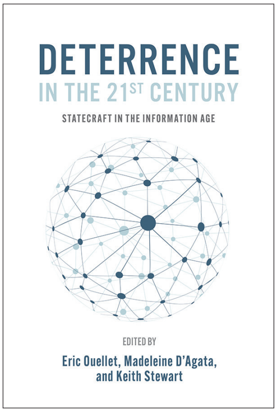
UNIVERSITY OF CALGARY
Press


DETERRENCE
IN THE 21ST CENTURY
STATECRAFT IN THE INFORMATION AGE
EDITED BY
Eric Ouellet, Madeleine D'Agata,
and Keith Stewart

DETERRENCE IN THE 21ST CENTURY: STATECRAFT IN THE INFORMATION AGE

Edited by Eric Ouellet, Madeleine D’Agata, and Keith Stewart

ISBN 978-1-77385-404-5

UNIVERSITY OF CALGARY
Press
press.ucalgary.ca

Acknowledgement: *We acknowledge the wording around open access used by Australian publisher,* **re.press**, *and thank them for giving us permission to adapt their wording to our policy* http://www.re-press.org

10

Digital Tribalism and Ontological Insecurity: Manipulating Identities in the Information Environment

Sarah Jane Meharg

In a world of growing anxiety and fear, new renderings of tribalism emerge to decrease individual anxieties related to belonging. While tribes are relational and emergent in their scope and scale, they are often cast in the same light as *engineered* populist movements that generate hatred and othering to increase fear, resentment, and contestation, in effect increasing individual anxieties and contributing to the production of anxious publics. Organic tribes, on the other hand, are a relational and network-based grouping of like-minded people seeking ontological security to assuage a growing sense of uncertainty in an ever-globalizing, placeless lived experience. "Cultural anxiety and turmoil" are a consequence of the effects of globalization—people are becoming unsettled because they feel they are losing links to their local or national communities (Lieber & Weisberg, 2002). While mainstream media and some scholarly efforts conflate populism with tribalism, this chapter examines digital tribalism as a pathway to reducing ontological insecurity in individuals by focusing on the affective dimensions of belonging and the routinization of such belonging. The chapter examines individual ontological (in) security, rather than international relations scholarship applied at the state level, as the source for the search for belonging that metes itself out in digital materiality. To deter nefarious intentions weaponized through engineered digital tribalism from destabilizing material worlds, the chapter sheds light on ontological security theory (OST) as a theoretical framework to understand the stabilizing effects produced through organic digital tribalism.

The manipulation of ideologies, the molestation of identities, and the era of digital and material *cancel culture* is a hallmark of twenty-first-century public spheres. The deleterious effects on people from the manipulation of narratives of identity and the destruction of places and histories, understood as *identicide* (Meharg, 2001, 2006, 2011) mark uncertain times for peace and stability. What are digital tribes capable of? How quickly can they mobilize against/inside of liberal democracies? How are they being manipulated? To what effect? Are all questions for twenty-first-century deterrence scholars focused on methods for deterring actions? Also, equally important, how do we balance the creation and contestation of powerful competing narratives through private, for-profit social media platforms that simultaneously seal us into our online bubbles while allowing us to see the other in new frames of reference? Understanding ways to take advantage of and manipulate people through ontological- and identity-based means in the information environment may expose how adversaries shape digital tribes to achieve political, economic, religious, and cultural agendas. This chapter examines OST and digital tribalism as a way to understand why and how liberal democracies could be manipulated by adversaries. In reflecting on uncertain identities generated by the breakdown of the liberal democratic rules-based order, there emerge a number of broad deterrence implications in the information domain—namely, information operations undermining ontological security of the people and groups that make up a nation-state. Preliminary considerations are introduced in this chapter, with a focus on the connection between sub-state ontological security, digital tribalism, and identicide.

The ubiquitous social media platforms of the 2000s have contributed to intensified focus on public engagement (Alvares & Dahlgren, 2016) while being less proficient at promoting democratic values, as shown by the results of European and American election results. The intrusion of the Internet into all facets of life has fundamentally changed the spatial aspects of the geospheres experienced by publics. "An individualization of civic cultures has emerged in tandem with the growth of mediated populism through the use of new technologies, with a tendency towards personalization in the public domain." (Alvares & Dahlgren 2016, p. 46). This includes effects on transnational and diasporic identities, as well as hyper-local and new identities. "The innovative affordances of new media technologies, such as social networking sites, podcasts, blogs, open-source software and wikis" (Husain, 2012, p. 1028), pave the path for an individualized civic environment (Gerodimos, 2012), with engagement in the public domain being "subjectively experienced as more a personal rather than a collective question" (Dahlgren, 2013, p. 52). While these engagements can be fair and democratic, emerging organically through processes of informal belonging and identity groups, they can also be hostile and aggressive weaponizations of identity, engineered by nefarious puppeteers intent on manipulating publics to advance agendas. This balance between belonging and manipulation comes to the fore through the examination of tribalism.

Tribalism

Since the 1950s, tribalism has been understood as a distinctive reproductive organizational form based on kinship structures and "social organizations defined by ascribed traditions of common descent, language, culture and ideology, and reliant on the maintenance of territories and boundaries" (St. John, 2018, p. 5). Tribalism was part of an *assemblage* of discourses and practices that contrasted traditional societies and that was synonymous with agrarian, patriarchal societies with modern nation-states. Characteristics of tribalism included Indigeneity, kinship, and bounded territory. Other elements of membership included face-to-face belonging, recognition, and mutuality/reciprocity. Groupings shared cultural symbols, signs, and practices that ranged from the vernacular to the sacred. Western writings on tribalism, and particularly its uses for rationalizing the foreign control or influence of faraway places, cannot be understood outside of constructions of race, class, and gender inherent in (neo)colonialism. Recent contributions by settler colonial writers, including Wolfe (2006) and Grosfoguel (2013), show how colonial discourses rationalized the forcible removal of Indigenous groups from their ancestral lands, thereby allowing them to claim *terra nullis* and ignore the territorial claims of Indigenous peoples (Wolfe, 2006). Colonialists not only controlled this territory with superior military technologies, they also attempted to erase Indigenous knowledge by burning texts, removing Indigenous children from their families, and establishing residential schools. Some have called this cultural genocide, and others epistemicide (Grosfoguel, 2013) and identicide (Meharg, 2001). We will return to identicide understandings later in this chapter.

Tribalism is the production of safety, security, and belonging in concurrence with the strengthening of identity and cohering of autobiographical narratives. These two activities seek to reduce and minimize anxiety, fear, and uncertainty in members of a tribe. The reduction of these emotions strengthens a sense of self, producing certainty of oneself now and in the future. Tribalism, in its digital form, is a conceptual haven creating a sense of togetherness that transcends the superfluous notion of physical connectedness. An alternate theory to explain the drive to enhance in-group identity is *uncertainty reduction* as a social category prototype to define a framework for how group members view each other and how they ought to act and interact, thereby rendering behaviours (including one's own behaviours) predictable (Grimson, 2010; Hogg, 2001). Group members also take comfort from the idea that a social identity has persistence. By contrast, threats to the group's continuity will cause members to feel uncertainty, which in turn can lead to increased conformance to group norms/prototypes, greater levels of intolerance and ethnocentrism, higher in-group solidarity and cohesion, and acts of derogation or retaliation against the out group. Threats that generate such responses include physical threats (harm to group members, group structure, vernacular places, including homes), symbolic threats (damage to values, prestige, symbols, distinctiveness, etc.), physical extinction threats (destruction of the group), and symbolic extinction threats (destruction or permanent loss of prestige, symbols, and sacred and symbolic places) (Meharg, 2001, 2011; Niedbala & Hohman, 2019; Osborne, 2001; Wohl et al., 2010).

With its accessibility, convenience, and popularity, the Internet has enabled tribalism to take on a new form and force. While in-place belonging exists strongly, a new form of belonging has emerged that is both placeless and attractive. "Digital tribalism" refers to the formation of groups in the digital realm centred around commonalities, including ethnic background, nationality, culture, hobbies, and political affiliation. The use of the word "tribe" is intentional, referring to the instinctive need for humans as social animals to recognize and bond with others that are similar; indeed, a "tribal level of organization is the most striking derived feature of human social organization," with "no close analog in other animals" (Richerson & Boyd, 2000). Characteristic of tribalism (as opposed to simple groupings) is a sense of "internal identification and loyalty," which results in a "cohesive extended familyhood" (Plater, 1990). It is the intensity of this affiliation that sometimes causes tribalism to be cast in a negative light, with connotations of exclusion, suspicion, competition, and conflict.

Organic or Engineered Tribes?

Engineered tribes weaponize their membership through securitization, organization, and financing. No longer on a level playing field, these engineered tribes invoke contestation and elimination of alternative opinions: voices viewed as counter to a weaponized agenda are targeted and removed. This elimination is a form of identicide (Meharg, 2001, 2006, 2011) as the spaces, symbols, and people are targeted and destroyed in a form of attack that has moved conflict into the digital realm. Private-sector digital technologies are a weapon system to shape structures and agents in incalculable ways, resulting in intense levels of contestation that can violently erupt back into the material world. Technologies are not tools accessible by the state, but can be conceptualized as available to the highest bidder. Weaponizing tribal identity in the digital information domain using technologies with effects-based operations has brought conflict to the Internet. Online wars are less messy, easier to manipulate, and take place in a relatively plastic environment through which to implement policies, programs, and policing. While it is relatively easy to understand the religious radicalization of people through digital means, it is now not unusual for humanitarian-minded tribes to choose sides and escalate through the early stages of hostilities against their perceived contested "other." Balance, fairness, and free speech are yesterday's ideals—the new game is information control, which leads to control of people, funding, and identities. These new threats to democracy and freedom are advanced through autocratic dictatorships functioning inside states, where they operationalize and weaponize identity narratives producing ontological insecurity at the cost of the many for the gain of a few. Information operations are rarely scrutinized and mostly go unnoticed by people, and this inspires a growing scholarly and practical interest in deterrence. Concurrently, the manipulation of publics is a growing marketing specialization, with companies like Cambridge Analytica being thrust into the limelight.

The Search for Security

People are seekers of neither *routine* nor *certainty*, but of *belonging*. Anxious publics seek belonging, choosing to find a tribe despite the knowledge that they might be manipulated by ads, videos, fake news, deepfakes, and incentives to share and retweet incendiary content. In the face of this, people still choose to belong together online. OST has strong relevance to our understanding of this desire to belong and connect together, highlighting new modalities of deterrence that may contain digital togetherness where it is, online, rather than drawing contestation and violence into the material world.

OST suggests that identities are constructed in an ongoing, continuously constituted process of identification in interlinked processes of agents' identity, narrative constructions, and their performance through practice and action. The need for coherence between identity, narrative, and routinized actions contributes to ontological security (Hom & Steele, 2020). The corollary *insecurity* emerges through incoherence and inconsistencies in state autobiographical narratives, and in the de-routinization of familiar and expected practices (Mitzen, 2006) in places or inside communities. People attempt to preserve predictability and re-establish routines that remind them of previous practices. Analysis of how tribal routines maintain pattern and variety provides insights into how synchronic routine processes are connected to diachronic routine processes (Feldman et al., 2020, p. 508). When routines are changed or broken, people go through a process of building, strengthening, and reassertion, seeking processes of stability. An examination of digital routine-breaking raises questions about *cancel culture*, digital character assassinations, digital hit squads, being jailed by Facebook, or algorithmically induced echo chambers, to name just a few examples, and the effects of contestation between groups/tribes online resulting in concerns about digital tribalism intruding upon the material world and claiming material territory. Digital and social media literature examining online groups is divided between negative discourse and positive discourse. When they are experienced as advancing democracy, globalism, pluralism, or cosmopolitanism, they are *good* and more commonly referred to as communities or social justice movements, yet conversely, when they are experienced as advancing populism, radicalism, and fundamentalism, they are *bad* and referred to as *tribal*. Tribalism is not inherently bad, but it can lead to ideological thinking and sacred values that distort cognitive processing of objective information in ways that affirm and strengthen the views of one's group. Such tribal tendencies lead to ideologically distorted information processing in any group—whether conservative or liberal, left or right (Clark & Winegard, 2020). Questions arise when observing whether organic or engineered digital tribalism is at its core contentious and nefarious or ambivalent and benign.

Individual and State Security in a Digital World

Deterrence theory has been a cornerstone of strategic thinking since the end of the Second World War, when fears of nuclear escalation led Western states to focus on methods of conflict resolution that did not involve direct military confrontation (Freedman, 2020). During the Cold War, deterrence dogma was premised on the aggression of the Soviet Union, creating the dominant paradigm of deterrence as punishment—demonstrating to an aggressor that the cost of an attack would be unbearable due to the retaliation that would follow. However, such an attitude saw the development of scholarship on deterrence theory become trapped in a rigid framework of analysis incompatible with rapidly evolving information, technology, and the benefit of hindsight (MccGwire, 1986). Only in recent decades have other aspects of deterrence been explored, including defensively minded strategies (deterrence by denial), as well as when and how deterrence can be employed (Mazarr, 2018).

The current trend has been to apply deterrence theory beyond the traditional nuclear scope, taking into account the social and technological advancements of the twenty-first century. Scholars have sought to apply varying deterrence theories to new modes of conflict, resulting in a mass of new literature in areas such as counterterrorism (Trager & Zagorcheva, 2006). Most recently, deterrence in cyberspace has captured the attention of researchers, but whether it will last long in the limelight is a matter of much debate (Schulze, 2019). While the literature has largely focused on military networks, government databases, and other state-level digital structures as the prime battlefields of cyberspace, the sub- and supra-state levels have yet to be explored in depth.

"Digital tribalism" describes the creation of socially cohesive groups in an online space. Tribes can be founded from commonalities—for example, shared cultures or hobbies—leading to a strong sense of kinship between tribe members. This can pose a security threat, as platforms for individuals to congregate with like-minded peers may create an environment encouraging radicalization. Tribes can create connections within and/or across borders, and within their closed communities disseminate extremist views; for example, many Islamist and far-right groups who feel that they have lost their identities through globalization resort to using digital tribes to spread their ideologies (Abbas, 2017). Misinformation in such closed communities spreads in a virus-like fashion, misleading members and inciting them to potentially violent action (Cronkhite et al., 2020; Lewandowsky & Smillie, 2020). Thus it is important to understand how to identify the role digital tribes play in cyberspace, when they become dangerous, and how to prevent them from becoming a threat to national security.

Interactions between users on social media mirror those in real life, leading to the formation of communities composed of distinct groups, intermediaries, and follower networks (Przemyslaw et al., 2012). The need for communication and connection through digital means is a growing global trend. In the United States, approximately 75 per cent of households have Internet access, with seven in ten Americans using social media (Pew Research Center, 2021a, 2021b). Studies of African countries, where the number of households with Internet access is below 20 per cent, cite social media as a primary motivator for increasing Internet adoption (Stork et al., 2013). One would assume that with lower Internet access and social media participation compared to other countries, digital tribes would have less influence in such areas. This is not the case: tribes have caused just as much national upheaval in Africa through online congregation and the spreading of misinformation as their counterparts in the United States. For example, fake news sites and troll armies of Twitter users, coordinated by public relations firms, were used to spread narratives about the South African president, with such tweets receiving thousands of interactions through circulation within the troll army. These high engagement numbers imply to outsiders the legitimacy of the information being spread (Wassermann, 2020).

I wish to amplify the apparent asymmetry of tribalism's two spatial imaginaries, the material and imagined processes and outcomes of belonging-seeking, in order to suggest that, in their unlikely compatibility and alignment, something critical about how deterrence operates above and beneath the state is to be gleaned. To comprehend digital tribalism's belonging-making potential and limitations for producing ontological security, we require deeper understandings of how they become meaningful, how they are felt/sensed, and how they are (re)produced in, and as part of, everyday identity narratives of political, economic, and cultural belonging. As we progress through the twenty-first century, how will tribalism continue to evolve and/or be deterred?

Tribalism in the Twenty-First Century

In recent years, the subject of tribalism has had a renaissance of sorts, increasing its cross-disciplinary appeal. Contestation of the other can lead to increased anxiety culminating in degrees of cultural intolerance, and exposure to other groups, world views, cultural objects, routines, and more can be accelerated and appreciated in the intensively interconnected world of the twenty-first century (Karim, 2020). The contemporary variant is neither related to collectivities based on kinship structures nor anchored to a territorially bounded space. Current iterations use tribalism to understand such phenomena as political polarization (Chua, 2018; Hobfoll, 2018; James, 2006; Mason, 2018), nativism, white nationalism, extreme xenophobic intolerance to difference and populism. Chua (2018), for example, contends that American political tribalism as manifest in partisan polarization and political dysfunction in Washington threatens to fragment and weaken the social cohesion of the state—once comprised of a *super group*, one whose narrative, while critical to the coherent autobiographical narrative of the people making up the nation-state, is often ignored, contested, or outright unknown by foreign interveners or the institutions making up the liberal democratic rules-based world order. Chua draws parallels with the Robbers Cave experiment by Harvard social psychologist Muzafer Sherif in 1953, when researchers divided boy campers into two groups and orchestrated situations designed to provoke mutual distrust and animus.

However, the Robbers Cave experiment was preceded by an experiment at Middle Grove, which Sherif chose not to publish because the findings undermined his preferred narrative (Perry, 2018). In this earlier experiment, two groups of boy campers chose to co-operate rather than turn on one another, despite deliberate efforts on the part of Sherif's team to prompt competitive and vengeful inter-group behaviours. Partly because they had come to know and befriend one another prior to the experiment, the boys co-operated to uncover the source of a series of hapless incidents (Perry, 2018). Adding to these dynamics are shared loyalties to persons, whether political or popular chieftains, and concepts evoked and maintained through affects and emotions. Members of digital tribes, unlike the Middle Grove and Robbers Cave subjects, do not typically know each other in person, but shared affects create a strong sense of belonging between and among members, compelling them in contexts of nationalism to bridge the divide between the material and digital worlds to lay claims in both (Duile, 2017, p. 252; Janowitz, 2009). Similarly, those in contexts of leisurely pursuits (sports, for example) have created a safe *belonging* space for participants to escape from society and produce a territory to defend (Baumann, 1996; Delanty, 2011; Hayday et al., 2021; Kauss & Griffiths, 2012). These social, psychological, and political research experiments suggest that organic tribalism itself is neither inherently competitive nor violent; rather, the contextual conditions create a permissive environment for these behaviours and the potential weaponization of people to achieve political, economic, and/or cultural agendas.

An Appeal to Emotion

A tribe's interpellation of political discourse to their publics must resonate within tribe members' affective dimensions of their personal life-world and enhance their autobiographical narratives or suffer rejection. Note that discourses are usually built on simplifications and strong emotional appeals (Alvares & Dahlgren, 2016). All information is potentially politicized and rendered vulnerable to malign intent (Waisbord, 2018). Political discourse embodies rhetorical dimensions that speak to citizens' emotional sides, and populist agendas in Europe are no different; political engagement per se would not take place were it not in part driven by affective dimensions (Alvares & Dahlgren, 2016; Dahlgren, 2006; Papacharissi, 2015), and instant communication between members of digital tribes, facilitated by social media, to incite escalation into real-world mass mobilizations. Emotionally driven narratives describing a trigger event can provoke action in material worlds. Following the death of George Floyd, for example, trending hashtags on Twitter and memorial posts on Instagram were used to quickly coordinate mass protests. Social media allowed users to communicate quickly with each other while also evading detection, as calls to stage protests would be posted and removed in the course of a single day to make developments difficult for authorities to track (Heaney, 2020). Thus it becomes easy for the puppeteers of contrived belonging and engineered tribalism to use social media to turn the Internet into a massive, anonymous, and instant protest organizational body, which is almost impossible to track or prevent by local authorities. Ergo, thousands of online users can band together over an emotionally charged topic and attempt to exact justice in the material world. This is worsened when influential users weigh in on issues, broadcasting calls to action to their large follower bases and increasing the likelihood of action. While this sometimes has positive consequences, such as the firing of an employee for a racist tirade in public, it can escalate into violent attacks and material damage of other identity groups, as with the razing of over two dozen churches in Canada following the discovery of mass graves outside residential schools. Additionally, the 2021 Capitol riot in the United States was orchestrated by groups on Twitter, Facebook, and Parler over the course of months. Prior to the riot, subgroups had already formed to coordinate rallies, plan travel routes, collect funds, and identify targets (Atlantic Council Digital Forensic Research Lab, 2021). Psychological factors influenced the groups' ability to collaborate and carry out an armed attack: followers of political leaders with authoritarian personalities tend to have a preference for aggression, and are more willing to legitimize actions going beyond normative expectations (Petersen, 2020). Later studies showed that there was an enhanced correlation between the participants in the riot and members of Trump-supporting communities that perceived themselves to be socially isolated (Van Dijcke & Wright, 2021). In essence, members of digital tribes that feel threatened may be more motivated to resort to acts of violence as a twisted means of self-defence, especially when the tribe is formed around an extreme political cause. Orchestrators lurking behind engineered tribes can operationalize and harness trigger events for ideological gains.

Ontological (In)Security

Ontological security scholars have been influenced by Gidden's structuration theory (1984, 1991), which draws on the work of R. D. Laing's understanding of security of the self as that which denotes a state of confident autonomy (2010). From this understanding, Giddens defines ontological security as "confidence or trust that the natural and social worlds are as they appear to be, including the basic existential parameters of self and social identity" (Giddens, 1984, p. 375). Giddens contends that, through social interaction, individuals learn the rules and codes of conduct, which guide predictable and routinized behaviours, and render fear and anxiety manageable and constitute self-identity. Routinized practices make life knowable. However, when conditions change to the extent that the future is no longer knowable and predictable, whether due to forces beyond an individual's control, or the result of decisions and actions by an individual, a person experiences ontological insecurity. Since persons exercise agency, they are not totally under the whim of forces outside their control or of their own making. They may act in ways that attempt to restore the status quo, or to create routinized behaviour and practices. Both courses of action are designed to restore a knowable, predictable future in which reassurance emerges, and anxiety is mitigated.

In their study on ontological insecurities and the politics of populism, Steele and Homolar (2019) expand on Giddens's ideas by describing the psychological need for continuity as the gateway for populist politics that leverages promises to regenerate and reinforce past notions of spatialized belonging and inclusion, in particular when agents experience trauma and anxiety. Self-identity consists of the development of a consistent feeling of *who one is* in relation to others, offering biographical continuity in which an individual is able to sustain a narrative about oneself and answer questions about doing, acting, and being, informed from a bifurcated reality of *us* and *others*.

International relations (IR) scholars have drawn on this concept of ontological security from the fields of psychology and sociology to understand state and interstate relations and to scale up the analytical level from the individual to the state and interstate relations. While traditional realist approaches focus on the politics of fear under conditions of anarchy, ontological security scholars are careful to differentiate fear from anxiety. They define fear as an emotion that is directed at a specific object, such as the death of one's child, or business closures enforced through COVID-19 pandemic politics or the threat of violence from a transnational terrorist group such as al Qaeda or ISIS, which elicits a fight, freeze, or flight response. In contrast, anxiety is a psychic condition or mood associated with uncertainty that can trigger a range of emotions and responses not limited to fight/freeze/flight. Attention to anxiety derives from the view that anxiety is increasing in the context of human displacement and migration, employment precariousness, and global inequality linked with globalization, climate change, pandemics, and digital technologies (Kinnvall, 2004; Kinnvall & Mitzen, 2018).

States defend against ontological insecurity with a range of behaviours. These include a turn toward authoritarianism and populism, as evidenced by the electoral victory of the Law and Justice Party in Poland and slogans like "Take Britain back again" and "Make America great again" by Brexiteers and Trump supporters, respectively (Browning, 2019; Kinnvall, 2018). Anxiety is also linked with othering and scapegoating, in which groups are named as a threat to the nation's imagined identity, prompting hard-line foreign affairs and security policies with regard to immigration and border control. Examples of extreme security policies include the so-called Muslim travel ban in the United States, the construction of border walls and fences in Israel-Palestine, the US-Mexico border, and Hungary's fence in the context of the migration to Europe. Scapegoating is not limited to groups like migrants and refugees but extends to philanthropists like George Soros and Bill Gates through anti-Semitic or conspiratorial campaigns. Anxiety is also linked with the concept of a *risk society* (Beck et al., 1992) and efforts to identify and manage national and transnational risks.

The second-generation scholarship attempts to overcome the reliance on Giddens's ideas about ontological security, particularly his emphasis on the need to maintain psychological well-being and avoid existential anxieties, which centre on stasis and cannot fully account for change. Kinnvall (2018) moves away from Giddens's approach of ontological security as a security of being in favour of a focus on ontological security as a process of becoming (2018). Connecting to process relational philosophy, we can understand tribes, their members, and the geoscape in which tribes are (re)produced and maintained as being in various states of subjectivity and digital materiality.

Current examinations of ontological security through an IR lens are pushing the boundaries in a number of directions relevant to this chapter. Looking at the first boundary—the under-specification of unconscious processes—Cash (2020) employs a psychoanalytic approach to explore unconscious defences against anxiety. Cash makes reference to Isabel Menzies Lyth's 1960 case study of the norms and rules of behaviour governing nurse conduct in a UK hospital to defend against the anxieties evoked in the process of executing their care duties to ill and terminal patients. Menzies Lyth argued that nurse trainees adopted routines and practices to socialize themselves to manage such anxieties. These included minimizing patient contact, maintaining strict hierarchies and deference to superiors, restricting independent judgment and discretion, and limiting any sharing of feelings about their work with experienced staff. Cash sees this as "a cultural repertoire, predominantly encoded with psychic mechanisms of splitting and projection, organized role-identities, practices, emotions, and social relations in order to support the ontological security of nurses who regularly have to deal with anxiety-provoking situations" (2020, p. 315).

Another boundary is the tendency of proponents like Mitzen (2006) and Steele (2008) to focus on the actions of actors to preserve their self-identity and restore or protect ontological security. Browning and Joenniemi (2017) argue ontological security scholarship is prone to collapsing notions of self, identity, and ontological security. By focusing on how perceived threats to an actor's established identity undermine their ontological security and rationalize security moves to defend and reinforce self-identity, securitization is equated with moves to enhance stability, and de-securitization is linked with instability. But since identities are always in flux and "never fully stable, settled and complete, the promise of stability in securitization practices is illusory" (Browning & Joenniemi, 2016, p. 34). Browning and Joenniemi argue that it may be more productive to understand how actors come to self-identify and articulate identity claims instead of emphasizing identity stability. Instead, they argue that "more focus is needed on how reflexivity towards identity is also central to ontological security . . . [and that] desecuritization—and not just securitization—may be central to re-stabilization processes" (Browning & Joenniemi, 2016, p. 34).

An overview of related arguments (Kinnvall & Mitzen, 2020, pp. 251–2) suggests that when ontological insecurity is experienced, there are options for the anxious and fearful, producing a reflexive opportunity to engage uncertainty and dwell in ambivalence (Cash, 2016; Kinnvall, 2018; Solomon, 2015). "The amorphous, ambivalent character of politics, while often frustrating for analysts, is also a long-term strength for democracy, allowing citizens to engage, participate and ally themselves in ever-new constellations" (Alvares & Dahlgren, 2016, p. 51).

Lastly, ontological security studies in IR have scaled up the work to the state level but have not adequately addressed the international level (Rumelili, 2020). For this chapter in particular, understanding the production of anxiety and belonging-seeking at the supra-state level will be an area of further research relevant to engineered digital tribalism and the deterrence of negative effects of such belonging.

The need for ontological security, a sense of continuity and order, is deep, and attachment to routines is profound and universal. Change to an individual's established routines can be disruptive, ranging from something as simple as a highway detour to something more complex like the arrival of a new baby, loss of employment, or homeschooling during the COVID-19 pandemic. Empirical research in various areas of social psychology confirms that uncertainty generates identity insecurity, which is resolved through routines. The basic insight of anxiety/uncertainty management (AUM) theory, for example, supported by experimental work, is that uncertainty is both a cognitive and affective problem (Grinson, 2010; Hogg, 2001). Humans need to *make sense* *of their world*, and when there is insufficient information or meanings are unsettled, individuals suffer anxiety. "When 'normal' expectations are not met . . . reactions are anomic and demonstrate confusion. Ontological security is the mechanism individuals employ to get on with their daily lives" (Steele & Homolar, 2019, p. 215). Ontological insecurity produces existential anxiety.

Identicide

When identities and autobiographical narratives are disrupted, various forms of insecurity emerge. This can be intentionally induced through identicide: the deliberate, systematic, and targeted destruction of one's established places, symbols, objects, and routines, including ideas, values, and aesthetica, and other cultural property that represent the identity of a people, with the intent to erase the cultural narrative and memory of that people, demoralize a population, absorb it into another cultural/political verity, or to rid an area of that people altogether (Meharg, 2001, 2006, 2011).

Identicide can include the calculated targeting of the places and objects that hold identity for a contested group, but also the intentional targeting of places and objects in cyberspace—namely, elements of digital materiality that generate meaning for people online. Identicide is more easily observed in the destruction of physical buildings and symbolic objects, limiting the ability of an identity group to carry out well-established and important rites and practices, and arresting and harming individuals who are responsible for maintaining and passing down crucial societal information, oral histories, and customs. It is less easily detected, while no less harmful to people, in the destruction of intangible digital-material aspects of modern life that generate life-worlds and contribute to ontological security. The destruction, suspension, and manipulation of online content, digital assassinations, bullying and vilification of ideological views and sacred values, disappearance of truth and the generation of deepfakes produces levels of anxiety in people, and the results of such destruction can trigger ontological insecurity in individuals, groups, and entire nations and states. Identicide is a precursor stage of genocide but does not necessarily result in genocide. As a conflict strategy it deliberately targets and destroys the cultural elements of a people through a variety of means in order to contribute to the eventual acculturation, removal, and/or total destruction of a particular identity group, including its contested signs, symbols, behaviours, values, heritages, places, and performances. Identicide is the intentional killing of the relatedness between people and place that eliminates the bond underpinning individuals, communities, and national identities. Identicide takes many forms but serves a single function: to negatively affect the relationships between people and their places (Meharg, 2011), whether these places exist in the physical world, the imagined world, or the digital world. The resulting condition of anomie destabilizes one's sense of the future, and this leads to inconsistencies in actions, attitudes, and social behaviours. When important places and symbols, as well as their digital-material counterparts online, have deep cultural meaning and are intentionally targeted and destroyed during periods of contestation as a strategy to rid an area of a marginalized people and to reduce their cohesion, ontological security becomes a useful framework for understanding strategies that secure identity and offer a certain future for affected peoples and their tribes.

Yet the implications of human behaviour and identity on stability and the wider security dimension have frequently been disregarded by those seeking to assess a situation and to potentially intervene. By making alternative perspectives, identities, histories, and narratives invisible, identicide effectively negates the presence and value of others, and allows for their reconstruction in a manner that is untethered from existing structural and socio-cultural realities. Negation is a necessary precondition for reconstructing identities in specific ways. It is through routines and relationships and narratives that identities are constructed (Mitzen, 2006; Subotić, 2016). Identity has two instrumental aspects—in other words, it has a form expressing agency. This agency can then turn into action when there is a threat or a perceived notion of a threat. Therefore, it is critical that the discussion-to-action transition is deterred.

Deterrence and Digital Tribes

Attempting to provide oven-ready policy prescriptions that represent effective deterrence in the context of all "digital tribes" is far from a fruitful approach. The complexity of these tribes and the threats that they may pose is such that one cannot hope to cover the necessary degree of tailoring strategies in a single chapter. Nevertheless, this section will use some of the core principles of deterrence theory to explore the broad contours of key considerations in shaping a deterrence posture in direct reference to digital tribes.

The definition of deterrence has been given in too much detail elsewhere to reiterate here, but it is worth noting that the "fourth wave" of deterrence research has led to "new constructivist and interpretive scholarship that explores the practices of deterrence" and that acknowledges the social construction of deterrent strategies (Lupovici, 2010). This acknowledgement of identity and ideology as a point of serious consideration in relation to deterrence is of particular importance in this case. It is also crucial to note that deterrence is inherently relational. That is, deterrence posture is connected to place, actors, and action. What deters in one relationship between adversaries cannot be assumed to deter in another, and an action that one actor perceives to be necessary to deter may not be mirrored by another actor. It is also unavoidably connected to the concept of costs and cost imposition. Even if a necessarily broad understanding of "costs" is used, deterrence is predicated on one actor deciding that the costs associated with accomplishing a certain action are either greater than the anticipated benefit, or that the response to that action, even if the action were to be accomplished, would impose such costs as to render the initial action unwise (Gray, 2000). The nature of these costs may be diverse, and what is considered "costly" can differ spectacularly, but it is here that the confluence of perceptions of belonging, digital tribalism, and the mitigation of threat occurs.

It is evident that digital tribalism and its psychological effects on identity building can be highly influential in pre-emptively dissuading an aggressor from taking action. Interference with a group's sense of self can pacify aggression, interrupt communication, or (de)construct identities. Such consequences reflect deterrence attributes such as fear (fear that digital tribes will be disrupted and coordination made impossible), denial measures (creating a stronger digital tribe that is a repository of information and seems futile to attack), and cost-benefit analysis (having a digital tribe disrupted in retaliation for an attack) (McKenzie, 2017).

There are, therefore, three key questions associated with deterrence and digital tribalism. While they may seem straightforward, their articulation is central to understanding an appropriate deterrent posture: (1) Who is to be deterred? (2) What actions are we intending to deter? And (3) what costs can be leveraged on a digital tribe?

The action to be deterred is not simply stand-alone behaviour, but part of a continuum (Mazarr et al., 2018). The behaviours leading to this point may not be desirable or considered reasonable, but they are nevertheless (at worst) tolerated, and it is a particular action that is the focus of deterrence. This provides an opportunity to make a warning signal to turn a digital tribe from continuing their route toward physical violence prior to the threats central to the deterrence posture being carried out, but also necessitates a conversation about the extent of action or conversation that is allowed to occur. Thus, one could posit a posture that attempts to deter the formation of any or all digital tribes. This would be challenging, but in theory it is an arguably robust approach to preventing existing social orders from being broken down. Perhaps more reasonably, one could seek to deter digital tribes from considering or discussing the use of violence in the physical realm. While it would undoubtedly be to the benefit if no one within a digital tribe realistically conceived to use violence to advance their aims, in practical (and clichéd) terms, talk is cheap. The real harm of the discussion of violence in itself is, in short, limited. Setting aside the potential requirement that violent action requires discussion prior to its use, where the discussion of violence becomes actually problematic for digital tribes, and therefore the key focus of deterrence, is the potential crossover from the discussion of violence to its manifestation in a material environment. As such, we must conceive of the costs that a digital tribe can impose as an amalgam of drawing individuals into the tribe to the extent that they consider themselves in opposition to the identity narrative of the state, and radicalizing such individuals to the extent that they take physical and violent action against the state. The recruitment and development of the digital tribe may be problematic in eroding what unity exists within a state, but it is the violent action that is the absolute focus of the deterrence.

Similarly, we must think of the threatened imposition of costs that comprise deterrence as actions that would disrupt a member of the digital tribe, or the tribe as a whole. The costs to be imposed on a digital tribe can therefore fall into three categories: (1) those that affect an individual member; (2) those that affect intra-tribe bonds; and (3) those that affect the material ability of the tribe to effect its desired goals. The influence of all three of these in certain scenarios is discussed in more detail below.

Deterrence and deterrence theory encompasses a multitude of facets and approaches, but it is two core (and interlinked) pairs of precepts that must remain the focus of consideration here. The first pair relates to the form of deterrence that is to be leveraged—deterrence by punishment, or deterrence by denial (Mazarr, 2018). In practice, of course, it is rare for one to occur without the other, but in dictating a deterrent posture one may lean more heavily on the communication of an ability to defend oneself, or the ability to counter-attack. Parsing these two approaches in isolation is helpful in illuminating the nature of the threat posed by digital tribes and the most efficient deterrent posture in this context. The second pair underpins the way in which deterrence is successful. Returning to the decisional basis of the theory, the deterree (in this case, the digital tribe) must decide that their adversary has the capability and resolve to carry through the threats signalled by their deterrent posture (Jarvis, 1976). Obviously, if these threats are actually carried out, then deterrence has failed, but successful deterrence requires a belief that the deterred action would be carried out, and impose significant costs if done so. Thus, whatever strategy or posture is adopted to deter digital tribes, it must be feasible and realistic.

Deterring Digital Tribes by Denial

Deterring by denial, that is, demonstrating that the costs incurred in conducting a particular action would outweigh the benefit (either because the target is resilient and the action would not produce the intended psychological or strategic outcome, or because the targeted actor would not allow the action to occur at all), inherently provides the more normatively acceptable policy approach—since, in principle, wielding a shield against which an adversary's attacks will founder has fewer negative connotations than the use of the sword to impose direct costs on an adversary, even if this is in response to their attack (Snyder, 1960; Wilner & Wagner, 2021). Similarly, it is preferable to deter through the ability to prevent an attack, rather than rely on the retaliatory imposition of costs—in the case of deterrence failure (that is, the adversary takes the action that one has attempted to deter), denying the adversary the ability to accomplish their goals would, in all likelihood, mean that one has not had to weather significant costs.

However, deterrence by denial brings with it some particular challenges. First, there is a universal inability to accurately ascertain whether the defences that one has in place are, in fact, sufficient to deter, let alone defeat, an adversary's attack. Second, violence does not generally occur with absolute suddenness, but is a product of a longer arc of behaviour that culminates in such action. This raises questions about identifying the moment at which deterrence has failed and pre-emptive action is required. In this case, the challenge is about knowing when violent online discourse will be turned into violent action, or how long the deterrent posture will hold such action at bay.

That said, deterrence by denial in the context of digital tribalism may be worthwhile. The resiliency approach may not, however, be efficacious. The act of physical violence in itself can have a meaning beyond the damage that it causes, delineating even more clearly the "other." Thus, even if a digital tribe conducted an action that caused significant destruction, merely demonstrating that the destruction made no meaningful difference to the routines of the attacked party may not deter similar future actions, regardless of the response.

In deterring by denial, we must therefore look to the threat of pre-emptive action. In this case, such a posture relies on the ability to monitor the communications of digital tribes and successfully identify the key moment at which the threat is bound to become realized. As noted, this is a difficult task. Nevertheless, by threatening the disruption of groups through the removal of key individuals (permanently or temporarily) from engagement with others within the tribe, or removing equipment if there is an expectation of imminent violence, it is possible to ensure that potentially dangerous digital tribes steer clear of violent action in the material world. The individualized effects of violence in the digital world is thus far not fully understood by sociologists, cultural geographers, and ethnographers, to name but a few, and therefore will have to await future diagnosis with regard to deterrence. For now, we can rely on understandings of violent action in the material world. In an example, the challenge of disrupting groups in the United States through the removal of guns is, of course, rendered more difficult due to Second Amendment rights, but the belief of the deterree that the deterrer has an ability to impose costs through actively pre-empting an attack can be a powerful disincentive to commence preparation.

Considering the possible success of such actions requires turning to the potential ability to signal capability and resolve to effectively pre-empt the transition to physical violence. Such capability must be demonstrated across three levels. The first is in the ability to monitor the communications of the digital tribe in order to ascertain the shift in likelihood of physical violence. The second is the ability to take action against individuals within the tribe. The third, more broadly, is the ability to effectively coordinate knowledge and action across what have traditionally been understood to be intelligence boundaries. Part of the distinction of digital tribes is their potentially cross-national structure. This is not totally unique—the emergence of terrorist groups and other non-state military actors has followed a similar trajectory in recent years—but digital tribes represent a slightly new challenge. While, at least in the West, terrorist organizations have been universally condemned, or at minimum understood to be dangerous actors, understandings of the actual goals of, and threats posed by, a digital tribe may differ between the various state actors that play a role in deterring their transition to violence. As such, coordination is likely to be not only a matter of security and logistics, but also of delicate negotiation that must take into account distinctions in political, economic, religious, and social cultures.

It is also worth considering the normative and practical challenge of monitoring the communications of a digital tribe. The well-acknowledged labyrinth of secure digital communications and complexity of symbolism can make the identification of centres and trajectory of discourse difficult (Parker et al., 2019), exacerbated by the disruption of platforms that forces groups into different online locations.

Capability is demonstrated by indicating an ability to intercept communications before they reach a critical or dangerous stage. This raises a further challenge in "tipping one's hand" to potentially dangerous actors. By indicating that a particular channel of communication is monitored, rather than convincing them of the futility of planning an attack, it may simply cause a shift to another, unknown, channel of communication. Similarly, overt monitoring of communications could further strengthen the bonds between digital tribe members, even if no further action is taken, creating a more dominant framing of the tribe as outsiders who are viewed with suspicion, if not hostility.

Signalling the capability to take action against individuals within the digital tribe and/or digital objects owned by the tribe can only occur through demonstrated action. This is a challenge for deterrence, which is fundamentally about not performing the threatened action. Nevertheless, if the potentially dangerous digital tribes are viewed as discrete units, then the successful interdiction of one tribe (and thus the failure of deterrence in that case) could potentially deter others from taking similar steps. Such action would also be a key demonstration of resolve, signalling that a state is willing to take preemptive action despite the legal and normative justifications that such action would require in the post-event environment.

Deterring Digital Tribes by Punishment

Perhaps the more traditional understanding of deterrence, particularly with regard to strategic nuclear weapons, rests on the concept of punishing an actor for taking the action that was the focus of deterrence, such that the costs imposed vastly outweigh the benefits of the action. Punishment in the context of digital tribes could focus on individuals, but unlike the "denial" approach, it may also target the digital tribe more broadly. That is, the punishment for translating violent discourse into violent action would be the obliteration of that tribe or the erosion of its identity such that it no longer exists as a meaningful actor.

This is, however, a simplistic response, paralleling the attempted deterrence of terrorist groups (or other non-state violent actors) whose existence has been characterized by physical violence through selectively punishment of particular individuals and/or the group as a whole. The literature on leadership decapitation indicates that this is not universally helpful (Jordan, 2009). Although the threatened punishment of leaders for violent actions should not be discounted as a potential deterrent, this does not appear to be a particularly straightforward or effective mode of punishment. Particularly on the understanding that a digital tribe has developed organically, punishing leadership is rendered more challenging by a potential lack of an identifiable hierarchy or leadership. While ideas and symbols may be communicated, this does not necessarily occur within the forms of structures that have emerged in governments or among non-state actors. One current example of this is the incel movement, a roughly aligned digital tribe whose members have conducted a number of violent actions, but for whom there does appear to be a central hub of coordination (Brzuszkiewicz, 2020). Punishment is therefore meted out only to those who conduct violent actions. However, in the context of digital tribes who share a common understanding that their cause transcends individuals, or in the context of a digital tribe who believes that the costs they impose on another group, regardless of a member's own destruction, may create a martyr, rather than a deterrent.

As such, the solution would appear to be the punishment of the digital tribe as a whole, the forcible dissolution of bonds that link members of the tribe, thereby preventing their reconnection so as to undermine the reinforcement of beliefs. Such an act would be, to all intents and purposes, a form of identicide. In some cases, such action may not appear to represent a particular problem, but these seemingly clear cases veil the true normative challenge: At what point does the violent actions of one individual within a digital tribe necessitate the entire tribe's complete destruction? The forcible removal or alteration of identity is an action that should not be entered into lightly. The destruction of a digital tribe is also given a further level of complexity due to the speed with which everyday or common symbols can be co-opted and internalized as part of a particular identity, without necessarily requiring conversion into physical objects. Preventing connection between members is therefore a significant challenge, and when achieved, may induce higher levels of anxiety in members, contributing to insecurity writ large.

In addition, once again the threat of punishment, if not communicated effectively, may be counterproductive. The uniqueness of the digital tribes in relation to the way in which they create or develop a sense of belonging that transcends physical space allows for the carving out of a distinct sphere of influence and tight bonds of belonging between members. Once created, this bond's potential destruction is an act of considerable violence, and may further inculcate a perception of shared otherness. In combination with the perception that the tribe to which they belong holds a unique position of normative or social rightness, its threatened destruction can provide further confirmation of members' position within existing social frameworks, and the threat may further strengthen bonds or result in pre-emptive attack.

Consequently, demonstrating capability and resolve to destroy such tribes is a considerable challenge. Again, it may be helpful to view digital tribes in distinct silos, and to understand that the destruction of one may deter others, but measuring the likely effectiveness of this is extremely difficult. Despite these challenges, deterrence is critical, particularly given the disconnect between certain digital tribes and Western society, and the possibility of the spillover into physical violence in the material world.

However, the nature of tribalism and the acceptance in the West of the value of, and right to, alternative viewpoints also necessitates the consideration of parallel approaches. Deterrence must always be seen on the spectrum of (inter)action that spans persuasion and compellence. If we can accept an understanding of the basis of these tribes that stems from a perception of a lack of belonging, it is also possible to conceive of an approach that involves persuasion whereby the group is not perceived to be an *other* and an understanding their networks of belonging are at least tangentially connected to those of the state.

Of course, we cannot condone the existence of groups that advocate violence against us, nor should this involve even a tacit acceptance of the values of a digital tribe deemed fundamentally at odds with our own. Nevertheless, without going so far as to promote a fully global community (which indeed is a cause of some concern to certain digital tribes) it is only through creating a sense of unity in diversity that the possibility of violence can be reduced. The threatened imposition of costs alone can provide only limited comfort that the transition from violent discourse to violent action will not occur.

Conclusion

People experiencing globalization (especially in the West) as a negative experience are seeking connection and belonging because of unconscious anxieties caused by ontological insecurity. This is more than the ubiquitous call to “find your tribe!” Rather, it exists as the existential experience of belonging to a group that reinforces autobiographical narratives of identity. Evidence of this activity is seen with the rise of powerful leftist and rightist digital tribes like QAnon, European and American populist political groups, and COVID-19 pro-vaccination warriors, as well as social justice groups like Black Lives Matter, Stop AAPI Hate, and benign groups with hugely supportive fan bases such as YNABers (You Need a Budget, ynab.com). This type of belonging-seeking with groups of like-minded people ensures the reduction—even the elimination—of specific threats of globalism—namely, threats against the hierarchy of needs expressed by Maslow, most particularly individualized security, esteem, and belonging. A never *truly belonging* state of mind can become chronic. Belonging-seeking is a pathway to reinforcing a coherent sense of one’s autonomy and ontological security. Uncertainty of one’s future leads one to cling to the familiar and continue to recreate the familiar through material acts aimed at the *routinization of belonging*. In this time of social networking, popular social media sites are the place to find one’s tribe and to satisfy the need to belong.

These connections are forged through social media networks in ways that mirror the forging of connections in places, and they contribute profoundly salient elements to one’s identity narratives. Routinization of belonging to a digital tribe takes place online through specific, culturally contextualized action(s). This produces the effect of belonging. While contrived and weaponized digital tribalism can advance counter-democratic processes, organic digital tribalism is an activity enjoyed by people who are mostly doing nothing more than assuaging their deep psychological-biological need to belong.

The connection between OST and deterrence is belonging. To reduce existential anxieties in fringe or marginalized groups, we must focus on reducing anxieties (encouraging belonging) rather than building on fear (removal of Facebook pages, cancel culture, pulling down web content). These are essentially undemocratic activities that lean toward identicide, and as such democratic stakeholders should abstain from these actions if their purpose is the deterrence of non-aligned ideologues. If marginalized, or even nefarious, engineered digital tribes are targeted and contested, their organizers may reorganize, disappear, appear. This itself is a cause of uncertainty in tribe members and can be at the root of belonging-seeking, and such uncertainty can artificially suspend—perhaps indefinitely—the satisfaction of the most basic of human needs. Online tribalism reduces the traditional conflict/war effects within the geoscape, therefore, with regard to deterrence, encouraging digital *tribing* may reduce the movement between digital and material worlds. While our security apparatuses are set up for conflicts in the physical world, much work must still be done to recalibrate these apparatuses to confront conflicts in the digital world, and to contain them where they derive from.

There is no singular narrative or super group, as Chua (2018) claims, but rather multiple complementary, conflicting struggles over identity coexisting in the media terrain of the geoscape. Reducing existential anxiety through belonging—particularly in the form of routines—is a pathway to deterring behaviours that, if actioned, could confine violence to discourse rather than action inside democratic states. Coupling material and digital environments creates a more permanent certainty for people. Kinnvall and Mitzen (2018) offer a prescription for such anxiety: "To hold existential anxiety at bay, focus on practices of the 'everyday,' such as routines and maintaining a coherent autobiographical narrative" (p. 245). Minimizing belonging to engineered tribes by exposing the nefarious intentions of orchestrators may reduce anxieties related to political, economic, and cultural identity in participating publics, who in a manipulation process of information operations advance anti-democratic and anti-humanitarian agendas.

Therefore, deterrence strategists do not need to allocate resources and assets to understand broadly defined identities and autobiographical narratives of a state, an adversary, or a digital tribe to gain an advantage. Rather, strategists could allocate resources to analyze the routines of tribes representing identities. In situations in which identity routines have been disrupted, OST offers a lens through which to understand modalities of identity, narratives, and digital materiality. New renderings of tribalism as anxiety-reducing mechanisms produce a psychological sense of certainty in an otherwise uncertain state of anxiety.

Acknowledgements

This chapter benefited, directly and indirectly, from the many enlightening conversations and collaborations that I have had over the years with my esteemed colleague Brian Osborne, who knows a lot more than I do about people, identity, and belonging. I would also like to thank the editors for their helpful and insightful comments. Any mistakes and omissions are entirely my own. For research guidance on deterrence, many thanks to A. Thomas Hughes. For research assistance on this chapter, thank you to Mona Ghali, Hailey Ng, and Nick Ramsay.

REFERENCES

Abbas, T. (2017). Understanding the nature of online extremist narratives. In *The Challenge of Jihadist Radicalisation in Europe and Beyond* (pp. 90–9). European Policy Centre. https://www.epc.eu/content/PDF/2017/The_Challenge_of_Jihadist_Radicalisation.pdf

Alvares, C., & Dahlgren, P. (2016). Populism, extremism, and media: Mapping an uncertain terrain. *European Journal of Communication, 31*(1), 46–57. https://doi.org/10.1177%2F0267323115614485

Atlantic Council Digital Forensic Research Lab. (2021, 10 February). "#Stopthesteal: Timeline of social media and extremist activities leading to 1/6 insurrection. *Jest Security*. https://www.justsecurity.org/74622/stopthesteal-timeline-of-social-media-and-extremist-activities-leading-to-1-6-insurrection/

Baumann, G. (1996). *Contesting culture: Discourses of identity in multi-ethnic London*. Cambridge University Press.

Beck, U. (1992). *Risk society: Towards a new modernity*. University of Munich Press.

Browning, C. S. (2019). Brexit populism and fantasies of fulfilment. *Cambridge Review of International Affairs, 32*(3), 222–44. https://doi.org/10.1080/09557571.2019.1567461

Browning, C. S., & Joenniemi, P. (2016). Ontological security, self-articulation and the securitization of identity. *Cooperation and Conflict, 52*(1), 31–47. https://doi.org/10.1177%2F0010836716653161

Brzuszkiewicz, S. (2020). *Incel radical milieu and external locus of control*. International Centre for Counter-Terrorism. https://www.icct.nl/sites/default/files/import/publication/Special-Edition-2-1.pdf

Clark, C., & Winegard, B. M. (2020). Tribalism in war and peace: The nature and evolution of ideological epistemology and its significance for modern social science. *Psychological Inquiry, 31*(1), 1–22. DOI: 10.1080/1047840X.2020.1721233

Cash, J. (2020). Psychoanalysis, cultures of anarchy, and ontological insecurity. *International Theory, 12*(2), 306–21. https://doi.org/10.1017/S1752971920000147

Chua, A. (2019). *Political tribes: Group instinct and the fate of nations*. Penguin Books.

Cronkhite, A. B., Zhang, W., & Caughell, L. (2020). Special commentary: #Fakenews in #natsec. *US Army War College Quarterly, 50*(1), 5–22.

Dahlgren, P. (2006). Doing citizenship: The cultural origins of civic agency in the public sphere. *European Journal of Cultural Studies, 9*(3), 267–86. https://doi.org/10.1177%2F1367549406066073.

Dahlgren, P. (2013). Force-fields of the web environment. *The political web: Media, participation and alternative democracy* (pp. 36–64). Palgrave Macmillan.

Delanty, G. (2011). Cultural diversity, democracy and the prospects of cosmopolitanism: A theory of cultural encounters. *British Journal of Sociology, 62*(4), 633–56. https://doi.org/10.1111/j.1468-4446.2011.01384.x

Duile, T. (2017). Islam, politics, and cyber tribalism in Indonesia: A case study on the Front Pembela Islam. *International Quarterly for Asian Studies, 48*(3/4), 249–72. https://doi.org/10.11588/iqas.2017.3-4.7443

Freedman, L. (2020). *The revolution in strategic affairs*. Routledge.

Freedman, L. (2021). Introduction: The evolution of deterrence strategy and research. In F. Osinga, & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies* (pp. 1–10). Asser Press. https://doi.org/10.1007/978-94-6265-419-8

Gerodimos, R. (2012). Online youth attitudes and the limits of civic consumerism: The emerging challenge to the Internet's democratic potential. *Information, Communication & Society, 15*(2), 217–45. https://psycnet.apa.org/doi/10.1080/1369118X.2011.572983

Giddens, A. (1984). *The constitution of society*. University of California Press.

Gray, C. S. (2000). Deterrence in the 21st century. *Comparative Strategy, 19*(3), 255–61. https://doi.org/10.1080/01495930008403211

Grimson, A. (2010). Culture and identity: Two different notions. *Journal for the Study of Race, Nation and Culture, 16*(1), 61–77. https://doi.org/10.1080/13504630903465894

Grosfoguel, R. (2013). The structure of knowledge in westernized universities: Epistemic racism/sexism and the four genocides/epistemicides of the long 16th century. *Human Architecture: Journal of the Sociology of Self-Knowledge, 11*(1), 73–90.

Hayday, E. J., Collison, H., & Kohe, G. Z. (2021). Landscapes of tension, tribalism, and toxicity: Configuring a spatial politics of esport communities. *Leisure Studies, 40*(2), 139–53. https://doi.org/10.1080/02614367.2020.1808049

Heaney, M. T. (2020). Protest at the center of American politics. *Journal of International Affairs, 73*(2), 195–208. https://jia.sipa.columbia.edu/protest-center-american-politics

Hobfoll, S. E. (2018). *Tribalism: The evolutionary origins of fear politics*. Palgrave Macmillan.

Hogg, M. A. (2001). A social identity theory of leadership. *Personality and Social Psychology Review, 5*(3), 184–200. https://doi.org/10.1207%2FS15327957PSPR0503_1

Hom, A. R., & Steele, B. J. (2020). Anxiety, time, and ontological security's third-image potential. *International Theory, 12*(2), 322–36.

James, P. (2006). *Globalism, nationalism, tribalism: Bringing theory back in*. SAGE.

Janowitz, K. M. (2009). Netnographie—Ethnographische Methoden im Internet und posttraditionelle Vergemeinschaftungen. In P. Ohly (Ed.), *Tagungsband zur Wissensorganisation '09 "Wissen—Wissenschaft—Organisation," 12. Tagung der Deutschen* (pp. 1–9). https://nbn-resolving.org/urn:nbn:de:0168-ssoar-65241

Jarvis, R. (1976). *Perception and misperception.* Princeton University Press.

Jordan, J. (2009). When heads roll. *Security Studies, 18*(4). https://doi.org/10.1080/09636410903369068

Kinnvall, C. (2004). Globalization and religious nationalism: Self, identity, and the search for ontological security. *Political Psychology, 25*(5), 741–67. https://www.jstor.org/stable/3792342

Kinnvall, C. (2018). Ontological insecurities and postcolonial imaginaries: The emotional appeal of populism. *Humanity & Society, 42*(4), 523–43. https://doi.org/10.1177%2F0160597618802646

Kinnvall, C., Manners, I., & Mitzen, J. (2018). Introduction to 2018 special issue of *European Security*: "Ontological (in)security in the European Union." *European Security, 27*(3), 249–65. https://doi.org/10.1080/09662839.2018.1497977

Lewandowsky, S., & Smillie, L. (Eds.). (2020). *Technology and democracy: Understanding the influence of online technologies on political behaviour and decision-making.* Publications Office of the European Union. https://data.europa.eu/doi/10.2760/709177

Lieber, R. J., & Weisberg, R. E. (2002). Globalization, culture, and identities in crisis. *International Journal of Politics, Culture, and Society, 16*(2), 273–96. https://www.jstor.org/stable/20020163

Lupovici, A. (2010). The emerging fourth wave of deterrence theory. *International Studies Quarterly, 54*(3), 705–32. https://www.jstor.org/stable/40931133

Mason, L. (2018). *Uncivil agreement: How politics became our identity.* University of Chicago Press.

Mazarr, M.J. (2018). *Understanding deterrence.* RAND Corporation. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

Mazarr, M. J., Chan, A., Dmus, A., Frederick, B., Nader, A., Pezard, S., Thompson, J. A., & Treyger, E. (2018). *What deters and why.* RAND Corporation.

MccGwire, M. (1986). Deterrence: The problem—not the solution. *International Affairs, 62*(1), 55–70. https://doi.org/10.2307/2618067

McKenzie, T. M. (2017). *Is cyber deterrence possible?* Air University Press.

Meharg, S. J. (2001). Identicide and cultural cannibalism: Warfare's appetite for symbolic place. *Peace Research, 33*(2), 89–98. https://www.jstor.org/stable/23608075

Meharg, S. J. (2004). *Identicide in Bosnia and Croatia: The destruction, reconstruction, and construction of landscapes of identity* [Unpublished PhD dissertation, Queen's University]. Library and Archives Canada.

Meharg, S. J. (2006). Identicide: Precursor to genocide. Working Paper 5. *Centre for Security and Defense Studies.*

Meharg, S. J. (2011). Restoration and reconstruction for environmental security. In G. E. Machlis, T. Hanson, Z. Spiric, & J. E. McKendry (Eds.), *Warfare ecology: A new synthesis for peace and security* (pp. 117–88). Springer.

Mitzen, J. (2006). Ontological security in world politics: State identity and the security dilemma. *European Journal of International Relations, 12*(3), 341–70. https://doi.org/10.1177%2F1354066106067346

Niedbala, E.M., & Hohman, Z. P. (2019). Retaliation against the outgroup: The role of self-uncertainty. *Group Processes & Intergroup Relations, 22*(5), 708–23. https://doi.org/10.1177%2F1368430218767027

Osborne, B. S. (2001). Landscapes, memory, monuments, and commemoration: Putting identity in its place. *Canadian Ethnic Studies, 33*(3), 39–77.

Papacharissi, Z. (2015). We have always been social. *Social Media + Society, 1*(1). https://doi.org/10.1177%2F2056305115581185

Parker, D., Pearce, J. M., Lindekilde, L., & Rogers, M. B. (2019). Challenges for effective counterterrorism communication. *Studies in Conflict and Terrorism, 42*(3), 264–91. https://doi.org/10.1080/1057610X.2017.1373427

Perry, G. (2018). *The lost boys: Inside Muzafer Sherif's Robbers Cave experiment*. Scribe.

Petersen, M. B. (2020). The evolutionary psychology of mass mobilization: How disinformation and demagogues coordinate rather than manipulate. *Current Opinion in Psychology, 35*, 71–5. https://doi.org/10.1016/j.copsyc.2020.02.003

Pew Research Center. (2021a, 7 April). Internet/broadband fact sheet. *Pew Research Center.* https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

Pew Research Center. (2021b, 7 April). Social media fact sheet. *Pew Research Center.* https://www.pewresearch.org/internet/fact-sheet/social-media/

Plater, Z. J. B. (1990). Keynote essay: A modern political tribalism in natural resources management. *Public Land Law Review*, 11, 1–17.

Richerson, P. J., & Boyd, R. (2001). The evolution of subjective commitment to groups: A tribal instincts hypothesis. In R. M. Nesse (Ed.), *Evolution and the capacity for commitment* (pp. 184–220). Russell Sage Foundation.

Rumelili, B. (2020). Integrating anxiety into international relations theory: Hobbes, existentialism, and ontological security. *International Theory, 12*(2), 257–72. https://doi.org/10.1017/S1752971920000093

Schulze, M. (2019, 21 August). Cyber deterrence is overrated. *Stiftung Wissenschaft und Politik*. https://www.swp-berlin.org/10.18449/2019C34/

Snyder, G. H. (1960). Deterrence and power. *Journal of Conflict Resolution, 4*(2), 163–78. https://doi.org/10.1177%2F002200276000400201

Steele, B. J. (2008). *Ontological security in international relations: Self-Identity and the IR state*. Taylor and Francis.

Steele, B. J., & Homolar, A. (2019). Ontological insecurities and the politics of contemporary populism. *Cambridge Review of International Affairs, 32*(3), 214–21. https://doi.org/10.1080/09557571.2019.1596612

St. John, G. (2017). Civilised tribalism: Burning Man, event-tribes and maker culture. *Cultural Sociology, 12*(1), 1–19. https://doi.org/10.1177%2F1749975517733162

Stork, C., Calandro, E., & Gillwald, A. (2013). Internet going mobile: Internet access and use in 11 African countries. *Info, 15*(5), 34–51. https://doi.org/10.1108/info-05-2013-0026

Subotić, J. (2016). Narrative, ontological security, and foreign policy change. *Foreign Policy Analysis, 12*(4), 610–27. https://doi.org/10.1111/fpa.12089

Trager, R. F., & Zagorcheva, D. P. (2006). Deterring terrorism: It can be done. *International Security, 30*(3). 87–123. https://www.jstor.org/stable/4137488

Van Dijcke, D., & Wright, A. L. (2021). *Profiling insurrection: Characterizing collective action using mobile device data*. Becker Friedman Institute.

Waisbord, S. (2018). The elective affinity between post-truth communication and populist politics. *Communication Research and Practice, 4*(1), 17–34. https://doi.org/10.1080/22041451.2018.1428928

Wassermann, H. 2020. Fake news from Africa: Panics, politics, and paradigms. *Journalism*, 21(1), 3–16. https://doi.org/10.1177%2F1464884917746861.

Wilner, A., & Wagner, A. (Eds.). (2021). *Deterrence by denial: Theory and practice*. Cambria.

Wohl, M. J. A., Branscombe, N. R., & Reysen, S. (2010). Perceiving your group's future to be in jeopardy: Extinction threat induces collective angst and the desire to strengthen the ingroup. *Personality and Social Psychology Bulletin, 36*(7), 898–910. https://doi.org/10.1177%2F0146167210372505

Wolfe, P. (2006). Settler colonialism and the elimination of the native. *Journal of Genocide Research, 8*(4), 387–409. https://doi.org/10.1080/14623520601056240