3

Gendered and Postcolonial Perspectives on Data Weaponization in Armed Conflict

The Case of Afghanistan

Julia-Silvana Hofstetter

Introduction

After the Taliban seized control over significant parts of Afghanistan in August 2021, concerns were raised regarding the masses of personal data collected and shared over 20 years by various international actors that could put hundreds of thousands of Afghans at risk. Confirming these fears, the Taliban communicated early on that they had gained access to biometric data and started using it to identify and hunt down Afghans who had worked with international actors and the former Afghan government. Thousands of Afghans also rushed to delete their online identities and digital histories and remained in hiding over a year after the takeover, still fearing death by data. In the aftermath of the seizure, technology companies, such as Facebook and Twitter, and international and regional civil society organizations quickly came to help Afghans, providing support and guidance on how to erase their online identities and evade surveillance.

The case of Afghanistan has forced the international community to reassess how data collection and digital communication tools become risk factors for vulnerable populations in times of crisis. Yet, while a growing body of research and policy debate addresses how digital technologies increasingly impact conflict dynamics and provide authoritarian regimes and conflict parties with new instruments to perpetrate violence and persecute adversaries, the risks of data weaponization in armed conflict are still underexplored, particularly regarding gender-specific vulnerabilities.

Based on an empirical analysis of Afghanistan, the chapter explores how conflict actors weaponize personal data to prosecute adversaries and how

Julia-Silvana Hofstetter, *Gendered and Postcolonial Perspectives on Data Weaponization in Armed Conflict*
In: *Critical Perspectives on Cybersecurity*. Edited by: Anwar Mhajne and Alexis Henshaw, Oxford University Press.
 DOI: 10.1093/oso/9780197695883.003.0004

this affects women and other marginalized groups. It discusses the role of data collected by international actors—from foreign militaries to international humanitarian organizations and national government agencies—and personal information, available online and accessed through surveillance technology. The chapter also discusses the limitations of the international community's emergency response strategies. Finally, analyzing the case of Afghanistan through a postcolonial and feminist perspective, the chapter further builds theory on how gendered and colonial discriminatory structures and ideologies enable and shape data weaponization in conflict contexts and also outlines how deconstructing these underlying factors serves to improve data management and crisis response mechanisms addressed at mitigating the risks of data weaponization in conflict contexts, emphasizing citizens' digital agency and the need to address gender-specific vulnerabilities.

Literature Review and Research Gaps

The chapter speaks to three main areas of policy debate and scholarly literature that approach data weaponization through different angles: digital authoritarianism, humanitarian data governance, and gender-based cyber violence. Especially the discussion on technocolonialism in the humanitarian sector and feminist approaches to cybersecurity hold valuable insights for a deeper discussion of a postcolonial and gender-sensitive analysis of data weaponization, as discussed in more detail later in the chapter.

Under the term "digital authoritarianism," a growing body of literature analyzes how authoritarian regimes increasingly use digital technologies for political repression, including strategies ranging from censoring online content to spreading online propaganda and disinformation, online harassment, or digital surveillance (e.g., Dragu and Lupu 2021). Digital repression strategies aim to not only assert control by prosecuting political opponents directly but also limit civic spaces for political mobilization. In extreme cases, states establish an all-encompassing and society-wide surveillance ecosystem, instrumentalizing vast amounts of digital data ranging from social media activities to online consumption behavior, travel bookings, medical records, and cell phone location data to identify possible threats to their authority. In this context, "data weaponization" can be defined as a digital repression strategy in which data gathering and digital surveillance are used to identify and locate political opponents or specific demographic groups to

control and, in severe cases, physically harm them. Digital data and modern technologies allow repressive governments to assess or identify who is a political opponent or part of the target group as well as to locate already identified targets with greater efficiency and precision. Current discussions in the field also address the critical role of private companies cooperating with authoritarian regimes, providing invasive surveillance technologies or sharing user data from apps and social media platforms. While feminist scholars have long pointed to the dangers of authoritarian regimes using gender politics and prosecuting women human rights defenders to secure their power (e.g., Lorch and Bunk 2016), less research exists on how technology facilitates these tactics. In the literature on digital authoritarianism, the weaponization of data aimed at discriminating against women as well as other gender and sexual minorities has not been systematically studied yet. The few scholars that analyze digital repression strategies by state actors through a gendered lens primarily focus on online harassment and disinformation against women in politics (Bardall 2023) and LGBTQ groups (Acconcia et al. 2022), and some authors have also looked at the gendered impacts of internet shutdowns (Shoker 2022). Recent examples of data sharing between reproductive health apps providers and anti-abortion politicians in the US or reports of government agencies infiltrating dating apps to identify and arrest LGBTQ individuals in Egypt, Iran, and Lebanon also indicate the need for further analysis of the gender-specific vulnerabilities of seemingly non-weaponizable data in light of state surveillance.

Human rights organizations are also increasingly documenting cases where governments use surveillance and other strategies of digital repression in the context of armed conflict. For example, well documented is the Syrian regime's systematic expansion of a mass surveillance system resulting in arrests, torture, and deaths of opponents (Dávila et al. 2021). Also, recent examples from Myanmar, where online harassment against women drastically increased in the aftermath of the military's seizure of power in February 2021 (Al Jazeera Staff 2023), raise questions on how fragile contexts and armed conflict settings alter and increase certain gendered risks associated with digital authoritarianism.

While systematic research on the specificities of digital repression in armed conflict is still lacking, the literature on humanitarian data governance can provide some insight into the difficulties of data protection and privacy in fragile contexts (see, e.g., Jacobsen and Fast 2019). Humanitarian organizations have considerable experience with collecting and managing

highly sensitive data in conflict-affected contexts and how the potential abuse of sensitive data puts vulnerable populations at risk—not only in cases where sensitive information falls into the hands of warring factions due to data leakages or data breaches, but also where humanitarian organizations voluntarily share data with third-party actors such as host governments, multilateral organizations, and private service providers likewise opening up opportunities for the weaponization of sensitive data. Under the terms of "surveillance humanitarianism" (Latonero 2019) and "technocolonialism" (Madianou 2019), humanitarian organizations have been criticized for their extensive use of biometric technology, which reproduces colonial forms of exploitation, extraction, and control. By theorizing colonial mechanisms that shape data collection in armed-conflict contexts, this literature also helps better understand the enabling factors of data weaponization in fragile contexts. However, while the literature on humanitarian data governance offers essential insights into the dangers of digital data in armed-conflict contexts, especially biometric data, other data sources and types, such as public data collected by national governments or social media and other online data, are not being addressed. Also, a gender perspective is still largely missing. Although data governance guidelines from the humanitarian sector acknowledge women and other gender and sexual minorities as especially vulnerable groups, an in-depth discussion on the gendered risks associated with humanitarian data does not exist.

The growing field of policy and academic literature on gender-based cyberviolence helps address this gap to a certain extent. "Cyberviolence" refers to a wide range of technology-facilitated violence, from cyberstalking to online hate speech and harassment, the nonconsensual sharing of private information, and attacks on communication channels. This literature offers insights into the gendered risks associated with cyberviolence not only at the individual level, for example, where women and other gender and sexual minorities are at a higher risk from privacy breaches that lead to physical violence (Yao 2019; Brown and Pytlak 2020), but also at the societal level, for instance, when limited access to technology or verified online information further limits these groups' access to economic opportunities or education or when online violence leads to the (self-)silencing of these voices in public discourse. Beyond gendered cyberviolence, current discussions in the broader field of cybersecurity policy also consider gender-specific risks associated with cybersecurity threats that are not gendered, for example, when cyberattacks on critical infrastructure have

different consequences for different population groups. However, much of the literature on gender-based cyberviolence focuses on the citizen-to-citizen level. It is based on a traditional understanding of cybersecurity where the state is seen as the primary security provider and is generally not considered a cyber-threat actor for its citizens. Acknowledging that the state can be a perpetrator of gender-based cyberviolence as well would be crucial to capture gendered cybersecurity risks in their entirety while allowing one to make a connection to the digital authoritarianism literature. Critical cybersecurity studies have long advocated for such a shift in the conceptualization of cybersecurity toward a human-centric approach (see, e.g., Deibert 2018). While conventional definitions of cybersecurity focus on businesses and state infrastructure as targets of cyberattacks and nonstate-threat actors with criminal objectives as perpetrators, human-centric cybersecurity focuses on threats to citizens. It allows for conceptualizing the co-production of cybersecurity (on citizen co-production of cybersecurity, see Chang Zhong and Grabosky 2018), where citizens and civil society are contributors to the security infrastructure. The traditional focus of cybersecurity scholars and practitioners on state institutions as targets of cyberattacks is also reflected in the emerging field of cyberwar research, which focuses on interstate cyber conflict and critical infrastructure and military data as targets of cyberattacks (e.g., Shires 2020; Smeets 2018; Thomas and Zhang 2020).

This chapter adds to the literature discussed above by analyzing data weaponization in armed conflict, relying on a human-centric definition of cybersecurity and adding a feminist and postcolonial lens. It connects different research strains and fills a gap in the discussions on the nexus between digital repression, gender, and armed conflict.

Postcolonial and Feminist Theory

For the empirical analysis of data weaponization in the context of the 2021 Taliban takeover in Afghanistan, the chapter applies concepts from feminist and postcolonial studies as a theoretical framework. Theoretical notions of technocolonialism help explain the formation of the digital infrastructure in fragile contexts that enables data weaponization, while feminist theory allows informing the discussion on how patriarchal ideology shapes data weaponization opportunities and gender-specific vulnerabilities.

Technocolonialism

Two main logics help describe how the use of technology in the context of humanitarian operations reflects and reconstructs colonial relationships and power hierarchies between international actors and local populations (broadly based on Madianou 2019): Colonial rationality places primacy in the governing potentials of external actors and inferiorizes local populations, which strips their agency and rights and reproduces relationships of dependency; the discriminatory structures of colonial legacies enable the extraction of value from humanitarian data through public and private actors, especially when humanitarian crises are treated as testing sites for new technological applications.

The colonial logic legitimizes international actors to prioritize the collection of vast amounts of data and the deployment of invasive surveillance technologies to assert control in crisis situations over local populations' rights to data privacy and agency. This de-prioritization of the local population's digital rights creates a "digital underclass" forced to share data in exchange for basic needs without the dignity of choice (Latonero 2019).

The technocolonialist critique also sheds light on how this colonial logic enables various stakeholders, from humanitarian organizations to donor countries and private companies, to use humanitarian crises for value extraction. Moreover, this extractive dynamic is reinforced by technology as it introduces a "capitalist logic" to the humanitarian sector that merges humanitarian aid with business interests (Madianou 2019, 5), where humanitarian settings are seen as investment opportunities (see, e.g., Aglionby 2018) or used as testing sites for new technologies (such as the iris-scan devices deployed by EyeHood in UNHCR refugee camps; see Leurs et al. 2019, 94–96). Technocolonialism's critique, however, also expands to the colonial behavior of global technology companies and social media platforms in the Global South in general, where these actors pay less attention to data security standards of their devices and services, are often reluctant to invest resources in online content moderation that would make online spaces safer (Takhshid 2021), or provide free services to extract personal data (Vaidhyanathan 2018; Bhatia 2016).

Data Privacy and Surveillance in the Patriarchy

A gender analysis of data weaponization in armed conflict involves examining how gender roles influence individuals' needs, opportunities, activities, and

rights. A few key concepts from feminist research on patriarchy (Hunnicutt 2009; Runyan and Peterson 2013.) can help guide such an analysis. First, patriarchal ideology retains gender as a central organizing feature of society. Patriarchal societies are based on systems of male domination and female subordination. Men are positioned at the head of households, communities, and states, which incentivize heterosexual family structures and the repatriation of women to the private sphere. Thus, gender discrimination in patriarchal societies also has implications for defining what constitutes sensitive data. Whether data puts individuals at risk for political prosecution or discrimination depends on preexisting discriminatory structures reflected in society and in government institutions. Suppose the government is based on a patriarchal ideology that discriminates against women. In that case, specific categories of information that are not sensitive for men can put women and other gender and sexual minorities at risk. Moreover, patriarchal control is not only asserted with state violence. The social control mechanisms are also based on women's victimization and emphasis on threats to their security in public spheres, which places them in a constant state of fear and makes them compliant with the system by incentivizing self-censoring (Stanko 1985).

The Case of Afghanistan

Afghanistan and the recent Taliban takeover are crucial to address the research gap between the literature discussed earlier and build a theory on gender-specific vulnerabilities of data weaponization in armed conflict. While most of the literature on digital authoritarianism has looked at how authoritarian regimes gradually turned to technology to repress citizens—based on the same discriminatory structures but using new, digital means—Afghanistan constitutes a case of a relatively sudden regime change, where the technological infrastructure for surveillance and data weaponization was already in place, but where the regime change brought about a shift toward an extremist ideology of governing institutions. This shift in terms of who controls the data weaponization enabling infrastructure also has consequences for the types and sources of public and online data that potentially put people at risk and should be considered "sensitive" data. Thus, looking at the Taliban takeover allows us to think further about how data privacy considerations should consider shifts in the political environment. Afghanistan also allows adding to the literature that discusses specific risks associated with digital repression in contexts of armed conflict. The strong

presence of international actors, the vast amount of data gathered, and the biometric technology left behind when these actors left the country make Afghanistan a relevant case and allow us to analyze data weaponization from a postcolonial perspective. Moreover, analyzing the crisis response of various stakeholders in the context of the Taliban takeover also holds lessons for the improvement of data management and crisis preparedness of governments, multilateral actors, and foreign militaries, as well as regarding multistakeholder emergency response mechanisms that involve civil society organizations, technology platforms, and affected citizens. Lastly, since the Taliban's governance system is based on a highly patriarchal, misogynist ideology, this also allows analyzing how digital instruments of repression mainly affect women and other gender and sexual minorities.

The Who, What, and Why of Data Collection in Afghanistan

Started in the context of the global war on terror and the rising availability of new technological possibilities, the US and its allies built a vast infrastructure of data collection and surveillance in Afghanistan over the last two decades—in the name of security, government accountability, and modernization (Jacobsen 2021a). With as many actors involved in the funding, deployment, and management of data collection programs as in Afghanistan—from international institutions such as the World Bank and the United Nations that funded or helped build extensive databases of biometric and other personal data for the former Afghan government, with the support of foreign and national technology companies such as Grand Technology Resources, Leidos, and Netlinks, while foreign governments and militaries such as the US also collected data for their operations on the ground—it is difficult to trace who precisely collected which data, where the data is stored, who it was shared with, and if there might have been data breaches. However, several databases have faced criticism regarding the risks they pose if they fall into the wrong hands long before the Taliban takeover in 2021. Most concerns were raised regarding the possible abuse of the US Defense Department Automated Biometric Identification System (ABIS) and the Afghan Automated Biometric Identification System (AABIS) (Toft Djanegara 2021; Access Now 2021). While the biometric data collected in Afghanistan constitutes only a small part of the data-gathering practices of a much larger digital and nondigital information infrastructure, these databases received the most

attention. Biometric data is particularly sensitive since it is almost impossible for data subjects to deceive these information systems. Moreover, digitized, searchable databases make it much easier for malicious actors to use personal data to identify and surveil targets.

To analyze data collection processes in Afghanistan through a gendered and postcolonial lens, it is helpful to categorize three actor groups that somewhat differ in the rationales they had for data collection, the data security standards they implemented, and the segments of the Afghan population they collected data on: foreign militaries, especially the US military; the former Afghan government; and international humanitarian organizations, such as United Nations High Commissioner for Refugees (UNHCR) and the World Food Program (WFP).

The ABIS, which the US military operates with NATO and local forces, holds biometric data from over 2.5 million Afghans (Voeltz 2016, 187). The US military collected the data to identify individuals it believed might pose a security risk but also contained information on Afghans working for the US government. The data was reportedly used to identify persons on the battlefield thousands of times and was supposed to be a key innovation in the United States' counterinsurgency strategy, allowing the military to separate insurgents from the civilian population with great precision (Gershgorn 2019). Likely based on the assumption that combatants are usually men, the data gathered by the US military had a specific focus on males of fighting age (Shanker 2011). Notable about the system is that the US military also deployed portable scanning devices for iris, fingerprint, and face pattern recognition, the Handheld Interagency Identity Detection Equipment (HIID), that were widely distributed across security forces on the ground, and which allowed them to scan through millions of digital files in a matter of seconds, even at remote checkpoints.

Also, the former Afghan government collected vast amounts of (biometric) data with the help of international actors and technology corporations. Most notably: The AABIS, which was developed by the US and NATO and administered by the Ministry of Interior in Kabul, collected biometric data from criminals as well as army and police applicants, to keep Taliban infiltrators out of the Afghan army; the Ministry of Interior and Defense Afghan Personnel and Pay Systems (APPS) used to administer payments for the national army and police, and into which the AABIS was subsequently integrated in early 2021; and the Afghan National Biometric System, on of the Afghan national identity card system, called e-Tazkira, was based. Notable

about the APPS, which holds data on more than 700,000 security forces, is the range of information it contains for each profile. Its more than 40 data fields include sensitive relational data, such as employees' grandparents' names and ties to community members, and seemingly random details, such as recruits' favorite fruits and vegetables (Guo and Noori 2021).

While the ABIS, AABIS, and APPS contained security-sector-related data, the Afghan National Biometric System held data on diverse population segments and a wide range of public institutions used it. The database includes fingerprints and iris scans of about 9 million Afghans, which Afghanistan's National Statistics and Information Authority collected with the support of the International Organization for Migration (IOM). Moreover, the e-Tazkira system holds a wealth of personal and biometric data, including a person's name, ID number, place and date of birth, gender, marital status, religion, ethnicity, language, profession, iris scans, fingerprints, and photographs. The ID was needed to access a vast range of public services. For example, it was required to obtain passports; driver's licenses; birth, death, and marriage certificates; to register land and property; to take civil service and university entrance exams; for employment with the public sector and much of the private sector; to register mobile SIM cards (which were needed for mobile banking); obtain bank loans; and to vote. It was praised for empowering women, especially in registering land ownership and securing bank loans.

Two other databases that received much less international attention but which hold equally sensitive personal data are the payroll system of the Afghan Supreme Court, which has extensive personal data on all judges as well as their family members, including biometrics, current addresses, and license plate numbers; and the payroll system of the National Directorate of Security, the former Afghan state intelligence agency that was established by the US Central Intelligence Agency after 2001 and entirely funded by the US government, and which contains the same sensitive information on their staff.

Similarly, humanitarian actors have collected data linked to millions of Afghans, including biometric data, to improve the efficiency of aid delivery and prevent fraud. The WFP, for example, has registered more than 6 million Afghans in its biometric beneficiary management system for food and cash transfers (WFP 2020). Also, UNHCR introduced mandatory iris recognition as early as 2002 to collect data on millions of former Afghan refugees who returned from Pakistan over the past 20 years (UNHCR 2021).

While databases containing personal information on government and especially security-sector employees received much more attention after the takeover in 2021—regarding the risk of this data being used by the Taliban to prosecute adversaries—the abuse of databases such as the e-Tazkira ID system might impact Afghans daily lives on a much broader scale. Also, from a gender perspective, databases such as e-Tazkira and the payroll system of the Supreme Court and humanitarian data and databases that contain information on citizens that received government aid might have just as sensitive information as security-sector-related and biometric data.

A colonial perspective explains how the invasive data collection structure developed by foreign militaries (based on a securitization rationale) together with the striving for a comprehensive digitization of the Afghan administration and the extensive data gathering on government employees (which can be attributed to the need to meet donors' accountability expectations and ideas of good governance) ultimately led to prioritizing the fight against corruption and terrorism over Afghans' right to data privacy. It also highlights how the US military and humanitarian actors used Afghanistan as a testing ground for new technologies. The US military, for example, deployed biometric devices in Afghanistan to test their performance in different climates (Shanker 2011). But also humanitarian actors, such as the UNHCR and the WFP, ran pilot programs to test new technological applications despite the risks such experimental technologies carry, regarding not only data privacy but also the dangers of being denied access to humanitarian support in light of their high failure rates (Hosein and Nyst 2013).

How the Taliban Accessed and Weaponized Data

Following the withdrawal of foreign militaries from Afghanistan in August 2021, many feared the Taliban would gain access to the vast amounts of data that a variety of international and national actors had been collecting over two decades and use this data to identify Afghans that had worked for or collaborated with international actors and the former Afghan government. Early reports by human rights organizations and UN agencies documented hundreds of enforced disappearances and killings of individuals with ties to the former government, particularly members of the Afghan National Security Forces, from military personnel to police, intelligence service members, judges and prosecutors, and civil servants (Amnesty International

2022a). However, not only representatives from the security and justice sector became a target, but also regime critics, journalists, human rights activists, the LGBTQ community, and women working in any profession the Taliban deemed unsuitable for them were prosecuted. This forced hundreds of thousands of Afghans into hiding, frequently moving between safe houses or attempting to flee the country altogether.

While most concerns on the potential dangers of sensitive data falling into the hands of the Taliban focused on data collected by international actors and the former Afghan government discussed above, concerns have also been raised regarding the risks associated with two additional data sources: online data that might be used to get access to personal information to identify and prosecute political opponents and vulnerable groups (from social media platforms such as Facebook; to email and messaging apps; to websites of governments, businesses, civil society organizations, and media outlets) and surveillance technologies (e.g., by gaining control over the state-owned Afghan Telecom, which enables access to phone records and geolocation data). While it is difficult to determine which data the Taliban have access to, rumors and fear of such possibilities alone already had a decisive impact on the life of ordinary citizens in Afghanistan and even jeopardize their security, for example, in cases where the fear of having to undergo biometric screening prevented citizens from accessing public services such as healthcare facilities (Nader and Amini 2022).

However, evidence gathered by human rights organizations and the Taliban's official statements suggest that they are likely to have gotten at least partial access to biometric data on Afghan police and army members; former collaborators with foreign governments and aid agencies; payroll data of the national security agency and the Supreme Court (Watkins 2021; Human Rights Watch 2021; Gall 2021); US military biometric devices (Klippenstein and Sirota 2021); and data from the e-Tazkira ID system. Already in August 2021, the Taliban publicly stated that they had access to biometric data and scanning devices and that they had mobilized a special unit, the Al Isha, to use this data to identify and hunt down Afghans who had worked with US and allied forces (Roy and Miniter 2021). Moreover, concerns have been raised regarding the Taliban possibly gaining access to government databases only accessible by authorized users, by forcing former government employees or by hacking these systems, possibly with technical assistance from foreign governments, such as Pakistan's ISI intelligence service, a long-time ally of the Taliban, likely also interested in these data bases for its

national security agenda. But also Chinese, Russian, and Iranian intelligence are expected to offer such services. Equally concerning is the possibility that the Taliban could use biometric technology not only to access existing biometric databases but also to expand them by registering citizens on their own (Bajak 2021). The Taliban have reportedly approached former Afghan government employees in charge of the national data systems to extend national data sets.[1]

Fewer concerns were raised regarding the Taliban accessing the information on employees of international humanitarian actors and data collected on beneficiaries of humanitarian aid because international humanitarian organizations stored their data on servers outside of Afghanistan. However, despite the sector's decades of experience in managing sensitive data and high-security standards, risks remain that humanitarian data is not entirely out of reach for malicious actors in conflict regions. A cautionary example of this is a reported incident from early 2022, where the International Committee of the Red Cross (ICRC), a role model when it comes to data security standards in the humanitarian sectors, was the victim of a cyberattack in which hackers seized data from servers located in Switzerland and thereby gained access to personal data from over 515,000 extremely vulnerable individuals worldwide (ICRC 2022). Moreover, data is routinely shared among humanitarian actors and often with local governments and military actors on the ground that is administered by private security providers. UNICEF Afghanistan, for example, provided cash transfers to vulnerable families with adolescent girls as part of a program to support girls' education and prevent child marriage (Awad and Nezami 2020). Often administered through commercial service providers, cash transfer programs are hazardous regarding exposing sensitive data and making their recipients targets for the Taliban's prosecution.

Besides gaining control over biometric databases and technology, the Taliban quickly turned to social media platforms and other online data to identify and persecute opponents. Reportedly, they used information from social media platforms, like Facebook or LinkedIn and websites of governments, businesses, and civil society organizations, to identify people who have worked for the former Afghan government, foreign security forces, or international NGOs. They evaluated photos available online, for example, with facial-recognition software, and searched people's mobile phones for contacts in email and messaging apps at checkpoints and during home visits (Welchering 2021). Worried about retribution, many Afghans rushed to delete their online identity and digital history, erasing social media profiles,

deleting foreign contacts on their phones, and resetting devices to their factory settings (Stokel-Walker 2021). The Taliban's presence on social media platforms has also silenced regime critiques on social media.[2]

Concerns have also been raised regarding the Taliban's control over the state-owned telecommunication company Afghan Telecom, from which the Taliban regime could order phone records and geolocation data, for example, to trace calls to international actors or visits to military bases. While Afghan Telecom initially also managed the country's internet service, in the mid-2010s, the country started to open up to private telecommunication operators, such as the United Arab Emirates' Etisalat Group and South Africa's MTM Group (Cerulus 2021). Concerns have been raised that the Taliban might try to pressure these companies for access to data records and messaging logs to gather information on exit visa applications, for instance. Afghans also fear for their access to the internet and other telecommunication services, as these companies could eventually be forced or simply incentivized to discontinue their services in Afghanistan for good.

The Prosecution of Women Since the Taliban Takeover in 2021

Since the Taliban takeover in 2021, the Ministry for the Propagation of Virtue and Prevention of Vice has issued a series of policies and guidelines that increasingly restrict women's most basic rights and exclude them from public life, barring them from their workplaces, from higher education, and from moving freely (Davidian 2022). Human rights organizations also reported increased repressive measures against female human rights defenders and women who went to the streets to protest the new oppressive rules, from threats to arrests, detentions, torture, and forced disappearances. Most measures have made women invisible, pushed them back into private spaces, and silenced them in public debates. However, women's situation in Afghanistan not only worsened due to direct repressive measures by Taliban members but the new rules established by the regime have also been reported to be enforced by family and community members on their own accord or upon receiving instructions from the Taliban (Stancati 2021). In addition, outsourcing surveillance and repression to community and family members has allowed the Taliban to control women in physical or online spaces that the Taliban government itself does not have direct access to. While many

Afghan women have been faced with social control by their communities long before the Taliban takeover in 2021, the control that male community members can, and feel obligated to, exercise over women's daily lives was decisively and structurally increased due to new government decrees that made male family members responsible for women's and girls' adherence to the new rules and put them at risk for detention if female family members fail to comply (Amnesty International 2022b, 37).

While most of the new restrictions target Afghan women in general and put them at risk for prosecution and detention if they don't comply, there are also specifically vulnerable groups whose chances of becoming a target for prosecution is facilitated by the Taliban's ability to weaponize digital and online data. For example, the Taliban have been reported to take tough actions against women who protested and spoke out against the newly imposed restrictive rules. This also included women voicing their criticism on social media, even when using private profiles.

Moreover, survivors of domestic and sexual violence have faced a particularly dire situation since the Taliban took over in 2021. They closed down women's shelters and released domestic violence perpetrators from prison. Many survivors reported that their newly released perpetrators are now hunting them down, often husbands and family members, and by the Taliban, who have been reported to imprison former shelter residents. Survivors and divorced women or women who live separated from their husbands in general also fear being forcibly separated from their children. However, not only survivors of domestic and sexual violence are at risk, also many women who worked within the system of protective services for gender- based violence survivors—including shelter staff, psychologists, doctors, lawyers, prosecutors, judges, employees of the Ministry of Women's Affairs, and others—are hiding in secret locations, fearing revenge from the Taliban, as well as convicted perpetrators and family members of survivors (Amnesty International 2022b, 47). Service providers reported being forced to flee their houses and change their phone numbers, receiving daily threats. Especially former judges fear arrests by the Taliban due to their reported access to the Afghan Supreme Court payroll database, which holds extensive personal information. A judge known for her work on domestic violence cases reported that not only her own home but also her mother's house was searched by Taliban fighters the first night they had taken control of her city, with both addresses only maintained in the payroll database (Human Rights Watch 2022). But also other vulnerable groups that received support from

international actors were put at risk by the personal data they shared with support organizations. The Taliban have, for instance, been reported to have compiled "hit lists" for the Afghan LGBTQ community based on information that international organizations such as Rainbow Railroad, an international LGBTQ organization based in Afghanistan, voluntarily shared with the Taliban in the context of evacuation requests and through data leakages and phishing attacks (Nordstrom 2021).

Gender-Specific Vulnerabilities of Data Weaponization

Based on the empirical analysis of Afghanistan, this chapter identified gendered risks of data weaponization in patriarchal societies on three levels:

1. Preexisting discriminatory beliefs and structures in government and society define what type of information can be weaponized, which extends the range of data that can be risky for women and other marginalized groups and the range of weaponization strategies and implementing actors.
2. Discriminated, already vulnerable, groups are more likely to be captured as data subjects in humanitarian and government databases due to their higher dependence on support and protection services and restricted data privacy rights and provisions.
3. Women's and other marginalized groups' limited access to public spheres in patriarchy make them more dependent on ICTs in their daily lives and thus more vulnerable to digital surveillance and the repercussions from other digital repression strategies such as internet shutdowns.

Concerns regarding biometric and other digitized personal data gathered by international actors and the former Afghan government focused on the risks of personally identifiable data of former employees in the security sector and collaborators with international organizations. Likewise, efforts to erase this data before leaving the country focused on security-sector data that was considered especially sensitive. While women worked in these sectors, more men are affected by the risks this data poses. However, looking at the conceptualization of "sensitive" data through a gendered lens, it becomes evident that data from other sectors and government programs also pose severe

risks to individuals facing discrimination under the new Taliban regime. Information categories that would not be considered sensitive for men can be weaponized against women and other vulnerable groups. In the context of Afghanistan, evidence of any aspect of daily life that is restricted by the Taliban's gender roles and which could be considered immoral behavior for women—from women exercising fundamental rights such as working in a specific sector, owning a business or land, being enrolled at a university, exercising political rights, participating in sports, or simply being outspoken in public—has to be considered sensitive information that could put women at risk. This has consequences for considering what kinds of public databases and what types of online platforms hold sensitive information that can be weaponized. In Afghanistan, this included anything containing information that could be linked to activities considered immoral behavior for women, which ranges from registers of land ownership to data on bank loans, driver's licenses, and voter registries, as well as online data and identities, such as businesses websites, online journalism, political activism online, social media behavior, and messaging. Especially women involved in public life, from human rights defenders (PBS 2021), journalists (Banville 2021), politicians (Faheid 2021), business owners (Bhalla 2021), and activists (Smith and Mengli 2021), rushed to delete their online identities for fear of becoming a target of the Taliban's reprisals.

Preexisting discriminatory beliefs in the broader society also allow governing actors to outsource the surveillance and prosecution of women they want to target to community members, thus expanding the range of implementing actors and creating additional opportunities to weaponize the information they extract. The patriarchal system implemented by the Taliban can rely not only on those community members who already share their ideology as accomplices for data weaponization against women but also creates new accomplices by holding male family members responsible for women's behavior. This is facilitated through technology, as reaching out and mobilizing a large number of accomplices via social media platforms has become more manageable in the digital age, and the increased accessibility of spy- and stalker-ware enable the surveillance and tracking of family members through something as simple as a mobile app purchase.

Additionally, the impact data weaponization has on its targets is also gendered. For women living in patriarchal societies, publishing intimate photos or private conversations online can lead to alienation, harassment, and physical attacks within their communities. In contexts like Afghanistan, where

patriarchal ideology condemns the public display of any behavior that the Taliban confines to private spaces, the destruction of the inviolability of women's private spaces (physically in their homes and their digital devices or also virtually in private online communication spaces), due to the proliferation of invasive surveillance technology, creates an atmosphere of constant fear that their personal information could be used against them at any point, which means that women self-censor their behavior even in the private spaces they have been pushed back into. For example, beyond the context of Afghanistan, women rights activists have been reported to fear the repercussions of state surveillance in countries such as Jordan and Bahrain, with some women whose devices were hacked feeling forced to wear a veil even when home alone, afraid of being watched (Fatafta 2022).

Looking through a feminist and postcolonial lens also explains why women and other marginalized groups might be more likely to appear as data subjects in humanitarian and government databases. This is due to their vulnerable position in society, which makes them more likely to depend on government support and protection services in general and on humanitarian aid in fragile contexts in particular. In patriarchal societies, women might rely on state services and humanitarian assistance more often as they are more affected by gender-based violence, live in economically more precarious situations due to limited access to income and independent housing, and rely more on public shelters. In addition, they might carry more significant financial burdens due to childcare, to name just a few examples. Marginalized groups are also more often dependent on the support of civil society organizations and humanitarian actors as they might have to hide or flee from political repression. Afghan women and children, for example, made up the majority of refugees who fled to Pakistan and Iran after the armed conflict broke out in Afghanistan in 1979 (Khan 2002).

Moreover, patriarchal societies often assign women the role of victims, treating them as a vulnerable group in need of protection or equating them with legal minors who have no agency over their lives. A similar process of victimization and incapacitation can be observed in the humanitarian sector, where international actors treat local populations in fragile contexts as incapable and needing external protection. Both cases legitimize prioritizing protective measures over the individual's right to data privacy and agency, creating a power imbalance between the data subject and the controller. The greater the power imbalance between the data controller and the subject, the

more invasive or extractive the data collection process. Vulnerable groups are more likely to suffer from lower data privacy and protection provisions since they are in a weaker position to stand up for privacy rights or to give meaningful consent to sharing their data. In Afghanistan, databases that reflect such gender-based vulnerabilities and could be used to target women and other marginalized groups include databases containing information on support structures for victims of domestic and sexual violence (from hospital records to court files and shelter registries). These civil society support systems were in contact with or collected data on the LGBTQ community, government assistance programs for single mothers, refugee registries, financial aid programs for women's rights organizations, and many more. The extent to which databases contain sensitive information and who could become targets is not always straightforward. For instance, child protection databases could also hold sensitive information on single mothers and victims of sexual violence.

Lastly, women are particularly vulnerable to data weaponization due to their greater dependence on information and communications technologies when navigating their everyday life in patriarchal societies, where women's roles in and access to the public sphere are limited.

Following the withdrawal of US troops from Afghanistan, social media has been crucial for Afghans in sharing information, organizing to find support, and escaping the new regime. But the dependence on internet access and ICTs have disproportionally increased for women. With the Taliban restricting women's right to free movement and access to employment, education, healthcare, and other public services, many Afghan women have resorted to online use (Scollon 2021). In addition, patriarchy's banishment of women to the private sphere increases their dependence on ICTs in their private as well as political life to stay connected with family members and friends, to mobilize and advocate for their rights, or to access news or information, and, particular to crises, to reach out to the international community to share their stories or ask for help.

While the private space can also be a powerful site for advocacy, and technology might facilitate agency and provide an alternative platform to stay connected, women's resulting use and dependence on ICTs also make them more vulnerable to the risks of digital surveillance and cause more significant harm to them if their access to ICTs is restricted, due to internet shutdowns for example.

International Responses to Data Weaponization in Crisis Situations

This section discusses the international community's response to the risk of data being weaponized by the Taliban after their takeover in 2021. It examines how different actor groups can help vulnerable populations protect and delete sensitive data in crises. It also highlights the downsides and challenges of erasing sensitive data in these contexts. The section subsequently argues that international actors need to develop a comprehensive strategy for dealing with sensitive data in conflict contexts and crises, emphasizing the role of a multistakeholder approach. It also discusses how these strategies can be improved by applying a gendered and postcolonial lens, from data governance practices and data privacy considerations in fragile contexts to emergency response mechanisms addressing the risks of online data weaponization.

How Different International Actors Supported the Erasure of Sensitive Data After the Taliban Takeover

In the run-up and aftermath of the Taliban takeover in 2021, foreign governments and international organizations rushed to delete data they had collected, and technology companies, such as Google, Facebook, and Twitter, as well as civil society organizations, supported Afghans in erasing their online identities and evading surveillance.

Aware of the danger that sensitive data might fall into the hands of the Taliban after coalition troops left the country, foreign militaries, humanitarian actors, and diplomats destroyed equipment, scrubbed databases, and removed evidence of Afghan employees and collaborators from government websites before they evacuated (Jacobs et al. 2021). Social media platforms reacted quickly to the Taliban takeover in August 2021 by helping Afghans safely remove their social media profile content or temporarily suspend their accounts, making it more challenging to search others' social media profiles (Culliford 2021). Facebook, for example, created a "one-click tool" that allowed citizens to delete their accounts and temporarily removed the ability for people to view or search the friends lists of accounts in Afghanistan. Twitter closely monitored and suspended suspicious accounts and contacted the NGO Internet Archive to delete sensitive tweets archived on the

platform. Similarly, LinkedIn temporarily hid the connections of its users in Afghanistan so the Taliban could not see individuals' network contacts.

However, the efforts by international actors who operated the vast data infrastructure in Afghanistan have been criticized for their shortcomings in a comprehensive emergency data erasure strategy, leading to rushed and insufficient measures. Human rights organizations also called out international actors for missing to inform data subjects in Afghanistan about the use of their data, which should have included revisiting data risk assessments and communication with data subjects regularly but also calling on them to improve transparency regarding data breaches as the crisis unfolded in 2021 (Human Rights Watch 2022).

Social media companies have been criticized for reacting too slowly to help Afghan people safely remove their profile content and for not translating help pages into local languages (Glaser and Smith 2021). Calls were also raised for search engines, such as Google, to accelerate the delisting of sensitive information and for technology companies to pledge to deny governments backdoors to private data and to invest in encryption and prevention of data leakages.

Stepping in for governments' and private actors' shortcomings, regional and international civil society networks played a crucial role in supporting Afghans with information on deleting their digital history and evading biometrics. Organizations such as Access Now, the Digital Rights Foundation, and Human Rights First ran helplines for Afghans seeking advice on erasing their digital traces. In addition, they quickly translated guidelines on evading biometrics and deleting digital histories in local Afghan languages.

Challenges with Data Protection and Trade-Offs of Deleting Online Information

While the case of Afghanistan has proven that the erasure of online identities and sensitive data collected by public actors is crucial to protect vulnerable populations in crises, there remains challenges and considerable downsides associated with the removal of online information and the deletion of official data in such contexts.

Practical challenges of deleting sensitive data include, for example, the possibility that data can be forensically reconstructed and delistings circumvented with virtual private networks (VPNs). Some humanitarian

organizations even abstain from having clauses on data deletion in data collection consent forms, seeing themselves unable to guarantee this in light of complex data-sharing processes and fragile contexts (Jacobsen 2021b). Moreover, there might be more time to erase online data only once a crisis arises. For example, in Afghanistan, the Taliban had already kept records on journalists, government employees, and women's rights activists before the takeover of Kabul.

Even if data deletion is successful, erasing personal data in crises comes with considerable trade-offs. Many Afghans, especially the ones who collaborated with foreign militaries and the former Afghan government but also other groups that were outspoken critics of the Taliban, such as journalists, found themselves faced with a dilemma: the exact data that put them at risk for being targeted by the Taliban was also a crucial proof of their status as refugees when applying for emergency evacuation and asylum. Also, dependence on social media and mobile phone contacts to stay in touch with allies within Afghanistan and abroad to exchange information and seek support made deleting profiles and contacts difficult. Similarly, taking down social media profiles and online content produced by female journalists and activists also meant silencing women's voices in the public sphere. Moreover, data sets and online articles documenting international crimes and other human rights abuses in Afghanistan, while holding significantly compromising information for victims and witnesses, constitute essential evidence for international prosecution of war crimes (Milaninia 2021).

Lastly, trade-offs are associated with erasing online information that raises critical questions from a democratic perspective. There is an inherent trade-off between people's right to privacy and free access to information. Especially in fragile contexts, concerns regarding the proliferation of sensitive information online could be abused by authoritarian regimes as a pretext to cover-up human rights abuses or censor regime critics—thereby serving rather than preventing digital repression. There is also a common concern regarding the discretion given to corporations, such as Google, in weighing personal safety risks versus public interest when deciding what information is delisted in search results for instance.

Coming up with a comprehensive response to the risks associated with data weaponization in the context of armed conflict will thus have to balance these trade-offs, which might include extending strategies of digitally archiving information securely or temporarily limiting access to online content, as well as in-depth discussions on how decision-making processes in

the context of removing sensitive online information can be democratized. Moreover, given the time sensitivity of crises, the difficulty will be in speeding up these processes as part of a comprehensive multistakeholder emergency response mechanism.

Rethinking Data Governance and Cybersecurity Emergency Support Through a Gendered and Postcolonial Lens

The analysis of Afghanistan has demonstrated the need for better emergency support mechanisms involving multiple stakeholders—from multilateral actors, technology companies, and civil society organizations—and for improved data management practices to prevent data weaponization in crisis and regime change situations.

Regarding the emerging threat of the weaponization of online identities, the international community will need to develop best practices and emergency response mechanisms for the erasure of sensitive data while mitigating potential trade-offs. A more in-depth discussion must be held on how to prevent the establishment of data infrastructures that enable the weaponization of data when it comes to data collected and managed by public actors, from national governments, multilateral organizations, and foreign militaries. Next to more transparent communication regarding data breaches and emergency support for affected individuals once a crisis has unfolded, these efforts will have to address the root causes of extractive data collection in conflict contexts. Once collected, securing and erasing sensitive data in a crisis is almost impossible to guarantee, especially in light of an extensive data infrastructure that involves as many actors as in Afghanistan. Accordingly, discussions on data management in the aftermath of the Taliban takeover centered on lessons learned and preventative strategies and urged international and humanitarian actors to commit to storage time and purpose limitations (Human Rights Watch 2022).

While the humanitarian sector's decades of experience with the collection and management of highly sensitive data in fragile contexts has produced valuable best practices and guidelines (see, e.g., ICRC 2020; Inter-Agency Standing Committee 2021) on data protection and ethical data governance in fragile contexts, including critical concepts such as "do no digital harm" and "data minimization," as well as remedy mechanisms for victims of data protection violations, the analysis of Afghanistan sheds light on how these

discussions need to be elaborated by filling blind spots on gender-specific vulnerabilities and by further deconstructing colonial logics.

Analyzing Afghanistan through a gender lens has pointed out three levels on which such blind spots need to be addressed in the current discussion on data weaponization after the Taliban takeover: Gender impacts (1) what has to be considered "sensitive" information, expanding the scope of relevant databases and online information beyond the security sector; (2) the means and mechanisms of data weaponization, shedding light on the role of community members as accomplices and shifting the focus on the surveillance of private homes, mobile devices, and private online spaces; and (3) the security threats resulting from digital repression, which urges one to consider not only direct physical violence and prosecution but also indirect and structural consequences of data weaponization such as creating an atmosphere of constant fear and the self-silencing of women.

The first blind spot implies the need to improve data management practices and emergency response mechanisms to be informed by gender-specific risk analyses. The second blind spot highlights that international efforts to mitigate the risks of data weaponization also need to address and condemn the proliferation of surveillance technology and hold technology platforms accountable for securing online spaces, including guaranteeing data privacy standards and withholding from sharing sensitive data with third actors. Also, women's specific vulnerabilities regarding the risk of silencing them completely in public (online) spaces within Afghanistan and abroad must be considered in this context. Finally, it also makes the case that the international community needs to assess risks associated with surveillance technologies and online security beyond the immediate crisis and regime transition period, as the consequences of data weaponization under the newly established extremist patriarchal regime hold not only direct threats to women's physical safety but also has society-wide, long-term consequences.

The field of feminist data governance and internet principles (see, e.g., APC's "Feminist Principles of the Internet") hold valuable insights for addressing the challenges discussed above. Next to emphasizing a human rights perspective on internet governance, relevant feminist concepts on which this field is based include consent, anonymity, and control over one's online memory. This includes, for example, the critique of guaranteeing meaningful consent in light of lacking transparency on privacy breaches and deceptive terms of services. Using allegories of victim blaming, this literature also discusses the problem that digital hygiene solutions put the burden of

cybersecurity on the user rather than addressing structural risks in digital infrastructure directly, for example, holding technology companies and telecommunication service providers accountable.

Colonial logics underpinning the establishment of data infrastructures in contexts of armed conflict also have implications for the improvement of data weaponization mitigation strategies, as they not only establish the vast amount of data that is being collected in these contexts but also restrict local populations' ability for digital self-protection due to lack of inclusion and transparency.

Armed-conflict contexts have a high surveillance potential and vast amounts of data collected. These extractive data collection practices are based on the deprioritization of local populations' digital rights, combined with the presence of numerous international actors employing different kinds of technological innovations for various reasons (securitization, efficiency, donor accountability, or market logic). Additionally, the reproduction of colonial power hierarchies also increases the local population's dependence on international actors regarding data protection and cybersecurity in crisis situations. Local people's lack of agency regarding the data collected on them also expands to a need for more agency regarding data handling in crisis response mechanisms. Missing to involve affected citizens in data management mechanisms has especially dire consequences if, like in Afghanistan, international actors in charge of data management flee the site of the conflict and leave citizens behind to bear the risks associated with the collected data but not with the agency to mitigate them.

The disinterest of ICT providers and technology platforms to invest in data protection standards of digital devices, online content moderation, and local language capacities in the Global South opens up opportunities for the weaponization of online identities and restricts local citizens' ability to mitigate these threats on their own accords.

Current discussions in humanitarian data management and decolonial approaches to technology use and proliferation more broadly offer insight into providing citizens with greater agency regarding their data. Human rights–based approaches to humanitarian data management advocate the concept of "data agency," which includes the concepts of informed consent, participation, and notification of data collection and uses (Greenwood et al. 2017). Broader discussion from decolonial data and technology research (see, for example, Couldry and Mejias 2023) expand on these notions calling to boycott extractivist technologies and use alternative tools to reappropriate

data and the products of data on behalf of the data subjects to hold technology companies accountable for the damage done by their products and to educate the public on digital literacy, cybersecurity, and digital rights. Discussion in the context of digital self-determination further calls for digital infrastructures that promote individuals' self-determination, including equal and free access, better privacy protections, and control over their online identities, emphasizing the role of digital literacy on how to protect oneself from government and corporate surveillance and exploitation online, sometimes also referred to as "digital self-defense" (on the concept of digital self-defense, see Kwet 2020).

While civil society organizations have made efforts to restore the agency of local populations in the context of Afghanistan by strengthening their digital literacy—including awareness raising regarding digital hygiene and surveillance protection strategies and translating social media protection protocols to local languages—postcolonial approaches to data management, data agency, and digital self-determination could help the international community to come up with more comprehensive crisis response strategies to mitigate data weaponization risks. Emphasizing the need for a multistakeholder approach and cybersecurity co-production should include the following:

- Holding technology companies accountable.
- Relying on local civil society organizations' expertise regarding affected populations' needs.
- Empowering citizens by strengthening their digital agency and the ability for digital self-defense.

Conclusion

Building on theoretical concepts from feminist and postcolonial studies and insights from an empirical analysis of data weaponization in the aftermath of the Taliban takeover in 2021, the chapter built theory on how gendered and colonial discriminatory structures and ideologies shape data weaponization strategies in the context of armed conflict and regime change, and it discussed how deconstructing these underlying factors should inform data management and crisis response mechanisms to mitigate the risks of data weaponization.

The chapter argued that colonial logics adopted by international actors—from international humanitarian organizations to multilateral donor organizations, foreign militaries, and technology companies—create a digital infrastructure that is based on invasive technology use and extractive data collection practices and that deprioritizes local populations' data protection and digital rights, leading to the collection of vast amounts of data containing highly sensitive personal information, which lays the groundwork for data weaponization enabling digital infrastructure. It further finds that in contexts where the ruling regime holds a patriarchal ideology, especially in contexts of sudden regime change toward this ideology, women and other marginalized groups face additional risks. In patriarchal societies, gender defines what has to be considered sensitive information, how data weaponization is implemented, and its consequences on the individual and societal levels. Patriarchal ideology extends the scope of information that can be weaponized. It allows outsourcing the implementation of digital repression strategies to citizens who hold the same doctrine. It makes women and other marginalized groups more likely to become data subjects due to their higher dependence on government support and protection services and limited ability to assert their data privacy rights. Additionally, women and other marginalized groups limited access to public spheres in patriarchy makes them more dependent on ICTs, increasing their susceptibility and vulnerability to digital repression.

The chapter also discussed how international and regional actors helped Afghans to protect and delete sensitive data in the aftermath of the Taliban takeover, and it pointed out the challenges and trade-offs associated with the erasure of sensitive data in crisis situations, referring to practical difficulties with data deletion (insufficient or too late), to the trade-off of crucial information getting lost (in the light of Afghans' dependence on online identities when trying to flee the country; their reliance on social media and digital contact databases to stay in contact with allies within the country and abroad; the silencing of women and other vulnerable groups voices in the national and international public sphere; the documentation of human rights violations that is crucial evidence for the international prosecution of war crimes); and broader anti-democratic implications (if data protection is used by authoritarian governments as a pretense to cover up human rights abuses; risks giving decision power to technology companies on what online information gets removed). Analyzing these dynamics through a postcolonial and gendered lens also helped identify blind spots in international actors' emergency

response. The gender lens helped identify additional relevant data sources beyond the security sector and made the case to expand considerations to the complicity of implementing data weaponization strategies by community members but also technology companies proliferating surveillance capabilities, and it made the case why these response strategies also need to consider long-term structural consequences of gendered vulnerabilities of data weaponization in terms of creating an atmosphere of fearing constant surveillance and censorship of women. The postcolonial lens emphasizes the need to strengthen affected populations' digital rights and agency in conflict contexts, holding not only international actors accountable that collect and manage sensitive data but also technology companies gatekeeping people's safety online, drawing from local civil societies' knowledge of the situation on the ground and strengthening citizens' ability for digital self-defense.

Building theory on gendered vulnerabilities of data weaponization in armed conflict, the chapter helped fill gaps in several bodies of literature dealing with data weaponization: The literature on digital authoritarianism, which lacks a gender perspective and does not account for the specific vulnerabilities in the context of armed conflict and regime change; discussions in the context of humanitarian data governance and technocolonialism, which miss emphasizing local populations' right to data agency beyond data protection and neglect the risks and responsibilities associated with online identities; and research on gender-based cyberviolence, which mainly focuses on the citizen-to-citizen level and dangers posed to the individual, failing to make bridges to structural consequences on a societal level. Moreover, adding a new perspective to discussions on the cyberdimension of armed conflict, the chapter makes a case for bringing together critical cybersecurity studies notions on human-centric cybersecurity—which emphasizes that the state can be a perpetrator of cyberviolence toward its citizens and that cybersecurity should be co-produced by multiple stakeholders including individual citizens—with discussions around international cyberwar and multilateral cybersecurity efforts, the latter of which usually center on responsible state behavior in the context of interstate conflicts and threats posed by external cybersecurity threat actors.

The critical cybersecurity perspective and the emphasis on cybersecurity co-production are especially relevant in fragile contexts, where the state cannot guarantee citizens' data privacy and safety online, or in authoritarian regimes where the state is a threat actor. Multilateral cybersecurity discussions should address the international community's role and responsibilities in

contexts where state actors cannot provide their citizens with cybersecurity. Especially regarding the provision of an emergency response to data weaponization risks in armed conflict, the international community should consider its responsibilities as a cybersecurity provider. Following human-centric conceptualizations of cybersecurity co-production, such efforts should be conceptualized as multistakeholder processes, acknowledging the crucial role that national and regional civil society organizations play in providing local expertise and the need to emphasize strengthening citizens' ability for digital self-defense and data agency.

Notes

1. Interview with a representative of an international human rights organization, January 2023.
2. "Their intelligence is monitoring everything. . . . Whatever I do, there will be a reaction from the Taliban," reported a participant of the street protests that followed the Taliban's invasion of Kabul in August 2021 about her social media postings, when interviewed by Amnesty International (Amnesty International 2022).

References

Access Now. 2021. "Civil Society Calls on International Actors in Afghanistan to Secure Digital Identity and Biometric Data Immediately." https://www.accessnow.org/cms/assets/uploads/2021/08/Civil_Society_Afghanistan_Biometrics_Letter.pdf.

Acconcia, G., A. Perego, and L. Perini. 2022. "LGBTQ Activism in Repressive Contexts: The Struggle for in Visibility in Egypt, Tunisia and Turkey." *Social Movement Studies*, 1–19. DOI: 10.1080/14742837.2022.2070739.

Aglionby, J. 2018. "World Bank Urges Private Sector Interest in Refugee Camps." *Financial Times*, May 5. https://www.ft.com/content/e2d6588a-5042-11e8-b3ee-41e0209208ec.

Al Jazeera. 2023. "Myanmar Women Target of Online Abuse by Pro-Military Social Media." Al Jazeera, January 26. https://www.aljazeera.com/news/2023/1/26/myanmar-women-target-of-online-abuse-by-pro-military-social-media?utm_source=substack&utm_medium=email

Amnesty International. 2022a. "Afghanistan" In *Amnesty International Report 2021/22*, 64–68.

Amnesty International. 2022b. *Death in Slow Motion: Women and Girls Under Taliban Rule*. https://www.amnesty.org/en/documents/asa11/5685/2022/en/.

APC. 2016. "Feminist Principles of the Internet." https://www.apc.org/en/pubs/feminist-principles-internet-version-20.

Awad, M., and S. Nezami. 2020. "Cash Transfer Supports Girls' Education in Afghanistan." UNICEF. loombergn

Bajakt, F. 2021. "U.S.-Built Databases, Biometric Data a Potential Tool of the Taliban." PBS, September 7. https://www.pbs.org/newshour/world/u-s-built-databases-biometric-data-a-potential-tool-of-the-taliban.

Banville, K. 2021. "'We see silence filled with fear'": Female Afghan Journalists Plead for Help." *The Guardian*, August 16. https://www.theguardian.com/world/2021/aug/16/we-see-silence-filled-with-fear-female-afghan-journalists-plead-for-help.

Bardall, G. 2023. "Nasty, Fake and Online: Distinguishing Gendered Disinformation and Violence Against Women in Politics." In *Gender and Security in Digital Space*, ed. Gulizar Haciyakupoglu and Yasmine Wong, 109–123. Routledge.

Bhalla, N. 2021. "'Now, we are back to zero': Afghan Businesswomen on the Run." Reuters, August 26. https://www.reuters.com/article/us-afghanistan-women-business/now-we-are-back-to-zero-afghan-businesswomen-on-the-run-idUSKBN2FR1SJ.

Bhatia, R. 2016. "The Inside Story of Facebook's Biggest Setback." *The Guardian*, May 12. https://www.theguardian.com/technology/2016/may/12/facebook-free-basics-india-zuckerberg.

Brown, D., and A. Pytlak. 2020. *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom.

Cerulus, R. 2021. "Fears Loom over Afghanistan's Internet." POLITICO, August 25. https://www.politico.eu/arti cle/Afghanistan-braces-for-fight-over-taliban-internet-information-control/.

Chang, L. Y., L. Y. Zhong, and P. N Grabosky. 2018. "Citizen Co-Production of Cybersecurity: Self-Help, Vigilantes, and Cybercrime." *Regulation & Governance* 12, no. 1: 101–114.

Couldry, N., and U. A. Mejias. 2023. "The Decolonial Turn in Data and Technology Research: What Is at Stake and Where Is It Heading?" *Information, Communication & Society* 26, no. 4, 1–17.

Culliford, E. 2021. "Facebook, Twitter and LinkedIn Secure Afghan Users' Accounts Amid Taliban Takeover." Reuters, August 20. https://www.reuters.com/article/us-afghanistan-conflict-social-media-idCAKBN2FK2D7.

Davidian, A. 2022. "The Situation of Women and Girls in Afghanistan." Press Briefing, UNWOMEN. https://www.unwomen.org/en/news-stories/speech/2022/07/press-briefing-the-situation-of-women-and-girls-in-afghanistan.

Dávila A, S., N. Guruli, and D. Samaro. 2021. "DIGITAL DOMINION: How the Syrian Regime's Mass Digital Surveillance Violates Human Rights." UIC Law White Papers, March 2021. https://repository.law.uic.edu/whitepapers/20

Deibert, R. J. 2018. "Toward a Human-Centric Approach to Cybersecurity." *Ethics & International Affairs* 32, no. 4: 411–424.

Dragu, T., and Y. Lupu. 2021. "Digital Authoritarianism and the Future of Human Rights." *International Organization* 75, no. 4: 991–1017.

Faheid, D. 2021. "These Female Afghan Politicians Are Risking Everything for Their Homeland." NPR, August 18. https://www.npr.org/2021/08/18/1029014825/afghan-women-politicians-taliban-resistance.

Fatafta, M. 2022. "Unsafe Anywhere: Women Human Rights Defenders Speak Out About Pegasus Attacks." Access Now. https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/.

Gall, C. 2021. "As the Taliban Tighten Their Grip, Fears of Retribution Grow." *New York Times*, August 29. https://www.nytimes.com/2021/08/29/world/asia/afghanistan-taliban-revenge.html.

Gershgorn, D. 2019. "Exclusive: This Is How the U.S. Military's Massive Facial Recognition System Works." *OneZero Medium,* November 6. https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d.

Glaser, A., and S. Smith. 2021. "As Taliban Search Phones, Experts Fear Security Features Aren't Enough to Keep Afghans Safe." NBC News, August 20. https://news.yahoo.loombeiban-violence-drives-afghans-wipe-154040354.html.

Greenwood, F., C. Howarth, D. E. Poole, N. A., Raymond, and D. P. Scarnecchia. 2017. "The Signal Code: A Human Rights Approach to Information During Crisis." Harvard Humanitarian Initiative. https://hhi.harvard.edu/publications/signal-code-human-rightsapproach-information-during-crisis

Guo, E., and H. Noori. 2021. "This Is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban." *MIT Technology Review*, August 30. https://www.technologyreview.com/2021/08/30/1033loombergnstan-biometric-databases-us-military-40-data-points/.

Hosein, G., and C. Nyst. 2013. "Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries." https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326229.

Human Rights Watch. 2021. *"No Forgiveness for People Like You": Executions and Enforced Disappearances in Afghanistan Under the Taliban*.

Human Rights Watch. 2022. "New Evidence That Biometric Data Systems Imperil Afghans." Human Rights Watch, March 30. https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans.

Hunnicutt, G. 2009. "Varieties of Patriarchy and Violence Against Women: Resurrecting 'Patriarchy' as a Theoretical Tool." *Violence Against Women* 15, no. 5: 553–573.

Inter-Agency Standing Committee. 2021. *IASC Operational Guidance on Data Responsibility in Humanitarian Action*. https://interagencystandingcommittee.org/operational-response/iasc-operational-guidance-data-responsibility-humanitarian-action.

International Committee of the Red Cross. (ICRC). 2020. *Handbook on Data Protection in Humanitarian Action*· 2nd ed. https://www.icrc.org/en/publication/430501-handbook-data-protection-humanitarian-action-second-edition.

International Committee of the Red Cross. (ICRC). 2022. *Cyber Attack on ICRC: What We Know.* https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know#:~:text=Update%3A%2024%20June%202022.,in%20a%20sophisticated%20cyber%20attack.

Jacobs, J., N. Wadhams, and J. Wingrove. 2021. "U.S. Embassy in Kabul Told to Destroy Files in Case Taliban Wins." Bloomberg, August 13. https://www.bloomberg.com/news/articles/2021-08-13/u-s-embassy-shredding-burning-documents-in-case-taliban-wins.

Jacobsen, A. 2021a. *First Platoon: A Story of Modern War in the Age of Identity Dominance*. New York: Dutton.

Jacobsen, K. L. (2021b). "Biometric Data Flows and Unintended Consequences of Counterterrorism." *International Review of the Red Cross* 103, no. 916–917, 619–652.

Jacobsen, K. L., and L. Fast. 2019. "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care." *Disasters* 43: S151–S168.

Khan, A. 2002. "Afghan Refugee Women's Experience of Conflict and Disintegration." *Meridians: Feminism, Race, Transnationalism* 3, no. 1: 89–121.

Klippenstein, K., and S. Sirota. 2021. "The Taliban Have Seized US Military Biometrics Devices." *The Intercept*, August 17. https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/.

Kwet, M. 2020. *People's Tech for People's Power: A Guide to Digital Self-Defense & Empowerment*, September 1. https://ssrn.com/abstract=3748901 or http://dx.doi.org/10.2139/ssrn.3748901.

Latonero, M. 2019, "Stop Surveillance Humanitarianism." *New York Times*, July 11. https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html.

Leurs, K. 2019. Migration Infrastructures. In *The Sage Handbook of Migration and Media*, ed. K. Leurs, K. Smets, M. Georgiou, S. Witterborn, and R. Gajjala, 91–102. London: Sage.

Lorch, J., and B. Bunk. 2016. "Gender Politics, Authoritarian Regime Resilience, and the Role of Civil Society in Algeria and Mozambique." GIGA-German Institute of Global and Area Studies Working Paper 292.

Madianou, M. 2019. "Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises." *Social Media + Society* 5, no. 3, 1–13.

Milaninia, N. 2021. "Evidence Destruction and the Crisis in Afghanistan." Just Security, August 20. https://www.justsecurity.org/77831/evidence-destruction-and-the-crisis-in-afghanistan/.

Nader, Z., and N. Amini. 2022. "The Taliban Are Harming Afghan Women's Health." *Foreign Policy*, March 2. https://foreignpolicy.com/2022/03/02/the-taliban-are-harming-afghan-womens-health/.

Nordstrom, L. 2021. "The Taliban Has a Hit List for the Afghan LGBT Community, NGO Says." *France24*, November 2. https://www.france24.com/en/asia-pacific/20211102-the-taliban-has-a-kill-list-for-the-afghan-lgbt-community-ngo-says.

PBS. 2021. "Taliban Interrogating Women Activists, Creating a 'Climate of Fear and Intimidation." August 18. https://www.pbs.org/newshour/show/taliban-interrogating-women-activists-creating-a-climate-of-fear-and-intimidation.

Roy, S., and R. Miniter. 2021. "Exclusive: First-Ever Interview with Terror Leader Who's Hunting Americans and Allies in Afghanistan." *Zenger News*, August 28. https://www.zenger.news/2021/08/28/taliban-team-is-using-us-made-biometric-database-and-scanners-to-hunt-american-and-afghan-enemies/.

Runyan, Anne Sisson, and V. Spike Peterson. 2013. *Global Gender Issues in the New Millennium*. 4th ed. Boulder, CO: Westview Press.

Scollon, M. 2021. "Armed With Online Option, Afghan Girls Say 'Bring It On' When It Comes to Taliban Education Ban." RFERL, November 5. https://www.rferl.org/a/afghan-girls-online-education/31547925.html.

Shanker, T. 2011. "To Track Militants, U.S. Has System That Never Forgets a Face." *New York Times*, July 13. https://www.nytimes.com/2011/07/14/world/asia/14identity.html.

Shires, James. 2020. "The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics." *Texas National Security Review* 3, no. 4: 10–28.

Shoker, S. 2022 "What Can Internet Shutdowns Tell Us About Gender and International Security?" In *Gender and Security in Digital Space*, ed. Gulizar Haciyakupoglu and Yasmine Wong, 33–48. London: Routledge.

Smeets, Max. 2018. "The Strategic Promise of Offensive Cyber Operations." *Strategic Studies Quarterly* 12, no. 3: 90–113.

Smith, S., and A. Mengli. 2021. "Wave of Killings Targets Afghan Female Judges, Journalists, Intellectuals." NBC News, January 24. https://www.nbcnews.com/news/world/wave-killings-targets-afghan-female-judges-journalists-intellectuals-n1255302.

Stancati, M. 2021. "After Taliban Return, Afghan Women Face Old Pressures from Fathers, Brothers." *Wall Street Journal*, December 15. https://www.wsj.com/articles/after-taliban-return-afghan-women-face-old-pressures-from-fathers-brothers-11639564204.

Stanko, E. 1985. *Intimate Intrusions: Women's Experiences of Male Violence*. London: Routledge.

Stokel-Walker, C. 2021. "Afghans Are Racing to Erase Their Online Lives." *Wired*, August 17. https://www.wired.co.uk/article/afghanistan-social-media-delete.

Takhshid, Z. 2021. "Regulating Social Media in the Global South." *Vanderbilt Journal of Entertainment and Technology Law* 24: 1.

Thomas, Elise, and Albert Zhang. 2020. "Snapshot of a Shadow War in the Azerbaijan-Armenia Conflict." *The Strategist*, October 9. aspistrategist.org.au/snapshot-of-a-shadow-war-in-the-azerbaijan-armenia-conflict.

Toft Djanegara, N. 2021. *Biometrics for Counter-Terrorism: Case Study of the US Military in Iraq and Afghanistan*. Privacy International.

UN High Commissioner for Refugees (UNHCR). 2021. "Government Delivered First New Proof of Registration Smartcards to Afghan Refugees." May 25. https://www.unhcr.org/pk/12999-government-to-deliver-first-new-por-smartcards-to-afghan-refugees.html.

Vaidhyanathan, S. 2018. *Anti-Social Media*. Oxford: Oxford University Press.

Voelz, G. 2016. "Catalysts of Military Innovation: A Case Study of Defense Biometrics." *Defense AR Journal* 23, no. 2: 178.

Watkins, A. 2021. "An Assessment of Taliban Rule at Three Months." *CTC Sentinel*, 14, no. 9, 1–14.

Welchering, P. 2021. "'Taliban jagen ihre Gegner auch via Netz." *Golem*¸ August 20. https://www.golem.de/news./afghanistantaliban-jagen-ihre-gegner-auch-via-netz-2108-158996.html.

World Food Program. (WFP). 2020. *Annual Country Report 2020: Afghanistan*. https://www.wfp.org/operations/annual-country-report/?operation_id=AF01&year=2020#/20257.

Yao, S. 2019. "Gender Violence Online." In *Handbook on Gender and Violence*, ed. L. Shepherd, 217–230. Cheltenham, UK: Edward Elgar.