SCANDINAVIAN JOURNAL OF MILITARY STUDIES

Military Security and Research Ethics: Using Principles of Research Ethics to Navigate Military Security Dilemmas

PRACTICE-ORIENTED ARTICLE

SØREN SJØGREN
JAKOB CLOD ASMUND
MAYA MYNSTER CHRISTENSEN
KARINA MAYLAND
THOMAS RANDRUP PEDERSEN
*Author affiliations can be found in the back matter of this article

SCANDINAVIAN MILITARY STUDIES

ABSTRACT

Collecting data and working with classified information in restricted military settings can present significant research challenges. Academic ideals of transparency and openness clash with the military's need for secrecy and closedness. This article engages with existing literature on security requirements and research ethics in discussing practical challenges researchers face in military research. Even though military security requirements and principles of research ethics are often perceived as opposites, they also share characteristics: both realms are context-driven, non-objective, and require professional judgment to assess. Through a four-part analysis corresponding to different steps in a research process, the authors develop a practice-oriented guide for researchers accessing and working with classified information in discussing mundane examples of how "insiders" with "privileged access" navigate between ethical research principles and security issues. The article also incites a broader debate on research governance, (self-)imposed restraints and the conditions for critical inquiry in the military domain.

CORRESPONDING AUTHOR:
Søren Sjøgren
Royal Danish Defence College, Denmark
sosj@fak.dk

KEYWORDS:
Research Ethics; Military Security; Secrecy; Classification; Research design

TO CITE THIS ARTICLE:
Sjøgren, S., Asmund, J. C., Christensen, M. M., Mayland, K., & Pedersen, T. R. (2024). Military Security and Research Ethics: Using Principles of Research Ethics to Navigate Military Security Dilemmas. *Scandinavian Journal of Military Studies*, 7(1), pp. 34–47. DOI: https://doi.org/10.31374/sjms.185

DOI: 10.31374/sjms.185

INTRODUCTION

A new security landscape after the Russian invasion of Ukraine in 2022 has sparked a renewed focus on military security. While the formal security provisions have not changed, their interpretation and observation have. This has consequences for military research. In light of this new perception of threat, academic virtues such as openness, transparency, and sharing knowledge with the public are brushed aside for security, secrecy, and closedness. It is also a truism amongst students at the Royal Danish Defence College (RDDC), to which the authors are affiliated, that one should avoid topics that might be classified. It is simply too much of a hassle to write a thesis about matters involving military security. Many theses, therefore, use public policy documents or unclassified foreign doctrine as their empirical data. We observe a similar tendency amongst faculty researchers who share stories of difficulties accessing military archives, documents, interviewees, or sites for fieldwork. The problem is that significant aspects of organisational life within restricted settings cannot be accessed. Similarly, we are sceptical that prior knowledge of what happens in classified settings can simply be bracketed in a research project by stating that one intends to use only unclassified empirical material to drive the analysis. Researchers holding a formal security clearance must reflect on potential security issues.

Still, researchers are sometimes allowed into military organisations and produce research based on observations in restricted settings that advance our understanding of the military profession. However, in the daily grind of the military organisation, somebody needs to make a case for this "bigger picture." In our experience, this will be the researcher's task. In this article, we ask how the researcher can navigate the ethical and security dilemmas of studying the military.

To answer this question, the article takes an autoethnographic approach, reflecting on our experiences researching the military. The authors of this article are affiliated with the RDDC and have worked with either formally classified material or gathered data in restricted security environments whilst aiming for publication in unclassified outlets. We all use qualitative data and rely on documents, images, interviews, and participant observation. Some of us are active-duty military officers, and others are civilian researchers affiliated with the RDDC; three of us are male, two are female. Our academic backgrounds also differ, but we are formally similarly positioned concerning our affiliation. Still, our experiences differ. While our position might be "privileged" regarding access to classified settings, it is not unproblematic.

While writing this article, we discussed the research process, from initial planning to dissemination. Our initial idea was to write an inspirational guide for students and faculty at staff colleges illustrated by a set of vignettes. To our surprise, our experiences researching and getting access to the military organisation vastly differed. Some of us have been asked to hand in interview guides, transcripts, and the final product for security review; some have never met such demands. Some of us have had commanders or other members of a given military organisation interfere in the dissemination phase; some interventions seemed legitimate, and others seemed to challenge our research integrity; most of us have had to re-negotiate access to our sources regardless of a formal acceptance of our research methods and access. An internal research seminar at the RDDC in 2023 based on a very early draft of this article floated even more stories, diverse approaches, challenges and occasionally dead ends related to security and ethics. Furthermore, very different attitudes and stances exist in our respective academic fields (military studies, sociology, anthropology, and philosophy) on broader methodological topics such as anonymisation, paternalism, reflexivity on our positionality, and the prudent level of research participants' involvement in the research process. When discussing "the methodological literature" as a form of coherent canon, we have continuously talked past each other. It simply does not exist.

These combined experiences lead us to conclude that there is not *one* process or *one* military protocol that researchers must follow, as Moore seems to imply (Moore, 2014, p. 126). Nor is it our experience that "the hierarchical nature of the military makes sure that once an order is given to provide access research instruments can be applied rather straightforwardly" (Ben-Ari & Levy, 2012, p. 15). Instead, various approaches exist, often conflating questions concerning military security and research ethics, which confuses both researchers and the military establishment. This article presents illustrative cases of that process. It exemplifies

DOI: 10.31374/sjms.185

how research ethics may be used to navigate military security dilemmas in military research summarised in a general guide rather than the authoritative manual that we envisioned. We advise researchers to continuously ask the question: how would a responsible ethical research practice look in the context of these (military security) demands?

We review the existing literature on military security and research ethics. Next, we present some methodological considerations of this article. After this, we present the research process in four phases related to the identified ethical and security issues. We conclude that working with classified information or collecting material in restricted environments is not impossible, but it does require special attention throughout the entire research process. And, when in doubt, we advise researchers to consult the ethical codes of conduct and ask how responsible ethical practices would look in this kind of setting.

MILITARY SECURITY AND RESEARCH ETHICS IN THE LITERATURE

Existing methodological literature in the form of handbooks and reference books on military sociology and military science does not address military security head-on (Caforio, 2006; Lindley-French & Boyer, 2014; Soeters et al., 2014; Sookermany, 2020; Williams et al., 2016). If addressed or recognised, it is one problem, amongst others, of outsiders gaining internal access to the organisation. This military security problem is often solved with a formal agreement ensuring that the researcher can only access unclassified information. Most of the methodological literature on military research arises from this outsider perspective. While there are still many questions regarding reflexivity, positionality, and research ethics in these cases, observing military security is easy since the military authority has taken on the entire task. However, it might have severe consequences for the research results if the organisation controls the empirical material. Other approaches ignore the question of military security, accepting that only unclassified policy documents or public statements can be used as empirical data.

The literature addresses the wider concept of "secrecy" and the problems of working with and in state agencies with "bureaucratic" secrets (De Goede et al., 2019; Lippert et al., 2016; Schwell, 2019). As one example of the genre, Schwell (2019, p. 86) discusses how one might navigate "difficult terrain" in which state entities are trying to protect bureaucratic secrets. Thus, her puzzle becomes how agencies try to control research and how those obstacles might become interesting empirical data while accepting that some public bureaucracies are and will probably remain both secretive and inaccessible. There is research that builds on data collection in restricted environments and is published in unclassified outlets. We have done this, and have seen others do it, too (King, 2019; Pedersen, 2021; Shakoor, 2023; Sjøgren, 2023b). But even this research rarely details how it came into being; it reports the findings.

So, the problem in the methodological literature is twofold. First, most literature arises from outsider perspectives, and the military authority determines entirely what can be collected. This makes the question of military security redundant since the military organisation has taken on the entire task. Second, research conducted on sites that are both secretive and inaccessible rarely accounts for all the work that takes place backstage – the negotiations, the demands for security reviews, and what had to be left out to comply with security issues to reach the level of unclassified academic publication (for the rare exceptions, see Shakoor, 2022, pp. 38–40; Storm Jensen, 2023, pp. 54; 77–83).

A related discussion is whether specific individuals have privileged access to understanding certain social phenomena. In the social sciences, this binary dichotomy between insiders and outsiders regarding privileged access to knowledge has been rejected in favour of the view that the individual is not a single status, but a status set existing somewhere in between (Griffith, 1998; Mercer, 2007; Merton, 1972; Wegener, 2012). The sociology of military research literature supports this understanding (Ben-Ari & Levy, 2012; Walker, 2016). While we agree at the theoretical level, we have found that the researcher's position as either insider or outsider directly implicates the level of access that can be granted to them, the questions that they can ask, and, ultimately, the research that can be carried out (see also Schwell, 2019, pp. 89–92).

A broader methodological and ethical debate also exists on the nature of "insider" or "embedded" research, which questions how critical one can be when they are an "insider" who is "embedded." We also noted a similar debate on the nature of closed or classified research.

DOI: 10.31374/sjms.185

We intend to park this broader discussion, since, pragmatically speaking, failure to comply with the demands of military security would mean that much of our research would not have been possible at all. The alternative would either be no research or only research from an outside standpoint. Our pragmatic approach aside, we also notice that critical methodological debates are taking place in other fields and thus call for a broader debate in the military domain on questions of research governance, (self-)imposed restraints, and the conditions for critical inquiry in military research.

A crucial first step is for researchers to reflect on how we navigate at times conflicting demands.

CONTEXT AND APPROACH

At the beginning of this project, we aimed to use our own experiences to write a guide to show how military security requirements overlapped with the demands of research ethics. The first author wrote a framework comparing ethics and security theoretically, inviting other researchers across the different institutes to contribute with shorter vignettes. To our surprise these vignettes did not neatly support the suggested framework. They differed and contradicted each other; we had all experienced difficulties balancing conflicting demands. However, we had experienced them at different stages and forms and developed our own ways of overcoming them. One key difference was how each of us were constructed as either insiders or outsiders and subsequently met by different demands by the military organisation. As already mentioned, we realised that there was not *one* process or *one* military protocol that researchers must follow (Moore, 2014, p. 126), nor that "the hierarchical nature of the military makes sure that once an order is given to provide access research instruments can be applied rather straightforwardly" (Ben-Ari & Levy, 2012, p. 15). In our combined experience, the validity of this claim concerns how one is constructed as an insider or an outsider; and this status may change during a project.

The project shifted into an autoethnographic-inspired approach that aimed at mapping and discussing these issues to understand the nuances, accepting that they were context-dependent, non-objective, messy and entangled based on our own experiences and that of our colleagues (Adams et al., 2015; Stahlke Wall, 2016). Thus, we did not aim to produce a narrative or autoethnographic analysis *per se* but to use our combined experiences to talk back to the theoretical framework and show how the same security provisions and ethical principles were understood differently depending on the case. And from here, to develop a helpful guide. From the pool of vignettes, we chose those most illustrative of the problems we, our students, and our fellow researchers have encountered. We organised our discussion of them into a chronological order of when the researcher typically met them in the research process and linked these experiences to the relevant security and ethics considerations. However, the four-step linear process we present below is an ideal that makes comprehension easier, not necessarily how research projects unfold in reality.

THINKING THROUGH A RESEARCH PROJECT

The following will present the main problems arising in military research. We use small cases in our presentation to underline that questions concerning military security and research ethics are socially constructed, negotiated, context-dependent, and require case-by-case reasoning. The quotes written in Italics are personal vignettes from our research, written for the purpose of this article. We also acknowledge impasses. Some forms of research might not be feasible, some descriptions might have to be left out if they are too revealing, and certain conclusions might warrant subsequent classification.

THE INITIAL PLANNING PHASE: WHAT MAY BE CLASSIFIED?

Any researcher approaching the military organisation, especially from the inside, must know the basic military security provisions. The subsequent question involving classified information is to understand what might be at stake and for whom. In our experience, both researchers and the military organisation struggle to separate questions of ethics and security. Therefore, we will briefly outline the differences. There are two different terms related to information: classified and sensitive (for an overview, see Table 1). The demands of labelling information

DOI: 10.31374/sjms.185

as classified or sensitive often overlap; in practice, they are often conflated, and some types of information belong in both realms.

Sensitive information is information whose release might harm the participant. It includes religious beliefs or racial or ethnic origin, for example. Handling sensitive data is an ethical principle under the heading "responsible conduct of research" (ALLEA, 2017; Ministry of Higher Education and Science, 2014). Data collection and management are also governed by the so-called GDPR law (European Parliament, Council of the European Union, 2016). Most researchers will recognise sensitive information, and most textbooks on research ethics and qualitative research methods will address it.

Classified information is information that might endanger national security. It requires a formal security clearance to work with it, and the researcher will be legally obliged to observe that classification is upheld. Military security aims to protect "against threats directed to personnel, materiel, information, information- and communications systems, operations, and establishments" (Forsvarskommandoen, 2023, p. 1–1). Thus, under the subtitle "Military Security," we can find everything from not disclosing the identity of military professionals to the required thickness for a weapon safe or the height of the fence protecting a restricted area. Military security is, therefore, an overarching concept. The most relevant elements related to research are personal security, document security, information security, and operational security. And while we have explicitly referenced Danish security provisions, these are aligned with NATO's and, thus, the principles should be recognisable to Western militaries (NATO, 2020).

Table 1 The two realms of Military Security and Research Ethics.

MILITARY SECURITY	RESEARCH ETHICS
Purpose: To protect against threats to personnel, equipment, information, information and communications systems, operations, and establishments.	Purpose: To ensure and strengthen high-quality research, integrity should pervade all research phases
Regulated by: The National Defence Command, the Military Penal Code, and the criminal law.	Regulated by: National and Organisational Code of Conduct and GDPR.
Related terminology: • Classified information • Permission from authorities • Confidentiality as a legal principle • Formal security clearance • "Need-to-know" • Organisational or national interests • Data management	Related terminology: • Sensitive information • Consent from individuals • Confidentiality as ethics • Integrity • Curiosity • Personal interests of the participants and the researchers • Data management

The most basic principle in military security is the "need-to-know" principle. This implies that one is only allowed insight into the amount of classified information needed to fulfil one's task, assuming proper security clearance. The problem is that the researcher might not yet know what information is required to complete their inquiry. Researchers must develop a sense of prudence. They should ask themselves on an ongoing basis whether obtaining such information would advance the project. If the answer is yes, they (might) need to know.

The second principle is that the issuer of information classifies information, and only the issuer can declassify it. There is, however, no strict guide that describes what classified information is. It often depends on the situation. Typically, classified information tells about weaknesses, capabilities, or intelligence-gathering methods. The same goes for future operations or plans. Classification often becomes redundant after the operation. It is worth noting, for instance, the sheer amount of publicly available material on the invasion of Iraq in 2003 – the key here being that the authority who classified the materials in the first place has released them.

Classified written material is often relatively straightforward to handle. Outsiders without security clearance should not be given access to classified material. An insider can simply look at the header or footer of the document, read the classification, and act accordingly. And while we have emphasised that military security is constructed, context-dependent and requires judgement, classified written materials differ. Regardless of how they are obtained and how old they might be, they belong to the issuing authority and must be returned, destroyed,

DOI: 10.31374/sjms.185

or declassified in cooperation with that authority. Accordingly, they cannot be shared with third parties.

As an insider, particularly with a formal security clearance, researchers might get access to data collections with fewer hindrances. Here, the problems might come in reverse; when informants consider the researchers as insiders, they often pass on classified and sensitive information, assuming the researcher can handle this. This inevitably happens in participant observations of work in restricted environments. Researchers will need to know which realm different types of information belong in.

Interviews, field notes, and audio-visual data from participant observation are, therefore, trickier since the classification issue now resides with the individual researcher. One prudent approach is to classify one's raw field notes. If they are collected in a restricted setting, the notes are also restricted. The first round of de-contextualization might happen when the notes are transformed from paper notes to notes on the computer. Specific references to places and capabilities can be deleted, and the research participants can be anonymised. Instead of using names, rank or function can be disclosed, or perhaps a letter, a number, or a pseudonym to distinguish them from each other. In other settings, this first round of de-contextualisation needs to take place within the secured premises and the researcher may need two notebooks with different classifications. When analysing the material, the researcher must assess whether the analysis of classified material should warrant a classification or if it could be reformulated in a way that removes the need for classification. If not, the analysis must be classified and treated accordingly. Observations or dilemmas from classified settings could also be rephrased as more general or de-contextualised questions in a subsequent unclassified interview. Another option is simply to skip such concrete examples, accepting that observing military security does restrain what can be handled in unclassified outlets.

Classification requires judgement and the researcher must use and hone their professional judgement as well. This is best done by addressing the problems at the earliest stages of the project and discussing options with peers.

In summary:

- Know the difference between research ethics and military security. What might be at stake and for whom?
- Read the methods section of papers similar to what you intend to do. Focus on the practicalities!
- Go through the questions in a Data Management Plan (see DMP online: https://dmponline.deic.dk) and consider what needs to be added to comply with military security.

NEGOTIATING ACCESS: GETTING INTO THE ORGANISATION

Before asking for access, researchers must have reasonable ideas of handling and balancing the military's needs against their research interests. Securing institutional sponsorship is a practical and essential step in the process. In practice, this can be done by writing an email directly to the authority one wishes to gain access to and succinctly stating the project's ambitions, methods, and plans for dissemination. Oftentimes, the appropriate point of entry is the chief of staff, second in command, or military assistant, and it might work best to go through one's network. This inquiry aims to understand the organisation's concerns and thus enables the researcher to assess the risk before formally approaching the organisation. At times, it may be more prudent to approach individual research participants. Our advice doesn't change: Address military security and research ethics succinctly during the initial stages, so that research participants know exactly what they consent to. Our experience is that access is never settled once and for all. Researchers should expect continuous renegotiations with local gatekeepers who, as part of their job, are tasked with protecting information.

This is one practical issue of the insider/outsider construction described above. This distinction is neither binary nor set in stone. Researchers might be outsiders when applying for access but achieve insider status once inside the organisation. A researcher affiliated with a war college might be an insider holding a formal security clearance but still be positioned as an outsider and vice versa. We stress that the researcher's status will be continually reconstructed and renegotiated throughout the research process. Questions concerning access might re-emerge,

DOI: 10.31374/sjms.185

and obliging contacts might become critical. Mere affiliation with a war college, rank, military uniform, or veteran status does not warrant unlimited, unique, or privileged access. A lack of prior military affiliation or formal security clearance does not necessarily bar a researcher from entry; rather, researchers must show that they can comply with the demands of military security and research ethics.

While secrecy is often perceived as an obstacle to gaining access, we also propose that it can be productive to approach secrecy as an object of analysis. And while this might not be what the project set out to do, it might be what is possible. The first of our own vignettes illustrates this point:

> *In my research on military support for the police's counterterror operations in Denmark, secrecy has indeed been an issue that has caused delay and diversion. With an empirical focus on how the armed forces and the police interact, collaborate, and compete when assessing and responding to risks and security threats associated with terror and a more specific interest in exploring the role and use of armed forces in counterterror operations, my study touches on several sensitive and secretive issues.*
>
> *How and on what grounds are counterterror operations carried out, what material and capabilities are used, and why do some efforts fail or succeed is closely guarded information. If vulnerabilities are revealed and information falls in the wrong hands, it can jeopardise operational security and undermine future operations. But surprisingly, perhaps, difficulties in obtaining access to the field have mainly resulted from sensitivities related to inter-agency collaboration and different cultures of secrecy and approaches to classification in the police and the defence. Here, access to the field has depended on joint, cross-sectoral agreements with the Danish Defence Command, who delivers support for the joint operations, and with the Danish Security and Intelligence Service, who commands and takes operational responsibility for the joint operations.*
>
> *A critical point of departure for obtaining access to archival material and permission to conduct qualitative interviews with military operators deployed to counterterror operations has been a formal agreement with the Danish Defence Command, stipulating, among other issues, how to handle classified and sensitive personal information as well as procedures for internal processes of review before publication. In practice, however, access has depended mainly on more informal negotiations with central authorities acting as gatekeepers. The gate has never been fully open despite formal approval and long-term negotiations. For instance, the allowance to conduct qualitative interviews with military operators from the special forces has been given based on careful screening and subsequent adjustment of interview guides. It has been agreed that research outputs touching on operational issues shall be classified as "secret" and distributed only internally with selected stakeholders based on "need to know" principles* (personal vignette).

Instead of examining why the lack of access leads to failed research, we may ask, "What does mapping the contours of secrecy *add* to our analysis?" (De Goede et al., 2019, p. 3). Drawing inspiration from this shift in perspective – turning the barriers of secrecy and lack of access into the object of study – researchers could also view secrecy and the negotiations surrounding access as a productive departure point for exploring research questions. Approaching secrecy as relational (Barbour, 2017) and as a lens through which social interactions, exchanges, and distributions of power can be scrutinised (De Goede et al., 2019, p. 20), it becomes possible to illuminate the central practices and processes of collaboration, competition, and command that inform, in this case, joint operations. These practices and processes are, at least from an academic viewpoint, far more relevant to scrutinise than classified information on specific counterterror operations. The point we wish to make here is that while "getting past" the gatekeepers is most commonly regarded as an essential step in accessing the field and in accessing classified information, gatekeepers themselves, the secrets they protect, and how they protect them can be approached as sources of knowledge and as constitutive of the research field. Indeed, "field access is already an integral part of ethnographic research" (Schwell, 2019, p. 81). And while it might not be the research one intended to do, it might be what is possible in that context.

In summary:

- Understand the organisation's concerns and situation before you address the commander and ask for access. You will need to address the risk calculus. Remember that this negotiation of access is also empirical material.
- Do not assume that a security clearance, a uniform or prior service warrants unrestricted access, or that researchers outside the military are barred from access. Expect the insider/outsider construction to be never fully settled.
- There might be a need for a formal agreement between the military organisation, the researcher, and the researcher's institution.

DURING THE PROJECT: DO NO HARM

Protecting research participants is one theme during the project where military security and research ethics overlap. The military establishment is interested in protecting military research participants from the perspective of military security. Researchers are obliged by codes of conduct and GDPR to protect the identity of their participants under the general principle of "do no harm." In this way, the ability to protect one's participants relates to the level of confidentiality researchers can build with their participants. Anonymisation of research participants serves both military security and research ethics purposes, and it has practical implications for the quality of the qualitative data.

Fully anonymising qualitative research data is challenging. Anyone with intimate knowledge of our research settings will likely be able to recognise the participants and their surroundings (Saunders et al., 2015). Anonymisation must, therefore, be viewed as a continuum rather than a binary concept. And it must address both external and internal parties (Tolich, 2004). Ultimately, the fundamental question of anonymisation is: How much to remove, change, or abstract? What is "enough anonymisation"? In theory, "the data remaining after anonymisation tells us a story without telling whose story it is" (Thomson et al., 2005). We must balance data integrity and distortion against recognising and protecting our research participants.

It is often possible to anonymise research parties efficiently to external parties simply by assigning a different name (or letter or number) to research participants. This is known as pseudonymisation and is often required to comply with military security. Anonymising participants in a way that everyone from recognising participants ranges from difficult to downright impossible. Our experience is that if we make sure that our participants are protected through anonymisation from external parties, we have been compliant with both military security and research ethics. Still, the two realms should not be confused or conflated. Research participants in classified outlets aimed only at an internal audience should also be protected, not because of military security, which would be an issue in public outlets, but as an ethical principle of protecting their privacy. A military classification does not automatically solve ethical demands. Indeed, when the audience is smaller, or targeting the military profession directly, researchers should take even more care to protect the participants.

To underline the complexity of anonymisation, we will again turn to one of our own cases:

> *There was an issue with 1st Lieutenant (LT) Winter, one of my principal research participants. Had I anonymised him, or had I not? Had I, or had I not, used the 1st LT's real name in the manuscript I was preparing for publication? My point of contact in the Operations Staff of Defence Command Denmark, a usually very obliging lieutenant colonel, demanded to know. I was taken aback by the question and the firm tone of voice in which it was raised. What was going on?*
>
> *I had indeed anonymised 1st LT Winter. Why? Because we, as researchers, in terms of military security and research ethics, have a responsibility to protect the safety and privacy of our research participants. Moreover, I doubt that 1st LT Winter would have been willing to share his often personal and sensitive insights with me if I had not allowed for anonymisation. As such, anonymisation is an ethical practice and a methodological move enabling our research access and allowing our participants to share stories that would otherwise remain hidden. That said, by default, I initially offered the 1st LT (and my other participants) the option of non-anonymisation. It could be that 1st LT Winter did not want my protection and wished to be identifiable*

> *for reasons such as having his story or contribution recognised. Ultimately, none of my participants opted to be identifiable by their names. Still, no one objected to being identifiable by publishing their picture in different research outlets. Importantly, my guardians of military security, the Operations Staff in Defence Command Denmark, did not have an issue with the identifiability of my depicted participants, not as long as each participant in question provided me with their written consent.*
>
> *In the case of 1st LT Winter, I have made use of the most common form of anonymisation, namely pseudonymisation: I replaced the 1st LT's real name with a pseudonym, "Winter', thereby selecting a pseudonym that resonated with the 1st LT's cultural and religious background. Inadvertently, however, it turned out that Winter, which is not quite a common name in Denmark, happened to be the actual name of another Danish Afghanistan veteran. Hence, the abovementioned response by the lieutenant colonel. After all, he ensured I did not compromise military security by disclosing classified information. In addition to using pseudonyms, I have anonymised 1st LT Winter and other participants by introducing red herrings, that is, I have changed biographical elements, such as turning a Jutlander into a native of Funen, without changing the core of my ethnography. Furthermore, I have in a few cases, including the lieutenant colonel in this vignette, referred to my participants not by pseudonyms but by subject positions, e.g., rank and function, or by categories, such as age groups and geographical regions* (personal vignette).

Research takes time, and time helps with anonymisation if we choose to use subject positions. The lieutenant colonel in the case above would probably be challenging to identify, even for insiders. And still, disclosing rank and function is enough to understand how this person played a crucial role as a gatekeeper. As another example, one of us gathered our primary data in a military headquarters in 2020–21, but those data did not reach the publication stage before 2023. In 2023, few people even remember who served as G3 (current operations) during an exercise in 2021. In this case, the term "staff officer" proved enough to convey the meaning in the relevant context in the final publications (Sjøgren, 2023a).

While anonymisation should be the default choice, it is not always the right choice. It might be that the research participants want to be heard and do not want or need the protection the researchers offer them or that their case is so special that anonymisation would be impossible. Therefore, researchers should consult with participants and gatekeepers throughout the research process. The impact and desirability of anonymisation should be discussed with the research participant, including the possibility of using participants' actual names if they consent. And in military research, it might be that the military security organisation will override such consent and insist on anonymisation anyway as a condition for using the data or granting access. Facing such onerous demands, we again encourage the question: how would a responsible ethical research practice look in the context of these demands?

Protection of research participants also includes letting them know what they agree to if they participate in your research. The institutional solution to this problem often insists on written consent forms. However, in some situations, this might not be feasible. What is essential is not that the researcher collects signatures on paper but ensures that the participants know what they consent to. The written consent form might work well in in-person interviews and it might be required by the institution for online interviews as well. Either way, addressing what interviewees consent to should already be done in the initial email. Fieldwork and participant observation in actual working conditions is often much trickier. Let us again show an example:

> *My primary group informants were staff officers working in the headquarters I followed. During exercises, staff officers are heavily engaged in solving practical tasks required to fulfil their function. When I approached staff officers working at their desks, observed, or even engaged in a tactical discussion, they often seemed to answer me as a colleague in uniform rather than a researcher; they used the same military jargon, gave me access to their tools, and allowed me to sit in on meetings, assuming that I knew the ropes (which I did). Of course, I explained why I was there; I learned to keep this introduction very short. If not, I would be cut off. In such situations, continuous reminders of consent would destroy the rapport needed to gather empirical*

> *material in the headquarters. This is neither a problem of disclosure on my part nor of understanding on the staff officers' part but a practical problem of them being busy and me being respectful of their time. In one article, a similar description led one reviewer to comment that they hoped the participants knew they were participating in research. Did they? I think so, but I must also recognise that they were probably much more concerned with doing their jobs. Thus, protecting them became my job* (personal vignette).

The example above underlines how "insider" research or privileged access might produce new dilemmas. Insisting on getting a signature on a written consent form in this setting would derail the opportunity to collect empirical material in the headquarters. In such situations, we advise again to consider ethics in context. In this case, the researcher took care to anonymise the research participants, combining their expectation that an insider will "be able to handle what I tell you," as one participant put it, with the research principle of "do no harm." This extends to the subsequent analysis of the data. Handling data well also means that the participants' voices are heard, that we try to empathise with them, understand their worldview, and make sure their perspectives are understood.

In summary:

- When you approach research participants, explain briefly what they consent to, how they can opt-out later, and how data is managed, stored, analysed, and eventually deleted.
- Per default, active-duty personnel should be anonymised. In some cases, this might not be possible or appropriate.

AFTER THE PROJECT: YOUR CONCLUSIONS ARE YOURS

The issue of classification arises again in the dissemination phase. The researcher must again ask: are these findings classified? Curating open-source information into an analysis as a military researcher might also mean that the final product should be classified. Any sudden demand for classification in the dissemination phase must be weighed against public interest and research interest. Research should be open and unclassified unless one is tasked to report on a classified issue. Since classification is not binary, there is often room to present an argument even at this stage. However, in the military hierarchy, there is also an order at some point. For the insider, this is the equivalent of checkmate.

To illustrate this problem, we will turn to one of our own examples:

> *I had planned to convert my thesis into an article to provide input for the public debate concerning the subsequent defence agreement. Therefore, I used only open-source, unclassified information, as I wanted to share an unclassified product freely. After I handed in the thesis, I set about rewriting it into an article. Subsequently, my commander asked to read the article before it was submitted for peer review. My commander returned with a clear position: the article should be classified. Despite using open sources, an officer experienced in air defence made the analysis, in this case, me! I have detailed knowledge of weaknesses in the Danish Defence, which meant that the article sometimes confirmed unclassified information. Being an air defence officer in the Royal Danish Air Force, the analysis was on the edge of what I was allowed to write under the obligation of operational security. Suddenly, my article switched from having to be published in a recognised journal to being a classified document. In addition, I was asked not to share the article since my commander also wished to limit the distribution to selected persons within the Danish Defence.*
>
> *At that point, my options were limited. I started by rewriting the article into an unclassified version, this time in close dialogue with my commander, to ensure I didn't cross classification boundaries. The updated version became significantly shorter and far less attractive. Rather than provide specific knowledge about Denmark's air defence, the article was now more of a general text about what air defence is. This could just as well be read in doctrines and other teaching texts. At this point, it became clear to my commander and me that the article should remain in the classified version* (personal vignette).

DOI: 10.31374/sjms.185

The commander argued that they could not publish the article because it exposed too many weaknesses in Danish air defence. They claimed that the officer's background knowledge elevated the "unclassified" information and would make them vulnerable if published. Due to this, the author first tried to rewrite the work in more vague terms. Unsatisfied with how the generalised findings read, they eventually gave up, and the report remains classified.

The insider affiliated with a war college might be able to get their insights into the organisation in a classified format, either in a written report or in classified briefings. We have seldom experienced a direct order that dictates the classification of the final product – but it is not unthinkable, as shown above. Again, we advise researchers to think through the challenges ahead of the project, engage in a conversation, and present the argument if issues arise. Recall that issues of classification always rest on professional judgement. In this case, the earlier involvement of the commander might have prevented the subsequent conflict. In this phase, the researcher constructed as an insider might be left to their own devices while the outsider might have to submit transcripts and the final analysis for security review. There is not one clear answer to where this line must be drawn, and again, the researcher must develop a sense of prudence.

A variation of the problem above is the demand for "thick" descriptions in case studies. Some of us have been met by demands from reviewers and editors to provide more context for a particular discussion in a restricted setting – and, accordingly, have to state that this is impossible. The catch is that the researcher cannot explain in details why it is not possible to make thicker description, because that would include passing on classified information. We find that explaining that something is not possible with reference to military security is generally acceptable.

Finally, the hierarchical nature of the military organisation will sometimes confuse research with consultancy or plain staff work, leading commanders or other staff officers to try to interfere with the researcher's conclusions. This is a line researchers should not cross. In our experience, this is caused by misunderstandings about the nature of research more than bad intentions from those intervening. An example illuminates this tendency:

> *Following one of the first oral presentations after I had published the article, I was contacted by the commanding officer, who had initially accepted the project and agreed to the terms. The officer pointed to specific findings in my presentation, with which he disagreed and insisted that those specific claims and conclusions should be left out of future presentations. We had a long conversation where I substantiated and expanded my claims based on the theoretical framework, empirical findings, and arguments. Also, I pointed out that once data is interpreted and analysed, it is the property of the researcher and not for the organisation to decide upon.*
>
> *I did not change my conclusions or presentation but was even more meticulous in explaining my findings and theoretical and methodological design in conducting future presentations. In the research design phase, I focused on the meso level to move beyond individual sensitivity and focus on the cultural and institutional embedded collective. Even so, the findings and conclusions of the project proved to be highly sensitive to individuals in the organisation* (personal vignette).

With this description, we want to underline that critical inquiry in the military organisation is possible; it must be! The alternative would undermine our research integrity. While we advocate cooperation and the alignment of interests concerning military security and ethics, the military organisation should not interfere with the researchers' conclusions. The organisation might disagree with the analysis – just as any other might. However, it cannot and indeed should not be allowed to interfere with conclusions. Still, as noted above, we sometimes experience this pressure. A good way to avoid mutual confusion is to be very clear on the terms of the cooperation before the project is initiated. The researchers' institutions will often be helpful and interested in this phase.

The reader might notice that our story above does not hold any military security issues, per se. However, we also see a risk for such disagreements to be recast as a security concern. This move shifts the burden of proof from a relatively clear-cut case of preserving research integrity to one of military security, which gains priority and tends to marginalise the researcher's

concerns. The key in such cases is to differentiate between the two realms: military security and research ethics. What has changed since the project's conception? If the problem is that the organisation is not entirely satisfied with the conclusions or that they contradict official statements or policy, recasting it as a security concern is a deceptive tactic and should be countered with the help of the researcher's institution. However, as the air defence case showed, it might be a legitimate claim.

In summary:

- Protect your integrity; your conclusions are yours.
- The authority that granted access could be offered to read the final products.
- Consider classifying the final product or cut details, but only as a last resort.

CONCLUSION: THINKING THROUGH PREMISES AND DILEMMAS

In this article, we have presented the central tenets of military security and discussed ethics and military security concerns in specific contexts using a handful our of examples. They make apparent how different the challenges related to research ethics and military security can be. We have also shown how even experienced researchers and military professionals can sometimes reach research impasses. Questions concerning who has constructed the impasse, or how it can be made into an object of analysis, are relevant and worth pursuing. We must also acknowledge that classification and access are grey zones, and our best advice is to think it through, share concerns with peers, and present arguments to the authority that needs to grant access.

Our general advice is to consider research ethics and military security questions related to the specific project before embarking on military research. Researchers should ask themselves how an ethical research practice would look in this (classified) context.

Setting our pragmatic approach aside, we also observed significant methodological discussions in various other fields. There might be methodological questions in military research worth pursuing; could this alignment of interests that we advocate as a pragmatic approach lead to self-censorship or less critical inquiries to maintain a good relationship? How critical can one be of one's own? And what would that mean to the possibility of future research projects? As a result, we are calling for a more extensive debate on methodological approaches in military research. It should address the challenges of working in restricted settings, research governance, and (self) imposed constraints. An essential first step is to discuss our challenges more openly.

APPENDIX: RESEARCH ETHICS AND MILITARY SECURITY GUIDELINE

The initial planning phase	• Familiarise yourself with research ethics as stated in the code of conduct and the provisions for military security. What might be at stake for whom? • Read the methods sections of research similar to what you intend to do. Focus on practicalities! • Go through the questions in a Data Management Plan (see DMP online: https://dmponline.deic.dk). Consider the need for additional questions related to military security.
Negotiating access	• Understand the organisation's concerns and situation before you address the commander and ask for access. You will need to address the risk calculus. Remember that this negotiation of access is also empirical material. • Do not assume that a security clearance, a uniform or prior service warrants unrestricted access, nor that researchers outside the military are barred from access. Expect that the insider/outsider construction is never fully settled. • There might be a need for a formal agreement between the military organisation, the researcher, and the researcher's institution.
During the project	• When you approach research participants, explain briefly what they consent to, how they can opt-out later, and how data is managed, stored, analysed, and eventually deleted. • Per default, active-duty personnel should be anonymised. In some cases, this might not be possible or appropriate.
After the project	• Protect your integrity; your conclusions are yours. • The authority that granted access could be offered to read the final products. • Consider classifying the final product or cut details, but only as a last resort.

ACKNOWLEDGEMENTS

The authors would like to thank Rasmus Dahlberg and Jeanette Serritzlev at RDDC for commenting on the very first draft, and Thomas Vladimir Brønd and Jesper Hein Olsen, also RDDC, for their thoughtful comments at the internal RDDC research seminar, which floated even more stories and diverse ways of navigating conflicting demands among the research faculty.

COMPETING INTERESTS

Søren Sjøgren has, since this article's submission, stepped in as editor of the Scandinavian Journal of Military Studies.

AUTHOR AFFILIATIONS

Søren Sjøgren orcid.org/0000-0002-7299-9752
Royal Danish Defence College, Denmark

Jakob Clod Asmund orcid.org/0000-0001-8186-2080
Royal Danish Defence College, Denmark

Maya Mynster Christensen orcid.org/0000-0003-3424-8584
Royal Danish Defence College, Denmark

Karina Mayland
Royal Danish Defence College, Denmark

Thomas Randrup Pedersen orcid.org/0000-0002-9426-4618
Royal Danish Defence College, Denmark

REFERENCES

Adams, T. E., Holman Jones, S., & **Ellis, C.** (2015). *Autoethnography*. Oxford University press. https://books.google.dk/books/about/Autoethnography.html?id=ygV_BAAAQBAJ&redir_esc=y. DOI: https://doi.org/10.4324/9781315427812

ALLEA. (2017). *The European Code of Conduct for Research Integrity Revised Edition*. ALLEA – All European Academies.

Barbour, C. (2017). *Derrida's secret: Perjury, testimony, oath*. Edinburgh University Press. DOI: https://doi.org/10.1515/9781474425018

Ben-Ari, E., & **Levy, Y.** (2012). Getting Access to the Field. In *Routledge Handbook of Research Methods in Military Studies*. Routledge. DOI: https://doi.org/10.4324/9780203093801.ch2

Caforio, G. (Ed.). (2006). *Handbook of the sociology of the military*. Springer. DOI: https://doi.org/10.4324/9780429398186

De Goede, M., Bosma, E., & **Pallister-Wilkins, P.** (2019). *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork* (1st ed.). Routledge. DOI: https://doi.org/10.4324/9780429398186

European Parliament, Council of the European Union. (2016). *Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Forsvarskommandoen. (2023). *Bestemmelser for den militære sikkerhedstjeneste FKOBST 358-1*. The Danish Defence Command (DCD)/Forsvarskommandoen.

Griffith, A. I. (1998). Insider/Outsider: Epistemological Privilege and Mothering Work. *Human Studies*, *21*(4), 361–376. DOI: https://doi.org/10.1023/A:1005421211078

King, A. (2019). *Command: The twenty-first-century general*. Cambridge University Press. DOI: https://doi.org/10.1017/9781108642941

Lindley-French, J., & **Boyer, Y.** (Eds.). (2014). *The Oxford handbook of war* (1. publ. in paperback). Oxford Univ. Press.

Lippert, R. K., Walby, K., & **Wilkinson, B.** (2016). Spins, Stalls, and Shutdowns: Pitfalls of Qualitative Policing and Security Research. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *17*(10).

Mercer, J. (2007). The challenges of insider research in educational institutions: Wielding a double-edged sword and resolving delicate dilemmas. *Oxford Review of Education*, *33*(1), 1–17. DOI: https://doi.org/10.1086/225294

Merton, R. K. (1972). Insiders and Outsiders: A Chapter in the Sociology of Knowledge. *American Journal of Sociology*, *78*(1), 9–47. DOI: https://doi.org/10.1086/225294

Ministry of Higher Education and Science. (2014). *Danish code of conduct for research integrity*. Ministry of Higher Education and Science.

Moore, B. L. (2014). In-depht interviewing. In J. Soeters, P. M. Shields, & S. Rietjens (Eds.), *Routledge Handbook of Research Methods in Military Studies* (1st ed.). Routledge.

NATO. (2020). *C-M(2002)49-REV1*.

Pedersen, T. R. (2021). Facing the Warrior: An Ethnographic Montage on Post-9/11 Warriorisation of Danish Military Professions. In A. R. Obling & L. V. Tillberg (Eds.), *Transformations of the Military Profession and Professionalism in Scandinavia*. The Scandinavian Journal of Military Studies Press. DOI: https://doi.org/10.31374/book2-e

Saunders, B., Kitzinger, J., & **Kitzinger, C.** (2015). Anonymising interview data: Challenges and compromise in practice. *Qualitative Research*, *15*(5), 616–632. DOI: https://doi.org/10.1177/1468794114550439

Schwell, A. (2019). Navigating Difficult Terrain. In M. De Goede, E. Bosma, & P. Pallister-Wilkins (Eds.), *Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork* (1st ed.). Routledge. DOI: https://doi.org/10.4324/9780429398186

Shakoor, T. R. (2022). *The Intelligence Cycle in Denmark: Unwinding and reconceptualising the Process of formulating Intelligence Requirements surrounding the Middle East in the Danish Defence Intelligence Service* [Syddansk Universitet. Det Samfundsvidenskabelige Fakultet]. https://portal.findresearcher.sdu.dk/en/publications/the-intelligence-cycle-in-denmark-unwinding-and-reconceptualising. DOI: https://doi.org/10.1080/08850607.2023.2193133

Shakoor, T. R. (2023). Unwinding the Intelligence Cycle in Denmark. *International Journal of Intelligence and CounterIntelligence*, 1–19. DOI: https://doi.org/10.1080/08850607.2023.2193133

Sjøgren, S. (2023a). War, PowerPoint, and hypnotised chickens. *STS Encounters*, *15*(2). DOI: https://doi.org/10.7146/stse.v15i2.139807

Sjøgren, S. (2023b). What we disagree about when we disagree about doctrine. *Journal of Strategic Studies*. DOI: https://doi.org/10.1080/01402390.2023.2251170

Soeters, J., Shields, P. M., & **Rietjens, S. J. H.** (Eds.). (2014). *Routledge handbook of research methods in military studies*. Routledge/Taylor & Francis Group. DOI: https://doi.org/10.4324/9780203093801

Sookermany, A. M. (Ed.). (2020). *Handbook of Military Sciences*. Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-02866-4

Stahlke Wall, S. (2016). Toward a Moderate Autoethnography. *International Journal of Qualitative Methods*, *15*(1), 160940691667496. DOI: https://doi.org/10.1177/1609406916674966

Storm Jensen, M. (2023). *Offensive Cyber Capabilities and Alliances: Questionable Assets for Prestige, New Risks of Entrapment* [Syddansk Universitet. Det Samfundsvidenskabelige Fakultet]. DOI: https://doi.org/10.21996/F1K8-7974

Thomson, D., Bzdel, L., Golden-Biddle, K., Reay, T., & **Estabrooks, C. A.** (2005). Central Questions of Anonymization: A Case Study of Secondary Use of Qualitative Data. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *6*(1, Art. 29), 18.

Tolich, M. (2004). Internal Confidentiality: When Confidentiality Assurances Fail Relational Informants. *Qualitative Sociology*, *27*(1), 101–106. DOI: https://doi.org/10.1023/B:QUAS.0000015546.20441.4a

Walker, D. (2016). Putting "Insider-ness" to work: Researching Identity Narratives of Career Soldiers About to Leave the Army. In A. Williams, K. N. Jenkings, M. F. Rech, & R. Woodward (Eds.), *The Routledge companion to military research methods*. Routledge, Taylor & Francis Group.

Wegener, C. (2012, August 29). *"Would you like coffee?" Using the researcher's insider and outsider positions as a sensitizing concept in a cross-organisational field study*. Liverpool, United Kingdom: Ethnographic Horizons in Times of Turbulence.

Williams, A., Jenkings, K. N., Rech, M. F., & **Woodward, R.** (Eds.). (2016). *The Routledge companion to military research methods*. Routledge, Taylor & Francis Group. DOI: https://doi.org/10.4324/9781315613253

TO CITE THIS ARTICLE:
Sjøgren, S., Asmund, J. C., Christensen, M. M., Mayland, K., & Pedersen, T. R. (2024). Military Security and Research Ethics: Using Principles of Research Ethics to Navigate Military Security Dilemmas. *Scandinavian Journal of Military Studies*, 7(1), pp. 34–47. DOI: https://doi.org/10.31374/sjms.185

Submitted: 28 October 2022
Accepted: 16 February 2024
Published: 05 March 2024

COPYRIGHT:
© 2024 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. See http://creativecommons.org/licenses/by/4.0/.

Scandinavian Journal of Military Studies is a peer-reviewed open access journal published by Scandinavian Military Studies.