SECURITY DIALOGUE

Special Issue on *Vernacular Security*

Security Dialogue
1–17
© The Author(s) 2025
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/09670106251362733
journals.sagepub.com/home/sdi
Sage

# Methodological insights into digital vernacular (in)security: Developing from netnography to appnography on Snapchat in Marseille, France

**Joseph Downing**
Aston University, UK

## Abstract

While vernacular security studies pays scant attention to the digital field, there are significant untapped opportunities in the digital world. This article aims to contribute to these research opportunities by offering a method and methodological intervention to capture the multimodal, user-generated and self-destructing data on the mobile phone application Snapchat. It does this by adapting netnography into an 'appnography' to navigate the data access issues presented by the proliferation of smartphone applications. The article seeks to make two contributions. As method, it outlines how appnography can get around data access issues faced by researchers on many smartphone applications. As methodology, it seeks to push vernacular security studies and critical security studies to further consider the complex, sophisticated, multimodal outputs that articulate (in)security on smartphone applications which are often unmediated by media bureaucracies. The article finishes by offering some empirical and conceptual insights into constructions of (in)security from below in the context of Marseille, France. These empirics demonstrate significant opportunities for understanding how fictional and cultural symbols (such as Bart Simpson or Pablo Escobar's character from the *Narcos* Netflix show) are adapted and co-opted by users to construct security from below. The appnography also uncovers the ways in which branding and commercial strategies are incorporated by individuals in navigating (in)security. Finally, the self-destructing data was also found to be an unmonitorable conduit for a range of conspiracy theories.

## Keywords

Drug dealing, Marseille, methodology, mobile applications, netnography, social media

## Introduction: Digital vernacular security and appnography

Both vernacular security studies (Bubandt, 2005; Jarvis, 2019; Risør, 2010; Vaughan-Williams and Stevens, 2016) and critical security studies methods and methodologies (Aradau et al., 2015; Salter and Mutlu, 2013) have diversified the security studies research agenda. Neglected within both of

**Corresponding author:**
Joseph Downing, Aston University, Aston Street, Birmingham, West Midlands, B47ET, UK.
Email: j.s.downing@aston.ac.uk

these developments is work on digital technologies in the 21st century. This article argues that these technologies not only present empirical opportunities but also necessitate a rethinking of security studies methods and methodologies. It seeks to contribute to this emergent research field by presenting a modified netnography (Kozinets, 2002; Kozinets and Gretzel, 2024), an 'appnography', to investigate vernacular security discussions from below. In recent work Kozinets and Gretzel (2024) have argued for netnography to be continually modified to keep pace with the digital developments. The present article does not claim to reinvent the wheel by using the term 'appnography' but rather seeks to continue the valuable work of netnography by applying it to the rapidly emerging and dynamic field of smartphone applications.

The distinction between netnography and appnography can be seen here as twofold. Firstly, the ephemeral nature of data produced by apps such as Snapchat necessitates adaptations to capture security voices from below. Secondly, app-based social media platforms enable individuals to engage in the production of complex, multimodal user-generated content in the development of their action frames (Bennett and Segerberg, 2012; Caraway, 2018) that initial developments in netnography have not fully grasped. This has significant potential to impact the empirical understandings of vernacular (in)securities by opening up the field to understand a range of behaviours taking place on, and facilitated by, mobile applications.

This article highlights three particular areas to evidence the possibilities for empirical advancement. Firstly, appnography has captured how drug dealers formulate their action frames using creative symbolic repertoires with reimagined fictional cultural (such as characters from the Netflix series *Narcos*) and local urban symbols (such as the Notre Dame Cathedral in Marseille). Secondly, the empirics open up a discussion of the integration of commercial strategies, such as branding, in how individuals construct their relationship to insecurities. Thirdly, appnography has enabled the capturing of the proliferation of conspiracy theories in the short video 'snaps' and demonstrates that ephemeral data is a unmonitorable space for the proliferation of conspiracy theories with significant implications for understanding how conspiracy theories relate to (in)security.

The rapid growth and impressive scope of smartphone apps, now numbering above 8.9 million, (Koetsier, 2020), offer opportunities for innovative research, while presenting challenges, existing at the 'uneasy intersection between transparency and opacity, being both "open" interfaces and "opaque" algorithms used on proprietary platforms' (Aradau et al., 2019: 2550). Despite some rare interventions from the critical security studies field (Aradau et al., 2019), apps are still under-researched. This article seeks to contribute to this research gap by examining the mobile phone application Snapchat,[1] particularly challenging because of its ephemeral, 'self-destructing' data (Bayer et al., 2016), deleted from the application's servers 24 hours after creation whether viewed by other users or not. This varies from data sources such as as X (formerly Twitter) that enable scholars to obtain large datasets for offline analysis (inter alia Downing et al., 2022). It is into this novel and disruptive research niche that this article seeks to make a primarily methodological contribution.

This requires four steps. Firstly, it is required to conceptualize vernacular security studies as well as critical security studies methods and methodologies. In particular, this problematizes notions of security and (in)security through examining how individuals use smartphone apps to structure their relationships to (in)security.

The second step is to outline data and ethics questions. Social media data access is ephemeral 'self-destructing' data (Bayer et al., 2016); many other social media applications such as Grindr, TikTok and Telegram are also problematic for data collection and the method presented here could help to overcome this for researchers. The ethical implications of this study also require attention.

The third section harnesses critical security studies orientations that foreground the need for methods and methodological experimentation and reflection (Aradau et al., 2015, 2019). This enables the modification of well-conceptualized netnographic approaches (Kozinets, 2002) to develop an 'appnographic' approach. This involves both the specific methods nuts-and-bolts process of conducting an appnography, but also the methodological, conceptual contribution to vernacular security studies in attempting to capture the multimodal output of action frames (Bennett and Segerberg, 2012; Caraway, 2018) presented in Snapchat. This requires using detailed field notes as well as considering how to capture the increasingly complex, multimodal nature of user-generated content.

The fourth and final section seeks to further make the case for the utility of appnography in the critical security studies space by offering some empirical and conceptual insights gained by sampling discussions and practices of (in)security on Snapchat. Appnography enables the capture of both ephemeral data and the increasingly multimodal and sophistic ways individuals create action frames (Bennett and Segerberg, 2012; Caraway, 2018). This facilitates the capture of ranges of narratives and symbols constituting (in)security voices from below, in this case using branding, international popular cultural idioms and local themes.

## Conceptualizing security methods vernacular security studies

To lay the groundwork for the development of an appnography, the literature on vernacular security needs to be thoroughly reviewed. Secondly, as this is primarily a methodological contribution, the valuable canon of work on critical security studies methods and methodologies is also key in considering the conceptual, normative and philosophical orientations of critical security studies.

### *The vernacular turn and conceptualizing voices from below*

Vernacular security studies emerged as a response to the overly elite focus in early critical security studies research, such as the Copenhagen school (Buzan et al., 1997), where elites speak security and laypeople listen, with this elite focus highlighted as a key part of the school's 'racism' (Howell and Richter-Montpetit, 2020). This elite vernacular security studies examines voices 'from below' of non-elites (Bubandt, 2005; Fisher and Leonardi, 2021; Jarvis and Lister, 2012; Vaughan-Williams and Stevens, 2016) to glean greater understandings of how 'citizens . . . construct and describe experiences of security and insecurity in their own vocabularies, cultural repertoires' (Croft and Vaughan-Williams, 2017: 22). This has important synergies with critical security studies' thinking about technologies such as CCTV cameras as part of 'little security nothings' (Huysmans, 2011), and smartphones reconfiguring the relationships 'between producers and consumers and between elites and "audiences"' (Hansen, 2011:52).

Three key aspects of vernacular security studies are important for this study. Firstly, vernacular security studies situates security as 'a fundamentally empty concept – one that is capable of being "filled" in a potentially infinite number of ways' (Jarvis, 2019: 118). This allows inductive research into 'public experiences, understandings, anxieties and fears' (Jarvis, 2019: 107) about global, national and/or local security concerns (Bubandt, 2005). Vernacular security studies has enabled research into innovative contexts including environmental security in Madagascar (Huff, 2017), and 'spiritual security' (Fisher and Leonardi, 2021) in Africa. Thus, theoretical emptiness is well suited to understanding the unpredictability of the multimodal outputs possible on social media. This opens up possibilities for understanding security as constituted by discourse, text and, importantly, as video, image, meme, user-generated content, all of which incorporate national, local and fictional cultural idioms and symbols.

Secondly, vernacular security studies refuses 'to prioritise particular populations by virtue of their identity or socio-political positions' (Jarvis, 2019: 107) enabling the study of marginalized populations such as sex workers in Fiji (George, 2017). This facilitates the examination of populations and activities that traditional security would deem deviant and seeking to threaten the referent object of state security – for example drug dealing and resulting deaths from violent crime in the context of Marseille examined here (Pujol, 2016; Sellami, 2016). This study acknowledges the complex, intersubjective nature of security and threat – described well by the Paris school of security studies as a 'Mobius strip' (Bigo and McCluskey, 2018) where security and insecurity are embedded into intimate, inseparable relationships that problematize such traditional, conservative, 'common-sense' understandings of security that activities like drug dealing and sex work produce insecurity. While they may in certain spheres, such as the well-documented violence and murders resulting from Marseille's drugs trade (Pujol, 2016; Sellami, 2016), these activities may also represent attempts by individuals to physically and economically secure themselves under conditions of post-industrial, neo-liberal economic decline common to port cities in the Global North in the beginning of the 21st century (Mah, 2014). This article does not set out to resolve these security complexities, but rather use vernacular security studies to glean insights into how those traditionally defined as creating insecurity can be understood in their own voices, and in particular understanding the discursive, symbolic and narrative repertoires they utilize. Vernacular security studies contributes here by rejecting universalist notions of violence and through studying 'safety making' in mob justice in Cameroon (Orock, 2014) and in examining violence and safety making in Bolivia (Risør, 2010).

Thirdly, vernacular security studies avoids 'the universalistic assumptions of more explicitly cosmopolitan approaches' (Jarvis, 2019: 110). This highly context-specific approach has been central from the founding of vernacular security studies to understand idioms of uncertainty and fear about global, national and/or local security concerns (Bubandt, 2005). Vernacular security studies prioritizes the stories of those marginalized on account of global politics and seeks to understand how 'citizens . . . construct and describe experiences of security and insecurity in their own vocabularies, cultural repertoires' (Croft and Vaughan-Williams, 2017). This has found some application into the digital field in work on security memes and how both influencers and other users have subverted, reinvented and contorted security themes leaning heavily on idioms, stories and narratives from the local context of Marseille, France (Downing, 2021). This limited application to the digital sphere highlights an important research gap not only within the vernacular field, but also in critical security studies more broadly, with some limited exceptions. This includes important work in critical terrorism studies focusing on the construction of foreign ISIS fighters in online comments (de Silva and Crilley, 2016), how examining social media outputs on jihadi bride Shamima Begum can further understandings of gendered constructs of terrorism (Evans and da Silva, 2023) and how terrorism and British Muslims are constructed on X (Downing et al., 2022).

The literature on collective and personal action frames offers important insights into how to dovetail the output generated by social media apps to the conceptual openness of vernacular security studies. In a study of Walmart worker protests, Caraway (2018) demonstrates 'a growing role for personalised forms of communication in the production and circulation of collective action frames' (Caraway, 2018: 7). This offers important insight into how social media means that people can collaborate in the creation of collective action frames 'without the mediation of bureaucratic organisation' (Caraway, 2018: 12) – i.e. they can subvert, reconfigure ideas, images etc. in their own ways. This has also received attention with regard to how user-generated content shared across social media networks – i.e. memes – is important in this process (Bennett and Segerberg, 2012). These ideas are helpful in demonstrating that user-generated content – crucial to the output of users sampled in this study – has much broader application and implications than individuals utilizing user-generated content to market illegal substances. This is important to the methodological contribution presented in this article, because netnography has yet to fully take into account these changes (Kozinets and Gretzel, 2024) and the proliferation of social media apps with data access problems such as Grindr, Telegram and Snapchat means new approaches tailored to these apps are required to capture these important conceptual and empirical changes in the field, both for critical security studies and in the social sciences beyond.

## *Method and methodological advances in critical security studies*

The critical schools of security studies have been critiqued for neglecting methods in favour of focusing on the critical (Salter and Mutlu, 2013). Additionally, vernacular security studies has been methodologically diverse, having used ethnography (Bubandt, 2005, Owens, 2025), focus groups (Jarvis and Lister, 2012), semi-structured interviews (Oyawale, 2022), photo-elicitation (George, 2025). And yet with the exception of Downing (2021), few inroads into digital methods have occurred.

It is into this gap that this article aims to deliver on furthering digital methods. This is aided by the significant existing methodological innovation undertaken in critical security studies. It is important also to foreground a key point – that method and methodology are not considered the same not only in the social sciences but in a range of scholarly fields (King, 1994; McGregor and Murnane, 2010). Here methods are the nuts-and-bolts procedure of what is done (King, 1994; McGregor and Murnane, 2010) and 'methodology' is the far broader theoretical and conceptual reflection on what is being done. This article offers both 'nuts-and-bolts' method insights and broader methodology reflections in terms of how this relates to the approaches of critical security studies more generally. The method points are the ways in which netnography is expanded into applications, in particular to address some of the data collection issues that applications present. However, there is also a broader methodological, conceptual contribution in taking this approach and applying it to vernacular security studies in that it helps to open up further discussions around individuals using apps to produce multimodal, unmediated, user-generated content in their constructions of the complexities of (in)security.

Critical security studies scholars have argued against seeing methods as a purely instrumental step that connects a broader approach to the nuts and bolts of research. As such, we should not simply see methods as 'a bridge between a theory and a technical instrument of analysis' (Aradau et al., 2015: 3) but as a practice. This practice should be informed by the deeper 'methodology' concerns of broader conceptual and theoretical reflection (King, 1994; McGregor and Murnane, 2010). A critical approach to methods 'displaces methods from a tool of representing reality to a securitizing practice' (Aradau et al., 2015: 4). As such, one can see many of the professional security practices employed by states, such as 'analysis, precaution, horizon scanning, mapping, visual representation' (Aradau et al., 2015: 5), as being important methods and methodologies used by states. Thus methods utilized within the security sector are ripe for analysis from critical perspectives (Aradau et al., 2015). This has included a range of techniques such as mapping, or from other perspectives social network analysis, ethnographic practice (Salter and Mutlu, 2013), as well as sociological approaches' (Bigo and McCluskey, 2018) discursive methods (Hansen, 2006). This diversity of 'data' sources requires significant methodological reflection (Aradau et al., 2015). It is into this growing expansion of data sources and approaches that the appnography presented in this article emerges.

Key here is acknowledging that 'the worlds we inhabit and seek to study do not come to us pre-packaged in disciplinary form' (Kalyan, 2020: 161), requiring us to be messy 'without presuming that we know what we are talking about' (Squire, 2013: 37). Innovation and risk taking are also key, allowing space to 'wonder' (Lobo-Guerrero, 2013) about how the social world works. Indeed, this was the entry point of this study – wondering what was happening behind the Snapchat handles scribbled in graffiti on doors, walls and bus seats in Marseille. This aids in developing an experimental 'bricolage'[2] (Aradau et al., 2015: 3) approach. This highlights both the 'problem of change that captures the critical sensibility of critical security studies' (Aradau et al., 2015) and also the issue that 'disruption, innovation and creative change takes place in experimentation' (Aradau et al., 2015). This approach has borne fruit in better understanding how refugee apps use data and connect to external APIs through 'digital parasitism' (Aradau et al., 2019).

## Digitizing methodological bricolage: From critical security studies ethnography, through netnography, to developing an appnography

This article now turns to considering the development of a netnographic approach to a smartphone application. Critical security studies has been important in pushing ethnographic methods into a range of fields including critical terrorism studies (Stump and Dixit, 2013) and indeed in the vernacular turn (Bubandt, 2005). However, it is important to note here that this article does not simply present the application of an existing netnographic approach to a new field, rather it develops something bespoke and novel. This first step of this is in detailing the 'bricolage' 'to-and-fro' (Aradau et al., 2015) process fundamental to producing a viable appnography. The need to address smartphone apps increasingly in a range of security research (as highlighted by Aradau et al., 2019) is a direct result of their increased penetration into a range of social and economics contexts with the proliferation of the smartphone. However, as with many emergent research areas, there is a dearth of both detailed technical methods and the broader conceptual thinking required to take account of their roles in security debates.

This is specifically pronounced within the world of social media, where the rapid pace of change necessitates the adaptation and reinvention of netnography to reach new areas of digital output (Kozinets and Gretzel, 2024) where apps have increasingly taken over from web-based social media interfaces, with the explosion of app-based platforms including Instagram, TikTok and – the case here – Snapchat. Within this methodological development several key areas require consideration. Firstly, there are the specifics of the data access and ethics questions presented by such a study that have significant implications for future efforts by vernacular security scholars seeking to make use of the vast array of opportunities presented by the digital field. Secondly, there is the discussion of the adaptation of netnography into an 'appnography' and what particular considerations and constraints are presented by this novel approach. Finally, it is important to present some initial reflections on some of the possible conceptual and empirical insights this approach offers vernacular security scholars.

### *Data access and ethics for a security studies appnography*

Data access has never been straightforward for social media research of any kind (Ahmed, 2021), but the move to apps has further complicated this. This is because Snapchat has data expiration written into its operation and data expiration is mandatory. This 'self-destructing' data (Bayer et al., 2016) presents significant issues for researchers as the 'snaps' disappear after being viewed, and if not viewed, disappear from the Snapchat servers after 30 days. Additionally, taking a screenshot with the device being used to view the data results in the data's producer being informed that you are trying to capture their data. Many of the accounts monitored as part of this study contain explicit reference to this – that anyone taking a screenshot would be blocked from accessing any future snaps. This is part of Snapchat's process of innovation over and above more 'traditional' platforms like Facebook (Utz et al., 2015) and has given users new possibilities for self-expression

(Utz et al., 2015) as well as being ‘reserved for closest relationships, not strangers’ (Poltash, 2012). This self-destructing data affords users higher levels of privacy (Bayer et al., 2016). As such, Snapchat has gained traction for being suitable for confidential activities such as ‘sexting’, using the app to exchange intimate pictures and videos because of its ephemeral nature, hinting at the app being more appropriate for intimate content (Poltash, 2012; Vaterlaus et al., 2016).

There is no way to capture a vast quantity of data in bulk, whether for pay or for free, by keyword or hashtag from an API. The X API has previously been an important component of other digital security research on platforms such as X (Downing et al., 2022) but its use has even become problematic. Thus, a different approach was required. This study’s key approach to data collection was through the development of a network. Snapchat works by individuals having a specific username by which they can be added and followed in a passive sense. Some accounts require the user to approve this, others do not depend on user-defined settings; however, at any time one can be blocked by the user. Once you have successfully added a user, you can then view their image or video ‘snaps’, but for an extremely limited time before they are no longer available for view. This study was initiated by adding handles taken from public graffiti that openly advertised drugs, but which would not give sufficient participants for a study. Thus a modified form of snowball sampling was used (Goodman, 1961), relying on participants to recommend other users in their snaps to be sampled. The network took time to build (circa 90 days) and was subject to users entering the network, and then leaving, sporadically as the study continued. Thus, one linear, straightforward recruitment phase was not possible, and a much messier and continual approach was required.

In total, the study observed a total of 35 participants over the course of 18 months from March 2020 to September 2021, viewing a total of 11,530 individual snaps, an average of 21 snaps per day, each day at 9am and 9pm. However, there was significant variance in the number of snaps per day, with some days hitting a low of nine and other days hitting a high of as many as 32. This was a function of both the size of the network and also the variance in the number of snaps per day by established users.

Entering and building a network is only one part of the broader questions raised by such research. While the recording of the data will be discussed in the process of the step-by-step operationalization of appnography from netnography in the following section, here it is important to address the ethical issues inherent in performing such research. Ethnography comes with significant ethical concerns, stemming from its problematic development and use during European colonialism (González, 2003). Indeed, the development of digital ethnography, ‘netnography’, also comes with ethical concerns (Kozinets, 2002). There exists a key split between ‘active’ and ‘passive’ netnography (Alavi et al., 2010), ‘passively monitoring the community and integrating the gathered information’ (Alavi et al., 2010: 87). There are many critiques of a ‘passive’ non-participatory netnography (Costello et al., 2017) as clearly this does not allow the voice of the participant to emerge. In a security context where it is highly likely to be disengaged by participants if a researcher identifies themselves as such, it was not viable, nor advisable, for the researcher to identify themself and thus a ‘passive’ appnography was used. Indeed, the passive monitoring of online communities also comes into contravention with key critical security studies approaches to ethnography, which should be ‘cultural exchange or embeddedness rather than a unidirectional extraction’ (Salter, 2013: 55), and specifically that ethnography in vernacular security studies should ‘move away from seeking out isolated experiences’ (Owens, 2025). However, there is also the acknowledgement that the security studies milieu presents significant research difficulties where the use of ‘semi-covert’ ethnographies have had to be used, such as Ratelle using a semi-covert ethnography to investigate Russian security practices in the Caucasus (Salter, 2013: 55). Additionally, ‘An ethnographer must be practical, flexible, and creative’ (Stump and Dixit, 2013: 81). The literature on netnography dovetails with these requirements, arguing that passive approaches are suitable for studying politically sensitive and illegal acts (Gilchrist and Ravenscroft, 2011; Langer and Beckman, 2005). This method has found wider adoption outside of just examining sensitive topics and has been applied to the study of consumer behaviour (Kozinets, 2002). This presents a key concern for ethics because it does not allow the researcher to satisfy the requirements for informed consent of human participants.

To satisfy requirements and obligations of ethics clearance to conduct this research, strategies were developed and deployed to ensure the research was not done to the detriment of the participants. Conduct of this research was contingent on appropriate data management strategies being strictly deployed. One possible option for data collection was to use a second smartphone or digital camera to capture photo images or videos of snaps. This was deemed as ethically problematic because it would have resulted in the collection of images without the participant's consent, which could be stored with their social media usernames, which could have possibly then compromised their anonymity. Thus data management was seen as key to overcoming ethical issues and the priority would be on the protection of individuals involved. A requirement was that all data, including Snapchat account handles, had been anonymized and owing to the data being automatically removed from the company's servers after 30 days, data triangulation by law enforcement and/or the tech company itself is now not possible. These measures, however, should not be read to negate the significant ethical challenges that the use of such a passive approach to investigate vernacular, or indeed other forms of, security faces. A key lesson for researchers seeking to employ similar approaches is to be mindful of ethical implications specific to their target populations. If we are to take seriously that the local context is key in understanding security from critical perspectives, then the immediate research context is key in formulating ethical considerations. Indeed, it is also important to be mindful of ethics before, during and after the conduct of social science research, as new ethical considerations are likely to be raised as the research unfolds, owing to the unpredictability of the online sphere. In terms of this study, no unforeseen ethical challenges emerged during the conduct of the research.

## *Operationalizing netnography into an appnography for security studies*

The appnography presented here builds upon recent observations that netnography needs to develop to account for the rapid pace of change in online output (Kozinets and Gretzel, 2024). The appnography differs from traditional netnography in two ways. Firstly, netnographic studies have focused on analysing textual online spheres, to the detriment of multimodal outputs (Costello et al., 2017). This is important given the literature on action frames and how these are developed on social media (Bennett and Segerberg, 2012; Caraway, 2018) that enable individuals to articulate themselves in novel multimodal ways, away from traditional media bureaucracies. This represents a conceptual contribution of the appnography presented here in opening up conversations on how apps offer rich ground for research on multimodal outputs both for the broader social sciences and specifically for vernacular security studies. The second contribution of this appnography is in finding a way around data access issues presented by social media applications. The self-destructing data (Bayer et al., 2016) means that a novel way needs to be developed to both record and interpret these multimodal forms of data that automatically disappear. However, this is also more generalization, given the difficulty in downloading data from a range of applications (such as TikTok and Telegram) both for practical and also for legal and financial reasons. While not the key focus of this study, it is important to note that observing and taking detailed field notes on app-based outputs can get around the legal and financial constraints that social media apps like Grindr, TikTok and Telegram can present to researchers. These concerns will only continue to grow as an issue as social media apps continue to proliferate in ever-increasing aspects of daily life.

Questions around the operationalization of netnography, like ethnography before it, are not new and raise some very important issues, as there is no one-size-fits-all approach (Tunçalp and Lê, 2014). Here a valid critique is that scholars often take the idea of a netnographic method as self-evident and neither describe nor evaluate the process of their netnography (Tunçalp and Lê, 2014). This is important due to the divergent and diverse nature of the methodology and also a variety of approaches (Tunçalp and Lê, 2014). This is especially true when we need to consider how the idea of an online netnography patches into both the question of application to the specifics of apps and then in the context of seeking to study and understand the complexities of (in)security. This room for innovation and interpretation renders arguments about the importance in critical security studies of methodological bricolage and a 'to-and-fro' reflective approach ever more pertinent (Aradau et al., 2015).

The study here followed a six-step process (Kozinets, 2002). This involved research planning, entrée, data collection, data analysis, ethical standards and research representation (Kozinets, 2002). This should not be seen as a strictly linear process because, as with real-world ethnography, there has to be room for the data to lead the researcher. Additionally, the nature of studying networks means that throughout the study participants were added by adding their individual handles to the app when they were mentioned or recommended in the snaps of other users. However, users also fall away. It was not possible to know why users left the network – they could have deleted the app, blocked the research account, or indeed been deplatformed by Snapchat for violating its terms of service. Here a modified form of snowball sampling was used (Goodman, 1961). Snowball sampling in person involves asking research participants, possibly identified at random, to name further possible participants and so on (Goodman, 1961). Indeed, this does not have to be random, and qualitative sociology has used this sampling technique to great effect, especially in the investigation of deviant populations that are hard to reach (Etikan, 2016). This involves a non-random identification of someone from this hard-to-reach population, who then recommends individuals from their network (Etikan, 2016).

This study employed a passive form of 'promotional snowball sampling'. This was developed and employed because of two key concerns. Firstly it was not possible to ask participants to recommend further participants because of the deviant nature of their activities and the covert nature of the passive netnographic approach. Put simply, a request for sample suggestions would likely have resulted in being blocked. Secondly, it became quickly evident that this approach was not required as in the context of Snapchat, participants would frequently recommend and promote the services of associates from other domains. For example, drug dealers would not promote other drug dealers, but they would promote a sex worker or a document fraudster. The exception here was sex workers, who would promote each other frequently. Thus the first two planning and entrée phases would be revisited on the induction of new network members.

The second key issue stems from the very nature of Snapchat's data. As mentioned, data collection would not be as simple as downloading data or being able to keep a direct digital copy because of the app notifying content creators of screen capture. This was overcome by taking extensive field notes at the twice-daily checking of the Snapchat network – at 9am and 9pm. This approach is not limited in its application to Snapchat as apps like Grindr, Telegram and Tiktok, while not making use of ephemeral data, make it impractical for users to capture data in bulk for later analysis. Yet these applications present important sites of user-generated discourses that are not mediated by media bureaucracies (Caraway, 2018) and thus offer important sites of study for both critical security studies and other social science disciplines. This process was completed digitally and directly into a Word document over a two-year period from September 2019 until September 2021.

The period of data collection was significant, with data collected being rich and varied, resulting in extensive and detailed field notes. There is no consensus on how field notes should be written or even their value in ethnographic research (Naidoo, 2012). Field notes are important because they involve the ‘critical acts of sense making and interpretation’ (Naidoo, 2012: 9). Appnography is specifically designed to get over data access problems with mobile applications’ ephemeral data, and a detailed narrative analysis was better suited to capturing the richness of the data in terms of the complex multimodal action frames deployed by users (Caraway, 2018). This required significant details to be kept about what the idioms of expression were, and how this related to broader local or global questions of (in)security. A straightforward example of this was in snaps produced by drug dealers on apps which used characters from TV shows such as *Narcos* where the image of the Colombian crime figure Pablo Escobar was printed on the retail packaging of drugs.

However, on reflection, some issues did arise in applying this netnographic method to social media. Perhaps too much data was collected. An issue with netnography, and perhaps ethnography more broadly, is indeed when to stop. It was not required to have such a significant time investment in the project (730 days) nor to view so many individual snaps (5110) to get at the key theoretical take-home messages. The time investment is something important to consider when designing a netnographic approach to social media analysis because of resource allocation and the possibility of diminishing returns in terms of uncovering novel conceptual and, to a point, empirical content. However, this should not negate the interesting and novel insights generated using this theoretical approach.

## Capturing the multimodal complexities of vernacular (in)securities

Empirically this article seeks to highlight three key contributions from the much broader range of empirical themes that emerge (see Table 1). This is because it takes primarily a methods and methodology approach whereby empirics serve primarily to offer insight into the possibilities that can be opened up by this methods and methodological innovation. This is presented here as three key areas of contribution. Firstly, there is the finding that the multimodal outputs analysed offer important insights into how voices from below subvert and co-opt cultural (such as characters from the Netflix series *Narcos*) and local urban (such as the Notre Dame Cathedral in Marseille) symbols into their discourses of security in interesting ways. Secondly, there is the discovery that constructions of security from below can be seen to adopt a range of commercial and business idioms, such as branding and special offers. Finally, there is the important observation that the ephemeral self-destructing data on Snapchat allows multimodal narratives drawing on conspiracy theories to be propagated and shared through unmonitorable channels.

This study started by following a snap handle openly advertising drugs, and other drug dealers were recommended by sex workers. This has major implications for the local context of Marseille,

**Table 1.** Codes and tallies of analysed Snapchats.

| Themes | % | Number |
|---|---|---|
| Non-relevant | n/a | 4727 |
| Relevant | n/a | 6803 |
| Sex work | 31 | 2049 |
| Drug dealing | 29 | 2015 |
| Fraud | 20 | 1370 |
| COVID-19 | 11 | 724 |
| Conspiracy theories | 9 | 645 |

being a centre of drug trafficking (Pujol, 2016; Sellami, 2016), which saw its deadliest year of gang violence in 2023 with 47 deaths and 118 injuries related to the drugs trade (Leroux, 2023). The observation that drug dealers use social media is not in itself new (Bakken, 2021; Demant and Bakken, 2019; Moyle et al., 2019; van der Sanden et al., 2021). Previous works make important observations that online business practices are rapidly transforming drug markets across the globe (Coomber et al., 2023); they are not simply a retail 'eBay for drugs' but rather focus more on wholesale business-to-business transactions (Aldridge and Décary-Hétu, 2014). For example, the Silk Road was an online drugs market on the dark web that was used to trade in illegal recreational drugs using bitcoin (Aldridge and Décary-Hétu, 2014); it was closed by the FBI in 2013.

The literature has evolved as platforms and their use by the drugs trade have evolved. The myriad different platforms used to sell drugs has both improved the efficiency of supply and reduced exchange-related risks for both buyers and sellers (Coomber et al., 2023; Moyle et al., 2019). 'Digitally mediated drug dealing' uses social media apps; in Scandinavia this was dominated by Facebook, followed by Instagram, but also using Snapchat (Demant and Bakken, 2019). The platforms function as entry-level markets for young drug consumers, but also demonstrate a high degree of instability as groups are closed down through content moderation channels (Demant and Bakken, 2019). There exists significant national and regional variation in the platforms used (Demant and Bakken, 2019; Demant et al., 2019), with Snapchat in particular taking a more prominent role in online drug sales in New Zealand (van der Sanden et al., 2021) than in Scandinavia. These important studies, however, lack a detailed analysis of the security discourses and narratives that drug dealers use in their social media outputs, and also on how non-drug-dealing groups, such as sex workers, can work as critical nodes to publicise drug dealers on apps such as Snapchat.

The creation of multimodal action frames by users under the theme of drug dealing highlighted the use of two symbolic visual repertoires. Firstly, there is the remaking and subversion of popular culture themes to brand drugs. This involves custom-made packaging printed with characters from popular culture: Bart Simpson, Heisenberg from AMC's *Breaking Bad* and characters from Netflix's *Narcos*. This demonstrates that the focus of vernacular security studies is on the intersection between the national, local and international (Bubandt, 2005) and theoretical emptiness and avoiding universalistic assumptions about what security is (Jarvis, 2019). However, this begins to make a significant contribution conceptually in that it shows the importance of fictional characters in the user-generated content of individuals. This is a vital part of the way that users create action frames that are not mediated by media bureaucracies (Bennett and Segerberg, 2012) and vernacular security studies would do well to consider in greater depth the use of fictional, popular cultural symbols in discussions of security.

The second important visual repertoire was the use of specific symbols from Marseille itself – such as the number 13 (the number of the city's department in France) and the silhouette of the city's main church, which serves as a de facto symbol of the city itself. Thus the intersection of the national, international and 'local' so important to vernacular security studies (Bubandt, 2005) is not simply a place where security is practised, or an arena in which to mobilize against security practices imposed from outside, but also a repertoire of symbols and idioms that individuals draw on to construct their place in narratives of security.

Additionally, the results gleaned from this appnography bring into focus the importance of commerce, business and economic concerns in the ways in which (in)security is practised. While critical security studies has been active in investigating organized crime (Edwards and Gill, 2002; Stritzel, 2012), it is yet to conceptualize the ways in which the retail interface of organized crime adopts recognizable practices from the commercial business world. Thus the branding of vernacular insecurity from below draws upon not only characters, symbols and idioms from mainstream culture, but also the mainstream logic of capitalist retail business practices. Firstly, special offers

– a free lighter and rolling papers with every purchase, or a free small quantity of other drugs with a purchase of a particular drug type – demonstrate the co-option of mainstream capitalism techniques. Additionally, the users used Snapchat, as observed in other themes of crime and insecurity, to collect and showcase feedback and testimonials. This was done through showing screenshots of the app's private messaging feature with complimentary comments about their products and services. Testimonials also took the form of videos, where the identity of the buyers was masked while they were shown being able to choose their own purchase from a range of the same drugs, with text overlaid saying 'the customer is king'. However, this open approach to location and branding had far darker and more worrying elements in their open flaunting of military-grade weapons alongside the vast quantities of drugs showcased in their snaps – including a Kalashnikov assault rifle on the table with their drugs. Their logo, which they showed graffitied in a large (circa 1.5 meters high) mural on a wall, included a Disney cartoon character smoking a joint and firing a Kalashnikov. This is important in the local context of Marseille, as the Kalashnikov is not simply an abstract symbol of broader, global insecurity, but rather something very prominent in the local context of insecurity (Downing, 2021). This demonstrates again the utility of vernacular approaches in examining the unexpected ways in which themes, symbols and idioms of security are subverted and reinvented by voices from below.

Another a potential future contribution of the data generated from this study is a greater understanding of the dynamics of conspiracy theories on social media applications. This is important given the recent attention generated by conspiracy theories and their associated security dynamics. While conspiracy theories are nothing new, having circulated since ancient history (Zwierlein and de Graaf, 2013), social media has given such theories a greater reach (Bartlett and Miller, 2010). The growth in conspiracy theories has been associated with negative outcomes in health, democratic citizenship, intergroup relations and the possibility of inspiring direct acts of violence (Jolley et al., 2022). Indeed, social media has even been the theatre in which new conspiracy theories have developed, such as QAnon, which have been implicated in criminal acts of violence (Amarasingam and Argentino, 2020). Important themes emerged in the conspiracy theory content picked up in the data for this study– for example, antisemitic conspiracy theories deploying common tropes about a Jewish financial conspiracy controlling the world. Social media has been examined from the perspective of being a key place where antisemitic conspiracy theories have re-emerged and been propagated (Allington and Joshi, 2020; Allington et al., 2021). However, the ephemeral nature of the data on Snapchat poses questions about how the security dynamics of conspiracy theories can be understood in a context where data disappears, making the tracking of the consumption and production of conspiracy theories more difficult.

## Conclusion: Digital vernacular security and appnography

The point of departure for this study was to seek to push the boundaries of vernacular security studies by furthering the methodological perspectives of critical security studies in light of the rapid rise of digital communications technologies thus far in the 21st century. In particular, these advances in communications technologies offer enormous potential to investigate how citizens 'construct and describe experiences of security and insecurity in their own vocabularies, cultural repertoires' (Croft and Vaughan-Williams, 2017: 22). While critical security studies has come under criticism from within for its tendency to prioritize being critical over methodological rigour (Salter and Mutlu, 2013), much important work has been done to advance both the methods and methodologies of the critical schools of security studies (Aradau et al., 2015; Salter and Mutlu, 2013). However, both vernacular security studies and the critical schools of security studies require further innovation and progression to keep pace with the rapidly changing digital sphere. Proposing the development of an appnography to take into account the proliferation of mobile applications is an attempt to do this, but one that comes with some significant challenges.

Digital research using an appnography is not a simple process, however, and this article has attempted to foreground some of the key issues that digital research presents for the critical security studies scholar. Data access has always been problematic, and sometimes expensive, for researchers from a range of disciplines (Ahmed, 2021). The example here reinforces this, because Snapchat is based upon a model where data is 'self-destructing' (Bayer et al., 2016) and cannot be captured en masse in the same way as from platforms such as X, which have enabled some digital forays into vernacular security and critical terrorism studies (Downing et al., 2022). This has broader applications for a range of social media app-based platforms, such as Grindr, TikTok and Telegram, that present scholars with significant data access problems. Access, however, was not the only issue encountered here, as the ethics of doing digital research, especially in the security context, is not straightforward. While netnography presents itself as a method that can be used totally online without interacting with offline populations (Kozinets, 2002), and such passive approaches are well documented (Alavi et al., 2010; Gilchrist and Ravenscroft, 2011; Langer and Beckman, 2005), they present significant ethical concerns. The present study has attempted to overcome some of these ethical problems by both anonymizing all data and waiting for publication until after the data had been automatically deleted by the company's servers. However, it is important to note that the ethical questions presented by the use of the appnographic approach are not completely settled and scholars doing digital research into vernacular security studies are advised to carefully consider the ethical implications of their research both before, during and after the data collection phases and the possible impacts of research on participants.

In the detailed 'nuts-and-bolts' description of the appnographic approach, this article has sought to offer scholars from both critical security studies and, indeed, a wider set of disciplines insights into how the methodological openness of both vernacular security studies and the broader critical turn has enabled such methodological innovation. In particular, foregrounding the need for methods and methodological experimentation and reflection (Aradau et al., 2015, 2019) has been a vital foundation upon which to build this methodological approach. Within this, adopting the practice of field notes from ethnography and, by extension, netnography enabled this investigation to overcome the issues presented by Snapchat's features of self-destructing data, but also the problems created by its notification system that informs users when screenshots are taken of their posts. This combination of passive digital observation and somewhat 'analogue' data collection in the form of field notes demonstrates how methodological experimentation and openness provided by critical security studies can help scholars overcome some of the challenges posed by the online, digital sphere.

While this study's contribution is primarily in the field of developing critical security studies methods, it is important to also demonstrate that such time-intensive methodological work can offer some conceptual and empirical innovation in understanding vernacular security studies and, in particular, how the previously neglected voices from below that seek to foster insecurity express themselves. Important in methodological reflection is considering the ways in which multimodal, unmediated user-generated content can be better integrated into vernacular security studies' understandings of security discussions. The most frequent theme recorded in the data was drug dealing; however, this highlighted two important discussions on the ways in which voices from below are constructing (in)securities on Snapchat. The multimodal output possible with such applications allowed individuals to showcase interesting ways in which they subvert and reimagine popular cultural idioms such as characters from TV shows, and indeed local, geographical urban landmarks such as churches when discussing (in)security. These are important possible veins of future research that vernacular security studies can pick up on.

Within and alongside this, the study also highlighted how commercial and business strategies such as branding and special offers become intertwined with security discourses. Future directions in both vernacular security studies and critical security studies would do well, especially in today's increasingly commercial world, to consider how concepts and practices such as branding can help understand how (in)security is constructed. This uncovered an important means to digitally investigate an aspect of insecurity that has been central to both the image (Mah, 2014) and the actual practice (Pujol, 2016; Sellami, 2016) of (in)security in Marseille in the past decades.

Finally, the app's key feature of ephemeral, self-destructing data made it all the more concerning that this study uncovered Snapchat as a means whereby users can utilize the multimodal creation tools of the app to adapt and share content on conspiracy theories on a platform that is effectively unmonitorable.

## Funding

The author received no financial support for the research, authorship, and/or publication of this article.

## ORCID iD

Joseph Downing https://orcid.org/0000-0001-7173-8043

## Notes

1. Snapchat was developed in the USA, released in 2011. It has 406 million daily users creating an estimated 5 billion 'snaps' per day in 2024, ranking it as globally the ninth most popular social media app (Shepherd, 2024). It allows users multiple functions, including private messaging. However, the main function is to send 'snaps' – either a still photo or a 10-second video. These are sent to, depending on account settings, a closed network of friends you have added, or anyone that has added your account using your unique username. These snaps are deleted from the application's servers after 24 hours whether they have been viewed or not.
2. 'Bricolage' is a French term roughly translatable as an ad-hoc 'improvisation', 'do it yourself' approach.

## References

George N (2025) Imaging security from gender violence in the Pacific Islands: Rights and Rightfulness through a vernacular lens. *Security Dialogue* 56(5).

Ahmed W (2021) Using Twitter as a data source an overview of social media research tools. *Impact of Social Sciences*. Available at: https://blogs.lse.ac.uk/impactofsocialsciences/2021/05/18/using-twitter-as-a-data-source-an-overview-of-social-media-research-tools-2021/ (accessed 10 July 2024).

Alavi S, Ahuja V and Medury V (2010) Building participation, reciprocity and trust: Netnography of an online community of APPLE using regression analysis for prediction. *Apeejay Business Review* 11(1): 82–96.

Aldridge J and Décary-Hétu D (2014) Not an 'Ebay for drugs': The cryptomarket 'silk road' as a paradigm shifting criminal innovation. *SSRN*. Available at: https://papers.ssrn.com/abstract=2436643 (accessed 10 July 2022).

Allington D, Buarque B and Barker Flores D (2021) Antisemitic conspiracy fantasy in the age of digital media: Three 'conspiracy theorists' and their YouTube audiences. *Language and Literature* 30(1): 78–102.

Allington D and Joshi T (2020) 'What others dare not say': An antisemitic conspiracy fantasy and its YouTube audience. *Journal of Contemporary Antisemitism* 3(1): 35–54.

Amarasingam A and Argentino MA (2020) The QAnon conspiracy theory: A security threat in the making? *Combating Terrorism Center at West Point* 13(7): 37–46.

Aradau C, Blanke T and Greenway G (2019) Acts of digital parasitism: Hacking, humanitarian apps and platformisation. *New Media & Society* 21(11–12): 2548–2565.

Aradau C, Huysmans J, Neal A and Voelkner N (2015) *Critical Security Methods: New Frameworks for Analysis*. The New International Relations Series. Abingdon: Routledge.

Bakken SA (2021) Drug dealers gone digital: Using signalling theory to analyse criminal online personas and trust. *Global Crime* 22(1): 51–73.

Bartlett J and Miller C (2010) The power of unreason: Conspiracy theories, extremism and counter terrorism. *Demos*. [online]. Available at: https://westernvoice.net/Power%20of%20Unreason.pdf (accessed 10 July 2024).

Bayer JB, Ellison N and Schoenebeck S (2016) Sharing the small moments: Ephemeral social interaction on Snapchat. *Information, Communication & Society* 19(7): 956–977.

Bennett WL and Segerberg A (2012) The logic of connective action. *Information, Communication & Society* 15(5): 739–768.

Bigo D and McCluskey E (2018) What is a PARIS approach to (in)securitization? Political anthropological research for international sociology. In: Gheciu A and Wohlforth WC (eds) *The Oxford Handbook of International Security*. Oxford: Oxford Academic, 116–130.

Bubandt N (2005) Vernacular security: The politics of feeling safe in global, national and local worlds. *Security Dialogue* 36(3): 275–296.

Buzan B, Waever O and Wilde J (1997) *Security: A New Framework for Analysis*. Boulder, Colorado: Lynne Rienner Publishers.

Caraway B (2018) Collective action frames and the developing role of discursive practice in worker organisation: The case of OUR Walmart. *Work Organisation, Labour and Globalisation* 12(1): 127–124.

Coomber R, Childs A, Moyle L and Marratt M (2023) Social media applications and 'surface web' mediated supply of illicit drugs: Emergent and established market risks and contradictions. In: Tzanetakis M and South N (eds) *Digital Transformations of Illicit Drug Markets: Reconfiguration and Continuity*. Leeds: Emerald Publishing Limited, 15–28.

Costello L, McDermott M and Wallace R (2017) Netnography: Range of practices, misperceptions, and missed opportunities. *International Journal of Qualitative Methods* 16(1): 1–11.

Croft S and Vaughan-Williams N (2017) Fit for purpose? Fitting ontological security studies 'into' the discipline of International Relations: Towards a vernacular turn. *Cooperation and Conflict* 52(1): 12–30.

de Silva R and Crilley R (2016) 'Talk about terror in our back gardens': An analysis of online comments about British foreign fighters in Syria: Critical Studies on Terrorism. *Critical Studies on Terrorism* 10(1): 162–186.

Demant J and Bakken S (2019) Technology-facilitated drug dealing via social media in the Nordic countries. Available at: https://www.euda.europa.eu/drugs-library/technology-facilitated-drug-dealing-social-media-nordic-countries_en (accessed 26 May 2025).

Demant J, Bakken S, Oksanen A and Gunnlaugsson H (2019) Drug dealing on Facebook, Snapchat and Instagram: A qualitative analysis of novel drug markets in the Nordic countries. *Drug and Alcohol Review* 38(4): 377–385.

Downing J (2021) Memeing and speaking vernacular security on social media: YouTube and Twitter resistance to an ISIS Islamist terror threat to Marseille, France. *Journal of Global Security Studies* 6(2): 1–17.

Downing J, Gerwens S and Dron R (2022) Tweeting terrorism: Vernacular conceptions of Muslims and terror in the wake of the Manchester Bombing on Twitter. *Critical Studies on Terrorism* 15(2): 239–266.

Edwards A and Gill P (2002) The politics of 'transnational organized crime': Discourse, reflexivity and the narration of 'threat'. *The British Journal of Politics and International Relations* 4(2): 245–270.

Etikan I (2016) Comparison of snowball sampling and sequential sampling technique. *Biometrics & Biostatistics International Journal* 3(1): 00055.

Evans C and da Silva R (2023) #ShamimaBegum: An analysis of social media narratives relating to female terrorist actors. *Politics* 43(3): 351–368.

Fisher J and Leonardi C (2021) Insecurity and the invisible: The challenge of spiritual (in)security *Security Dialogue* 52(5): 385–400.

George N (2017) Policing 'conjugal order': Gender, hybridity and vernacular security in Fiji. *International Feminist Journal of Politics* 19(1): 55–70.

Gilchrist P and Ravenscroft N (2011) Paddling, property and piracy: The politics of canoeing in England and Wales. *Sport in Society* 14(2): 175–192.

González MC (2003) An ethics for postcolonial ethnography. In: Claire RP (ed.) *Expressions of Ethnography: Novel Approaches to Qualitative Methods*. Albany, NY: SUNY Press, 77–86.

Goodman LA (1961) Snowball sampling. *The Annals of Mathematical Statistics* 32(1): 148–170.

Hansen L (2006) *Security as Practice: Discourse Analysis and the Bosnian War*. Abingdon: Routledge.

Hansen L (2011) Theorizing the image for Security Studies: Visual securitization and the Muhammad cartoon crisis. *European Journal of International Relations* 17(1): 51–74.

Howell A and Richter-Montpetit M (2020) Is securitization theory racist? Civilizationism, methodological whiteness, and antiblack thought in the Copenhagen School. *Security Dialogue* 51(1): 3–22.

Huff A (2017) Black sands, green plans and vernacular (in)securities in the contested margins of southwestern Madagascar. *Peacebuilding* 5(2): 153–169.

Huysmans J (2011) What's in an act? On security speech acts and little security nothings. *Security Dialogue* 42(4–5): 371–383.

Jarvis L (2019) Toward a vernacular security studies: Origins, interlocutors, contributions, and challenges. *International Studies Review* 21(1): 107–126.

Jarvis L and Lister M (2012) Vernacular securities and their study: A qualitative analysis and research agenda. *International Relations* 27(2): 158–179.

Jolley D, Marques M and Cookson D (2022) Shining a spotlight on the dangerous consequences of conspiracy theories *Current Opinion in Psychology* 47: 101363.

Kalyan R (2020) Decolonising visual ethnography: A transdisciplinary intervention. In: Choi S, Selmeczi A and Strausz E (eds) *Critical Methods for the Study of World Politics: Creativity and Transformation*. Abingdon: Routledge, 161–177.

King KE (1994) Method and methodology in feminist research: What is the difference? *Journal of Advanced Nursing* 20(1): 19–22.

Koetsier J (2020) There are now 8.9 million mobile apps, and China is 40% of mobile app spending. Available at: https://www.forbes.com/sites/johnkoetsier/2020/02/28/there-are-now-89-million-mobile-apps-and-china-is-40-of-mobile-app-spending/ (accessed 12 May 2025).

Kozinets RV (2002) The field behind the screen: Using netnography for marketing research in online communities. *Journal of Marketing Research* 39(1): 61–72.

Kozinets RV and Gretzel U (2024) Netnography evolved: New contexts, scope, procedures and sensibilities. *Annals of Tourism Research*. 104: 103693.

Langer R and Beckman SC (2005) Sensitive research topics: Netnography revisited. *Qualitative Market Research: An International Journal* 8(2): 189–203.

Leroux L (2023) Drug crime: 2023 was Marseille's deadliest year. *Le Monde.fr*. Available at: https://www.lemonde.fr/en/france/article/2023/12/27/narcobanditry-2023-marseille-s-deadliest-year_6378791_7.html (accessed 31 May 2025).

Lobo-Guerrero L (2013) Wondering as a research attitude. In: Salter MB and Mutlu CE (eds) *Research Methods in Critical Security Studies: An Introduction*. London: Routledge, 25–28.

Mah A (2014) *Port Cities and Global Legacies - Urban Identity, Waterfront Work, and Radicalism*. London: Palgrave.

McGregor SLT and Murnane JA (2010) Paradigm, methodology and method: Intellectual integrity in consumer scholarship. *International Journal of Consumer Studies* 34(4): 419–427.

Moyle L, Childs A, Coomber R, et al. (2019) #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy* 63(1): 101–110.

Naidoo L ed. (2012) *An Ethnography of Global Landscapes and Corridors*. InTech. doi:10.5772/586.

Orock RTE (2014) Crime, in/security and mob justice: The micropolitics of sovereignty in Cameroon. *Social Dynamics* 40(2): 408–428.

Owens H (2025) A politics of living (in)security: The case for decentring security through spatial ethnographies in Vernacular Security Studies. *Security Dialogue* 56(5).

Oyawale A (2022) The impact of (counter-)terrorism on public (in)security in Nigeria: A vernacular analysis. *Security Dialogue* 53(5): 420–437.

Poltash NA (2012) Snapchat and sexting: A Snapshot of baring Your Bare essentials. *Richmond Journal of Law & Technology* 19(4): 1–24.

Pujol P (2016) *La Fabrique du monstre*. Paris: Les Arènes.

Risør H (2010) Twenty hanging dolls and a lynching: Defacing dangerousness and enacting citizenship in El Alto, Bolivia. *Public Culture* 22(3): 465–486.

Salter MB (2013) The Ethnographic turn: An introduction. In: Salter MB and Mutlu CE (eds) *Research Methods in Critical Security Studies*. Abingdon: Routledge, 51–58.

Salter MB and Mutlu CE (2013) *Research Methods in Critical Security Studies*. Abingdon: Routledge.

Sellami S (2016) Le vrai visage du narco-banditisme à Marseille. *Le Parisien*. Availible at: https://www.leparisien.fr/faits-divers/le-vrai-visage-du-narco-banditisme-a-marseille-02-05-2016-5760745.php (accessed 30 May 2025).

Shepherd J (2024) 25 Essential Snapchat statistics you need to know in 2024. Available at: https://thesocialshepherd.com/blog/Snapchat-statistics (accessed 12 May 2025).

Squire V (2013) Attuning to mess. In: Salter MB and Mutlu C (eds) *Reseach Methods in Critical Security Studies*. Abingdon: Routledge. Available at: https://researchprofiles.herts.ac.uk/en/publications/a-politics-of-living-insecurity-the-case-for-decentring-security-

Stritzel H (2012) Securitization, power, intertextuality: Discourse theory and the translations of organized crime. *Security Dialogue* 43(6): 549–567.

Stump JL and Dixit P (2013) Ethnography of the terrorist subject. In: Stump J and Dixit P (eds) *Critical Terrorism Studies: An introduction to research methods*. Abingdon: Routledge, 79–91.

Tunçalp D and Lê LP (2014) (Re)Locating boundaries: A systematic review of online ethnography. *Journal of Organizational Ethnography* 3(1): 59–79.

Utz S, Muscanell N and Khalid C (2015) Snapchat elicits more jealousy than Facebook: A comparison of Snapchat and Facebook use. *Cyberpsychology, Behavior, and Social Networking* 18(3): 141–146.

Vaterlaus JM, Barnett K, Roche C, et al. (2016) ‘Snapchat is more personal’: An exploratory study on Snapchat behaviors and young adult interpersonal relationships. *Computers in Human Behavior* 62: 594–601.

van der Sanden R, Wilkins C, Romeo JS, et al. (2021) Predictors of using social media to purchase drugs in New Zealand: Findings from a large-scale online survey. *International Journal of Drug Policy* 98: 103430.

Vaughan-Williams N and Stevens D (2016) Vernacular theories of everyday (in)security: The disruptive potential of non-elite knowledge. *Security Dialogue* 47(1): 40–58.

Zwierlein C and de Graaf B (2013) Security and conspiracy in modern history. *Historical Social Research* 38(1): 7–45.

Joseph Downing is author of “French Muslims in Perspective” (https://link.springer.com/book/10.1007/978-3-030-16103-3) and “Social Media and Security” (https://link.springer.com/book/10.1007/978-3-031-20734-1). He is senior lecturer in International Relations at Aston University where he teaches courses on security and the politics of technology. Previously he was fellow in nationalism in the European Institute, London School of Economics and Political Science, and Marie-Curie fellow at the Laboratoire méditerranéen de sociologie, CNRS, Université Aix-Marseille Marseille and the School of Oriental and African Studies, University of London.