial videos. In Congress, two major events occurred. First, the U.S. House Intelligence Committee convened a hearing in June 2019 to scope deepfake concerns and potential solutions. Particularly interesting moments from this event included Committee Chairman Adam Schiff's (D-CA) opening display of sample deepfakes, followed by an awkward explanation of their layered artifice ("National Security Challenges,", 2019, p. 4):

> So the only problem with that video is [comedienne-impersonator] Kate McKinnon actually looks a lot like [U.S. Senator] Elizabeth Warren, but the one on the left was actually – both were Kate McKinnon, one just had Elizabeth Warren's face swapped onto her, but it shows you just how convincing that kind of technology can be.

Another video, Schiff concluded, indicated how deepfake could "turn a world leader into a ventriloquist's dummy" (p. 3). Faced with this evidence, he concluded, "one does not need any great imagination to envision even more nightmarish scenarios that would leave the government, the media, and the public struggling to discern what is real and what is fake" (p. 4).

Another speaker in this hearing, former FBI agent and current Distinguished Research Fellow at the Foreign Policy Institute, Clint Watts, offered an ominous prediction. China and Russia would continue to use deepfake to "discredit domestic dissidents and foreign detractors, incite fear and promote conflict inside Western-style democracies, and distort the reality of American audiences and audiences of American allies" (p. 20). Whether practiced by "oligarchs, corporations, political action groups, public relation firms . . . [or] activists with significant financial support," Watts concluded, "the net effect will be the same: degradation of democratic institutions and elected officials, lowered faith in electoral processes, weakened trust in social media platforms, and potentially sporadic violence by individuals and groups. . ." (p. 21). In response to these developing themes, committee member Rick Crawford (R-Ark.) attempted to leaven the proceedings with generational humor: "Well, we have come a long way since Milli Vanilli, haven't we?" (p. 47).

In the U.S. Senate, subsequently, members directed the Department of Homeland Security to annually assess deepfake threats and responses. "National security experts," their bill noted, "are concerned that the continued dissemination of deepfake content across trusted media platforms could increasingly be used to dupe audiences and amplify false narratives about American cultural norms and interests domestically and abroad" ("Deepfake Report Act,", 2019, p. 2). "The Federal Government," it concluded, "should proactively identity [*sic*] the tools and techniques used by our adversaries to develop deepfake technologies and content, and develop countermeasures and tools to identify and counter deepfake content" (p. 3).

Critiquing the reflexive securitization of deepfake: the contributions of mimesis and ontological security

Our discussion so far has depicted a robust movement to securitize deepfake as an alarming and perilous development in digital media – one whose affordances are likely to "incite political violence, sabotage elections, and unsettle diplomatic relations" (Stanton, 2019). In this section, I explore how gnomic images of communication operate at a recessed level in this controversy. That is, deepfake's reflexive securitization indicates how attributions of digital media threat may mask the persistence of visceral defenses, mounted by cultural groups against the disturbing possibilities of communication *itself* (see Marvin, 1988). To explore this claim, we require instruments that clarify the distinctive "spirit" of communication (Katz & Aakhus, 2002) that is attributed through reflexive securitization to deepfake. As a result, we can better understand what drives such efforts, and fuels their reception among contemporary audiences. Below, I proceed by applying two, combined theoretical traditions: *mimesis* and *ontological security*.

Mimesis

Elsewhere (Taylor, 2017, p. 55), I have characterized the mimetic tradition as an "ancient and . . . sprawling" conversation, conducted among philosophers and theorists, concerning the nature of *imitation* (e.g. pretense and resemblance). Fundamentally, mimetic theory addresses the contingency created for ontological claims, made about seemingly original and independent entities, by their awkward entanglement with doubles engaged in projects of *simulation* and *adaptation*. It subsequently acknowledges how cultural figures such as *twins, impostors,* and *surrogates* stimulate the archetypal plots of comedy, drama, and tragedy. In related narratives, these devices perform this function by corrupting authenticity; mocking authority; inducing involuntary assimilation, and generally, complicating characters' experience of self-identity by asserting the rule of interdependency.

In that account, I traced the descent of "conservative" and "critical" traditions of mimesis through the literatures of communication and security studies. The first tradition stigmatizes imitation as a parasitic violation of the Real's integrity. The second tradition, alternately, foregrounds the possibility of redemptive ethics and politics arising from imitation – including the tactics of survival (e.g. camouflage, passing, etc.) practiced by vulnerable groups in hostile environments (von Boemcken, 2019). By problematizing how distinctions between the real and the fake shape influential conceptions of security, critical mimesis may "precipitate a crisis of authority in realist discourses that otherwise aspire to the production of certainty, finality, and totality" (Taylor, 2017, p. 57).

How, then, does mimesis shape the securitization of deepfake? Four influences are apparent. First, the techno-logic of deepfake is *premised* on imitation, as each of its GAN's seeks to learn and improve from the other by competitively synthesizing and evaluating multimedia texts (i.e. until the fake can no longer be detected). Second, mimesis saturates the *zeitgeist* of contemporary information warfare. Here, it is precisely the ability of deceptive actors to first, present themselves and their communication *as-if* benign phenomena that warrant acceptance, and second, to induce *the replication* of that communication by gullible audiences, which drives insecurity (Singer & Brooking, 2018). Third, this condition promotes a mimetic collapse of boundaries traditionally distinguishing the realms of *everyday media use, formal politics*, and *armed conflict*, such that each increasingly *resembles* the others.

Ontological Security

Most significantly, the mimetic qualities of deepfake threaten the "ontological security" of nation-states. Grounded in the theorizing of R.D. Laing and Anthony Giddens, this concept traditionally denotes the psychological ability of individuals to sustain a coherent and stable identity amid the stressful conditions of modern life. More recently, international relations scholars (Croft, 2012; Mitzen, 2006; Steele, 2008, 2012) have adapted it to theorize the fundamental role of identity in the motives and actions of nation-states. Generally, they argue that those actions may be attributed to the state's desire to experience itself as a rational, linear, and durable entity. In this process, state (and state-identified) actors default to interpreting and responding to events so as to maintain their preferred conception of its essential qualities and interests. Those actors subsequently experience gratification when audiences validate those performances. Conversely, when the state is unable to maintain this performance, its actors may display anxiety and paralysis, and lash out violently. Here, critics engage state performances as evidence of the state's ongoing desire to tell a plausible story *about* itself, *to* itself. Of particular interest, then, are those moments when the state loses control – through insurrection, miscalculation, or scandal – of its ability to maintain ontological security, and is confronted with intolerable images of its identity. Such moments open the state to a variety of discordant experiences, including *shame* over its actual behaviors, and *dread* concerning its potential disintegration. The state must then engage in unwelcome practices such as reflection and accountability.

The connection between mimesis, ontological security, and the reflexive securitization of deepfake follows logically. As Silverstone (1993) first argued, the reliability of broadcast programming schedules provided postwar media audiences with one means of maintaining a comforting, routinized existence. As well, decades of scholarship have confirmed the state's reliance on media systems to ritually solicit attributions of its legitimacy and authority from citizen-audiences (Miskimmon et al., 2014). We are thus led to question how particular images and accounts of state identity, represented to the state by digital media, affect its ontological security. Key here is how deepfake exemplifies the capability of digital media to disrupt state control over the circulation of relevant images, and to proliferate potentially subversive representations.

As discussed above, deepfake's "democratization of counterpower" (Steele, 2012, p. 105) has – so far – primarily triggered the liberal state's reactionary loathing of uncontrollable reflection. As Steele (2012, p. 10) notes, this effect may occur because liberal states know that their identities are *more* contested and precarious than those developed in other systems of governance. Additionally, because liberal states routinely engage in covert actions that they disguise and deny through the use of propaganda, it is not simply that deepfake disrupts a superficial economy of state-related images. Instead, that violation is more fundamental, as deepfake mimetically weakens the state's ability to *strategically modulate the very relation between truth and falsehood, as it would prefer*. Potentially, deepfake's uncanny reflections implicate the state as a narcissistic actor whose identity remains viable, only to the extent it is able to control the reproduction of its image.

Is deepfake redeemable? Critical alternatives to the securitization narrative

Given the argument above, it is unsurprising that there has been little discussion of deepfake's potential for creating *critical mimesis in (inter-)national security*. This is regrettable, because deepfake has demonstrated its ability to influence the state's repertoire of self-other dialectics. Conceivably, this process might serve valued critical ends, such as emancipation and demilitarization.

But does deepfake truly possess this capability? Given its predominant securitization in public discourse, some skepticism here is understandable (i.e. as an effect). Nonetheless, there are at least two arguments supporting the claim of deepfake's functional – and perhaps also political – malleability. The first argument cites as evidence growing public advocacy of deepfake's "positive" and "beneficial" uses. Here, for example, speakers envision deepfake's *potential* for facilitating the expression of vocally impaired medical patients, enabling cultural institutions to attract audiences by animating static visualizations, and fostering healthy audience caution as a component of media literacy pedagogy (Chandler, 2020; Kwok & Koh, 2020; Ovadya, 2019; Rees, 2019). These speakers also report *actual* progressive uses of deepfake, including for multi-lingual ventriloquism of celebrities in online appeals for international aid (Simonite, 2020), and the replacement by documentary filmmakers of vulnerable participants' recorded voices and images with those of volunteers (i.e. to protect their anonymity; Rothkopf, 2020). Significantly, while some speakers refer to this repurposed technology as "synthetic media" (Waddell, 2019), most continue to use the term "deepfake."

The second argument for tempering deepfake's securitization is more speculative, and invokes cultural contexts that liberate its *aesthetic* potential for influencing "security." One prominent context is *satire*, defined as "narratives [that] offer subversive social criticism, using irony and sarcasm to lampoon the rich and powerful . . . undermining a status quo seen as unjust or harmful" (Payne, 2013, p. 3). Satire becomes political when it engages institutional forms and practices that constitute a society's system of governance. Because the state historically claims security-provision as its *raison d'être*, security forms an especially rich target for political satire.

Conceivably, deepfake might sustain four traditions in related *security satire*. First, satire *destabilizes security regimes* by recovering complexities and contradictions that are typically effaced in their moralized claims to unity, necessity, and effectiveness (Harrington, 2012). Satire engages international conflict, for example, as an opportunity to explore competing stories of event causation, to critique premature justifications and distorted conclusions (e.g. surrounding the use of armed force), and to promote nonviolent security paradigms based on curiosity, humility, and improvisation. Second, security satire *"infects" the public personae of security actors*, hijacking their conventional production of narrative closure to create distorted imitations that undo familiar logics (e.g. binary) and premises (e.g. of ethnic and racial superiority). These practices dethrone security elites by highlighting their flaws, revealing them to be pompous and hypocritical – even grotesque (Payne, 2017, p. 218). Third, security satire *recovers the voices and points of view associated with "ordinary people,"* who would otherwise be marginalized as "mere" props, collateral damage, and/or witnesses for security officials who presume to serve as history's authors (Payne, 2013). In this way, finally, security satire *disrupts powerful regimes of memory and history* that rationalize security policy through "narratives of national heroism and sacrifice" (Edenborg, 2017, p. 306). Here, satire challenges narratives that provide audiences with alternately consoling and enflaming designations of victim, perpetrator, and defender identities. Satire *reconstructs* these articulations of identity (Rice, 2018), and *reclaims* security issues for treatment by a more organic and authentic politics.

For two reasons, critical media scholars should value deepfake's potential for performing security satire. First, satire is a practice that is *distinctively shaped by media logics*

(Hall, 2014). As a result, scholars are increasingly concerned with its digital forms and capabilities – including their stimulation of *vernacular* security discourses (Downing, 2020). Deepfake satire thus offers a plausible site of innovation in this sphere of digital practice. Second, that satire is likely to offer media scholars uniquely digital cases of *reflexive, self-sustaining controversy*. This possibility is influenced by two conditions. The first is that media formats strongly influence qualities of *immediacy, circulability, and ambiguity* that influence audience interpretations of security satire (Hansen, 2011). The second condition is that texts of security satire display intertextual relationships with other, prior mediations that they evoke and depict. Deepfake satire may promote media controversy, then, because these two conditions stimulate interaction between satire's producers, targets, commentators and regulators. This interaction may proliferate and escalate as mediated speakers report the release of deepfake texts; exchange attributions of traits and motives (e.g. hyper-sensitivity); debate which interpretations should be considered accurate and legitimate; and potentially, release modified versions of an "original" deepfake text. In this process, the defining boundaries between digital texts and their contexts, and between originating acts and subsequent reactions, may continuously blur and reconfigure.

In light of this discussion, it is not difficult to conjure examples of deepfake security satire. Deepfake might, for instance, depict security elites lapsing from their conventional scripts for public performance (e.g. defense ministers at press conferences), and violating audience expectations for resolute, patriotic, and hygienic discourse. These sudden eruptions of incongruity might voice cynicism, despondency, and irrationality that undermine the credibility of official security policy. Alternately, deepfake satire might visually morph the orthodox public staging of security actors' bodies (e.g. soldiers at medal-award ceremonies), creating new imagery that plausibly alleges their actual "conduct unbecoming" (e.g. violent treatment of unarmed prisoners). This multimedia fun-house mirroring would recover for collective consideration known but repressed qualities of security, including *cruelty*, *error, fear, indecision, insanity, regret*, and *waste*.

While imagining these possibilities can be gratifying, responsible critique must also anticipate conditions *limiting* deepfake's potential as a medium of security satire. Four conditions are particularly apparent. First, *the political effectiveness of that satire is by no means guaranteed*. Indeed, there is significant debate about whether mediated security satire of any kind is capable of directly or immediately producing revolutionary change (Jones, 2017). Sympathetic viewpoints in this debate instead emphasize satire's other virtues – including its creation of disruptions that may cohere and scale to support long-term change; its demonstration of the role of mundane transgression in security cultures; and its preservation of critical literacy and solidarity among an otherwise fragmented, dormant citizenry.

Second, deepfake's satirical effectiveness depends on *its ability to distinguish itself (and avoid appropriation) in an increasingly cluttered media landscape*. This is because large media corporations have recently embraced the programming of political satire to reinvigorate professional myths (e.g. of "watchdog" journalism), and appeal to apathetic younger audiences (Holland & Levy, 2018). In responding to this challenge, deepfake would likely exploit its unique ability to remediate existing satirical formats. In comparison to cartoons, memes and GIF's, for example, deepfake's could appeal to audiences by exceeding their relatively brief and static depictions, and expanding their narrative potential. In comparison to cinematic and televisual narrative, however, deepfake satire would display opposite advantages (e.g. of conciseness). The relationship between deepfake satire and online parody accounts, finally, would depend on whether the former is domesticated as stable content by known providers on commercial platforms, or continues to be released independently (and anonymously) online, relying for its one-off virality and evasion of censorship on users' unpredictable recirculation.

Third, deepfake's potential mockery of security *must contend with the infamously volatile and amoral politics of satire*. In particular, satire's de-differentiating logic rejects others' claims of exceptionality and entitlement – a practice that creates ontological *security* for satire's speakers (whose xenophobia is assuaged), but ontological *insecurity* for its targets (whose aspiration is diminished). As a result, deepfake security satire would likely stimulate energetic public debate concerning the digital mediation of political rights, justice, and equality. Those debates would invoke competing norms of decorum and tolerance to negotiate the tension created by that satire between ideals of individual liberty and communal responsibility. Potentially, these debates matter because mediated security satire is increasingly depicted in the divergent politics of global society as a performance of symbolic harm (if not violence), and a justification for revenge committed by its targets (Hansen, 2011). The actual effects of deepfake security satire, then, must plausibly correspond to the critical ideals it purports to serve. Here, producers of that satire would need to minimize audience members' current mistrust and rejection – principally, by revising their epistemological contract with them. That revision must somehow (e.g. through marking of related texts) reframe audience members' encounter with deepfake as the relatively voluntary pursuit of desirable political ends, achieved by engaging with provocative (and potentially discomforting) critique.

This requirement becomes even more challenging, finally, when we consider how *current western politics confounds the distinction between elite and popular discourse that conventionally underwrites security satire*. Specifically, the recent mainstreaming of authoritarian-populist discourse in liberal-democratic governance is partly paradoxical, in that powerful security actors subsequently represent themselves as-if anti-establishment outsiders. As vividly demonstrated by Donald Trump's use of Twitter, these *de facto* elites employ hyperbole, perversity, ridicule, and taboo in appealing to their anti-government sympathizers, and in depicting themselves as victims of "deep-state" conspiracy. These performances co-opt satire as a means of cloaking and justifying toxic discourses of misogyny, racism, and xenophobia. They also stimulate – and are reinforced by – the online use among political-extremist groups of deeply coded satire that simultaneously obscures and promulgates hateful rhetoric. These codes (e.g. frog memes and Hawaiian shirts) provide extremists and their platforms with some measure of deniability in defending against accusations of promoting hate. These defenses minimize vicious speech acts as "only joking," and their political content as non-ideological (Schwarzenegger & Wagner, 2018). In this way, deepfake security satire forms a dangerous critical opportunity, because extremist opponents are predisposed to reciprocate its use as a counter-leveling strategy.

Considered together, the two sets of argument developed in this section establish that deepfake's development does not – as its current securitization maintains– necessarily portend the *tragic destruction* of state identity. Instead, while its critical potential is admittedly limited and contingent, deepfake security satire might *productively stimulate* democratic politics. Those politics would doubtless be agonistic, but they might also encourage more robust debate of security policy among officials and citizen-audiences (Browning & Joenniemi, 2017).

Conclusion: until we cheat again

In this essay, I have critically intervened in the evolving intersection of security, communication, and digital media. In this tense site, the discourses of state authority and professional expertise typically rule – despite their frequent inconsistency and destructive consequences. That hegemony, however, is not monolithic or eternal. In illustration, I have depicted how recent innovation in information warfare has destabilized conventional relationships developed between media and security. Second, I have conceptualized communication affordances of digital media that are likely to provoke reflexive attribution of its threatening status. Third, I have demonstrated how public response to deepfake's emergence has seized upon those qualities to depict it as an existential threat. Fourth, I have theorized how the formal securitization of deepfake by U.S. officials similarly displays a distinctive anxiety, shaped by two intertwined logics of communication. Here, deepfake's mimetic capability to proliferate uncontrollable representation of state identity triggers the state's aversion to ontological insecurity.

To confirm, I do not seek here to dismiss this securitization campaign, which may usefully protect vulnerable figures and cherished institutions. Nonetheless, that campaign is prone to distortion arising from the state's perpetual drive to control its own becoming. Of particular concern here is the state's dubious claim to onto-political authority in defining standards of truth and falsehood that benefit its interests. For better and worse, deepfake exposes the arbitrariness of those standards, and implicates the forms of state identity they support. The case of the U.S. government demonstrates how, through reflexive securitization, the liberal state has – so far at least – discouraged other possibilities for deepfake's development that arise from valuing its aesthetic evocation of competing security truths. In response, I have explored *satire* as an alternate deepfake modality that may serve democratic ideals by promoting public deliberation of security outside the confines of conventional policy discourse. Principally, this reimagining of deepfake reframes the appearance of *involuntary encounter* with *malign deception* seeking to *subvert political agency* as a *voluntary encounter* with *provocative textuality* seeking to *empower political agency*. Crucially, my argument does not recover some original or essential deepfake identity that has been obscured by its securitization. Instead, it suggests how securitization and counter-securitization discourses *both* work to configure the symbolic and material properties of digital media, facilitating their articulation with larger political logics. In this way, precisely because it does not lead to a single or simple conclusion, the case of deepfake suggests how digital media will continue to offer scholars of communication, conflict, and politics a source of relevant – and challenging – problems.

Notes on contributor

Bryan C. Taylor is Professor of Communication at the University of Colorado-Boulder. A early version of this essay was presented at the 2019 NCA Conference. The author thanks Hamilton Bean, Boris Brummans, and Leslie Hahner for their comments on related drafts.

References

Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019, July 10). The state of Deepfakes. *DeepTrace*. https://deeptracelabs.com/mapping-the-deepfake-landscape/

Andersen, R. S. (2017). Video, algorithms and security. *Security Dialogue*, *48*(4), 354–372. https://doi.org/10.1177/0967010617709875

Beavers, O. (2019, Jan. 20). Washington fears new threat from 'deepfake' videos. *The Hill*. https://thehill.com/policy/national-security/426148-washington-fears-new-threat-from-deepfake-videos

Bijker, W. E. (2008). Technology, social construction of. *The International Encyclopedia of Communication*. https://onlinelibrary.wiley.com/doi/full/10.1002/9781405186407.wbiect025

Braddock, K. (2019). Communicatively countering violent extremism online. In B. C. Taylor, & H. Bean (Eds.), *Handbook of communication and security* (pp. 247–261). Routledge.

Bradshaw, S., & Howard, P. (2019). *The global disinformation order*. https://comprop.oii.ox.ac.uk/research/cybertroops2019/

Brandom, R. (2019, Mar. 5). Deepfake propaganda is not a real problem. *The Verge*. https://www.theverge.com/2019/3/5/18251736/deepfake-propaganda-misinformation-troll-video-hoax

Brown, N. I. (2019, May 13). Wait, is that video real? *USA Today*. https://www.usatoday.com/story/tech/2019/05/13/deepfakes-why-your-instagram-photos-video-could-be-vulnerable/3344536002/

Browning, C. S., & Joenniemi, P. (2017). Ontological security, self-articulation and the securitization of identity. *Cooperation and Conflict*, *52*(1), 31–47. https://doi.org/10.1177/0010836716653161

Chandler, S. (2020). Why deepfakes are a net positive for humanity. *Forbes*. https://www.forbes.com/sites/simonchandler/2020/03/09/why-deepfakes-are-a-net-positive-for-humanity/#e57172d2f84f

Chesney, B., & Citron, D. (2018). Deep fakes. *SSRN*. https://ssrn.com/abstract=3213954

Christian, J. (2018, Feb. 1). Experts fear face swapping tech could start an international showdown. *The Outline*. https://theoutline.com/post/3179/deepfake-videos-are-freaking-experts-out?zd=3&zi=dhfcbpat

Croft, S. (2012). Constructing ontological insecurity. *Contemporary Security Policy*, *33*(2), 219–235. https://doi.org/10.1080/13523260.2012.693776

Deepfake Report Act. (2019, Sept. 10). *Report of the U.S. Senate Committee on Homeland Security and Governmental Affairs*. https://www.congress.gov/116/crpt/srpt93/CRPT-116srpt93.pdf

Deepfakes are dangerous. (2019, June 16). *Washington Post*. https://www.washingtonpost.com/opinions/deepfakes-are-dangerous–and-they-target-a-huge-weakness/2019/06/16/d3bdbf08-8ed2-11e9-b08e-cfd89bd36d4e_story.html

Downing, J. (2020). Memeing and speaking vernacular security on social media. *Journal of Global Security Studies*, 1–17. https://watermark.silverchair.com/ogz081.pdf?token=AQECAHi208BE49Ooan9kkhW_Ercy7Dm3ZL_9Cf3qfKAc485ysgAAAtIwggLOBgkqhkiG9w0BBwagggK_MIICuwIBADCCArQGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQM2MECjFrMPMKuNbKyAgEQgIIChYqauTInKMoeQl6ANUYkYX3K1YyTBTCQU5mjQK9wN0hFlQtCNRiWPX6_f42TM9wNng0rKhgknDR2WHamXhIuPmpIn4uqGxat9QqJ-wUhUA8g5CAIu6B8SA4WFD3wIR203APbHJsm9d4Fmk4AO40o1n63pUynwJgeHWkH8F-NpGVFH953clp4qAKgg9FZRsuFeCtyUebMVOaTvisyAEQD42xmPNxMmT0qRIkrrIol529bHtNR_MsVNYvKL01Gktq3taZ1pCvSYk515ylEYjoSWOJsPpyx99h2UM3f2_j_-9bX-vA3kN3Vse1vNk3dbbZx-1kE04yJPbaiqQ46UX-3Ud4Fx3Rq_EHmyfPJL_nSA_psp5oJ6WACApNisyC8Wzb7YYC5Db-wjfBAoDhuQUla9ZdojBer4JEup_MO5atjet4J9nAMkft4itXtm-sAiK4LusYUIpBYFephad9TGHh5UXaYUvuH1UMdAnsJrT1EuWgKla29P2tLR9bcnAZnfsLyAw8iKhKvt19wH2Itu-374EwksN2Es1Kn9SdoQE_rk3dakdxr96_jWAUlJJSxydQOSkyS2SX5C416F1PlYkq-8_oGV_sOWt5gUVxHGAYxiM56ZXn2BE4kpGRz_jrO8QvJpM3Xns9nSoeING6kt1IYIER3AnNZ5O7lCH_bqGmZr2e1yXRNDm_syisHkBWz16jnYXM5tNUrpyRVNEqPemniuwqxEWkx1jhlBszObrVUtUoc2v3b6nnJbkada8aQOrpIP8dpzM6bpxHlpL1rgCWWAxFkdjMtae9F3Ztj1meh6uMc0jhbfTyHEnhcgNwIT9RJORhjbnj6O84MMjtiHL4W9MzwvqpABFw

Edenborg, E. (2017). Creativity, geopolitics and ontological security. *Postcolonial Studies*, *20*(3), 294–316. https://doi.org/10.1080/13688790.2017.1378086

Ekblom, P. (2012). Conceptual and methodological explorations in affordance and counter terrorism. In M. Taylor, & P. M. Currie (Eds.), *Terrorism and Affordance* (pp. 33–48). Continuum.

Feenberg, A. (2002). *Transforming technology*. Oxford University Press.

Feldman, B., Hart, B., & Read, M. (2019, Jun. 13). Are the Deepfake fears overblown? *New York Magazine*. http://nymag.com/intelligencer/2019/06/are-the-deepfake-fears-overblown.html

Foley, J. (2019, Nov. 15). 9 deepfake examples that terrified the internet. *Creative Bloq*. https://www.creativebloq.com/features/deepfake-examples

Glass, M. (1993). *Citizens against the MX*. University of Illinois Press.

Hall, I. (2014). The satiric vision of politics. *European Journal of International Relations*, *20*(1), 217–236. https://doi.org/10.1177/1354066112445187

Hansen, L. (2011). Theorizing the image for security studies. *European Journal of International Relations*, *17*(1), 51–74. https://doi.org/10.1177/1354066110388593

Hao, K. (2018, Dec. 1). Inside the world of AI that forges beautiful art and terrifying deepfakes. *MIT Technology Review*. https://www.technologyreview.com/s/612501/inside-the-world-of-ai-that-forges-beautiful-art-and-terrifying-deepfakes/

Harrington, S. (2012). The uses of satire. *Journalism*, *13*(1), 38–52. https://doi.org/10.1177/1464884911400847

Hart, C., Jin, D., & Feenberg, A. (2014). The insecurity of innovation. *International Journal of Communication*, *8*, 2860–2878. https://ijoc.org/index.php/ijoc/article/view/2774/1257

Hartnett, S. J. (2011). Google and the “twisted cyber spy” affair. *Quarterly Journal of Speech*, *97*(4), 411–434. https://doi.org/10.1080/00335630.2011.608705

HasianJrM., Lawson, S., & & McFarlane, M. D. (2015). *The rhetorical invention of America’s national security state*. Lexington Books.

Hicks, K., Friend, A., Federici, J., Shah, H., Donahoe, M., Conklin, M., … Sheppard, L. (2019). *By other means: Part I*. Rowman & Littlefield.

Holland, E. C., & Levy, A. (2018). *The Onion* and the geopolitics of satire. *Popular Communication*, *16*(3), 182–195. https://doi.org/10.1080/15405702.2017.1397674

Horowitz, M., Allen, G., Saravelle, E., Cho, A., Frederick, K., & Scharre, P. (2018). Artificial intelligence and international security. Center for a New American Security. https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security

Hsu, J. (2019, Feb. 28). Can AI detect Deepfakes to help ensure integrity of U.S. 2020 elections? *IEEE Spectrum*. https://spectrum.ieee.org/tech-talk/robotics/artificial-intelligence/will-deepfakes-detection-be-ready-for-2020

Jones, M. O. (2017). Satire, social media and revolutionary cultural production in the Bahrain uprising. *Communication and the Public*, *2*(2), 136–153. https://doi.org/10.1177/2057047317706372

Karpf, D. (2017). Digital politics after Trump. *Annals of the International Communication Association*, *41*(2), 198–207. https://doi.org/10.1080/23808985.2017.1316675

Katz, J. E., & Aakhus, M. (2002). *Perpetual contact*. Cambridge University Press.

Kearns, M. (2019). Deepfakes are deeply worrying. *National Review*. https://www.nationalreview.com/corner/deepfakes-deeply-worrying/

Kwok, O. J., & Koh, S. G. (2020). Deepfake. *Current Issues in Tourism*, 1–5. https://www.tandfonline.com/doi/epub/10.1080/13683500.2020.1738357?needAccess=true

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, *8*(1), 100–115. https://doi.org/10.1080/23269995.2017.1415082

Lawson, S. (2014). The US military’s social media civil war. *Cambridge Review of International Affairs*, *27*(2), 226–245. https://doi.org/10.1080/09557571.2012.734787

Lawson, S., & Middleton, M. (2019). Cybersecurity and communication. In B. C. Taylor, & H. Bean (Eds.), *Handbook of communication and security* (pp. 262–280). Routledge.

Littell, J. (2019). Don’t believe your eyes (or ears). *War on the Rocks*. https://warontherocks.com/2019/10/dont-believe-your-eyes-or-ears-the-weaponization-of-artificial-intelligence-machine-learning-and-deepfakes/

Marvin, C. (1988). *When old technologies were new*. Oxford University Press.

Meinrath, S. D., & Vitka, S. (2014). Crypto war II. *Critical Studies in Media Communication*, *31*(2), 123–128. https://doi.org/10.1080/15295036.2014.921320

Metz, R. (2019). The fight to stay ahead of deepfake videos before the 2020 US election. *CNN*. https://www.cnn.com/2019/06/12/tech/deepfake-2020-detection/index.html

Mirghani, S. (2011). The war on piracy. *Critical Studies in Media Communication*, *28*(2), 113–134. https://doi.org/10.1080/15295036.2010.514933

Miskimmon, A., O'Loughlin, B., & Roselle, L. (2014). *Strategic narratives*. Routledge.

Mitzen, J. (2006). Ontological security in world politics. *European Journal of International Relations*, *12*(3), 341–370. https://doi.org/10.1177/1354066106067346

National security challenges of artificial intelligence, manipulated media and "deepfakes.". (2019, Jun. 13). https://docs.house.gov/meetings/IG/IG00/20190613/109620/HHRG-116-IG00-Transcript-20190613.pdf

Ovadya, A. (2019). Making deepfake tools doesn't have to be irresponsible. *MIT Technology Review*. https://www.technologyreview.com/2019/12/12/131605/ethical-deepfake-tools-a-manifesto/

Paris, B., & Donovan, J. (2019). Deepfakes and cheap fakes. *Data & Society*. https://datasociety.net/output/deepfakes-and-cheap-fakes/

Parkin, S. (2019). The rise of the deepfake and the threat to democracy. *The Guardian*. https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the-rise-of-the-deepfake-and-the-threat-to-democracy

Parkinson, H. J. (2019). Let's get real before deepfake videos corrupt our democracy. *The Guardian*. https://www.theguardian.com/commentisfree/2019/jun/15/deepfake-videos-corrupt-democracy-mark-zuckerberg

Payne, R. A. (2013). Reading the Global War on Terror as comedy. Paper presented at the Annual Meeting of the International Studies Association, Washington, D.C. (Oct. 4-6).

Payne, R. A. (2017). Laughing off a zombie apocalypse. *International Studies Perspectives*, *18*(2), 211–224. https://doi.org/10.1093/isp/ekv026

Potzsch, H. (2017). Investigating the culture–media–security nexus. In P. Robinson, P. Seib, & R. Fröhlich (Eds.), *The Routledge handbook of media, conflict and security* (pp. 36–50). Routledge.

A reason to despair about the digital future. (2019, Jan. 6). *Washington Post*. https://www.washingtonpost.com/opinions/a-reason-to-despair-about-the-digital-future-deepfakes/2019/01/06/7c5e82ea-0ed2-11e9-831f-3aa2c2be4cbd_story.html

Rees, G. (2019). Here's how deepfake technology can actually be a good thing. *World Economic Forum Agenda*. https://www.weforum.org/agenda/2019/11/advantages-of-artificial-intelligence/

Reid, J. (2009). Politicizing connectivity. *Cambridge Review of International Affairs*, *22*(4), 607–623. https://doi.org/10.1080/09557570903325520

Rice, R. M. (2018). Negotiating the professional in media representation. *Tamara*, *16*(1/2), 25–36. https://tamarajournal.com/index.php/tamara/article/view/444

Rothkopf, J. (2020). Deepfake technology enters the documentary world. *New York Times*. https://www.nytimes.com/2020/07/01/movies/deepfakes-documentary-welcome-to-chechnya.html

Satter, R. (2019, Jun. 13). Experts: Spy used AI-generated face to connect with targets. *AP News*. https://apnews.com/bc2f19097a4c4fffaa00de6770b8a60d

Sayler, K. (2019, Nov 21). Artificial intelligence and national security. *Congressional Research Service*. https://fas.org/sgp/crs/natsec/R45178.pdf

Sayler, K., & Harris, L. (2019, Oct. 14). Deep fakes and national security. *Congressional Research Service*. https://crsreports.congress.gov/product/pdf/IF/IF11333

Schwarzenegger, C., & Wagner, A. (2018). Can it be hate if it is fun? *SCM Studies in Communication and Media*, *7*(4), 473–498. https://doi.org/10.5771/2192-4007-2018-4-473

Silverstone, R. (1993). Television, ontological security and the transitional object. *Media, Culture & Society*, *15*(4), 573–598. https://doi.org/10.1177/016344393015004004

Silvestri, L. E. (2015). *Friended at the front*. University Press of Kansas.

Simonite, T. (2020). Deepfakes are becoming the hot new corporate training tool. *Wired*. https://www.wired.com/story/covid-drives-real-businesses-deepfake-technology/

Singer, P. W., & Brooking, E. T. (2018). *Likewar*. Houghton Mifflin Harcourt.

Slack, J. D., & Wise, J. M. (2005). *Culture+ technology*. Peter Lang.

Stahl, R. (2016). Weaponizing speech. *Quarterly Journal of Speech*, *102*(4), 376–395. https://doi.org/10.1080/00335630.2016.1208365

Stankiewicz, K. (2019, Sept. 20). 'Perfectly real' deepfakes will arrive in 6 months to a year. *CNBC*. https://www.cnbc.com/2019/09/20/hao-li-perfectly-real-deepfakes-will-arrive-in-6-months-to-a-year.html

Stanton, C. (2019, Jan. 28). How should countries tackle deepfakes? *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/01/28/how-should-countries-tackle-deepfakes-pub-78221

Steele, B. J. (2008). *Ontological security in international relations*. Routledge.

Steele, B. J. (2012). *Defacing power*. University of Michigan Press.

Summerville, A. (2019, July 27). 'Deepfakes' trigger a race to fight manipulated photos and videos. https://www.wsj.com/articles/deepfakes-trigger-a-race-to-fight-manipulated-photos-and-videos-11564225200

Taylor, B. C. (2017). Imitation (In) security. *Communication Theory*, *27*(1), 48–69. https://doi.org/10.1111/comt.12104

Taylor, P. M. (2007). Munitions of the mind. *Place Branding and Public Diplomacy*, *3*(3), 196–204. https://doi.org/10.1057/palgrave.pb.6000064

von Boemcken, M. (2019). Smooth security. *Critical Studies on Security*, *7*(2), 91–106. https://doi.org/10.1080/21624887.2019.1644049

Vultee, F. (2010). Securitization. *Journalism Practice*, *4*(1), 33–47. https://doi.org/10.1080/17512780903172049

Vuori, J.A. (2017). Constructivism and securitization studies. In M.D. Cavelty & T. Balzacq (Eds.), *Routledge handbook of security studies*, (pp. 64-74). Routledge.

Waddell, K. (2019). Deepfakes for good. *Axios*. https://www.axios.com/deepfakes-for-good-4c778474-43c3-4a51-acec-4c7a796e70e7.html

Waever, O. (1995). Securitization and desecuritization. In R. D. Lipschutz (Ed.), *On security* (pp. 46–86). Columbia University Press.

Walsh, L., & Barbara, J. (2006). Speed, international security, and "new war" coverage in cyberspace. *Journal of Computer-Mediated Communication*, *12*(1), 189–208. https://doi.org/10.1111/j.1083-6101.2006.00321.x

Warner, B. (2019, July 24). Fighting deepfakes gets real. *Fortune*. https://fortune.com/2019/07/24/fighting-deepfakes-gets-real/

Woods, H. S., & Hahner, L. A. (2019). *Make America meme again*. Peter Lang.

Wright, M. (2019, Jan. 23). The age of deepfake. *The Hill*. https://thehill.com/opinion/technology/426536-the-age-of-deepfake-when-seeing-is-no-longer-necessarily-believing