The Blurring Politics of Cyber Conflict

A Critical Study of the Digital in Palestine and Beyond

Cristiano, Fabio

2022

Document Version:
Publisher's PDF, also known as Version of record

The Blurring Politics of Cyber Conflict

A Critical Study of the Digital in Palestine and Beyond

FABIO CRISTIANO
DEPARTMENT OF POLITICAL SCIENCE | LUND UNIVERSITY

The Blurring Politics of Cyber Conflict

The Blurring Politics of Cyber Conflict

A Critical Study of the Digital in Palestine and Beyond

Fabio Cristiano

LUND
UNIVERSITY

DOCTORAL DISSERTATION

by due permission of the Faculty of Social Sciences, Lund University, Sweden.
To be defended at the Department of Political Science, Eden hörsal, 2 June 2022 at 10:00.

Faculty opponent: Prof. Anna Leander, Geneva Graduate Institute

Organization LUND UNIVERSITY Department of Political Science Box 52 SE–221 00 Lund, Sweden	**Document name** DOCTORAL DISSERTATION **Date of disputation** 2 June 2022
Author Fabio Cristiano	

Title and subtitle
The Blurring Politics of Cyber Conflict: A Critical Study of the Digital in Palestine and Beyond

Abstract

This thesis explores how the politics of cyber conflict redefine violence, sovereignty, and territory in and through cyberspace. It does this by studying how the digital mediates different facets and experiences of conflict and security in Palestine. Through a comprehensive and context-informed approach, this research theorizes cyber conflict as a phenomenon spanning beyond the conventional sites, agencies, and categories of international cybersecurity and warfare. *Paper I* analyzes the game scenarios of international and national cyberwar exercises to understand how military strategists envision cyberwar and normalize the idea of cyberspace as a domain of warfare through the creation of simulacra of war. *Paper II* develops a disembodied perspective on the violence of cyber conflict by highlighting its harmful informational aspects through a reflection on how these have affected the process of knowledge production during the fieldwork of this dissertation. *Paper III* engages with the Palestinian national strategy for cybersecurity (and the lack thereof) to disentangle infrastructural/informational elements of the cyber/digital sovereignty narrative and reveal its emancipatory potential for actors other than the state. *Paper IV* interrogates the extent to which Israeli and Palestinian policies and strategies articulate cyberspace in territorial terms and reproduce its diverse spatial realities of annexation, occupation, and blockade in cyberspace. *Paper V* examines the relationship between conflict, technology, and freedom to critique the inclusion of internet access into the agenda on human rights by analyzing the political dynamics of connectivity in Palestine. *Paper VI* unravels how the video game's augmented reality of East Jerusalem constructs a spatial imaginary of the city that, by erasing the Palestinian urban space from digital representation, neutralizes the experience of play through a diminished reality. *Paper VII* explores how algorithms rearticulate security practices by making Palestinian users and contents hyper-visible to surveillance while also creating an aesthetics of disappearance through the erasure of Palestine from cyber and digital spaces. Through this comprehensive empirical approach, this research also contributes to cybersecurity scholarship by problematizing the epistemological relevance of traditional categories and thresholds of warfare and security for shedding light on the blurring politics of cyber conflict. Besides revealing the inadequacy of these categories, the study of cyber conflict in Palestine also shows how these ultimately affect political life and individual liberties via (the seizure of) the digital.

Keywords cybersecurity, cyberspace, violence, sovereignty, territory, infrastructure, digital rights, Palestine

Classification system and/or index terms (if any)

Supplementary bibliographical information	**Language** English
ISSN and key title 0460-0037 Lund Political Studies 206	**ISBN** 978-91-8039-260-0 (print) 978-91-8039-259-4 (electronic)
Recipient's notes	**Number of pages** 180
	Security classification

The Blurring Politics of Cyber Conflict

A Critical Study of the Digital in Palestine and Beyond

Fabio Cristiano

LUND
UNIVERSITY

Cover image by Filippo Minelli
Graffiti on the separation wall in Qalandia, Palestine.

Faculty of Social Sciences
Department of Political Science
Centre for Advanced Middle Eastern Studies

Lund Political Studies 206

ISBN 978-91-8039-260-0 (print)
ISBN 978-91-8039-259-4 (electronic)
ISSN 0460-0037

Printed in Sweden by Media-Tryck, Lund University, Lund 2022.

Media-Tryck is a Nordic Swan Ecolabel certified provider of printed material. Read more about our environmental work at www.mediatryck.lu.se
MADE IN SWEDEN

Ai miei genitori.

Contents

List of publications

I Cristiano, Fabio. "From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises." *Journal of War & Culture Studies* 11, no. 1 (2018): 22-37.

II Cristiano, Fabio. "Bodies of Cyberwar: Violence and Knowledge Beyond Corporeality." In *Experiences in Researching Conflict and Violence: Fieldwork Interrupted* (Policy Press, 2018): 15-32.

III Cristiano, Fabio. "Palestine: Whose Cyber Security Without Cyber Sovereignty?" In *The Routledge Companion to Global Cyber-Security Strategy* (Routledge, 2021): 418-426.

IV Cristiano, Fabio. "Deterritorializing Cyber Security and Warfare in Palestine: Hackers, Sovereignty, and the National Cyberspace as Normative." *CyberOrient* 13, no. 1 (2019): 28-42.

V Cristiano, Fabio. "Internet Access as Human Right: A Dystopian Critique from the Occupied Palestinian Territory." In *Human Rights as Battlefields: Changing Practices and Contestations* (Palgrave Macmillan, 2019): 249-268.

VI Cristiano, Fabio and Emilio Distretti. "Along the Lines of the Occupation: Playing at Diminished Reality in East Jerusalem." *Conflict and Society: Advances in Research* 3, no. 1 (2017): 130-143.

VII Cristiano, Fabio and Emilio Distretti. "Toward an Aesthetics by Algorithms: Palestinian Cyber and Digital Spaces at the Threshold of (In)visibility." In *The Aesthetics and Politics of the Online Self* (Palgrave Macmillan, 2021): 129-148.

The Blurring Politics of Cyber Conflict

1. *Introduction: aim and approach*

CYBER CONFLICT HAS COME, BUT NOT AS EXPECTED. Over the last three decades, cyberspace developed into a crucial frontier of international conflict, fierce geopolitical competition, and growing insecurity. States increasingly address the 'cyber domain' in their national security and military strategies, while international diplomacy stubbornly promotes shared norms of responsible state behavior in cyberspace through cooperation and multilateralism (Taddeo 2017). At the same time, expectations of state-fought and war-like conflicts generated in cyberspace have remained mostly unfulfilled. There exists ample evidence indicating that (dis-)information campaigns, espionage, and surveillance constitute the most common forms of conflict between states *in* and *through* cyberspace.

Rather than leading to the violent destruction of critical infrastructures or military targets, cyber operations most often feature low-intensity hacking and overwhelmingly pertain to the domain of information and its manipulation (Pawlak, Tikk, and Kerttunen 2020). It is also most often unclear whether these are conducted by states. Detecting sovereign characteristics — i.e., the extent to which a cyber operation can be attributed to a state — faces the challenge of a political agency that, in cyberspace, seems to blur through networks, anonymity/secrecy, automation, and merging boundaries between public and private. Moreover, the challenge of discerning which socio-material elements of cyberspace — from cables crossing the seafloor to the content visualized on our screens — are part of a country's national territory, and thus subject to its authority, represents an

additional element of ambiguity for understanding when and whether a cyber operation eventually targets/violates a country's national territory.

Despite these blurring categories, the idea that cyberspace constitutes a linear reproduction of the Westphalian international order of nation-states — with its inherent borders, anarchy, and propensity to war — seems not to have lost its appeal across theories and practices of *cybersecurity*. Military strategies, national policies, international diplomatic initiatives, and mainstream academic scholarship continue to envision conflict in cyberspace through the same essentialist war/security redux that dominated the field at the dawn of cyber scholarship (Demchak and Dombrowski 2011; Dunn Cavelty 2013; Lawson 2019).

To be clear, far from being a peaceful oasis, cyberspace represents a stage and an issue of international conflict, with states extensively engaged in safeguarding their sovereign and strategic interests through hacking and the manipulation of information. However, this conflict unfolds according to its peculiar and computational logic and socio-material mechanics, thus requiring a critical reconsideration of the lenses we use to understand and govern it. As argued in this dissertation, the blurring and emergent character of cyber conflict questions the appropriateness of the categories of war and peace to make sense of *what happens* in cyberspace. It has been argued that cyberspace features neither war nor peace but sets the international system in a permanent state of 'unpeace' (Kello 2017, 74).

The ambition to make sense of the *blurs* of cyber conflict has recently sparked a vibrant and critical academic debate that moves away from the traditional categories and thresholds of war and security. This dissertation shall be considered a contribution to this academic endeavor. At the same time, it aims at advancing the critique a step further. It wishes to understand how the perimeters of cyber conflict are constructed and experienced *politically*. This is done by engaging with cyber conflict as a phenomenon that spans beyond and occurs within international and national divides, and beyond warfare — thus comprising multiple *digital experiences of conflict and security*. As a result, this approach ultimately implies a problematization of the basic

empirical layered grammar of cyberspace: the one separating its infrastructural 'cyber' from the information and data it contains (Choucri and Clark 2019, 33-66; Cohen 2007).

With the ambition of exploring these blurring conceptual end empirical conundrums, this research studies the politics of cyber conflict in the context of *Palestine*. The Palestinian case offers unique empirical insights into cyber conflict's complex and comprehensive phenomenology and raises diverse theoretical and methodological interrogatives. Most importantly, the study of the digital in Palestine also illustrates that conflict in cyberspace and its governance through cybersecurity are fundamentally and uncompromisingly political. Against the backdrop of digital exceptionalism and universalism, or the technical mantras of policy expertise, conflict and security in cyberspace are rooted in their *contextual politics*. There, the digital remodulates conflict and security beyond the conventional sites, agencies, infrastructures, and categories of cybersecurity.

2. *Background and publications*

HOW DO WE RECOGNIZE CONFLICT IN CYBERSPACE WHEN WE SEE ONE? Scholars and policymakers have commonly recurred to the traditional categories and rhetoric of war and security to answer this question. In particular, the concept and narrative of *cyberwar* emerged initially as the dominant framework used to make sense of those — possible and unknown — events situated at the intersection of the 'virtuality' of cyberspace and the 'reality' of war (Arquilla and Ronfeldt 1993; Junio 2013; McGraw 2013). According to this perspective, this emergence from virtuality to reality depends on whether a cyber operation leads to the damage/destruction of physical infrastructures, becoming thus violent (Finlay 2018). Second, it needs to be conducted by a sovereign entity — a state or a proxy acting on its behalf (Maurer 2018). Third, it entails a territorial dimension, particularly

concerning the targeted country's authority over the damaged infrastructure or data/information.

Fitting the complex phenomenology of cyber conflict into the perimeters of this 'war redux' might work on paper, but the reality is always more complex than we want it to be. Cyber doom-like scenarios have not materialized, and it has since long become clear that such ideal-typical *cyberwar will not take place* (Rid 2013; Gartzke 2013). The concept of cyberwar has lost its appeal, slowly (too slowly?) fading away from the academic debate. At the same time, its underlying militarized, technical, legal, and securitizing logics and narratives have stayed. They continue to shape policies and influence security experiences while constantly reverberating across media — in connection to news-worthy cybersecurity incidents. Through cybersecurity governance, these narratives ultimately enter the digital experiences of conflict and security for users, and it is thus essential to engage with their political and historical genealogy.

In its early days, the study of cyber conflict emerged as an 'applied' discipline, theorized and developed across those Western academic circles with close ties to the military and policymaking (Dunn Cavelty 2007). At times when the 'war on terror' and pre-emptive doctrines dominated the military and security discourse, the so-called *digital revolution* entered national security and military strategies through the construction of new threats and the securitization of unknown and catastrophic futures in cyberspace (Dunn Cavelty 2013; Hansen and Nissenbaum 2009). In this context, national strategies blurred the national with the international and warfare with security in their construction of cyberspace as a strategic and policy domain (Saco 1999).[1]

Since 2013, the Snowden revelations, and the various global surveillance disclosures that followed, have opened the Pandora's box exposing how states have securitized cyberspace by blurring warfare, security, and surveillance in ways that also affect individual liberties and human rights

[1] The USA Patriot Act (2001) is an example of such development (Etzioni 2005).

(Deibert 2015). These Western-born militarized and securitizing approaches to cyberspace have 'traveled' all over the globe and are now the norm across the diverse policy domains dealing with cyber threats (Broeders, Cristiano, and Weggemans 2021). As a result, the cyberspace imagined by tech-utopians seems to be gone forever (if it was ever there).

This dissertation explores how *violence*, *sovereignty*, and *territory* define conflict in cyberspace outside the rigid frameworks of warfare and security, and vice versa. With this aim, this dissertation brings cybersecurity into conversation with other academic fields and perspectives: critical security studies, international political theory, peace and conflict studies, media and cybernetics scholarship, surveillance studies, human/urban geography, and science and technology studies (STS). This diverse scholarly approach sheds light on different empirical aspects of conflict in cyberspace and their contextual politics. The concept of cyber conflict shall thus be understood here as an umbrella term to conceal the multiple digital experiences of conflict and security studied across the different publications of this dissertation. Whereas usually studied unconnectedly, these different empirical entanglements constitute in this dissertation one comprehensive and context-informed research puzzle of conflict and security in cyberspace.

This dissertation proposes to solve this puzzle by looking at the politics of cyber conflict in Palestine, a context characterized by *blurring and highly contested political realities*. In Palestine, warfare and security continuously overlap and blur the conflict's local/national and international/global dimensions circularly (Collins 2011). Even 'before cyberspace,' the war/peace dichotomy had proved inadequate for capturing the somewhat intractable nature of conflict in Palestine. Scholarship on the conflict has since long pointed to the importance of contextual politics and narratives in the construction, operationalization, and contestation of categories such as violence, sovereignty, and territory in Palestine (Strömbom 2014).

The 'invention' of cyberspace seemed to represent an important and promising development for the Palestinian quest for freedom and justice insofar as it would allow, at the very least, to unsettle the status quo through

the liberating promise of digitalization. This dissertation shows that the current dystopic reality of Palestinian cyberspace questions these initial — and yet still dominating — techno-optimistic arguments about the internet's emancipatory potential for the Palestinian cause. Rather than enabling the escape (or hiding) from a highly securitized and militarized context by opening digital spaces of liberty, the digitalization of the Israeli-Palestinian conflict has instead exacerbated, through its expansion into the cyber realm, the asymmetry of the conflict. When studying the digital experiences of conflict and security in Palestine, it is essential to be reminded of Israel's role as a leading global power in commercial cybersecurity and surveillance technologies (Cristiano 2021). On these grounds, this dissertation studies the digital in Palestine through a critical awareness of how the making and branding of Israel as the 'start-up nation' directly affect the Palestinian experience of cyberspace in multiple ways (Senor and Singer 2011).

For the most part, scholarly work about cyber conflict has been blind to these aspects (Deibert 2018). Instead, it has primarily focused on the agency of states and on translating conventional warfare and security categories — i.e., weaponry, use of force, battlefield, and more — to the context of cyberspace. As a result, strategic, military, and legal academic perspectives dominate the field, while studies in international relations operate through the same state-centered epistemological perimeters. Empirically, this has implied a strong focus on studying cyber conflict as limited to cyber operations and strategies as variables used for 'assessing' state behavior in cyberspace and its legality — through an approach recently defined as 'cyber legalism' (Kello 2021).

In contrast to these dominant approaches to knowledge production, this dissertation broadens the study of cyber conflict to *what happens outside* the standard categories of warfare and security, thus digging into the broader socio-technical spectrum of digital experiences of conflict and security. The results of this comprehensive investigation are presented in seven different publications, here briefly outlined:

PAPER I analyzes the game scenarios of international and national cyberwar exercises to understand how military strategists envision and enable

cyberwar through the design of simulations, fictionally sketched in resemblance to conventional war. By prioritizing operational aspects over political ones, these game scenarios decisively move away from the actual phenomenology of cyber conflict to the point where they become 'simulacra of war.' This publication thus reveals how, through the characterization of cyberwar as the violent encounter between sovereign belligerents, these game scenarios ultimately normalize an understanding of conflict in cyberspace as a primarily techno-infrastructural and militarized phenomenon.

PAPER II explores the construction of violence as an element of cyber conflict. It provides a critical and reflective account of how violence has shaped this dissertation's research and fieldwork on Palestinian hackers. On the one hand, scholarship on cyber conflict conventionally envisions physical violence as a prerequisite for 'elevating' cyber operations to the status of war. On the other hand, policymakers and military strategists refer to the absence of such violence to argue for the desirability of offensive cyber strategies. The empirical work of this publication indicates that the violence of conflict in cyberspace goes beyond its kinetic and embodied infrastructural conceptualizations. Drawing on theories of embodiment, this publication shows how the absence of kinetic confrontation in cyber conflict does not imply the absence of violence *tout-court*. Instead, this very absence enables the emergence of a discursive and informational, nevertheless structural, violence which research on cyber conflict and practices of cybersecurity needs to account for.

PAPER III engages with the Palestinian national strategy for cybersecurity — and the lack thereof — to reflect on the concept of cyber/digital sovereignty. This publication shows how, with Israel in total control of the internet infrastructure, the Palestinian Authority (PA) and the Hamas administration seemingly retain limited sovereign functions in/about cyberspace. Whereas the PA's strategic approach takes the connotations of cybersecurity cooperation with Israel, Hamas extensively resorts to its cyber-wings to launch attacks aimed at breaking the Israeli digital blockade. Comparing these two different strategies reveals how the exercise of sovereignty in cyberspace entails more than controlling the physical/logical layers of the

infrastructure or service delivery. In this light, the Palestinian case offers essential empirical insights for detaching the concept of cyber/digital sovereignty from the political agency of the state and the dominant illiberal narratives on information security — this way revealing the concept's potential for critique and contestation.

PAPER IV analyzes how territoriality becomes an element of conflict and security in cyberspace. It does this by assessing whether the fragmented and diverse spatial realities across Palestine — annexation in East Jerusalem, occupation in the West Bank, and blockade in Gaza — can also be 'recognized' in cyberspace. This analysis reveals that these territorialization practices occur outside a normative and infrastructural understanding of the 'national cyberspace.' In this light, this publication ultimately argues that the processes of territorialization in/of cyberspace are not a function of infrastructural control, and instead, they are constructed dynamically — through both cybersecurity, hacking, and computational entanglements.

PAPER V engages with the relationship between conflict, technology, and freedom by critiquing the inclusion of internet access into the agenda on human rights. It does so by looking at how Israeli authorities, social media platforms/tech companies, the Palestinian Authority, and the Hamas government in Gaza recur to cybersecurity and information security for controlling and surveilling Palestinian users and content. In a context where 'being connected' signifies becoming a suspect, this publication shows how human rights' considerations about the 'open and free' internet cannot be only associated with accessing the infrastructure/technology. They also pertain to safeguarding the ways and the extent to which information and its circulation are owned, controlled, and securitized — thus exposing the ultimate liberal biases of the human rights agenda for the internet.

PAPER VI unravels the question of spatiality as an element of the encounter between conflict and digital representation. It does so through the case of the videogame Pokémon Go's augmented reality (AR). Drawing on walking sessions across the Green Line and the contested areas of East Jerusalem — Sheikh Jarrah, Silwan, Wadi al-Joz, Mount Scopus, and the Old City — this

research employs voids and lines as analytical categories. This empirical study reveals how the AR reproduces the spatial realities of the city in a way that is consistent with the Zionist imaginary of a Jewish and unified Jerusalem. Through the digital removal of the Palestinian urban space and the neutralization of the concrete tropes of the Israeli annexation in its representation, the AR of East Jerusalem ultimately depicts a harmonious and pacified characterization of the city.

PAPER VII introduces algorithms as novel socio-technical infrastructures and political actants of cyber conflict in Palestine. This publication reveals how algorithms operate as infrastructures of (in)visibility on social media, digital maps, navigation apps, and AR video games. On the one hand, they serve the Israeli system of control by making Palestinian users and content hyper-visible to surveillance. On the other, by imposing (self-)censorship and erasure from digital representations, algorithms ultimately contribute to deleting Palestine from cyber and digital spaces. In doing so, they do not only enact control and surveillance through automation, but they also inform the creation of an aesthetics of disappearance for Palestine through cyberspace and digital absence.

3. Conflict in cyberspace/conflict in Palestine

THE EMERGENCE OF CYBER CONFLICT has gained extensive scholarly, policy, and media attention because of the novel and daunting digital imaginaries it evokes. On the one hand, the argument of cyberspace's exceptionalism — i.e., the idea that cyberspace's unique systemic complexity brings unprecedented uncertainty — can explain such hype (Chenou 2014). It is partly because of this uncertainty — and the vast narrative possibilities it allows — that movies, tv-series, videogames, novels, etc., have been able to extensively and successfully popularize the 'cyber-doom scenario' (Shires 2020). These different and often dystopic narratives of conflict have informed policy and scholarly work to mutually reinforce the fearmongering

understanding of conflict in cyberspace as a war-like, catastrophic, and somewhat unknowable phenomenon.

On the other hand, dealing with something 'new' is commonly done by going back to 'old' frames. This process of 'epistemological adaptation' — i.e., understanding the new through the old — has been diverse and somewhat original, as shown in the width and heterogeneity of analogies used for making sense of conflict in cyberspace (Taddeo 2016; Betz and Stevens 2013). For instance, the health-inspired one envisions malware as viruses, computer systems as bodies, and cyber hygiene as a preventive strategy of security (Slupska 2021). Other forms of analogical reasoning about cyber conflict refer to the animal kingdom and classical history, wherein malicious software becomes worms or Trojan horses. Among these, the war analogy refers to malware as weaponry that can cause 'cyber–Pearl Harbor' events — a refrain that points to the overwhelmingly Western-centric and Manichean discourse about conflict in cyberspace. As shown throughout this dissertation, these constructs are informed by the political contexts and imaginaries in which they emerge, but they also ultimately affect the digital experiences of those 'at the receiving end' of cyber conflict and cybersecurity.[2]

Malware — i.e., the vast range of hacking and manipulation techniques used to inflict harm to programmable devices — is an excellent example of how different narratives are mobilized to make sense of the nature of cyber conflict. When thinking about malware in infrastructural terms, they can be considered as 'pieces' of code that operate through standardized mechanics and protocols. What makes them malicious and political is their use as the very same type of cyberattack would be framed differently depending on the specific context and the actors involved. At the very least, the construction and operationalization of the narratives of cyber conflict indicate the centrality of these political contextual considerations alongside socio-technical ones.

[2] As theorized in critical war studies, see Sylvester 2012.

The study of international conflict in cyberspace has employed the analytical categories of *violence*, *sovereignty*, and *territory* to shed light on the technical categories of harm, attacker, and target. When can a cyber operation be considered violent? How can we recognize the agency of states in cyber and information operations? What are the territorial boundaries of a country in cyberspace? Answers to these questions are political, and the peculiar blurring categories in cyberspace provide wide spaces for different answers to emerge. As this dissertation shows, not only the answers — but also the questions — are political.

For its peculiar uncertainties related to how violence, sovereignty, and territory are constructed, practiced, and experienced in the context of conflict, the case of Palestine represents a fundamental test ground for state-centered narratives informing the common understanding of cyber conflict. In the last seventy years, several major political events led to extensive territorial, political, and regulatory fragmentation and reconfigurations (Weizman 2012; Tawil-Souri 2019). These have resulted in different security regimes and political realities that continuously intersect and juxtapose in determining different everyday experiences of conflict and security for Palestinians in Israel, East Jerusalem, West Bank, and Gaza — as well as for Palestinian refugees and members of the global Palestinian diaspora (Gazit 2009).

In the study of Palestine/Israel, capturing such empirical complexity under one specific conceptual 'flag' proved to be challenging, as it also generates a unique degree of contestation. Whether the complex Palestinian reality configures as one of conflict, rather than one of settler colonialism/apartheid, remains a central issue of political and academic contention — undoubtedly one that has found cyberspace an essential space for its discursive articulation globally.[3] For this reason, warfare and state-centered considerations alone have proved to be unfit to capture and address the blurring political realities of conflict in Palestine (Turner 2019; Aggestam, Cristiano, Strömbom 2015).

[3] On settler-colonialism in Israel/Palestine, see Lloyd 2012; Shihade 2012; and Khalidi 2020.

Cyberspace has further complicated this task by adding a new specific empirical dimension to the Palestinian experience of conflict and security and contributing to the blurring of existing ones through digitalization. Besides allowing for cyberattacks between Palestinians and Israel, cyberspace provides authorities with new spaces and technologies for surveillance, espionage, and disinformation — a development referred to as 'digital militarism' in the specific context of Israeli strategies (Kuntsman and Stein 2020). In addition to these, cyberspace also enables and accelerates the spread of information and narratives — as in the case of Israel's public diplomacy and 'digital hasbara' (Aouragh 2016). In other words, the contested narratives surrounding the conflict have found a new *caisse de résonance* in cyberspace. This so-called 'battle of ideas' has marked a new phase in Israel-Palestine, one that has informed the conflict as genuinely global, while also allowing for the digital re-articulation of Palestinian identity through transnational encounters (Aouragh 2011).

All these empirical entanglements have a lot to say about those normative conceptual boundaries that have guided the study of cyber conflict: national/international, warfare/security, and cyber/information. As shown in this dissertation, these boundaries are better understood as *blurring continuums*, wherein such blurring does not only represent an unavoidable and neutral transformation brought by the 'digital revolution' — but constitutes a contested space of politics instead. Insofar as they inform and sustain the operationalization of the thick Israeli web of systemic technological control in Palestine, the blurring politics of cyber conflict (dis)enable violence, sovereignty, and territory also *beyond cyberspace*.

4. *Research question and strategy: an overview*

WITH THE AIM OF UNDERSTANDING CYBER CONFLICT through and within its political idiosyncrasies, and outside rigid disciplinary and empirical boundaries, this dissertation studies Palestinian cyberspace as a constructed issue of warfare and security, as a policy object, and as an infrastructural and informational space of control and contestation. This research strategy adopts an eclectic approach to methodology and alternates deductive and inductive reasoning, depending on each publication's specific aim and design. Palestine and 'its' cyberspace should thus be seen as both a case study for testing the applicability of relevant concepts, but also as a distinctive starting point for empirical investigation and theorizing. Taken together, these contribute to answering the following overarching research question:

How are conflict and security constructed and experienced in/through Palestinian cyberspace?

As mentioned earlier, three analytical concepts — violence, sovereignty, and territory — guide this dissertation's critical exploration into the blurring politics of cyber conflict in Palestine. These contested analytical concepts are at the core of mainstream narratives and debates on conflict and security in cyberspace. It is thus a crucial task for a critical scholarship to address their significance also beyond normative and traditional 'uses.' This is to say that violence, sovereignty, and territory *do matter* for our understanding of cyber conflict and security, even if we are to dismiss the broader warfare and security narratives from which they sprung. This dissertation thus also sheds light on how violence, sovereignty, and territory are constructed and experienced *in/through* Palestinian cyberspace.

The primary and overall data collection strategy for this thesis consists of four research stays in the Palestinian territories in the period 2013-2018, each

lasting three months.[4] These visits focused not only on data collection per se but also on acquiring a broader contextual knowledge about Palestine. This is consistent with the empirical approach of this dissertation project: to study conflict in cyberspace also beyond the analysis of cyber/information operations, military strategies, and/or national security policy (that is, as if cyberspace was a 'finite world'). Instead, producing knowledge about conflict and security in cyberspace involves here a *broader contextual engagement* with the political realities of Palestine, as well as with its culture, history, ideas, space, and technology (Goodin and Tilly 2006).

These research stays were instrumental in gathering the totality of data for this study, the so-called *data corpus*.[5] Making sense of this corpus is done through interpretation, as a process that, differing from formal inductive analysis, gains knowledge from a 'holistic grasp of data' (Simons 2014; Kurowska 2020). Given the style and purpose of the publications included in this thesis, only a small selection of data extracts — selected individual pieces of data — is directly referred to in the published papers. For the same reason, a dedicated methodology discussion was not included in some of the articles and was thus incorporated into this introductory chapter (see sections 6 and 7).

[4] These research stays were only allowed under tourist visas,which have a duration of three months. Israel imposes very strict travel restrictions on researchers that intend to conduct research in the occupied Palestinian territories. On this issue, see Abbott 2018.

[5] For a critical perspective on the concept of data in internet/digital research, see Lindgren 2018.

5. *Analytical concepts: violence, sovereignty, and territory*

THE PUBLISHED PAPERS forming this dissertation make contributions that, besides the empirical focus on Palestine, are of a primarily conceptual and theoretical character. These refinements are not thus repeated here in full. This section focuses instead on the three analytical concepts — *violence*, *sovereignty*, and *territory* — that have informed and guided this dissertation's critical exploration of the blurring politics of cyber conflict in Palestine and beyond. For each of these concepts, this section 1) briefly reviews relevant academic debates; 2) clarifies the type of analytical 'function' they perform for this research in contrast to dominant epistemologies; and 3) highlights how the analyses presented in the published papers specifically contribute to advancing the scientific understanding of each concept in relation to conflict and security in/through cyberspace.

VIOLENCE

The concept of violence has an often implicit, yet pivotal, role in the entire architecture of scholarship on cyber conflict. Strategic, normative, and legal perspectives conventionally look at the question of violence in relation to the degree of harm and damage caused by cyber operations (Schneider 2019; Rid 2013, 11-34). Unsurprisingly, this conceptual perspective developed alongside the cyberwar narrative and focuses on whether and to what extent the effects of cyber operations compare to kinetic violence — and eventually to war (Libicki 2009). In this light, malware and disruptive software have generally been referred to as harmful 'weapons' (Egloff and Shires 2021). Like other innovative weapons, cyber means have either been 'feared' for their lethal potential or praised for their ability to be both precise and reduce violence — through the well-known rhetoric of smart/perfect weapons (Demmers 2016).

At the beginning of the 2010s, the Stuxnet case decisively shaped the academic debate on the violent potential of cyber conflict. At a time when cyber warfare constituted, for the most part, only a hypothetical threat/opportunity across military and strategic debates, Stuxnet represented a fundamental empirical crossroad (Lindsay 2013; Zetter 2014). Allegedly developed and deployed by Israel in partnership with the US, the malware sabotaged the computer systems and the centrifuges of the Iranian nuclear facilities located in Natanz, decisively setting back the country's nuclear program. This unprecedented — and yet never repeated (Delerue 2020) — incident showed that cyberattacks could get close to the various (legal) thresholds of war. This consideration 'stirred up' military perspectives and further enabled the emergence of disaster scenarios for cyber conflict and the related securitization critique about how cyber threats are constructed and acted upon through cybersecurity (Hagmann and Dunn Cavelty 2012). At the same time, it also became clear that cyberattacks cause 'less harm and risk than the kinetic weapon' (Denning 2012, 687). Thanks to their ability to achieve strategic goals through highly targeted mechanics, the new strategic thinking sees cyber operations as desirable/legitimate means of international relations and statecraft for their lacking violent effects. In policy terms, this meant that the adoption of offensive cyber strategies became normalized, and the defense/offense appears increasingly blurred in national strategies (with formulations such as 'defending forward' and 'persistent engagement' now dominating the strategic discourse).

Whether envisioning cyber operations as possessing destructive potential or as non-violent, the dominant strands of academic reasoning about cyber conflict rely on a narrow conceptualization of *violence as physical and material harm*. This dissertation contributes an innovative perspective to the academic debate about the violence of cyber conflict. Intending to look beyond infrastructural damage as a defining element of cyber conflict's harm, it embraces a disembodied understanding of violence. This analytical perspective focuses on the 'affective implications of cyber weapons' — which 'might include feelings of insecurity or fear'— and the broader digitally mediated experiences of violence (Stevens 2017, 4). This also means that this

research does not employ the concept of violence to establish cyber operations' legality or desirability. Instead, it functions as a nuanced analytical perspective for analyzing the entangled experiences of conflict and security in and through cyberspace.

How is violence constructed and experienced in and through Palestinian cyberspace?

To provide a comprehensive answer to this question, this dissertation employs thus an understanding of violence that differs from the physical and infrastructural perspectives that dominate the analysis of conflict in cyberspace. As argued across the various publications, violence is understood here as socially constructed, discursive, networked, and affective. Through this approach, this research makes two broad contributions toward our scientific understanding of violence in cyberspace. First, it argues that the violence of cyber conflict is not only infrastructural but also informational. Second, it shows how the actualization of such violence also mediates violent experiences outside cyberspace.

These debates are primarily addressed in Paper I, Paper II, Paper V, Paper VI, and Paper VII. Through the analysis of game scenarios in the context of national and international cyberwar exercises, Paper I contributes to our understanding of how the construction of war-like scenarios of cyber conflict articulates physical and infrastructural violence. This empirical perspective speaks to securitization scholarship on the inflation of cyber threats. It does this by revealing how a kinetic and physical understanding of violence is functional to the construction and normalization of cyber conflict as a war-like phenomenon and cyberspace as a warfare domain. Paper II deconstructs this understanding of violence by taking a different perspective. This publication shows how violence occurs beyond narrow kinetic conceptualizations through a reflexive account of knowledge production about conflict in cyberspace. It does this by engaging with cyborg and feminist theories to situate violence beyond the infrastructural elements of cyberspace and towards its informational ones – i.e., toward other types of harm.

Expanding this disembodied perspective on the violence of cyber conflict, this dissertation also provides insights into how violence is constructed and experienced *through* cyberspace. Pointing at the implicit violence of infrastructural control and surveillance — in content moderation, internet access denial, and (self-) censorship — Paper V contributes to the understanding of harm in cyberspace by engaging with scholarship on human rights. While not referring to the concept of violence explicitly, Paper VI and Paper VII focus on how digital technologies also mediate and enable violent experiences outside of cyberspace. They advance scholarship on the violence of cyber conflict by showing how, while informational and representational, this violence can also be networked and experienced outside of cyberspace. Taken together, these publications contribute to advancing scholarship on the violence of cyber conflict by questioning its cyber/information divide. They show how infrastructural and informational aspects of cyberspace are not fully discernable but somewhat interdependent.

SOVEREIGNTY

From the very beginning, the emergence of cyberspace seemed to 'shake' the foundations of sovereignty. The networked ontology of cyberspace questioned the possibility of state authority and control while raising questions about how cyberspace could be imagined and governed in territorial terms. In 1996, cyber-utopians famously declared the independence of cyberspace from state sovereignty — and thus proclaimed it 'ungovernable' (Wu 1996; Barlow 1996). This argument, still widespread today and central to the critical reasoning about techno-determinism put forth in this dissertation, stems from an exceptionalist contemplation of the nature of cyberspace. As inherently networked, cyberspace would rebut any

substantial form of political authority and control, thus only enabling networked and horizontal political agencies.[6]

In recent years, the evolution of cyberspace into a domain of fierce geopolitical competition and conflict between different actors showed the techno-deterministic flaws of cyber-utopian perspectives — while initiating a state-centered scholarly debate about sovereignty in cyberspace. Besides addressing the idea of a territorial cyberspace (discussed in the following sub-section), scholarly thinking on the relationship between sovereignty and cyberspace focused on two intertwined debates. The first debate concerns how states' political authority and control in cyberspace are generally defined and articulated in connection to infrastructure, information, data, and digital technologies (Deibert and Pauly 2019). The second debate generally pertains to the agency of the state in cyber warfare and sovereignty as an element for the attribution of cyber operations, with the primary goal of assessing their legality and state responsibility (Liaropoulos 2013; Rid and Buchanan 2015).

Different cyber-related fields have dealt with these two central academic debates about sovereignty in terms of states' political agency and authority in cyberspace. Strategic studies have addressed sovereignty primarily in terms of the military and legal agency of states regarding the conduct of cyber operations (Betz 2017). Attributing cyber operations is, however, a difficult task. The realization that actors other than the state conduct most of the malicious activities in cyberspace urged strategic and legal scholarship to study how other actors can be considered 'state proxies' — acting on behalf of a sovereign (Maurer 2018).

Looking beyond an understanding of cyber conflict as limited to cyber operations, sovereignty in cyberspace generally refers to affirming some form of authority and control over information and infrastructure. With the cyber-utopian ungovernability argument marking time to geopolitics, a general agreement emerged that cyberspace must indeed be governed — but 'by whom' and 'how' remain intensely debated. Relevant scholarly work seems

[6] Network theorists take a similar position on the emancipatory potential of internet networks, see Castells 2011.

to exacerbate these questions by referring to 'digital,' 'cyber,' 'technological,' and 'data' sovereignty interchangeably to make sense of different policy strategies and governance perspectives for cyberspace (Hummel et al. 2021).

After all, this conceptual unclarity directly reproduces the different ways to think about the nature of cyberspace: that is, in connection to the infrastructural/informational dichotomy mentioned earlier. If political authority in cyberspace derives from controlling information and its circulation, actors other than the state enjoy vast sovereign prerogatives. Recent works in internet governance focus on how controlling either information or infrastructure should be thought of as conflicting and irreconcilable governance models for cyberspace (Mueller 2020). According to this perspective, the free and open internet stands for a cyberspace ruled by democratic values, while a 'sovereign cyberspace is inimical to the liberalized information and communications order' (Mueller 2020, 780).

While these debates generally disagree about the extent to which states can indeed exercise their sovereign prerogatives in cyberspace through political authority and control, the concept of sovereignty has been primarily treated and operationalized through an understanding of *sovereignty as the political authority of the nation-state*. This dissertation intervenes in this conversation by looking at sovereignty as a form of political authority and agency that is not necessarily formally and aprioristically 'granted' but one that can be constructed and contested through networks and beyond the agency of the state.

How is sovereignty constructed and experienced in and through Palestinian cyberspace?

To provide a comprehensive answer to this question, this dissertation employs an understanding of sovereignty that, while outliving considerations about (the possibility of) the formal authority of the state in cyberspace, remains aware of the power structures that shape the digital. At the same time, it critically engages with the idealization of networks as loci of ultimate political authority. Inspired by this approach, this research makes two main contributions to scholarship on sovereignty in cyberspace. First, it argues

that sovereignty in cyberspace is articulated both in/through infrastructural and informational politics. Second, it shows how sovereignty in cyberspace is not a prerogative of the state but resides rather in networks.

These arguments are primarily unpacked in Paper III, Paper V, and Paper VII. Focusing on cyber/digital sovereignty, Paper III argues that the Palestinian limited formal authority in cyberspace does not only depend on lacking control over the internet infrastructure. Such limited political authority can be explained as the result of specific contextual politics (and political choices) that, in the emblematic case of the PA, favor security cooperation with Israel on matters of cybersecurity, service delivery, and information security. As Palestine lacks formal and full sovereign prerogatives, this publication contributes to the debate on digital/cyber sovereignty by analyzing a unique empirical case. Paper V further contributes to understanding political authority and control in cyberspace through the perspective of human rights and in connection to information, data, and digital technologies more generally. Paper VII focuses on the political agency of algorithms in shaping conflict and security beyond cyberspace and contributes to scholarship on sovereignty by drawing attention to the quasi-sovereign role of automation and the non-human.

TERRITORY

Besides relating to political agency, the question of sovereignty in/through cyberspace also relates to the territorial dimension of authority. Whereas the question of cyber/digital sovereignty seems to polarize the academic debate, there is a substantial agreement regarding the territoriality of cyberspace. Cyberspace has been analyzed through a common — and by now, mostly given for granted — 'territorial ontology,' which 'unites' the different branches of cyber scholarship (Lambach 2020).

Scholarly work has theorized the territorial ontology of cyberspace as a 'world of its own,' somewhat separated, nevertheless connected to the offline world, where the 'real-life' unfolds (Kinsley 2014; Graham 2013). In the 1990s, critical geographers embraced the cyber-utopian ideology about the

internet and theorized the juxtaposition between the virtual and the real world (Gunkel and Hetzel Gunkel 1997). This presumed separation between the online and offline also subtends those narratives of cyberwar envisioning cyber conflict as the phenomenon that emerges from the 'virtual' to the 'real.' Surprisingly, these critical works are not different from the military and strategic conceptualization of cyberspace as a 'battlefield' and 'domain of warfare.'

Strategic and legal perspectives generally envision cyberspace divided into national territories and jurisdictions. In their study of cyber conflict, they have thus theorized whether, and the extent to which, cyber and information operations constitute a violation of a state's territorial sovereignty (Tsagourias 2021). The corollary of this dominant perspective is that a clear-cut distinction between 'national' and 'international' cyberspace exists. On the grounds of this somewhat arbitrary distinction that national and international cybersecurity crystallized as distinct approaches to the governance of cyberspace. Works in internet governance have questioned the (legal) idea that cyberspace can be fragmented into nationally controlled territorial segments (Mueller 2017a). According to this perspective, the tension between the reality of global cyberspace and the 'fantasy' of national cyberspace stands at the core of the failure of cybersecurity scholarship and policies (Mueller 2017b). At the same time, when considering cyberspace as the territory where information and data circulate, states have relatively little control over these flows. Yet, thanks to cyberspace, they can potentially have a far greater informational reach into the territory of other states.

In sum, network-oriented approaches have the merit of questioning the possibility of fragmenting and governing the internet into national territories (Herrera 2016). At the same time, they tend to overlook the territorializing potential that cyberspace provides to states and the other 'masters of information.' While disagreeing on whether cyberspace will fragment into national segments, these scholarly works similarly apply an understanding of the *territory as a physical and static space*. This dissertation intervenes in this conversation about territory and cyberspace by suggesting shifting the analytical focus from territory to territorialization.

How is territory constructed and experienced in and through Palestinian cyberspace?

To provide a comprehensive answer to this question, this dissertation employs an understanding of territoriality that does not entirely dismiss territorial thinking but moves beyond territory as a static analytical category. Instead, it employs territorialization as the political process that defines, delimits, and inscribes space, thus also potentially redefining political agency beyond national authority. Embracing approaches to territorialization as a political practice of 'space-making,' this research makes three main contributions. First, territoriality in cyberspace is constructed politically and beyond the fixed boundaries of the state. Second, it questions the national/international divide in cybersecurity. Third, the territoriality of cyberspace is not separated from the 'actual world.'

These arguments are primarily presented in Paper IV, Paper VI, and Paper VII. Paper IV contributes to this debate by detaching the question of territory in cyberspace from sole infrastructural considerations. It suggests abandoning the traditional canons of national territory and looking at conflict and security in cyberspace in terms of 'territorialization' – i.e., the becoming territorial regardless of territory. Paper VI further detaches the territoriality of cyberspace from its infrastructure by looking at how spatiality is constructed and experienced through digital representations of space and conflict (in the specific case of the AR of East Jerusalem). It does so by engaging with urban studies and psychogeography, thus also questioning the national/international divide customarily constructed in the different narratives on cyberspace. Similarly, Paper VII contributes to our understanding of the territoriality of cyber conflict by focusing on the representational and aesthetic realm of space and how different spatial representations shape users' digital experience outside cyberspace.

6. *Cyber conflict and knowledge production*

WHERE AND WHEN DOES ONE STUDY CYBER CONFLICT? Designing context-informed research requires, above all, a spatial and temporal delimitation of the field — what Spradley (1980, 39-45) broadly defines as 'locating a social situation.' Particularly during the first research stay in the West Bank in 2013, the plan of collecting data about conflict in cyberspace through traditional fieldwork in the Palestinian territories clashed with the perception of being 'in the wrong place at the wrong time.' In hindsight, locating the empirical boundaries of cyber conflict in Palestine proved to be the main challenge for the research design of this thesis. Because of its speed and lack of a determined physical location, cyber conflict cannot be observed as a conventional social situation, where actors and activities are 'confined' to a delimited space and interact/unfold in real-time and, most importantly, in plain sight. *After all, where and when is cyberspace?*

The challenge of producing situated and timely knowledge about cyber conflict is indeed real, also for scholarship primarily focusing on cyber and information operations conducted by states. If, on the one hand, perpetrators of cyber and information operations tend to recur to anonymity and secrecy to avoid accountability and possible retaliation, targeted victims often prefer to remain 'silent' not to publicize their vulnerability and to elude public scrutiny and reputational harm (Brown and Fazal 2021; Buchanan 2016). As a result, most cyber operations go unseen or are left unpublicized (at least for long periods). An abused leitmotiv within cyber security recites that 'we only get to know about bad cyber operations,' as 'good' ones often go undetected even by the targeted victims. The 'logic' of a cyberwar emerging from the 'virtual' to the 'real' has thus also an epistemological connotation: cyber conflict can be studied because cyber operations emerge/are made observable (Fouad 2021).

To become known, cyber and information operations need to be 'discovered,' a task habitually carried out by threat intelligence and private

cybersecurity — even for large-scale cyber operations such as Stuxnet 2010 and NotPetya 2017. Only then, an operation in cyberspace becomes an 'item' available to further academic inquiry. Based on these discoveries, scholarly knowledge typically advances by recalibrating analytical categories and thresholds of warfare, security, and (il)legality (Egloff and Dunn Cavelty 2021). Taking the leitmotiv mentioned above seriously, one could argue that traditional approaches to research on cyber conflict can only allow, after all, the study of 'bad' cyber operations.

This prevalent and somewhat standardized research practice relies on the availability of secondary data about cyber operations, such as technical reports and analyses. These have recently come under scrutiny for their biases, for instance, in their underrepresentation of those cyber operations that target civil society while having a privileged focus on specific states (Maschmeyer, Deibert, and Lindsay 2021). These technical 'discoveries' are not neutral nor objective, and they influence what eventually gets to be studied by cybersecurity scholars. As shown in Paper I, they depend on the analytical and normative categories used to reveal them (the lenses) and are produced by communities that, being often part or close to military-industry complexes, nurture specific values, interests, and narratives on the broader relationship between technology and society (Leander, 2005).

Primarily focusing on state-related and operational/mechanical aspects of cyber operations, the study of cyber conflict thus commonly pertains to what happens *within* the boundaries of cyberspace — the where — and can only be conducted *after* a cyber incident has been revealed — the when (Stevens 2016; Stevens 2018). In addition, as national security and military agendas increasingly prioritize cyber threats, policy and strategic oriented research has focused on their prediction, detection, risk assessment, and deterrence — which has meant, for scholarly research, to focus also on the *before* and *if* an operation eventually takes place (through empirical attention for military strategy and policy design). Many states have recently employed a similar pre-emptive logic to justify adopting offensive cyber operations — or 'defending forward' and 'persistent engagement' strategies — to use the terminologies most in vogue (Healey 2019; Smeets 2020). Critical security studies refer to

this as *anticipatory logic*, which justifies both the adoption of exceptional policies for securing and defending national interests (in cyberspace) and seems to guide research designs on cyber conflict often (Adams, Murphy, and Clarke 2009).

This dissertation looks beyond *discovery* and *anticipation* as the two main spatial and temporal logics of knowledge production about conflict in cyberspace. Following different empirical facets, it configures a comprehensive research strategy, which accounts for the spatial and temporal dimensions of cyber conflict also 'outside' cyberspace, beyond the study of cyber/information operations, and their distinction as two separate empirical domains. As mentioned earlier, the traditional distinction between cyber and information pertains to the contested nature of cyberspace and whether it is primarily an infrastructural space or an informational one.

These two perspectives differ in their understanding of the qualities of the 'cyber' space and its composing elements, but they agree on the fact that cyberspace is indeed a territorialized space. In the study of territorial and spatial aspects of cyber conflict (for Paper IV, Paper VI, and Paper VII), a different and broader understanding of space influenced the research design of this dissertation. This understanding has long guided empirical research in peace and conflict studies through fieldwork-based and comprehensive research strategies (Björkdahl and Buckley-Zistel 2016). These immersive research strategies do not define the spatial boundaries of 'their field' solely in territorial, infrastructural, or material terms but also in connection to how such spatialities are (de)constructed and experienced discursively and across the different digitalized experiences of conflict.

Whereas immersive research designs are not standard practice in cybersecurity, they have been applied across other disciplines nurturing a similar interest for experiences in and through cyberspace — such as sociology, anthropology, and media studies. Commonly framed as *digital*, *virtual*, or *cyber ethnography*, these empirical studies purport to translate and adapt ethnographic techniques to cyberspace to produce situated knowledge about digitally mediated experiences (Murthy 2008; Hine 2000; Hallett and

Barber 2014; Ward 1999). They relate to cyberspace as a traditional 'field,' in which ethnographic work entails a prolonged and immersive engagement with online communities and their 'websites.' For this very reason, they are generally better suited for focusing on the informational aspect of cyberspace rather than on its infrastructural one. These ethnographic studies have been, for instance, applied in research on social media, virtual simulations, video gaming, hackers, etc. They can indeed offer relevant insights into the informational and 'communitarian' aspects of conflict in cyberspace — as for the research conducted in Paper II.

However, immersive studies in cyberspace are easier said than done. In their application to the study of cyber conflict, these ethnographic methodologies are, however, limited by a) an understanding of cyberspace as a finite and territorialized space; b) a clear-cut distinction between online and offline experiences and temporalities; and c) being necessarily bounded to studying 'what is already visible' in cyberspace (in the form of data). In other words, cyber ethnographic methods tend to be blind to those digital experiences that are not directly visible because of intentional anonymity/secrecy or because they have been *made invisible* by various apparatuses of security and control (on this, see Paper V). In a highly militarized and securitized context like Palestine, these aspects are central to understanding how digital technologies operate (as argued in Paper VII), and thus cyber ethnography alone does not constitute a thorough research strategy.

Designing comprehensive and 'field-based' research about conflict in cyberspace ultimately faces some idiosyncratic and uncompromising spatial and temporal limitations. These have necessarily challenged the fieldwork-based strategy of this research. However, as the first research stay in Palestine progressed, different empirical 'traces' became visible and indicated that a cyber conflict was unfolding while not directly observable in a traditional spatial and temporal sense. This conflict was 'made of' Palestine's contextual politics, narratives, and digitalized experiences of conflict also outside of cyberspace. These unraveled not only in connection to and across the cyber/information divide but also across the online/offline one (as shown in Paper II, Paper VI, and Paper VII).

This thesis studies and connects these different empirical traces into one broader puzzle through a *phenomenological* approach (Cerbone 2014). In a nutshell, phenomenology studies discourse about a phenomenon as constitutive of the phenomenon itself. In practice, a phenomenological study of conflict in cyberspace focuses on the structure of various types of experience as elements that jointly and discursively constitute a cyber conflict. This 'opening-up' of the study of conflict in cyberspace to its contextual politics and discourses also allows for reflexivity and critical thinking on the broader relationship between technology and society (an issue particularly relevant for Paper V). Taking this broader perspective stems from (and nurtures) a political commitment to the Palestinian cause, which has matured for me through an in-depth engagement with its different expressions.

To sum up, with the ambition of coming to terms with its politics and narratives, this research studies cyber conflict not only in the form of discovered or anticipated (state) operations but also focuses on how these are experienced and made (in)visible through politics. In an asymmetric conflict context like Palestine (and in general), comprehensive research designs are helpful for accounting also for what is *made not observable* and for how this invisibility is experienced politically (also by the researcher, as shown in Paper II). The when and where of this research design thus also talk to those invisible spaces and experiences created by infrastructural dependency, technological obsoleteness, service denial, surveillance, cyberattacks, content moderation, disinformation, (self-)censorship, etc. that characterize conflict in and about cyberspace in and about Palestine. This thesis studies conflict in cyberspace through the practices and policies that govern it, its (fictional) and digital representations, its (dis)embodied experiences of violence, and how these shape everyday experiences of space and violence outside cyberspace.

7. *A variety of methods for a comprehensive phenomenon*

THE OPERATIONALIZATION of this comprehensive research design requires a varied repertoire of methods to grasp the phenomenological granularity of cyber conflict and its contextual politics in Palestine. This section outlines these methods and illustrates their application. For the reader's convenience, these have been organized in three subsections —interviews, participant observation, and media contents — but should be understood as one unified and blended strategy of data collection and empirical investigation.

INTERVIEWS

Different interviewing techniques are the primary device of data collection for this dissertation. In line with the phenomenological research design, the guiding principle of these interviews corresponds to what Roulston et al. (2008) define as the 'constructionist approach' to *reflective interviewing*: one that, while rejecting the idea of absolute authenticity, conceives both the subject and the phenomenon to be produced within its narratives. Interviews are a technique used to capture these narratives of cyber conflict and were conducted both online and offline and synchronously and asynchronously. Unstructured interviews and informal conversations with relevant actors and 'gatekeepers,' as well as with close and less-close acquaintances, were used to map networks and issues of interest, understand practical aspects of the fieldwork; build relationships, and generally refine the qualitative research design of the thesis.

The role of these unplanned, or 'less-planned,' moments of data collection has been generally praised for allowing researchers to 'get access' to the field, particularly in contexts where this access is denied or mediated by different systems of control (Brounéus 2011; Swain and Zachery 2020). At an early stage of this research, these also pointed to the importance of dynamics 'outside' cyberspace for studying its inherent conflicts. This is to say that they

enhanced my relational understanding of the *reach* of cyber conflict into broader digital experiences of conflict (such as those studied in Paper VI and Paper VII). Whereas not included in the publications as (raw) data, unstructured interviews also functioned as a technique for acquiring background knowledge in preparation for other data collection strategies or for triangulating data collected through a different technique. Above all, these informal exchanges were primarily used to investigate how cyber/information warfare, security, and online surveillance intersect with other regulatory systems of control in Palestine and how both are shaped by the historical and political narratives of the conflict.

This aspect eventually motivated me to study significant empirical facets of the conflict in historical terms (as an additional aspect of the 'when' of cyber conflict), focusing on the history of technology, infrastructures, and computation in Israel/Palestine. Engaging with local experiences and the history of the conflict further enabled a critical reflection on my positionality as a privileged outsider and my role as a researcher in a highly militarized and surveilled context.

Semi-structured and in-depth interviews were employed instead for acquiring or triangulating data about a specific event or issue. These planned types of interviews occurred both offline and online and synchronously and asynchronously, primarily depending on the specific degree of secrecy required and the interviewee's preferences (Kaufmann and Tzanetakis 2020). Interviewees for this thesis belonged to very different groups, thus relating to the question of secrecy/anonymity in very different ways: (pro-) Palestinian hackers, cyber security and tech experts, government and military/security officials, policymakers, NGO workers, (media) activists, journalists, and artists. When necessary, interviews were also used to triangulate the outcome of other research techniques. Whereas generally crucial for comprehensive research designs, triangulation is particularly crucial for researching cyber conflict (Flick 2004).

Besides constituting an operational aspect of cyber conflict, manipulating and sabotaging information and infrastructures also affect the research

process. To overcome the risk of falling victim to manipulated information, if ever possible, verifying sources and data through constant triangulation was central to this research design. Besides stemming from the aim of collecting data of 'good quality,' triangulation also relates to ethical considerations about the safety and privacy of interviewees (Richterich 2020). Interviews for which discretion was necessary were conducted through either video calls, chats, encrypted instant messaging, or email exchanges. The latter was beneficial as they allow for precise and thorough descriptions of a specific event and map networks of interest.

From a very early stage, this mapping of relevant networks and events through interviews indicated that the Palestine constituted and targeted through/by cyber conflict, and thus *the one to be studied*, was not only the (very contested) geographical or infrastructural cyberspace with the same name or country code extension (.ps). Instead, as Israeli offensive operations, surveillance, and censorship target Palestinians of the diaspora and advocates regardless of their physical location, the *Palestine of cyber conflict* also seemed to transcend its territorial connotation in cyberspace (an argument put forward in Paper IV). Similarly, (pro-) Palestinians targeting the Israeli cyberspace through cyberattacks or engaging in the 'battle of ideas' are not necessarily based in the OPT nor have particular ties to Palestinian authorities (i.e., they are not state proxies). Instead, they share political, cultural, or religious proximity to the Palestinian cause — what can be defined as *Palestinianness* across space and time (Suleiman 2016; Zureik 2001).

PARTICIPANT OBSERVATION

The width and heterogeneity of these phenomenologies of conflict in and beyond cyberspace studied here are thus better defined as a network of social situations rather than a single cluster formed because of physical proximity in space and time. At the same time, it is essential to remember that the Palestinian realities of conflict have a central material component, manifest in actual violence and territorial control by Israel. As argued across different

publications, these material experiences are enhanced, rather than dissipated, through cyberspace and the digital. This research design has employed traditional macro-ethnographic techniques to account for such materiality outside cyberspace.

The four research stays in Palestine offered several opportunities for data collection through traditional participant observation. These participatory techniques were either explicitly part of the research design from the outset or became unforeseen moments of learning as the research stays progressed. These two participation-based 'postures' vis-à-vis contextual research normally define the researcher's role as either one of *participant-observer* or *ordinary participant*. The former differs from the latter as, besides engaging in a social situation to participate in its activities, it observes them with an explicit research interest. For this research, examples of the former include collaborations with local networks of digital rights activists in the West Bank and Israel, partaking in demonstrations and marches in East Jerusalem and the West Bank; and cooperating with research groups in Ramallah. Ordinary participation, instead, better captures the character of those immersive and participatory experiences of the 'everyday' in the Palestinian territories: encounters with the Israeli military in the West Bank; travels or hikes around the occupied territories and Israel; diplomatic and public events; or even sports training at one of the Hebrew University's facilities in East Jerusalem where security forces and diplomatic personnel used to go.

In addition, my experience as coordinator of two student trips (in 2013 and 2014) can also be considered an additional element of the participatory techniques used for the data collection phase of this thesis. Under my supervision, two groups of students of the course' War and Peace in the Israeli-Palestinian conflict' from the Department of Political Science at Lund University visited the region for a week-long study trip across the West Bank, East Jerusalem, and Israel. During these visits, the groups met with local activists, NGOs, diplomatic missions, activists, and media workers.[7] Albeit

[7] Amongst the others, the groups met with the group Breaking the Silence, B'Tselem, The Palestinian Academic Society for the Study of International Affairs (PASSIA), the Temporary International Presence in Hebron (TIPH), the Swedish Embassy, and many more.

not directly or organically part of the research design, these study trips helped broaden my (local) networks and refine and enrich my research design relationally through students' perspectives.

Besides traditional participatory techniques, these were also used to explore the in-between of cyberspace and physical space. For Paper VI, walking was employed as the ethnographic technique used to reveal the encounter between the physical and digital spatialities of East Jerusalem as represented in the augmented reality of videogaming in *Pokémon Go*. Through a similar interest in how Palestinian space is constructed and experienced in and through digital representation, participant observation is also part of the study on the aesthetics of algorithms conducted for Paper VII. This allowed us to study the functioning of different apps and the aesthetic products of their algorithms (*Waze*, *Google Maps*, etc.). For these two studies, participant observation allowed for exploring in-between situations mediated by digital technologies with a direct impact on the experience of physical space. Again, both studies pointed at the privileged positionality of being a Western academic insofar as the digitally-mediated experience of conflict and territory differed from the ones encountered by Palestinian users for the same apps.

Besides offline and in-between participant observation, immersive techniques have also been adopted to collect *data online interactively*, similar to what was earlier defined as cyber/digital ethnography. These online interactions have been helpful for most publications included in this dissertation, as these include email exchanges with policymakers, military strategists, hacktivists, etc., and contributing to online fora and groups on social media. Yet again, because of cyberspace's ambiguous spatiality and temporality — and the type of interactions these allow — *participant observation in cyberspace* remains a contested issue. Can a researcher's interactions on social media be considered a form of participant observation even if they often lack synchronicity? And what about email exchanges?

Again, these questions are driven by the inherent bias of methodological adaptation, i.e., applying research techniques designed for other research

contexts to the study of cyberspace. This is not to say that such epistemological debates are irrelevant. It is, however, essential to be aware of the temporal and spatial limitations that cyberspace poses to participation and immersive research, and thus to account for these critically as done by this dissertation. Further studies are required into the relationship between online data and the positionality of the researcher vis-à-vis these digital artifacts and the extent to which online data can be considered research data (Lindgren 2020).

MEDIA CONTENTS

The ubiquitous mediatization and datafication of the Israeli-Palestinian conflict offer numerous possibilities to understand its events from different digitalized perspectives in cyberspace (Stein 2021). It is thus worth mentioning that the research conducted for this dissertation has also extensively relied on different media contents to produce its analyses and structure the research design. The already mentioned 'battle of ideas' online — that is, the informational confrontation of different narratives and contents — takes both the classical form of social media content and develops in other (visual) media forms. Different media contents about Palestine — texts, images, videos, and audio/podcasts — are continuously uploaded and shared in ways that mediatize every single aspect of the conflict. For this dissertation, these 'already available' digitalized data — have been studied to enhance an understanding of the context as they also often become items and issues of political contestation on their own terms.[8]

At the same time, the vast amount of online data about the conflict also opens the space to further manipulation and the blurring of true and false — an aspect that is central to the study of the informational dimension of cyber conflict and should be integrated into the analysis of (dis)information operations.

[8] As shown in various emblematic cases analyzed by Forensic Architecture, see here: https://forensic-architecture.org/location/palestine-israel

For Paper III, Paper IV, and Paper V, the analysis of social media content is particularly relevant for understanding the *informational and representational aspects* of the blurring politics of cyber conflict, with regards to how information security, warfare, surveillance, and content moderation operate in constituting truths and narratives. Social media platforms are the theatre of information warfare and security, where both (dis)information campaigns unfold and where counter-narratives and political contestation emerge and are targeted by censorship and surveillance. The approach to social media analysis was not study was not quantitative but qualitative and contextual. Yet, descriptive statistics on the condition of Palestinian social media were borrowed from secondary sources, such as the valuable and thorough reports published by The Arab Center for Social Media Advancement (*7amleh*).

More systematic and methodologically sound techniques —such as social media analysis, image/video forensics, text mining, etc. — offer essential insights and should be taken into consideration for future research on cyber conflict, as these allow the very understanding of cyber conflict as a comprehensive phenomenon that also includes its informational aspects. As argued in these three publications, the fact that tech giants can intervene in the policing contents and the formation of narrative indicates how the study of cyber conflict should pay attention to agencies other than the state.

An important innovation of this research has been to reflect on social media contents — i.e., their visibility, deletion, and erasure — in terms of textual content and the type of aesthetic and representation that their manipulation produces (as argued in Paper VII). This approach points to another critical aspect that is often overlooked in the study of cyber conflict: its representational realm. What does cyber conflict look like? What do these visual representations do politically? The nature of cyber conflict depends on the political imaginaries and contexts that sustain it. It is essential to study its imagery and visual representations (as done in Paper VI and Paper VII).

To understand cyberspace as a policy object and constructed domain of warfare and security, the research design of this dissertation recurred to the analysis of texts focusing primarily on policy texts (for Paper III and Paper

V) and scenarios (Paper I). During one of my research stays in the OPT, the PA's policy on cyber security was released and immediately affected how Palestinians used cyberspace.[9] The approach was to study these policies in terms of how they have been used to criminalize contestation online and offline by both the PA and the Hamas government. The comparison of these policies and strategies showed the different approaches toward Israel and was used to reflect on the relationship between infrastructure and information in connection to sovereignty and territory. Both the analysis of military game scenarios and national cyber security policies pointed at the merging of military, security, and surveillance —traits that characterize Palestine in other domains but, through cybersecurity, become increasingly normalized.

8. Conclusion: Palestine as more than a case study

ARE ALL CYBER CONFLICTS THE SAME? The different publications included in this dissertation intend to provide a somewhat comprehensive portrait of the blurring politics of cyber conflict in Palestine. These different empirical contributions point to the relevance of contextual elements and specificities for understanding how conflict and security are constructed and experienced in/through cyberspace. Against the backdrop of generalization, it seems now essential to go back to one of the initial arguments of this introductory chapter: the uniqueness of Palestine as a case study. Because of its peculiarities, Palestine tells a story about the digital that seems very much substantiated by the exceptional condition of Palestinian cyberspace. In this sense, the 'story' of Palestinian cyberspace sounds like the story of two exceptionalisms.

[9] For a comparative perspective on the emergence of cybersecurity policies in the Middle East, see Shires 2021.

The often-dystopic configurations of security and conflict in and through Palestinian cyberspace captured through this research would confirm the exceptionalist argument, i.e., the idea that Palestine represents a unique 'laboratory of the extreme' (Weizman 2017). In and through cyberspace, the boundaries between violent and non-violent, sovereign and non-sovereign, territorial and non-territorial have increasingly blurred for Palestinians. So have those between past and present, actual and virtual, true and fake, real and imaginary: cyberspace characterizes the Palestinian digital experience as one of diffused and distinctive conflict and oppression.

Through the digital, the exceptionalist argument about Palestine has found new momentum, as exemplified in the narrative of the 'laboratory' (Machold 2018). The laboratory argument contends that Israel's global leading role in security innovation has transformed Palestine into a laboratory where these technologies are tested before 'traveling' all over the globe. At the same time, it is important to consider that what is being tested is not only the technologies: 'it is the thresholds that are tested and pushed: the limits of the law, and the limits of violence that can be inflicted by a state and be internationally tolerated' (Weizman 2012, 96). For this reason, besides revealing the inadequacy of framing conflict in cyberspace as only an issue of warfare and security, the study of cyber conflict in Palestine also shows how the construction and operationalization of these narratives ultimately affect political life and individual liberties via (the seizure of) the digital — globally.

Bibliography

Abbott, Alison. “In the Palestinian territories, science struggles against all odds.” *Nature* 563, no. 7731 (2018): 308-311.

Adams, Vincanne, Michelle Murphy, and Adele E. Clarke. "Anticipation: Technoscience, life, affect, temporality." *Subjectivity* 28, no. 1 (2009): 246-265.

Aggestam, Karin, Fabio Cristiano, and Lisa Strömbom. “Towards agonistic peacebuilding? Exploring the antagonism–agonism nexus in the Middle East peace process.” *Third World Quarterly* 36, no. 9 (2015): 1736-1753.

Aouragh, Miriyam. “Hasbara 2.0: Israel’s public diplomacy in the digital age.” *Middle East Critique* 25, no. 3 (2016): 271-297.

Aouragh, Miriyam. *Palestine online: Transnationalism, the Internet and the construction of identity*. IB Tauris, 2011.

Arquilla, John, and David Ronfeldt. “Cyberwar is coming!.” *Comparative Strategy* 12, no. 2 (1993): 141-165.

Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” *Duke Law & Technology Review* 18, no. 1 (2019): 5-7.

Betz, David J. *Cyberspace and the State: Towards a Strategy for Cyber-power*. Routledge, 2017.

Betz, David J., and Tim Stevens. “Analogical reasoning and cyber security.” *Security Dialogue* 44, no. 2 (2013): 147-164.

Björkdahl, Annika, and Susanne Buckley-Zistel, eds. *Spatialising peace and conflict: Mapping the production of places, sites and scales of violence*. Springer, 2016.

Broeders, Dennis, Fabio Cristiano, and Daan Weggemans. "Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy." *Studies in Conflict & Terrorism* (2021): 1-28.

Brounéus, Karen. “In-depth interviewing.” *Understanding Peace Research: Methods and Challenges* (2011): 130-45.

Brown, Joseph M., and Tanisha M. Fazal. “# SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations.” *European Journal of International Security* 6, no. 4 (2021): 401-417.

Buchanan, Ben. *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press, 2016.

Castells, Manuel. *The rise of the network society*. John Wiley & sons, 2011.

Cerbone, David. *Understanding phenomenology*. Routledge, 2014.

Chenou, Jean-Marie. "From cyber-libertarianism to neoliberalism: Internet exceptionalism, multi-stakeholderism, and the institutionalisation of internet governance in the 1990s." *Globalizations* 11, no. 2 (2014): 205-223.

Choucri, Nazli, and David D. Clark. *International relations in the cyber age: The co-evolution dilemma*. MIT Press, 2019.

Cohen, Julie E. "Cyberspace as/and Space." *Colum. L. Rev.*107 (2007): 210-256.

Collins, John. *Global Palestine*. Columbia University Press, 2011.

Cristiano, Fabio. "Israel: Cyber Warfare and Security as National Trademarks of International Legitimacy." *Romaniuk SN and Manjikian M.(2021 eds.) Routledge Companion to Global Cyber-Security Strategy, Basingstoke: Palgrave Macmillan* (2021).

Deibert, Ronald. "The geopolitics of cyberspace after Snowden." *Current History* 114, no. 768 (2015): 9-15.

Deibert, Ronald. "Toward a human-centric approach to cybersecurity." *Ethics & International Affairs* 32, no. 4 (2018): 411-424.

Deibert, Ronald and Louis W. Pauly. "Mutual entanglement and complex sovereignty in cyberspace." In *Data Politics*, pp. 81-99. Routledge, 2019.

Delerue, François. *Cyber operations and international law*. Cambridge University Press, 2020.

Demchak, Chris C., and Peter Dombrowski. "Rise of a cybered westphalian age." *Strategic Studies Quarterly* 5, no. 1 (2011): 32-61.

Demmers, Jolle. *Theories of violent conflict: An introduction*. Routledge, 2016.

Denning, Dorothy E. "Stuxnet: What has changed?." *Future Internet* 4, no. 3 (2012): 672-687.

Dunn Cavelty, Myriam. "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse." *International Studies Review* 15, no. 1 (2013): 105-122.

Dunn Cavelty, Myriam. *Cyber-security and threat politics: US efforts to secure the information age*. Routledge, 2007.

Egloff, Florian J., and James Shires. "The better angels of our digital nature? Offensive cyber capabilities and state violence." *European Journal of International Security* (2021): 1-20.

Egloff, Florian J., and Myriam Dunn Cavelty. "Attribution and knowledge creation assemblages in cybersecurity politics." *Journal of Cybersecurity* 7, no. 1 (2021): 1-12.

Etzioni, Amitai. *How patriotic is the Patriot Act?: freedom versus security in the age of terrorism*. Routledge, 2005.

Finlay, Christopher J. "Just war, cyber war, and the concept of violence." *Philosophy & Technology* 31, no. 3 (2018): 357-377.

Flick, Uwe. "Triangulation in qualitative research." *A companion to qualitative research* 3 (2004): 178-183.

Fouad, Noran Shafik. "The non-anthropocentric informational agents: Codes, software, and the logic of emergence in cybersecurity." *Review of International Studies* (2021): 1-20.

Gartzke, Erik. "The myth of cyberwar: bringing war in cyberspace back down to earth." *International Security* 38, no. 2 (2013): 41-73.

Gazit, Nir. "Social agency, spatial practices, and power: the micro-foundations of fragmented sovereignty in the occupied territories." *International Journal of Politics, Culture, and Society* 22, no. 1 (2009): 83-103.

Goodin, Robert E., and Charles Tilly. *The Oxford handbook of contextual political analysis*. Oxford University Press, 2006.

Graham, Mark. "Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities?." *The Geographical Journal* 179, no. 2 (2013): 177-182.

Gunkel, David J., and Ann Hetzel Gunkel. "Virtual geographies: The new worlds of cyberspace." *Critical Studies in Media Communication* 14, no. 2 (1997): 123-137.

Hagmann, Jonas, and Myriam Dunn Cavelty. "National risk registers: Security scientism and the propagation of permanent insecurity." *Security Dialogue* 43, no. 1 (2012): 79-96.

Hallett, Ronald E., and Kristen Barber. "Ethnographic research in a cyber era." *Journal of Contemporary Ethnography* 43, no. 3 (2014): 306-330.

Hansen, Lene, and Helen Nissenbaum. "Digital disaster, cyber security, and the Copenhagen School." International studies quarterly 53, no. 4 (2009): 1155-1175.

Healey, Jason. "The implications of persistent (and permanent) engagement in cyberspace." Journal of Cybersecurity 5, no. 1 (2019): tyz008.

Herrera, Geoffrey L. "Cyberspace and sovereignty: thoughts on physical space and digital space." In *Power and Security in the Information Age*, pp. 81-108. Routledge, 2016.

Hine, Christine. “Virtual ethnography: Modes, varieties, affordances.” *The SAGE handbook of online research methods* (2008): 257-270.

Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. "Data sovereignty: A review." *Big Data & Society* 8, no. 1 (2021).

Junio, Timothy J. “How probable is cyber war? Bringing IR theory back in to the cyber conflict debate.” *Journal of Strategic Studies* 36, no. 1 (2013): 125-133.

Kaufmann, Mareile, and Meropi Tzanetakis. “Doing Internet research with hard-to-reach communities: methodological reflections on gaining meaningful access.” *Qualitative Research* 20, no. 6 (2020): 927-944.

Kello, Lucas. *The Virtual Weapon and International Order*. Yale University Press, 2017.

Kello, Lucas. "Cyber legalism: why it fails and what to do about it." Journal of Cybersecurity 7, no. 1 (2021): tyab014.

Khalidi, Rashid. *The Hundred Years' War on Palestine: A History of Settler Colonialism and Resistance, 1917–2017*. Metropolitan Books, 2020.

Kinsley, Samuel. “The matter of virtual geographies.” *Progress in Human Geography* 38, no. 3 (2014): 364-384.

Kuntsman, Adi, and Rebecca L. Stein. *Digital Militarism*. Stanford University Press, 2020.

Kurowska, Xymena. “Interpreting the uninterpretable: The ethics of opaqueness as an approach to moments of inscrutability in fieldwork.” *International Political Sociology* 14, no. 4 (2020): 431-446.

Lambach, Daniel. “The territorialization of cyberspace.” International Studies Review 22, no. 3 (2020): 482-506.

Lawson, Sean T. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Routledge, 2019.

Leander, Anna. "The power to construct international security: On the significance of private military companies." *Millennium* 33, no. 3 (2005): 803-825.

Liaropoulos, Andrew. “Exercising state sovereignty in cyberspace: an international cyber-order under construction?.” *Journal of Information Warfare* 12, no. 2 (2013): 19-26.

Libicki, Martin C. *Cyberdeterrence and cyberwar*. RAND corporation, 2009.

Lindgren, Simon. *Data theory: Interpretive sociology and computational methods*. John Wiley & Sons, 2020.

Lindgren, Simon. “The concept of ‘data’in digital research.” *The SAGE Handbook of Qualitative Data Collection* (2018): 441-450.

Lindsay, Jon R. "Stuxnet and the limits of cyber warfare." Security Studies 22, no. 3 (2013): 365-404.

Lloyd, David. “Settler colonialism and the state of exception: The example of Palestine/Israel.” *Settler Colonial Studies* 2, no. 1 (2012): 59-80.

Machold, Rhys. "Reconsidering the laboratory thesis: Palestine/Israel and the geopolitics of representation." *Political Geography* 65 (2018): 88-97.

Maschmeyer, Lennart, Ronald J. Deibert, and Jon R. Lindsay. “A tale of two cybers-how threat reporting by cybersecurity firms systematically underrepresents threats to civil society.” *Journal of Information Technology & Politics* 18, no. 1 (2021): 1-20.

Maurer, Tim. *Cyber mercenaries*. Cambridge University Press, 2018.

McGraw, Gary. “Cyber war is inevitable (unless we build security in).” *Journal of Strategic Studies* 36, no. 1 (2013): 109-119.

Mueller, Milton. “Against sovereignty in cyberspace.” *International Studies Review* 22, no. 4 (2020): 779-801.

Mueller, Milton. ‘Internet Fragmentation Exists, But Not In the Way That You Think,’ Council on Foreign Relations, 6 December 2017b, https://www.cfr.org/blog/internet-fragmentation-exists-not-way-you-think.

Mueller, Milton. *Will the internet fragment?: Sovereignty, globalization and cyberspace*. John Wiley & Sons, 2017a.

Murthy, Dhiraj. “Digital ethnography: An examination of the use of new technologies for social research.” *Sociology* 42, no. 5 (2008): 837-855.

Pawlak, Patryk, Eneken Tikk, and Mika Kerttunen. “Cyber Conflict Uncoded,” EUISS 2020.

Richterich, Annika. “Tracing controversies in hacker communities: ethical considerations for internet research.” *Information, Communication & Society* 23, no. 1 (2020): 76-93.

Rid, Thomas, and Ben Buchanan. “Attributing cyber attacks.” *Journal of Strategic Studies* 38, no. 1-2 (2015): 4-37.

Rid, Thomas. *Cyber war will not take place*. Oxford University Press, USA, 2013.

Roulston, Kathryn, V. J. McClendon, Anthony Thomas, Raegan Tuff, Gwendolyn Williams, and Michael F. Healy. "Developing reflective interviewers and reflexive researchers." *Reflective Practice* 9, no. 3 (2008): 231-243.

Saco, Diana. “Colonizing Cyberspace:‘National Security’and the Internet.” *Cultures of insecurity: States, communities, and the production of danger* 14 (1999): 261-290.

Senor, Dan, and Saul Singer. *Start-up nation: The story of Israel's economic miracle*. Random House Digital, Inc., 2011.

Schneider, Jacquelyn. "The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war." *Journal of Strategic Studies* 42, no. 6 (2019): 841-863.

Shihade, Magid. "Settler colonialism and conflict: the Israeli state and its Palestinian subjects." *Settler Colonial Studies* 2, no. 1 (2012): 108-123.

Shires, James. *The Politics of Cybersecurity in the Middle East*. Oxford University Press, 2022.

Shires, James. "Cyber-noir: Cybersecurity and popular culture." *Contemporary Security Policy* 41, no. 1 (2020): 82-107.

Simons, Helen. "Case study research: In-depth understanding in context." *The Oxford handbook of qualitative research*(2014): 455-470.

Slupska, Julia. "War, health and ecosystem: generative metaphors in cybersecurity governance." *Philosophy & Technology* 34, no. 3 (2021): 463-482.

Smeets, Max. "US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection." *Intelligence and National Security* 35, no. 3 (2020): 444-453.

Spradley, James P. *Participant observation*. Waveland Press, 2016 (1980).

Stein, Rebecca L. *Screen Shots: State Violence on Camera in Israel and Palestine*. Stanford University Press, 2021.

Stevens, Tim. "Global cybersecurity: new directions in theory and methods." *Politics and Governance* 6, no. 2 (2018): 1-4.

Stevens, Tim. "Cyberweapons: an emerging global governance architecture." *Palgrave Communications* 3, no. 1 (2017): 1-6.

Stevens, Tim. *Cyber security and the politics of time*. Cambridge University Press, 2016.

Strömbom, Lisa. "Thick recognition: Advancing theory on identity change in intractable conflicts." *European Journal of International Relations* 20, no. 1 (2014): 168-191.

Suleiman, Yasir, ed. *Being Palestinian: Personal reflections on Palestinian identity in the diaspora*. Edinburgh University Press, 2016.

Swain, Jon, and Zachery Spire. "The role of informal conversations in generating data, and the ethical and methodological issues they raise." In *Forum: qualitative social research*, vol. 21, no. 1. FQS, 2020.

Sylvester, Christine. "War experiences/war practices/war theory." *Millennium* 40, no. 3 (2012): 483-503.

Taddeo, Mariarosaria. "On the risks of relying on analogies to understand cyber conflicts." *Minds and Machines* 26, no. 4 (2016): 317-321.

Taddeo, Mariarosaria. “Deterrence by norms to stop interstate cyber attacks.” *Minds and Machines* 27, no. 3 (2017): 387-392.

Tawil-Souri, Helga. "Dis-formations of Palestine." *Culture, Time and Publics in the Arab World: Media, Public Space and Temporality* 4 (2019): 17.

Tsagourias, Nicholas. “The legal status of cyberspace: sovereignty redux?.” In *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing, 2021.

Turner, Mandy. “Fanning the flames or a troubling truth? The politics of comparison in the Israel-Palestine conflict.” *Civil Wars* 21, no. 4 (2019): 489-513.

Ward, Katie J. “Cyber-ethnography and the emergence of the virtually new community.” *Journal of Information technology*14, no. 1 (1999): 95-105.

Weizman, Eyal. *Forensic architecture: Violence at the threshold of detectability*. Princeton University Press, 2017.

Weizman, Eyal. *Hollow land: Israel’s architecture of occupation*. Verso books, 2012.

Wu, Timothy S. “Cyberspace sovereignty--the Internet and the international system.” *Harv. JL & Tech.* 10 (1996): 647.

Zetter, Kim. *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Broadway books, 2014.

Zureik, Elia. “Being Palestinian in Israel.” *Journal of Palestine Studies* 30, no. 3 (2001): 88-96.

Publications

Printed by Media-Tryck, Lund 2022 NORDIC SWAN ECOLABEL 3041 0903

Lund University
Faculty of Social Sciences
Department of Political Science

Lund Political Studies 206
ISBN 978-91-8039-260-0
ISSN 0460-0037