





Digitisation and Sovereignty in Humanitarian Space: Technologies, Territories and Tensions

Aaron Martin^a, Gargi Sharma^a, Siddharth Peter de Souza ^a, Linnet Taylor ^a,
Boudewijn van Eerd^a, Sean Martin McDonald^b, Massimo Marelli^c,
Margie Cheesman ^d, Stephan Scheel ^e, and Huub Dijstelbloem^f

^aTilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, Netherlands; ^bCenter for International Governance Innovation; ^cInternational Committee of the Red Cross, Geneva, Switzerland; ^dOxford Internet Institute, University of Oxford, Oxford, UK; ^eTransnational Cooperation and Migration Research, Institute of Sociology, University of Duisburg-Essen, Essen, Germany; ^fInstitute for Advanced Study, University of Amsterdam, Amsterdam, Netherlands

ABSTRACT

Debates are ongoing on the limits of – and possibilities for – sovereignty in the digital era. While most observers spotlight the implications of the Internet, cryptocurrencies, artificial intelligence/machine learning and advanced data analytics for the sovereignty of nation states, a critical yet under examined question concerns what digital innovations mean for authority, power and control in the humanitarian sphere in which different rules, values and expectations are thought to apply. This forum brings together practitioners and scholars to explore both conceptually and empirically how digitisation and datafication in aid are (re)shaping notions of sovereign power in humanitarian space. The forum’s contributors challenge established understandings of sovereignty in new forms of digital humanitarian action. Among other focus areas, the forum draws attention to how cyber dependencies threaten international humanitarian organisations’ purported digital sovereignty. It also contests the potential of technologies like blockchain to revolutionise notions of sovereignty in humanitarian assistance and hypothesises about the ineluctable parasitic qualities of humanitarian technology. The forum concludes by proposing that digital technologies deployed in migration contexts might be understood as ‘sovereignty experiments’. We invite readers from scholarly, policy and practitioner communities alike to engage closely with these critical perspectives on digitisation and sovereignty in humanitarian space.

Controversy and Power in Digital Humanitarian Action

Aaron Martin, Gargi Sharma, Siddharth Peter de Souza, Linnet Taylor and Boudewijn van Eerd

This forum¹ on digitisation and sovereignty in humanitarian space follows a series of high-profile political controversies over the past few years involving the use of data analytics and digital technology as part of humanitarian interventions. These controversies arose due to questions of transparency, accountability and the exclusionary nature in which the technologies in question were designed and deployed. In this introduction we set the stage by presenting three critical moments in particular, each of which has triggered considerable international debate and reflection among humanitarian practitioners, civil society and others on the sector's continued embrace of digital innovation, and draw attention to some of the emergent tensions within notions of digital sovereignty (cf. Pohle and Thiel 2020).

The first controversy is a partnership between the United Nations (UN) World Food Programme (WFP) and Palantir, an American data analytics firm (WFP 2019a). In 2019, WFP announced it would be using Palantir's technology to help streamline the delivery of food and cash-based assistance across its global operations. Civil society criticism of the partnership has addressed the possibility for Palantir to access sensitive information about WFP's beneficiaries, raised concerns about Palantir's business model and risks of technological lock-in and bemoaned the lack of transparency surrounding the agreement (Easterday 2019). On a structural level, the partnership also exposes tensions at the intersection of privately provisioned humanitarian technology and state sovereignty. WFP's operational data provides Palantir with deep insights regarding global food in/security. Their access to this information has heightened concerns among host states about the involvement of a private technology firm with strong ties to the US security establishment in sensitive humanitarian work. Palantir's CEO has even since stated that, "the core mission of our company always was to make the West, especially America, the strongest in the world, the strongest it's ever been, for the sake of global peace and prosperity" (as quoted in Feuer 2020). At first blush, such a mission statement is at odds with core humanitarian principles, namely those emphasising neutrality ("humanitarian actors must not take sides") and independence ("humanitarian action must be autonomous from political, economic, military or other objectives") in the humanitarian mission (UNOCHA 2012).

A second case involves a 2019 announcement by Facebook and several commercial and non-profit partners – including Mercy Corps, a global non-governmental, humanitarian aid organisation – to launch a cryptocurrency and cross-border financial infrastructure to empower the 'financially excluded' across the world. Critics have argued that this initiative conflates humanitarian rhetoric with a for-profit structure (Kaurin 2019). National regulators from all

corners of the world scrutinised the plans and pushed back on the initiative, in part due to a perceived encroachment on the state's monetary sovereignty. The project was scaled back to appease regulators (Rodriguez 2021; Stacey and Murphy 2020) and in early 2022 was quietly abandoned (Heath 2022). The international backlash against this perceived technological threat to state sovereignty – despite its legitimisation as a humanitarian enterprise – demonstrates the need for a critical analysis of these themes.

A third introductory case is WFP's decision, also in 2019, to suspend food aid distribution in parts of Yemen, following the local Houthi authority's refusal to accept the introduction of a biometric registration system. For WFP, biometrics are an important technological means to control food aid and to prevent fraud in aid distribution. The agency had argued that "the integrity of our operation is under threat and our accountability to those we help has been undermined" by the Houthis' refusal to allow the use of biometrics to facilitate the delivery of food aid (WFP 2019b). WFP's decision to suspend aid in this case set a critical precedent – it was the first time that a humanitarian organisation had withdrawn assistance in response to local resistance to the use of digital technology. As justification for their actions, the Houthis stated that they "refuse the enrolling of beneficiaries in a biometrics programme because it is counter to national security" and that the collection of biometric data by WFP is part of an intelligence operation (Parker and Slemrod 2019). While a compromise was eventually reached as regards the system design (Weitzberg et al. 2021, 3), it is telling that in this case the Houthis were not raising concerns over data protection or privacy per se – their resistance was primarily motivated by geopolitics and sovereignty concerns (cf. Couture and Toupin 2019), even though the Houthi movement is not an internationally recognised state.

Together, these three examples illustrate the timeliness of a dedicated reflection on the possible interpretations – and repercussions – of digitisation and sovereignty in humanitarian space. In the contributions that follow, humanitarian practitioners and critical scholars delve deeper into these thorny issues from different perspectives and offer insights on the most pressing concerns, including cybersecurity risks, the sovereignty challenges of repurposing technologies in humanitarian spaces, and the power imbalances between technology firms, aid organisations and the beneficiaries of aid. The contributions are both conceptual – exploring different meanings and tensions around the contours of sovereignty in the digital realm – and empirical: using case studies the authors offer insights into how sovereign power is exercised and contested in humanitarian spaces.

Following Collinson and Elhawary (2012), the forum understands the notion of 'humanitarian space' to have several different possible conceptualisations depending on the problem framing:

- Humanitarian space as ‘**agency space**’ reflects the idea of there existing a humanitarian environment within which agencies operate neutrally and impartially while maintaining a clear distinction between their roles and functions and those of other actors (military, political, etc.);
- Humanitarian space as ‘**affected community space**’ expands the range of actors whose interests are worthy of analysis. While humanitarian agencies are still important to this conceptualisation, it foregrounds the positions of affected communities, particularly in terms of rights, protection and aid;
- Humanitarian space as ‘**international humanitarian legal space**’ focuses on the actions of warring parties in particular and the legal obligations that serve to regulate the behaviour of these actors;
- Humanitarian space as a ‘**complex political, military and legal arena**’ emphasises the contexts in which humanitarian action takes place, highlighting both the deeply political nature of humanitarian intervention and that “humanitarian needs (and their relief) are a product of the dynamic and complex interplay of political, military and legal actors, interests, institutions and processes” (Collinson and Elhawary 2012, 2).

The three cases introduced above represent different manifestations of humanitarian space. Whereas the case of WFP’s partnership with Palantir could be seen as occupying (and challenging) humanitarian space *as agency space*, Facebook’s failed cryptocurrency proposals aimed to co-opt humanitarian space *as affected community space* by attempting to use financial inclusion as a means to evade global financial regulation. In the third controversy, the Houthi’s refusal to accept the use of biometrics in exchange for aid demonstrates how humanitarian space can be viewed *as a complex political, military and legal arena*. The forum’s interlocutors further build on these conceptualisations in their analysis of digital sovereignties of different kinds. In what follows we summarise these contributions and reflect on what they mean for power in humanitarian space.

Sean Martin McDonald, a data governance practitioner and scholar, lays the conceptual groundwork for the forum and in doing so problematises the debate on both the ‘digital’ and ‘sovereignty’. He observes different challenges facing humanitarian organisations, which not only depend on grants of sovereign authority to be able to operate, but also to be able to balance rights towards political neutrality, in order to fulfil duties to beneficiaries.

Building on this, Massimo Marelli, who leads the Data Protection Office at the International Committee of the Red Cross (ICRC), critically reflects on what emergent cyber risks and security incidents mean for the digital sovereignty of humanitarian organisations. He is particularly concerned with the sovereignty implications for International Organisations such as the ICRC,

which operate in what Collinson and Elhawary (2012) term ‘international humanitarian legal space’. He questions how humanitarian practitioners can manage and mitigate their dependencies on the digital systems and supply chains that introduce new vulnerabilities to the sector.

Margie Cheesman, a digital anthropologist, engages contemporary debates about humanitarianism and alternative economies from the perspective of the digitisation of payments to recipients of humanitarian aid using blockchain technology. She elucidates three cross-cutting aspects of sovereignty in these debates: frictions around national jurisdiction in humanitarian finance, unresolved questions about the expanding influence of technology firms in payment infrastructures, and doubtful visions of the autonomy of aid beneficiaries since aid organisations have ultimate monopoly over the choice of partner. She concludes that while blockchain is widely touted as a revolutionary ‘frontier technology’ of the digital age, that frontier is likely to be settled by the usual actors of corporate and state power.

In his contribution, the sociologist Stephan Scheel introduces the concept of ‘parasitic sovereignty’, which he develops to help explain the extension of the intended uses of digital technologies beyond their initial purposes through the exercise of sovereign power. Scheel raises attention to how these technologies often have a ‘dual use’ in the humanitarian sector, wherein their employment as tools of social care is offset by their use as tools of surveillance. Through the case of an accommodation management software developed for asylum seekers in Germany, Scheel shows how the technology is being used to facilitate people’s deportation.

The philosopher Huub Dijstelbloem’s contribution serves as a conclusion to the forum. He critiques historical, European-centric notions of sovereignty, arguing that territory and sovereignty are only loosely connected. In turn, contemporary digital technologies do not just interpret our world, but shape and remake it. He urges us to consider humanitarian technology as a canary in the coalmine for actors to reimagine power in the digital age through experimentality.

The analyses of digitisation and sovereignty in this forum position the distinction between power *over* and power *to* (Lukes 1974) as an urgent consideration in the governance of humanitarian space. Classic debates on sovereignty, as McDonald shows, have focused on power *over* territories, populations and other states. The contributions in this collection argue for re-centring questions of digitisation and sovereignty around power *to*, for example by asking how humanitarian organisations can arrange their digital sovereignty in ways that serve affected people and thus the humanitarian mission, rather than allowing technology to merely increase their (or their contractors and collaborators’) power *over* those people. Marelli makes this distinction in his account of humanitarian organisations’ struggle to distance themselves infrastructurally from powerful sovereign

actors who attract cyberattacks. Cheesman asks how organisations can avoid co-optation by commercial technology partners who seek power *over* markets through their proofs-of-concept in humanitarian space and their provision of infrastructure that creates dependencies on the private sector. Scheel illustrates the distinction in forms of sovereign power by showing how power *over* data equates to power *over* the mobility of refugees and asylum seekers, and Dijstelbloem also picks up the thread of power *over* mobility, and in consequence over other forms of autonomy, showing how technological infrastructure conveys the power *to* experiment with – and on – affected groups in humanitarian space. It is this potential for digital sovereignty on the part of humanitarian organisations that requires both scrutiny and governance, in order to keep the humanitarian mission as the central reference point for defining the value and uses of that sovereignty, and to ensure that humanitarian organisations and the people they serve are the ones providing that definition (cf. Salesforce 2019).

In the essays that follow, we bring together perspectives that focus not just on the role that humanitarian organisations play, but also on the implications that digital technologies have for the lived experiences of people affected by crises. We recognise, however, that the forum does not include direct voices of those who have been affected by humanitarian disasters, nor does it directly engage the perspectives of local grassroots organisations, which occupy an important role in many humanitarian spaces. We hope that this discussion stimulates a broader debate among a range of humanitarian actors and crisis-affected people specifically about the consequences of datafication in these spaces.

Digital Sovereignty and Its Discontents

Sean Martin McDonald

It is impossible to consider digital jurisdictions or national powers in humanitarian responses without using the word sovereignty – and yet, the term is a trap. The confusion is especially complicated for humanitarian responders, who – in refugee and migratory crises – often must juggle multiple, competing claims of jurisdiction over data and digital operations. The practicalities of how states conceive of and invoke digital sovereignty, when tested against urgent needs of a refugee crisis or the competing politics of a conflict zone, create real problems – not just for humanitarians, but for the integrity of the concepts themselves.

The problems embedded in concepts such as ‘digital sovereignty’ and ‘digital self-sovereignty’ do not come from the ‘digital’ so much as the ‘sovereignty’. In other words, when it comes to translating our fundamental rights –

and the structures that enable us to exercise them – into digital systems, the biggest problems are not *what* the systems mean, but about *how* they work – and do not. The core distinctions between what systems intend and how they operate are important, not only for understanding how sovereign rights work, but for designing how they might realistically work in framing national and individual agency in digital systems. And, as a result, how humanitarian organisations might design their digital interventions, balancing individual rights with claims of sovereign authority.

Let us start with what most people agree on: the mainstream definition of ‘sovereignty’ is ‘supreme authority’ over a specific issue or context. As noted by political scientists, however, authority very often requires the agreement of at least two parties (Peter 2017).² Most historic attempts at unilateral supremacy have proven challenging, if not globally repudiated, in the analogue setting. The number of ‘sovereign nations’ has more than tripled since the founding of the UN. While each sovereign nation would certainly argue for its own supremacy in some contexts, especially over its own affairs and people, the very idea of ‘sovereignty’ has gotten less, well, sovereign, since its global acceptance. That is not only true at the international level – globalisation and privatisation have created a meaningful realignment of authorities that structurally questions if there is a minimum-viable ‘unit size’ to sovereignty.

And so, sovereignty also has a second branch of definitions, which describe sovereignty as ‘self-governing’ and contain a similar, glaring irony. Self-governance is necessarily different from ‘exerting supreme authority’ and, in and of itself, raises questions around the breadth implied by ‘self’, as well as what amount of independence is required, or implied. In an analogue sense, most countries depend on globalised trade for some measure of their domestic well-being, as well as the weapons they use to ensure domestic security. The irony of modern sovereignty, of course, is that it is ‘achieved’ through the recognition of other sovereigns (Keating 2008), so one achieves global acceptance of ‘self-governance’ through the approval of other ‘self-governed’ sovereigns. And, once acknowledged as a sovereign, the majority of the powers then granted are based on the mutual agreement of other sovereigns – in other words, the process and impact of becoming a sovereign also reduces the definitional integrity of sovereignty.

The tension in definition between ‘supreme power over a specific topic’ and ‘capable of self-sustaining and governing’ is a useful way to understand the types of authority exercised by different ‘would-be’ sovereigns. While sovereignty began as a way to underline the hierarchy of national and international powers, it has become a set of duties and responsibilities to the governed. This transition is also happening in digital spaces, where a range of platforms, institutions and brokers accelerated digital transformation in order to assert their position – and are now reaping the impacts

of badly managed contextual expectations and liabilities. Perhaps more complicating, many would-be digital sovereigns are struggling with navigating their dependencies (see Marelli's contribution in this forum), whether platforms on labour, governments on capacity and capital, or markets on quality ensuring regulations. So, it would appear that no matter which definition you use, the process of defining digital sovereignty involves realising the mutual dependencies inherent in digital systems, somewhat undermining either framing in practice.

Notwithstanding these tensions, the term 'digital sovereignty' is used to refer to a range of things, but mostly to add a legal (*de jure*) legitimacy to justify the novel exercise of power in digital spaces (*de facto*). In an effort to help frame these uses in practical implementation, this contribution grounds the concept of 'digital sovereignty' in two ways: it (i) differentiates the definitions at the international and domestic levels; and (ii) interrogates common uses of the terms against a typology of jurisdiction, towards understanding the potential for implementation.

It is not clear that analogue interpretations of the word sovereignty are particularly useful in defining or designing modern digital rights, as it is unclear that either state is possible, let alone desirable. For example, there is broad agreement that we have not seen and likely do not want to see any demonstration of 'ultimate' authority in digital spaces at the international level. To date, 'digital sovereignty' has applied more directly to legitimacy (or lack thereof) of the exercise of analogue sovereign powers over issues that arise in digital contexts. Specifically, the ability to compel disclosure of commercial and/or sensitive data and the shutdown of Internet and mobile infrastructure. In humanitarian contexts, it is usually a sovereign's ability to compel disclosure of data about refugee and migrating populations under the auspices of security concerns,³ typically embodied in the agreements that allow organisations to operate in humanitarian settings (McDonald 2019).⁴

Similarly, the Internet somewhat frustrates the idea of 'self-governance', both at the international and domestic level. At the international level, digital sovereignty has largely been used to harden fault lines based on a range of policies, including political speech, local jurisdiction over data storage and labour policies. In other words, the 'self-governing' dimension of sovereignty, at the international level, has mostly been about creating architectures that preserve governmental authority over domestic affairs, as opposed to establishing independence from other sovereign influence or control. While there has been a significant amount of coverage of the geopolitical turn to the 'splinternet' – the idea of a growingly fragmented Internet that reflects opposing centres of control, there are very few examples (or definitions) of Internets that are independent of international actors (The Economist 2016). Russia, for

example, has announced its ability to independently sustain a domestic Internet (Marrow and Antonov 2021). Meanwhile, Cuba, by refusing to join the global Internet, domestically grew an Intranet.

In domestic application, ‘digital sovereignty’ typically focuses on the preservation of the state’s intelligence, investigatory and local enforcement authorities, as opposed to ensuring equitable, independent, or sustainable digital infrastructure. In other words, it is about ensuring that digital transformation aids the expansion of the ‘supreme power’ definition of sovereignty, as opposed to focusing on the ‘self-governing’ aspect of digital sovereignty. Here, again, Russia provides a fascinating example: it has outsourced significant portions of its mobile and 5 G Internet infrastructure provision to Huawei and Chinese interests (Kramer 2019). Russia is relying on an extranational company with deep ties to the Chinese government for the production of hardware and services, while internationally messaging about its ‘self-contained’ Internet.

Most discussions on digital sovereignty have been focused, not just on state power, but on analogising the logic of analogue jurisdiction into digital spaces. Here is a high-level, incomplete list of common terms used to describe digital sovereignty and its relationship to jurisdiction:

- **Infrastructural sovereignty** refers to the idea that mobile and Internet infrastructure, because it exists in a geography controlled by a government, should be under its exclusive control. This is a traditional approach to defining the boundaries of analogue, territorial jurisdiction, although it is increasingly dependent on physical infrastructure, like data hosting centres, located extranationally.
- **Data residency and/or localisation** are attempts to use the physical location of data to exert territorial jurisdiction over it. This is most often for subpoena⁵ and/or investigation purposes, but is increasingly playing a role in tax policy, and extending the rights afforded by data possession to the rights afforded to data use, towards being able to prevent others from making use of the same information.
- **Data sovereignty** is the idea that data, regardless of location, about a sovereign jurisdiction or the people governed by a sovereign’s authority, should be available to – if not exclusively controlled by – the sovereign. It is based on the more traditional concept of ‘subject-matter jurisdiction’ in law. Subject-matter jurisdiction gives a sovereign authority to preside over any issue with an impact in its jurisdiction, including over events that affect their powers, territory, or people.
- **Self-sovereignty** is a popular libertarian idea, which typically refers to an individual’s authority or agency in a digitally defined system. The idea of individual sovereignty is largely a response to the absence of systems for self-governance, or even basic rights protections and agency, and pushes

systems to design for that agency. Conceptually, however, the idea of self-sovereignty, like national sovereignty, glosses over its founding paradox: that its rights are created, realised and enforced by others, rendering the concept somewhat moot in any interpretation.

Digital sovereignty is therefore caught in the same fundamental paradox as analogue sovereignty. Perhaps ironically, the primary political barrier to creating digital sovereignty is the unwillingness of powerful actors to cede the potential for supremacy to meaningful self-governance. The politics of defining the authority to regulate digital sovereignty are undermining pretty much all meaningful progress towards establishing digital sovereignty, *de facto* and *de jure*. The seats of international governance – whether the UN, various industry standards bodies, or even emergency response efforts – are all struggling to rally the legitimacy to fulfil their historic missions, let alone resolve the issues digital transformation creates (McDonald 2021). And so there have been a huge number of calls, from across industry, academia and civil society, for some modern creation event for digital sovereignty, though the analogy varies from the creation of modern China (McDonald and Mina 2019) to the Peace of Westphalia (Demchak and Dombrowski 2013). Ultimately, even solutions that focus on convening aspirational digital sovereigns to establish the baseline, at least implicitly, import a political stance on who deserves representation (and why).

There is no question that sovereignty and, more accurately, the powers of the modern state, are a critical set of geopolitical instruments to define and enforce. Those tensions are especially poignant for humanitarian organisations, which not only depend on grants of sovereign authority for the ability to operate, but also on the ability to balance rights towards political neutrality, in order to fulfil duties to beneficiaries. There is an urgent and compelling need to define practice between states, between states and their people, and now, between states, humanitarian organisations and the tech companies they depend on.

Digital Dependencies, Cyber Risk and International Humanitarian Organisations⁶

Massimo Marelli

In 2020, a cyberattack on SolarWinds, a large information technology (IT) company, allowed hackers to spy on US private companies and government agencies alike. Whereas Stuxnet – a sophisticated zero-day vulnerability that was uncovered a decade earlier (Zetter 2014) – showed us that it is challenging to resist thoroughly planned and targeted operations perpetrated by well-

resourced adversaries, SolarWinds has demonstrated the massive scale that an adversary can achieve by targeting digital supply chain components that are widely adopted.

The SolarWinds hacking operation persisted throughout most of 2020 and was revealed and widely reported on in the media at the end of the same year (Jibilian and Canales 2021). It primarily targeted US government agencies and private companies. The US intelligence community believes the attack to be of Russian origin (CISA 2021). It is a ‘supply chain’ type of attack in that it vectored malware through updates of the Orion software product of SolarWinds, which is widely used to manage IT resources along business supply chains. It has been reported that, “while the SolarWinds hack primarily targeted in-house infrastructure, the breach has morphed into a multidimensional assault on key computing infrastructure, including cloud services” (Hope 2021). The alleged objective of the hack was therefore also to gain access to the systems of large-scale cloud providers such as Microsoft (Hope 2021; Lakshmanan 2020), whose president Brad Smith reported that more than 80% of the victims targeted were non-governmental organisations (NGOs) (Canales 2021). This prompted many NGOs to reflect on their cybersecurity strategies.

As I and others have argued elsewhere, there are several key operational, technical, organisational and legal elements that an international humanitarian organisation should consider when increasing their footprint in the cyber sphere (Marelli 2020; Rodenhäuser 2020). A key starting point in the development of a cybersecurity strategy is the analysis of the cyber environment within which a humanitarian organisation operates and the challenges and threats it faces therein. International humanitarian organisation also need to develop operational dialogue with external stakeholders to deal with some of these challenges.

Such a strategic approach involves a focus on adapting the application of the principles of humanity, neutrality, impartiality and independence to the international humanitarian organisation’s presence and activities in cyberspace. It also suggests the adaptation of privileges and immunities to ensure they remain effective in cyberspace to contribute to enabling the implementation of the mandate of the organisation, so that it can continue to enjoy trust, which is critical to secure access to conflict zones.

In this forum contribution, I want to further develop this analysis, focusing on two key concepts in particular: ‘data sovereignty’ and ‘digital sovereignty’. Borrowing loosely from the international law notion of territorial sovereignty of a state, I understand data sovereignty as indicating that a state or an International Organisation (IO) can exercise full control over the data it processes (which are not in the public domain), to the exclusion of any (other) entity. In other words, no (other) state may by application of law seek and obtain data of the ‘data sovereign’. As mentioned, and for the avoidance of doubt, the notion of sovereignty is borrowed loosely since IOs do not technically enjoy

sovereignty, and the legitimacy to seek ‘exclusive control’ over data, in so far as they are concerned, derives from their mandate under international law, status as an IO and the privileges and immunities they enjoy, including inviolability of correspondence and archives and immunity from jurisdiction. This can be sought by a combination of legal, technical and organisational measures.

While data sovereignty is very important, it needs to be complemented by a more developed and nuanced strategic approach, which conceptually includes something that can be referred to as ‘digital sovereignty’. The notion of digital sovereignty implies a broader form of ‘sovereign’ control that covers not just data, but also hardware and software supply chains, network infrastructure (cables, routers and switches) and communication supply chains. The concept does not necessarily mean that a state or an IO can produce or have total control over all the above, in a ‘digital autarky’ sense: considering the level of dependencies and interconnectedness in cyberspace today this may well be beyond the reach of even the most powerful actors who have been strategically investing enormous resources to achieve this aim. As a result, some could even question the usefulness of the term ‘digital sovereignty’, and may prefer to refer to notions of ‘digital in/dependence’. What digital sovereignty does require, however, is some level of assertion of control and assurance of independence in the choice and use of these tools and infrastructures, or in other words a capacity to manage ‘digital dependencies’ or – as it were – over-dependencies.

While both data sovereignty and digital sovereignty have been key factors in humanitarian organisations’ analysis of cyber risks, so far the emphasis has been mainly on the former. While ensuring data sovereignty would already be a major success for any international humanitarian organisation, because it would enable a response to most of the digital challenges identified so far, the SolarWinds hack highlights that this analysis should perhaps be taken one step further. International humanitarian organisations ought to pay more attention to questions of digital sovereignty.

In the humanitarian sector, the reaction to cyberattacks such as the SolarWinds hack is often defeatist: if the most renowned government agencies and security companies cannot protect themselves, is it even worth it for a humanitarian organisation to try? Another common reaction is to rely even more on cybersecurity professionals and technology firms equipped with significant resources and skilled workforces to secure data and systems. These two types of reactions, however, miss an important point: security is not an absolute concept, and it depends on each organisation’s vulnerabilities, threats, assets and opportunities.

Some humanitarian organisations have specific security assets that other kinds of organisation do not. For instance, the security assets of an organisation like the International Committee of the Red Cross (ICRC) include the recognition of a specific mandate under international law to pursue its

exclusively humanitarian mission, and the trust and acceptance generated by its principles of neutrality, impartiality and independence, as well as operating modalities based on (among others) confidentiality and bilateral confidential dialogue. The ICRC is used to leveraging these principles and operating modalities for its own security in the physical world, and also needs to define how to transpose them to the cyber world (Marelli 2020).

For over 150 years, the ICRC has been operating in conflict areas that are increasingly fragmented, polarised, volatile and difficult to read, where technical and technological innovation has often brought important challenges. The ICRC has therefore been keenly aware of the vulnerable situation it is in. Specific security rules take into account that, in some places, walking down the street or in a market could be dangerous: staff could get abducted or sometimes even killed simply because they are foreigners or they work for a humanitarian organisation. In those cases, security rules provide for movement restrictions, and staff are not allowed to leave the compound of the organisation, unless specific security measures are in place. It is also possible that vehicles of the organisation, moving to deploy and run its activities, may hit an improvised explosive device or be attacked, possibly by accident. Therefore, security rules provide for restrictions of movement along specifically greenlighted routes, notifying all the parties in the conflict or actors involved in a situation of violence about the anticipated movement in the area, and marking very visibly the vehicle of the organisation with emblems and flags to be recognised from afar.

This approach also assumes that humanitarian personnel working amid conflict and violence can rely on such protective assets as the trust and acceptance they can gain from warring parties, local authorities and populations.

Specific security rules are therefore in place to ensure that humanitarian workers always demonstrate the humanity, neutrality, impartiality and independence that may grant them the trust, acceptance, or sometimes tolerance, of all relevant stakeholders. The notion that the security of humanitarian staff is linked to trust and perception of neutrality, impartiality and independence, is indeed one of the pillars of security for organisations like the ICRC. Acceptance is a key pillar of security that highlights the need to be politically, operationally and culturally accepted as a neutral, impartial and humanitarian actor by all relevant stakeholders – it is a strictly essential operational modality that contributes to access and security.

This principled approach is further reinforced by a risk management-based security system that provides practical guidance for field staff as it navigates the acceptance-rejection sliding scale. This includes making sure that humanitarian personnel do not become collateral damage to an attack. For example, the ICRC would, in principle, not locate an office within or in proximity to a military base. Nor would, in principle, an ICRC office or staff

be protected by military personnel of one of the two parties to a conflict or actors in a situation of violence, as this would negatively affect its perception as a neutral and impartial humanitarian actor. It is, for instance, a widely accepted rule that humanitarian vehicles in transit are to drive at a safe distance from military convoys.

While a parallel between the physical world and cyberspace is not straightforward and may be imperfect, there are reasons to consider that a similar approach – even if more technically challenging – could be transposed to cyberspace. By depending too much on the tools, systems and networks used by one of the actors involved in the ‘great power’ (Kilcullen 2020) competition in cyberspace, a humanitarian organisation runs the risk of going against the logic of the security rules and principles mentioned above.

It may not be entirely clear whether the use of, or dependence on, digital tools calls into question a humanitarian organisation’s neutrality, impartiality and independence, and in turn whether it has an impact on its acceptance (or tolerance), as well as its security. But the use of and dependence on these tools does make a humanitarian organisation vulnerable to becoming a victim of attacks addressed to the great power that also relies on them. Just as a humanitarian organisation could be the victim of a rocket attack on a military base if it had its office physically located in or near the base.

The classic humanitarian approach to security as set out above may not be fully suitable for the digital sphere. But it does highlight that alternative approaches need to be explored and considered, whether these lead to already available tools and solutions or, more likely, need to be designed and built.

SolarWinds is merely the latest signal of what is currently unfolding in cyberspace: a competition between the ‘great powers’. Among others, Kilcullen (2020) has analysed this power struggle, including in cyberspace, stressing that what is at stake is not a series of isolated, one-off cyber incidents of a criminal nature, but a worldwide and increasingly strategic use of cyberspace to assert influence, and dominance, by global powers.

Any international humanitarian organisation that operates in a complex and volatile conflict environment on the basis of neutrality, impartiality and independence, must remain alert to these geopolitical dynamics, since they have an impact on the physical world in which they operate. As a result, any such organisation needs to ground its planning in a robust strategy that captures the implications of this great powers’ competition. What works for a multinational corporation may not necessarily work for an international humanitarian organisation.

Against the backdrop of these global tensions among the world’s major cyber powers, one could argue that using the same digital supply chain as one of the key actors, and counting on the security it provides, brings a humanitarian organisation dangerously close to the physical world parallel of positioning offices within or near a military base. While the infrastructure

may look reassuring, relying on it may affect other stakeholders' perception of your neutrality, impartiality and independence. This in turn may affect the trust and acceptance that enables the organisation to deliver on its exclusively humanitarian mandate. And even if the perception of the organisation's neutrality, impartiality and independence is not affected, it could find itself caught in the crossfire if the military base is attacked, simply because of its proximity to the target.

While examining the threats from this angle may not necessarily cover all possible types of potential attackers, it does provide an important additional security asset to leverage for protection from possible cyberattacks by states and state-sponsored groups, or non-state armed groups participating in great powers' competitive dynamics. Arguably, these are the more powerful, and well-resourced, type of attackers.

At present, there are not many alternatives to relying on the same supply chains as multinationals and governments and potentially being caught in the crossfire, at least for the entire stack of technology supporting the humanitarian cyber infrastructure, from hardware, to software, to networks and beyond. Work is ongoing in relation to different layers of the supply chain to introduce more capacity to 'verify and trust', for instance by capitalising on open-source solutions in software and hardware, which could eventually provide solutions, but realistically we are still far away from an 'easy switch' to solutions of this type, across the stack. The immediate reaction to such attacks should therefore be to ask: how can humanitarian organisations manage and mitigate their dependency on these supply chain systems that put them in such vulnerable positions in the first place?

Blockchain, Sovereignty and Humanitarian Payments

Margie Cheesman

Humanitarian agencies increasingly offer people cash assistance rather than food, goods, or coupons (IASC 2016). Cash transfers to crisis-affected populations allow people to make their own purchasing decisions. They are seen as an economic multiplier and a cheap, efficient mode of aid delivery, supporting financial inclusion and reducing the historic paternalism of aid organisations (ODI 2015). Coinciding with this turn towards cash is the digitisation of humanitarian payments, widely seen as one of the most significant contemporary developments in aid (UNOCHA 2020, 219). Digital payment infrastructures, using prepaid cards, mobile phones, biometric interfaces and other technologies, are now globally pervasive. Recent debates among humanitarian actors highlight concerns around digital payments: the intervention of for-profit motives, data protection challenges and political agendas in payment delivery. Some fear the erosion of fundamental humanitarian tenets: Do No

Harm, humanity, neutrality, impartiality and independence (Devidal 2021). Others deplore the risks of surveillance capitalism, informed consent issues, and risks of data breaches, calling for a moratorium on all digital aid payments (Currión 2021). Nevertheless, digital payments are more popular than ever in the context of the COVID-19 pandemic as they are widely seen as enhancing the safety and effectiveness of aid. Their implications not just for humanitarian data politics but also for the future of aid institutions, governance and finance are still emergent.

Blockchain is often viewed as a revolutionary, borderless digital infrastructure that could revolutionise humanitarian payments by circumventing the fragilities and fallibilities of would-be sovereign, national financial systems in the so-called Global South (Kshetri 2017). It is best known as the distributed database system underpinning the cryptocurrency Bitcoin, invented in the wake of the 2007–8 financial crisis to undercut the hegemony of central banks and states in the global financial system (Baym, Swartz, and Alarcon 2019). Blockchain has been closely associated with a crypto-anarchist, anti-surveillance politics: it allows financial transactions to be authorised and recorded among distrusting, anonymous entities, without reliance on centralised authorities. In the aid industry, blockchain is linked with divergent visions about the future of humanitarian finance. Notable projects include alternative community currencies, cryptocurrency funds for aid donations and ‘self-sovereign’ bank ID schemes (Cheesman 2020; Goering 2019; UNICEF 2020). Proponents maintain that blockchain could radically restructure humanitarian finance and/or strengthen grassroots, peer-to-peer economic activity among humanitarian beneficiaries and local markets, “redistributing sovereignty from elites to the people in financial, service and national infrastructures” (Disberse 2020; Manski and Bauwens 2020, 1).

This contribution connects current debates about data politics in humanitarian payments with the optic of sovereignty. I scrutinise claims about how blockchain interfaces with sovereignty regimes in aid. By sovereignty I refer to (i) claims to the control and ownership of data, but also more broadly to (ii) political authority and command over the circulation of capital. I ask: how do novel digital payment infrastructures intersect with issues of control and authority over both money and data? I examine three cross-cutting concerns: (1) national jurisdiction in humanitarian finance; (2) the expanding influence of technology companies in payment infrastructures; and (3) the socio-economic autonomy of aid beneficiaries. I focus on the aid industry discourses and debates surrounding blockchain-based cash transfer projects, tested by notable humanitarian organisations in Kenya, Jordan, the Pacific Islands, Nepal and elsewhere (IFRC 2018; Oxfam Pacific 2020; WFP 2020; World Vision/Nepal Innovation Lab 2018). These projects are a lens into the contested future of financial aid, because blockchain potentially disrupts

traditional sovereignty regimes in aid. In practice, however, humanitarian blockchain projects reveal major ambivalences in the workings of digitally mediated sovereignty.

First, I turn to national jurisdiction in humanitarian finance. In the digital era, ‘sovereignty’ has myriad meanings, but it is most strongly associated with concerns about national jurisdiction: in general, sovereignty refers to government authority and the rule of law in a nation state (Hummel et al. 2021, 1). Banking and finance are intimately connected with state authority (Baradaran 2015). In humanitarian contexts, payments (of capital typically from the Global North) flow from aid organisations to beneficiaries through the financial system of the region, involving local banks, financial service providers, and their processing fees, currency conversion rates, tax protocols and state regulations (e.g., Know Your Customer (KYC) and Anti Money Laundering (AML) rules (cf. Martin and Taylor 2021)). For many proponents, ‘stateless’ blockchain is the ‘ultimate market mechanism’, itself a ‘deified crypto sovereign’ (Swartz 2017; Hütten 2018, 8). Some humanitarian actors suggest that blockchain-based payments will allow aid organisations to entirely undercut costly, inefficient and weak financial systems in crisis-affected countries. For example, Oxfam’s ‘Unblocked Cash’ project in Vanuatu, which involves 35,000 ‘unbanked’ beneficiaries affected by Cyclone Harold and the COVID-19 pandemic, uses digital currencies (‘stablecoins’) as “a ‘borderless’ digital store of value”. This value comes to beneficiaries in the form of prepaid cards. Oxfam suggests the project has “introduced the potential for the institutional donors to fund, and track funds, across multi-country programs” (Development Aid 2020). With blockchains, transactions are verified and recorded across a distributed network of computers; transacting parties are registered, servers are located, and transaction data is stored in multiple, geographically disparate nodes.

The putative borderlessness of blockchains has generated persistent uncertainty and concern within aid organisations about whether and which laws apply, especially in the absence of blockchain-specific regulation and blockchain’s debated compatibility with established data protection regulations such as the European Union’s General Data Protection Regulation (Hallwright and Carnaby 2019; Coppi 2021, 240). Humanitarian organisations and donors are facing backlash from central banks when their payment infrastructures threaten to bypass sovereign financial systems because this potentially devalues fiat currency and cuts demand for local banking services (Andrada 2019; Coppi 2021, 240). For example, Kenyan banks have contested Sarafu, the ‘community currency’ scheme for Red Cross beneficiaries, because the scheme involves blockchain-based e-vouchers transferred using mobile phones, but, unlike the popular mobile money platform MPesa, does not require users to hold national fiat currency (Huillet 2019).

The above examples illustrate both receptiveness and fear within humanitarian organisations about blockchain payment infrastructures undercutting sovereign financial systems. However, on closer examination, all humanitarian blockchain projects interact with traditional financial authorities and banking services in some way, and indeed aid organisations are using blockchains to enhance regulatory compliance. Diverse logics intermingle in different blockchain projects. In aid as in other sectors, some blockchain proponents espouse crypto-anarchist viewpoints, some adopt the anti-authoritarian, market-centric ‘Californian ideology’ of Silicon Valley, while others are committed to traditional institutional structures and patterns of authority (Swartz 2017; Husain, Franklin, and Roep 2020; Hütten 2018). World Vision International’s Sikka project, which delivered digital tokens to communities affected by an earthquake in Nepal via feature phones, was born from a “spirit of compliance with national legislation, to keep providing assistance without infringing the Nepalese laws prohibiting mobile money and e-currencies (seen as a threat to tax collection and a means of corruption)” (Coppi 2021, 235). The social enterprise Disberse worked with a number of aid organisations to create a ‘distributed financial infrastructure maintained by a regulated financial institution’, tested in a regulatory sandbox with the UK Financial Conduct Authority (Currion 2018). Money and data are never in fact deterritorialised; they remain embedded in specific ‘code/spaces’ (Zook and Blankenship 2018; Zook and Graham 2018). Despite concerns about anarchic, borderless, revolutionary change, humanitarian organisations are incorporating blockchains into geographically specific sovereign structures of political and financial authority.

The second part of my analysis of sovereignty examines the expanding influence of technology companies in payment infrastructures. The definition of digital sovereignty has come to include the notion of “tapping into data wealth” (Hummel et al. 2021, 7). This refers to the use of and authority over data (including transaction data) for profit. The extractive data practices of profit-oriented technology companies have begun to intrude into governance functions previously handled by the state, bringing a shift, some argue, from territorial sovereignty to ‘functional sovereignty’ (Pasquale 2018). However, a strong faction of blockchain believers which we might refer to as ‘commonists’ suggest that decentralised infrastructure is a public good because it can destabilise surveillance capitalism and enable cooperative economics (Husain, Franklin, and Roep 2020, 386; Cheesman 2020, 17). Blockchains, by replacing powerful, toll-seeking intermediaries and human decision-making with automated consensus algorithms, could institute commons-based, collectively owned and governed rather than market-based financial systems (ibid). Commonist logics surface in the discourses of several humanitarian payment projects, where blockchain is seen as

a cooperation tool for aid organisations. WFP's Building Blocks promises to replace competing, proprietary payment systems with a 'neutral', mutually owned infrastructure for aid organisations to coordinate payments, while minimising profit for traditional payment intermediaries; Disberse aimed to use blockchain as the basis for an alternative, cooperative financial institution for the aid industry (Insureblocks 2020; WFP 2020).

However, nothing guarantees that humanitarian blockchain platforms will meaningfully challenge the extractive business logics exhibited in financial inclusion initiatives. Critical research suggests that poverty and disaster have become frontiers of capital accumulation and racialised expropriation by technology companies (Gabor and Brooks 2017; Bhagat and Roderick 2020). Through digital payment systems, companies incorporate mobile money transactions and location data into their 'rentier infrastructure', i.e. the channels by which they monopolise profits (Donovan and Park 2020). The biometric technology company IrisGuard currently holds iris scans of 2.7 million Syrian refugees across five countries and works closely with the Jordanian state; its involvement in WFP's Building Blocks has been criticised as extending national security and corporate interests in refugee camps (Fanselow 2018). Critics also suggest Oxfam's Unblocked Cash has allowed blockchain companies to gain entry into new spheres of influence and develop products, viewing Vanuatu as an experimental tax haven (Jutel 2021). Non-traditional public-private partnerships are required to implement blockchain-based projects, and there are unresolved questions about how far these partnerships facilitate tracking and profit, even when sensitive beneficiary information is not recorded 'on chain' (Coppi and Fast 2019, 19). Most humanitarian blockchain projects explicitly aim to track data such as transaction patterns, but in a secure, cryptographic way (Consensys 2019, 5). Optimists contest the idea that blockchain developers are 'neoliberal ideologues seeking to multiply their riches' (Manski and Bauwens 2020). Yet blockchain payment infrastructures serve technology companies' strategic interests in market dominance and functional sovereignty in humanitarian finance.

The third and final aspect of sovereignty relates to the socio-economic autonomy of humanitarian beneficiaries. Sovereignty is a key term in debates over the recognition, rights and agency of non-national colonised peoples, resistance movements and illegal networks (Hansen and Stepputat 2006; Sturm 2017; Hishara). Likewise, digital sovereignty refers to the "recognition of the fundamental rights of data subjects" (Hummel et al. 2021) including marginalised people such as Indigenous groups, stateless and displaced people, and refugees (Cheesman 2020; Cheesman and Slavin 2021; Kukutai and Taylor 2016). Some are confident that blockchain will empower disaster-affected communities with peer-to-peer tools to control both money and data. With Oxfam's Vanuatu project,

“vendors [local shops] can exchange their digital tokens into a local fiat currency between themselves, or purchase goods from each other without any intermediaries” (Consensys 2019; Development Aid 2020). ‘Unblocked Cash’ promises to facilitate unmediated, frictionless exchange, and the organic growth of a community-led local monetary ecosystem.

Yet aid agencies have ultimate monopoly power over the choice of partners, vendors and financial service providers, hence, some might suggest there is no such thing as a free market in humanitarian contexts. Blockchain payments are interlinked with, not separate from, wider humanitarian cash schemes, which always structure beneficiaries’ conditions of agency (Tazzioli 2019). These conditions can be more limiting than empowering (Donovan 2018). Blockchain proponents’ autonomy goals are ultimately hampered by the affected populations’ lack of choice in how to pay and be paid. Furthermore, humanitarian blockchain projects mostly embody neoliberal logics: beneficiaries are supposed to become self-reliant entrepreneurs, as market-led approaches to aid replace substantive social policies and reforms (Scott-Smith 2016). When blockchain projects responsabilise people to generate tokens and redeem them into local fiat currency, how do people negotiate the extra labour involved in cashing out? What recourse is in place when technology companies’ decentralised infrastructures disrupt people’s interactions with local institutions? Above all: who or what are these projects asking people to trust? Payment infrastructure regulates people’s ability to sustain life in global capitalism (Swartz 2020). Abandoning the myth that digital cash is ‘dematerialised’ (Devidal 2021), we need to examine how blockchain payments fit into local monetary ecologies. We need ethnographically informed accounts of sovereignty (Hansen and Stepputat 2006) that illuminate how people’s struggles for authority, rights and justice with regard to money and data play out in their social lives and fit (or don’t) into their socio-economic practices.

Blockchain is a lens into contemporary debates about humanitarianism and alternative economies at global margins. In blockchain experiments and debates, the aid industry and its critics are hashing out possible socio-economic futures. This contribution has examined three cross-cutting considerations about sovereignty: frictions around national jurisdiction in humanitarian finance; unresolved questions about the expanding influence of technology companies in payment infrastructures; and doubtful visions of the socio-economic autonomy of aid beneficiaries. Overall, blockchain is widely touted as a major ‘frontier technology’ of the digital age, but it is still an open question who, if anyone, will settle that frontier.

Function Creep and Parasitic Sovereignty

Stephan Scheel

Justified through slogans like ‘tech4good’, digital technologies such as biometric recognition systems or blockchain-based digital identity wallets are increasingly used in refugee protection and in the provision of social services to improve the efficiency and accountability of aid delivery (Cheesman 2020; Jacobsen 2015; Madianou 2019; Sandvik 2019). One central concern of the literature on digital humanitarianism is that digital technologies and the data they produce are ‘dual use’ in the sense that they can assist in the provision of aid and social care, but can also easily be turned into tools of surveillance and population control that support potentially harmful interventions of government. For instance, governments in Bangladesh, Lebanon, Malaysia and the US have requested access to UNHCR’s biometric data on refugees to use that data for security checks and the preparation of deportations (Jacobsen and Sandvik 2018; Staton 2016; The Engine Room 2020).

In this intervention I show that such concerns over function creep – the use of digital data beyond initially defined purposes – are well-founded, especially in the context of border and (forced) migration management, because function creep is part of the *modus operandi* of sovereign power. This parasitic nature of sovereign power shows itself most vividly in the context of the execution of deportations, which have become key sites for state performances of sovereign power. In the following I develop these arguments through the case of ‘QMM’ – a little-known database that is used on the local level at migrant reception centres in Germany to manage the accommodation of refugees and asylum seekers.

The acronym QMM stands for the German word for ‘accommodation management’ (*Quartiersmanagement*). It refers to a digital accommodation management system that was developed in 2015 – at the height of the ‘refugee crisis’ – by the IT company Cevisio. Today, the system is used in dozens of migrant reception centres across Germany. It consists of a software interface and a centralised database that is connected to a micro-chip equipped plastic card, which is handed out to all residents of migrant reception centres.

The QMM system is meant to manage the accommodation of asylum seekers and the provision of social services, such as medical care, food, clothes and so forth. Staff of all institutions involved in operation of the centre – like the Red Cross, the security service, the local immigration authority, the medical care unit, the Federal Agency for Employment, or the local branch of the Federal Office for Migration and Refugees (BAMF), which is responsible for the processing of asylum claims in Germany – have access to the QMM system and can see in the computer interface which steps of the registration procedure still have to be completed by a particular resident. This is possible because asylum seekers

have to swipe their cards over a card reader in any encounter with a service point at the centre – when they see a doctor, get a meal from the canteen, access or leave the centre, or complete one of the steps of the registration procedure. The crucial point is that digital records of these transactions are stored in individualised datasets of the QMM system. The centralised database is linked to the cards via a personal identification number – also referred to as the resident number – that is stored on the card’s RFID chip and also printed on the card. By swiping the card or doing a search with the resident number, any member of staff with access can retrieve a dataset from the QMM system. This dataset contains – besides a history of the card holder’s transactions – extensive personal information about the card holder: religion, age, medical conditions, country of origin, languages spoken, relatives living inside and outside the centre, etc., as well as information about the card holder’s room number and even bunk bed number within the accommodation unit (Cevasio 2016). Due to this extensive data collection, the QMM system was awarded the Big Brother Award in 2018. The extensive data collection of the QMM system results in “total control. Daily routines, habits, contacts, relatives, state of health, asylum status – all in one place. Linked and evaluable” (Big Brother Award 2018).

The potential implications of this vast data collection are well demonstrated by a form of function creep that was not known to the promoters of the Big Brother award. According to social workers employed in accommodation units for asylum seekers in the city-state of Hamburg, it became apparent that the QMM system is also used for the execution of deportations. This became obvious to social workers after members of staff of the deportation department frequently showed up, together with the police, at different accommodation units to get hold of deportable migrants. In all cases, the police showed up right after the person concerned had returned to their accommodation unit after a longer period of absence. Social workers suspected that the immigration authority office had used the QMM system – which obliges residents to use their card to check in or out whenever they enter or leave their accommodation unit – to check if the person they were looking for was present or absent. This repurposing of the QMM system from a refugee accommodation management system to a law enforcement tool was also implicitly admitted by the local government in a response to a parliamentary request in 2017. In response to the question “How often has the immigration authority’s office used the QMM system in the last quarter to verify the presence of individuals for the execution of deportations?”, the local authorities answered: “No records are kept on this” (Bürgerschaft Hamburg 2017, 2).

However, this repurposing of the QMM system is not reducible to an isolated case of misuse. It rather illustrates the parasitic nature of sovereign power which – in its attempts to deliver on its claim of acting with irresistible efficacy – is compelled to recruit all sorts of human and non-human actors as allies in order to usurp them for its own purposes.

As illustrated by the QMM system, we can observe this parasitic nature of sovereign power most vividly in the context of the execution of deportations – the physical removal of migrants from the territory of a nation-state. Precisely because deportations often involve the use of force and violence, deportations are key sites for performances of sovereign power by which ‘modern nation-states seek to give credibility to their alleged sovereignty and the related claim of a prerogative to control people’s access to, and conditions of stay in, their jurisdictions’ (De Genova et al. 2021, 73). Yet, deportations often fail. With embarrassing effects for the power claiming to be sovereign.

This is highlighted by the so-called ‘deportation gap’, that is, the discrepancy between the number of people issued with a deportation order and the number of people who are actually deported or voluntarily leave (Gibney and Hansen 2003). And this discrepancy is quite significant. On the European level, the so-called ‘effective return rate’ – the number of people with a return order who are physically returned to a so-called ‘third country’ – was approximately 36% in 2017 (ECRE 2019). If one deducts returns to accession countries in the Western Balkans (which accept EU-issued identity papers), the effective return rate is even lower: below 30%. According to these figures, only one in three people legally obligated to leave the EU is actually returned to a country outside the Schengen area. There are numerous reasons for this discrepancy: some people cannot be returned because the authorities of their country of origin refuse to issue them a new passport or because they successfully conceal their identity (Ellermann 2010). Others abscond or physically resist their deportation, which would put an abrupt end to their present life project. And partly, state authorities are hunting for ghosts because the deportation gap is, to a certain extent, a statistical chimera, since a significant number of deportable migrants does actually leave Germany (and the EU), but without notifying authorities about their departure, with the effect that these people are counted as non-returned deportable migrants in official migration statistics (Scheel 2021). The crucial point is that the recurrent failure of the state’s attempts to forcibly remove non-citizens from its territory and the deportation gap constitute an intolerable embarrassment for the modern nation-state because they point to another gap, an opening whose existence state authorities try to deny and undo by any means possible.

This other gap concerns the divergence between the two claims that – taken together – constitute sovereign power as an absolute power: the claim to decide with final authority and to act with irresistible efficacy (Connolly 2007). It is precisely the gap between the two – or more precisely state authorities’ desperate attempts to close and deny any gap between the two – which explains the parasitic nature of any power claiming to be sovereign, its tendency to leech on and usurp practices, data, forms of knowledge and entire institutions and professions for its own purposes. Ultimately, function creep emerges as the *modus operandi* of sovereign power, which “works because it does not work” (Serres 2007, 13).

The space constraints of this brief intervention compel me to conclude with three takeaway lessons: For scholars of borders and migration, the case of the QMM system shows that they should pay more attention to local, allegedly benign databases and digital technologies as this example shows. Due to the parasitic nature of sovereign power, more often than not these technologies are turned into tools of border and migration control. For practitioners working in the humanitarian sector and related fields, the example of the QMM system underscores the need to be much more cautious with the use of digital technologies, which have the potential to do significant harm, a potential that is likely to be realised due to the parasitic nature of sovereign power. Politically, its parasitic nature reveals sovereign power once more as a claim, and nation-state borders as stages where states try to substantiate this claim through performances that reveal this claim, more often than not, as a political delusion that, while mostly falling short of its promise, expresses a practical will with very real effects. Ultimately, the parasitic nature of sovereignty underscores once more the urgency of the political challenge to lay to rest ‘this anachronism that refuses to die’ (Butler 2004, 54).

The Sovereignty Test

Huib Dijstelbloem

One of the fascinating aspects of studying borders, human mobility and humanitarian aid is that research in this field simultaneously engages with empirical and conceptual boundaries. Scholarship almost by definition studies the international mobility of social, technological, informational and political entities, as well as the circulation of the concepts they relate to. It is not only people, goods, finances, technologies and information that move across states’ boundaries. The notions of territory, jurisdiction, authority, power and sovereignty, the conceptual container of nation-states, are movable entities as well – albeit not in symmetric ways. The contributions to this forum show that humanitarian space, data sovereignty and infrastructural sovereignty are emerging notions that come into being by the mobility of people and the

composition of socio-technical networks. Instead of hanging over human behaviour like a pristine blue sky, they move along with human traffic like turbulent weather conditions. Out of it arises a manoeuvring and transforming notion of power and state power that attempts to re-appear and make itself present again in different shapes at different locations.

Following, tracing and identifying forms of politics in the context of international migration requires a twofold approach that focuses on the material manifestations of politics, namely the technologies and organisations that carry it, and on the transforming meaning of politics, the changing load. Langdon Winner's (1980) famous question "Do artefacts have politics?" today therefore has a different meaning. Not only do we have to ask ourselves the question of where politics is to be found and through which forms and artefacts it speaks. Arguably more interesting than answering Winner's question with 'yes'/'no'/'it depends' is refining the question by directing it to issues of territory, jurisdiction, authority, power, sovereignty and technology. By doing so, we broaden the range of forms of technopolitics and the different modes in which they appear.

Today, Winner's question "Do artefacts have politics?" resonates in analyses of surveillance capitalism (Zuboff 2019, 219) and racism and discriminatory designs in digital worlds (Benjamin 2019, 90–92). Sprawl of digital technologies in the governance of international mobility and migration policies has all kinds of humanitarian and security consequences, varying from novel forms of visualisation and risk assessment (Amoore 2013; Ryan 2015) and issues of financial surveillance, data justice and privacy issues (Taylor 2016; Tazzioli 2017) to intense forms of profiling, selection, inclusion, exclusion and infrastructural violence (Heller and Pezzani 2016; Squire 2020; van Reekum 2019). Focusing on notions of territory, jurisdiction, authority, power and – perhaps most importantly in this regard – sovereignty, opens a way to analyse a specific aspect, namely the way sovereignty is reproduced and re-established via data infrastructures and 'mediated' through digital technologies.

To analyse this re-enactment of sovereignty, I will elaborate on the notions of 'experiments' and 'experimentality'. The notions of experiments and experimentality have been attended to increasingly in the literature on border politics and technologies. By elaborating on the notion of experimentality (Murphy 2017; Aradau 2020) the discussion on experiments in border laboratories (Dijstelbloem 2021) can be connected to multiple forms of border politics and other forms of experimental politics in which science, technology and regimes of knowledge recompose socio-technical relations (Murphy 2017, 82; Aradau 2020, 16). The outcome of this discussion, I hope, will contribute to our understanding of the simultaneous movements that take place in the various situations and spaces this forum visits, such as 'humanitarian space' as defined by Collinson and Elhawary (2012) (see Martin, Sharma, de Souza, Taylor and van Eerd), the specific nature and modus operandi of humanitarian organisations and the ways

they are embedded in technological security landscapes (see the contributions by Cheesman, Marelli and McDonald), and the risks and pitfalls of the two-sided sword of digital humanitarianism (Scheel).

In order to discuss the relations between sovereignty, technology, borders and political power and the kind of experiments that take place in this context, the political-historical origins of the notion of sovereignty require attention. Attending to the genealogy of sovereignty is not only a means to avoid reproducing flawed images of the past, it may also shed some light on the various changes the notion has already seen and how it developed as a mediating concept. This is clarified in Darshan's Vigneswaran's (2020) article with the very Latourian title *Europe Has Never Been Modern: Recasting Historical Narratives of Migration Control*. Vigneswaran argues that literature on state formation, sovereignty, borders and migration is often based on two assumptions. The first assumption is that the modern form of state power and the relationship between nation states and borders has the European state, starting from the peace of Westphalia, as its birthplace. The second assumption is that this form of government and control of mobility has spread globally from the west. It holds that "the core institutions and practices of modern territorial sovereignty originated in Europe before being gradually extended to other parts of the globe" (Vigneswaran 2020, 2). In contrast, institutional-historical archival research by Vigneswaran on the development of international migration policy suggests that "extra-European actors played a significant role in both originating and defining the nature of European sovereign territorial and transnational mobility norms" (Vigneswaran 2020, 3). Territorial migration control also arose outside Europe and migration policy in European countries was more the result of international negotiations and exchanges than bearing a Westphalian mark.

Previously, other authors have pointed out that the picture of a coherent Westphalian package deal offering a contract between territory and sovereignty is misleading. Territory, as Elden (2013, 323) argues, "is not simply land . . . nor is it a narrowly political strategic question that is closer to a notion of terrain. Territory comprises techniques for measuring land and controlling terrain". Just like the notion of territory, the concept of a border has various meanings and implications. It does not only operate in political and geographical registers of sovereignty, authority and jurisdiction but also in legal, technical and economic ones. Territory and sovereignty are much more loosely related and come in more variegated combinations than is often assumed (Dijstelbloem 2021).

How then to prevent an overly modernist and/or Eurocentric view on the origin and relation between notions of territory, sovereignty and borders? Since the title of Vigneswaran (2020) unmistakably refers to Latour's (1993) *We Have Never Been Modern*, I suggest revisiting this original

proposal for a comparative anthropology of the relations between politics, technology and knowledge. This leads us to the direction of experiments. But what kind of experiments?

As Aradau (2020, 5) explains, in the literature on borders two notions of ‘laboratories’ and ‘experiments’ prevail: a governmentality approach and an STS one. “In a governmentality approach, all bordering practices have an experimental element. In an STS approach, experiments and laboratories have a more specific meaning emerging from the history of experiments in modern science” (Aradau 2020, 5). By revisiting Latour’s argument, we will see in more detail how an analysis of experiments in the history of modern science is intrinsically connected with questions of politics, and how this opens the way to link it with issues of governmentality.

One of Latour’s central arguments is based on the famous debate between Hobbes and Boyle on the existence of a vacuum and the possible conditions of political power (Shapin and Schaffer 1985). Latour’s argument holds that the notion of sovereignty partly emerged from a controversy in which the division between science and politics was re-established by a dispute over the existence of a vacuum and the application of a socio-politico-technological experiment, namely the air pump.

Latour’s interpretation of (Shapin and Schaffer’s interpretation) of the debate runs as follows. The debate is often pictured as one between a political philosopher (Hobbes) versus an experimental scientist (Boyle). However, both were interested in science, politics, nature and society and adhered to a king, a parliament, the church and mechanistic philosophy. The difference between the two is that they favoured different approaches: experiments (Boyle) versus mathematical proof (Hobbes) (de Vries 2016, 120). They were also concerned with different questions. Whereas Boyle was interested in the possible discovery (or ‘introduction’ in constructivist terms) of the vacuum, Hobbes was driven by the fear of religious wars and how to end them. For that reason, the possible existence of a vacuum created a metaphorical vacuum in his political theory. If the cosmic order allows empty spaces, there will always be room for something else than politics, that cannot be affected by political action and remains uncontrollable for a sovereign (the Leviathan). Therefore, Hobbes proposed a theory of ‘plenism’ and suggested the existence of aether instead.

Against this background, the famous experiment with the air pump takes place. Part of the experiment is a feather in a glass tube. If a vacuum does exist, the feather should remain unmoved. If it would move, it would support Hobbes’ thesis of the substance of aether streaming in and filling the void. As we now know, it did not and the existence of a vacuum was confirmed (Shapin and Schaffer 1985, 181; Latour 1993, 22).

Latour does not read this story in terms of a ‘victory’ of Boyle over Hobbes. Instead, he regards it as a history about the coming into being of a new division between science and politics. According to Latour, the controversy was not an epistemic controversy, but a political and ontological one that included questions on nature, God, the position of the sovereign and the nature of evidence and the role of witnesses and experiments. The controversy is a debate about the question of which actors and which nonhuman entities ought to be taken into account. It is not Hobbes or Boyle who won, but the technological assemblage of the experimental setting that redefined the place of politics and sovereign power.

The advantage of this view is that it allows for reconsidering the connection between institutional and infrastructural approaches. Whereas institutionalists focus on diplomacy, negotiations, conflicts, agreements, contracts and treaties between different actors, historians of technology have redescribed globalisation, colonisation and Europeanisation from the perspective of infrastructure development. Infrastructures for transportation, industry, agriculture, finance, security and warfare are part of the development of states and the creation and expansion of political power. Instead of describing the birth of borders, territory and sovereignty mainly in institutional terms, the infrastructural perspective emphasises the way communication networks, highways, railroads and tunnels unify or divide people in a socio-technological manner (see also Pelizza 2019).

So, what happens if we connect the institutional and infrastructural approach to further the relationship between sovereignty and technology? If we want to draw an analogy between the Hobbes-Boyle controversy and notions of sovereignty and territory in humanitarian and security infrastructures, a possible next step is to ask what counts as the air pump, and what as the vacuum? Perhaps, in this unusual comparison, it is the digital technologies that can be regarded as the instrument and the control over mobility as the vacuum – turning the latter into a proposition of sovereignty, tested experimentally by the former.

The provisional conclusion is that, if specific scientific experiments can be redefined as technopolitical experiments, not only concerned with the advancement of knowledge but with determining the space for political action and sovereign power, then digital humanitarian and security technologies concerned with monitoring movements can be considered as experiments, as sovereignty tests, which examine the space for political power to control human mobility.

All in all, the test we have at hand is a remarkable one. We are not witnessing the birth of sovereignty, but its re-arising. What is going on here is not a chick emerging from the egg, but the rebirth of a phoenix. Via the experimental setting, sovereignty is re-enacted and re-established.

Sovereignty is fabricated via what Aradau (2020) calls ‘experimentality’. As stated previously, according to Aradau the notion of experimentality “can be seen as an attempt to bridge . . . differences between scientific experiments and practices of governing” (Aradau 2020, 5). Experimentality is an experimental endeavour in three respects. It denotes practices, policies and political security programmes that tend to work without protocols, that aim at specific interventions and that operate with a neoliberal logic (Aradau 2020, 7). Aradau suggests this kind of experimentality directs the notion of sovereignty into the sphere of speculative futures. And indeed, digital technologies varying from databases to visual tools concerned with border surveillance and monitoring human mobility can be regarded as a test setup. The distinguishing feature of these kinds of experiments in border politics, we can add to this analysis, is that they not only concern people, data, information and technologies, but the concept of sovereignty itself, to test its presence in order to be able to fill technologically emerging political power vacuums. However, this re-enactment also modifies the notion of sovereignty and does not leave its meaning untouched. When concepts are transported, they are also transformed and translated. And when concepts emerge out of experimental settings, they are susceptible to interventions and manipulations. The application of surveillance systems and humanitarian technologies in this sense carries the risk of shifting the idea of sovereignty to terra incognita, where it becomes part not only of speculative futures, but also uncertain and arcane or downright ominous futures, that will test the room for humanitarian space to its limits.

Notes

1. We would like to thank Chenchen Zhang and Carwyn Morris for organising the September 2020 symposium on *Borders, Bordering and Sovereignty in Digital Space*, where the idea for this forum originated. The Tilburg University team was funded by the European Research Council under the EU’s Horizon 2020 research and innovation programme (grant agreement n° 757247).
2. The idea described here hews to Weber’s view of legitimacy’s dependence on the acceptance of the governed – both in its expression of ‘violence’ and in the moral obligation to obey.
3. In most humanitarian response contexts, international organisations have to negotiate for safe access to provide their services. One of the conditions of that access is, typically, willingness to share information that the host government determines to have security value, which in conflict settings can be anything. And so, groups that want to provide increasingly digital services to populations, whether in a conflict zone or after they have sought refuge, create data that can become de facto intelligence assets for host governments.
4. These agreements are typically called Host Country Agreements, which outline the terms and conditions of an International Organisation’s ability to operate in a country (McDonald 2019). An example is the creation and capture of biometric data about the

Rohingya population, as asylum-seeking refugees in Bangladesh, and the subsequent sharing of that data with the military junta that committed the war crimes that prompted their migration (Rahman 2021).

5. A subpoena is a request for information, pursuant to a lawsuit. Governments use national security interests, emergency powers, and in specific cases, litigation to compel the disclosure of data pursuant to their interests.
6. The author previously published a brief analysis of this case as a blog post, *The SolarWinds Hack: lessons for humanitarians*: <https://blogs.icrc.org/law-and-policy/2021/03/18/solarwinds-hack-humanitarians/>

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the European Research Council [757247].

ORCID

Siddharth Peter de Souza  <http://orcid.org/0000-0003-4299-4878>

Linnét Taylor  <http://orcid.org/0000-0001-7856-7611>

Margie Cheesman  <http://orcid.org/0000-0001-9521-4658>

Stephan Scheel  <http://orcid.org/0000-0002-5065-3726>

References

- Amoore, L. 2013. *The politics of possibility: Risk and uncertainty beyond probability*. Durham: Duke University Press.
- Andrada, N. October 16 2019. 8 digital principal issues with UNICEF's Ethereum cryptocurrency donations. *ICTworks* <https://www.ictworks.org/uncief-ethereum-cryptocurrency-donations/>
- Aradau, C. 2020. Experimentality, surplus data and the politics of debilitation in borderzones. *Geopolitics*. doi:10.1080/14650045.2020.1853103.
- Baradaran, M. 2015. *How the other half banks: Exclusion, exploitation, and the threat to democracy*. Cambridge Massachusetts: Harvard University Press.
- Baym, N., L. Swartz, and A. Alarcon. 2019. Convening technologies: Blockchain and the music industry. *International Journal of Communication* 13:402–21.
- Benjamin, R. 2019. *Race after technology*. Cambridge UK: Polity Press.
- Bhagat, A., & Roderick, L. (2020). Banking on refugees: Racialized expropriation in the fintech era. *Environment and Planning A*, 1–18. doi:10.1177/0308518X20904070.
- Big Brother Award. 2018. The Big Brother Award 2018 in the “public administration” category goes to Cevisio Software und Systeme GmbH in Torgau , Germany. <https://bigbrotherawards.de/en/2018/administration-cevisio-software-systeme-gmbh>
- Butler, J. 2004. *Precarious life: The powers of mourning and violence*. London: Verso.

- Canales, K. February 23 2021. US Senate grilled SolarWinds, Microsoft over cyberattack. *Business Insider* <https://www.businessinsider.com/watch-live-senate-hearing-solarwinds-microsoft-fireeye-crowdstrike-cyberattack-2021-2200C>
- Cevisio. 2016. Cevisio QMM. Die software zur zentralen erfassung von flüchtlingen zur verwaltung von flüchtlingsunterkünften [Cevisio QMM. The software for central registration of refugees and management of refugee accommodation]. Product Information Leaflet of Civisio. https://kipdf.com/die-software-zur-zentralen-erfassung-von-flchtlingen-zur-verwaltung-von-flchtlin_5aaff76e1723dd379cc33e3e.html
- Cheesman, M. 2020. Self-sovereignty for refugees? The contested horizons of digital identity. *Geopolitics*. doi:10.1080/14650045.2020.1823836.
- Cheesman, M., and A. Slavin. 2021. Self-sovereignty and forced migration: Slippery terms and the refugee data apparatus. In *Digital identity, virtual borders and social media: Panaceas for migration governance*, ed. E. Korkmaz, 10–32. Cheltenham UK: Edward Elgar Publishing.
- CISA. 2021 January 5. Joint statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA). *The Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA). Cybersecurity & Infrastructure Security Agency* <https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure>
- Collinson, S., and S. Elhawary. 2012. Humanitarian space: A review of trends and issues. *Humanitarian Policy Group* 32:1–36. <https://odi.org/en/publications/humanitarian-space-a-review-of-trends-and-issues/>.
- Connolly, W. 2007. The Complexities of Sovereignty. In *Giorgio Agamben: Sovereignty and life*, ed. M. Calarco and S. DeCaroli, 23–42. Stanford CA: Stanford University Press.
- Consensus. 2019. Project unblocked cash: Revolutionising humanitarian cash transfers in Vanuatu. <https://consensus.net/blockchain-use-cases/social-impact/project-unblocked-cash-case-study/>
- Coppi, G. 2021. Introduction to distributed ledger technologies for social, development, and humanitarian impact. In *Blockchain, law and governance*, ed. B. Cappiello and G. Carullo, 231–41. Cham: Springer. doi:10.1007/978-3-030-52722-8_17.
- Coppi, G., and L. Fast. February 28 2019. Blockchain and distributed ledger technologies in the humanitarian sector. *Humanitarian Policy Group* <https://odi.org/en/publications/blockchain-and-distributed-ledger-technologies-in-the-humanitarian-sector/>
- Couture, S., and S. Toupin. 2019. What does the notion of ‘sovereignty’ mean when referring to the digital? *New Media & Society* 21 (10):2305–22. doi:10.1177/1461444819865984.
- Currión, P. June 25 2018. Four lessons learned launching blockchain financial services for NGOs. *ICT Works* <https://www.ictworks.org/lessons-learned-blockchain-financial-services>
- Currión, P. February 22 2021. The consequences of cash-based aid. *The New Humanitarian* <https://www.thenewhumanitarian.org/opinion/2021/2/22/the-case-against-humanitarian-cash>
- De Genova, N., et al. 2021. Minor keywords of political theory: Migration as a critical standpoint. A collaborative project of collective writing. *Environment and Planning C: Politics and Space* 1–95. doi:10.1177/2399654420988563.
- Demchak, C., and P. Dombrowski. 2013. Cyber westphalia: Asserting state prerogatives in cyberspace. *Georgetown Journal of International Affairs* (2013):29–38. <https://www.jstor.org/stable/43134320>
- Development Aid. October 23 2020. The unblocked cash project: Oxfam Pacific scales blockchain solution to revolutionize humanitarian aid. <https://www.developmentaid.org/#!/news-stream/post/77034/the-unblocked-cash-project-oxfam-pacific-scales-blockchain-solution-to-revolutionize-humanitarian-aid>

- Devidal, P. March 22 2021. Cashless cash: Financial inclusion or surveillance humanitarianism? *ICRC Humanitarian Law & Policy Blog* <https://blogs.icrc.org/law-and-policy/2021/03/02/cashless-cash/>
- Dijstelbloem, H. 2021. *Borders as infrastructure: The technopolitics of border control*. Cambridge MA: The MIT Press.
- Disberse. 2020. Our story. <https://www.disberse.com/>
- Donovan, K. P. 2018. Financial inclusion dis means your money isn't with you": Conflicts over social grants and financial services in South Africa. In *Money at the margins: Global perspectives on technology, financial inclusion, and design*, ed. B. Maurer, S. Musaraj, and I. V. Small, 155–78. New York: Berghahn Books. doi:10.2307/j.ctvw04bp0.
- Donovan, K. P., and E. Park. 2020. *Rentier infrastructure: Data, debt, and sovereignty in Kenya*. Presentation at Danish Institute for International Studies, Copenhagen. Accessed November 2021. <https://www.youtube.com/watch?v=AHdepHLItNo>
- Easterday, J. February 8 2019. Open letter to WFP re: Palantir agreement. *Responsible Data* <https://responsibledata.io/2019/02/08/open-letter-to-wfp-re-palantir-agreement/>
- The Economist. 2016 November 22. What is the “splinternet”? *The Economist* <https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet>
- ECRE. 2019 July 19. Return policy: Desperately seeking evidence and balance. *European Council on Refugees and Exiles* <https://www.ecre.org/ecre-policy-note-return-policy-desperately-seeking-evidence-and-balance/>
- Elden, S. 2013. *The birth of territory*. Chicago: University of Chicago Press.
- Ellermann, A. 2010. Undocumented migrants and resistance in the liberal state. *Politics & Society* 38 (3):408–29. doi:10.1177/0032329210373072.
- The Engine Room. 2020. Understanding the lived effects of digital ID: A multi-country study. *The Engine Room* <https://www.theengineroom.org/understanding-the-lived-effects-of-digital-id-systems/>
- Fanselow, Y. 2018. Cashing in on crisis? The refugee eye scan experiment. Redfish documentary. <https://www.youtube.com/watch?v=oUtl8Hpg15w>
- Feuer, W. January 23 2020. Palantir CEO Alex Karp defends his company's relationship with government agencies. *CNBC* <https://www.cnbc.com/2020/01/23/palantir-ceo-alex-karp-defends-his-companys-work-for-the-government.html>
- Gabor, D., and S. Brooks. 2017. The digital revolution in financial inclusion: International development in the fintech era. *New Political Economy* 22 (4):423–36. doi:10.1080/13563467.2017.1259298.
- Gibney, M., and R. Hansen. 2003. Deportation and the liberal state: The forcible return of asylum seekers and unlawful migrants in Canada, Germany and the United Kingdom. *New Issues in Refugee Research* 77:1–21. <https://www.unhcr.org/research/working/3e59de764/deportation-liberal-state-forcible-return-asylum-seekers-unlawful-migrants.html>.
- Goering, L. November 26 2019. Red Cross boosts disaster-prone communities with blockchain ‘cash’. *Reuters* <https://www.reuters.com/article/us-technology-aid-climate-change/red-cross-boosts-disaster-prone-communities-with-blockchain-cash-idUSKBN1Y01K1>
- Hallwright, J., and E. Carnaby. 2019. Complexities of implementation: Oxfam Australia's experience in piloting blockchain. *Frontiers in Blockchain* 2 (August):1–6. doi:10.3389/fbloc.2019.00010.
- Hamburg Bürgerschaft. 2017. *Schriftliche Kleine Anfrage Der Abgeordneten Christiane Schneider (DIE LINKE) Vom 27.0417 Und Antwort Des Senats Betr.: Quartiersmanagement in Flüchtlingsunterkünften II [Parliamentary Inquiry by Representative Christiane Schneider (The Left Party), Relating to: Accommodation Management in Housing for Refugees II]*. Bürgerschaft der Freien und Hansestadt Hamburg [Parliament of the Free and Hanseatic City of Hamburg].

- Hansen, T. B., and F. Stepputat. 2006. Sovereignty revisited. *Annual Review of Anthropology* 35 (1):295–315. doi:10.1146/annurev.anthro.35.081705.123317.
- Heath, A. January 31 2022. Zuckerberg's dream of launching a cryptocurrency is officially over. *The Verge* <https://www.theverge.com/2022/1/31/22911426/meta-diem-cryptocurrency-confirms-sale>
- Heller, C., and L. Pezzani. March 2016. Ebbing and flowing: The EU's shifting practices of (non-)assistance and bordering in a time of crisis. *Near Futures Online* <http://nearfuturesonline.org/ebbing-and-flowing-the-eus-shifting-practices-of-non-assistance-and-bordering-in-a-time-of-crisis/>
- Hope, A. 2021. Cloud services from major providers including Amazon and Microsoft vulnerable to the widespread SolarWinds hack. *CPO Magazine*, January 4. <https://www.cpomagazine.com/cyber-security/cloud-services-from-major-providers-including-amazon-and-microsoft-vulnerable-to-the-widespread-solarwinds-hack>
- Huillet, M. November 26 2019. Red Cross deploys blockchain to boost communities' economic resilience. *Coin Telegraph* <https://cointelegraph.com/news/red-cross-deploys-blockchain-to-boost-communities-economic-resilience>
- Hummel, P., M. Braun, M. Tretter, and P. Dabrock. 2021. Data sovereignty: A review. *Big Data & Society* January-June:1–17. doi:10.1177/2053951720982012.
- Husain, S. O., A. Franklin, and D. Roep. 2020. The political imaginaries of blockchain projects: Discerning the expressions of an emerging ecosystem. *Sustainability Science* 15 (2):379–94. doi:10.1007/s11625-020-00786-x.
- Hutten, M. (2018). The Soft Spot of Hard Code: Blockchain Technology, Network Governance, and Pitfalls of Technological Utopianism. *Global Networks*, 19(3). doi:10.1111/glob.12217.
- IASC. 2016. About the grand bargain. *Inter-Agency Standing Committee*. <https://interagencystandingcommittee.org/about-the-grand-bargain>
- IFRC. 2018 October 5. Blockchain open loop cash transfer pilot project. *International Federation of Red Cross and Red Crescent Societies* <https://preparecenter.org/resource/blockchain-open-loop-cash-transfer-pilot-project>
- Insureblocks. 2020 January 10. UN World Food Programme on the blockchain. *Insureblocks* <https://insureblocks.com/ep-143-un-world-food-programme-on-the-blockchain/>
- Jacobsen, K. 2015. Experimentation in humanitarian locations: UNHCR and biometric registration of afghan refugees. *Security Dialogue* 46 (2):144–64. doi:10.1177/0967010614552545.
- Jacobsen, K. L., and K. B. Sandvik. 2018. UNHCR and the pursuit of international protection: Accountability through technology? *Third World Quarterly* 39 (8):1508–24. doi:10.1080/01436597.2018.1432346.
- Jibilian, I., and K. Canales. April 15 2021. What is the SolarWinds hack and why is it a big deal? *Business Insider* <https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12>
- Jutel, O. 2021 January-June. Blockchain imperialism in the Pacific. *Big Data & Society* 1–14. doi:10.1177/2053951720985249.
- Kaurin, D. July 8 2019. Why Libra needs a humanitarian fig leaf. *Berkman Klein Center Medium Collection* <https://medium.com/berkman-klein-center/why-libra-needs-a-humanitarian-fig-leaf-79ae6a463c8>
- Keating, J. February 26 2008. How to start your own country in four easy steps. *Foreign Policy* <https://foreignpolicy.com/2008/02/26/how-to-start-your-own-country-in-four-easy-steps/>
- Kilcullen, D. 2020. *The dragons and the snakes: How the rest learned to fight the west*. New York NY: Oxford University Press.
- Kramer, A. E. June 6 2019. Huawei, shunned by U.S. Government, is welcomed in Russia. *The New York Times* <https://www.nytimes.com/2019/06/06/business/huawei-russia-5g.html>

- Kshetri, N. 2017. Potential roles of blockchain in fighting poverty and reducing financial exclusion in the Global South. *Journal of Global Information Technology Management* 20 (4):201–04. doi:10.1080/1097198X.2017.1391370.
- Kukutai, T., and J. Taylor. 2016. *Indigenous data sovereignty: Towards an agenda*. Canberra: Australian National University Press.
- Lakshmanan, R. December 31 2020. Microsoft says SolarWinds hackers accessed some of its source code. *The Hacker News* <https://thehackernews.com/2020/12/microsoft-says-solarwinds-hackers.html>
- Latour, B. 1993. *We have never been modern*. Cambridge MA: Harvard University Press.
- Lukes, S. 1974. *Power: A radical view*. London and Basingstoke: The MacMillan Press.
- Madianou, M. 2019. Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises. *Social Media + Society* 5 (3):1–13. doi:10.1177/2056305119863146.
- Manski, S., and M. Bauwens. 2020. Reimagining new socio-technical economics through the application of distributed ledger technologies. *Frontiers in Blockchain* 2 (January):1–17. doi:10.3389/fbloc.2019.00029.
- Marelli, M. 2020. Hacking humanitarians: Defining the cyber perimeter and developing a cyber security strategy for international humanitarian organizations in digital transformation. *International Review of the Red Cross* 102 (913):367–87. doi:10.1017/S1816383121000151.
- Marrow, A., and D. Antonov. July 22 2021. Russia disconnects from internet in tests as it bolsters security. *Reuters* <https://www.reuters.com/article/russia-internet-idCNL1N2OY13C>
- Martin, A., and L. Taylor. 2021. Exclusion and inclusion in identification: Regulation, displacement and data justice. *Information Technology for Development* 27 (1):50–66. doi:10.1080/02681102.2020.1811943.
- McDonald, S. 2019 August 15. Space to supply chains: A plan for humanitarian data governance. *SSRN Electronic Journal*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436179
- McDonald, S. M. April 8 2021. A humanitarian duty to integrity. *ICRC Humanitarian Law & Policy Blog* <https://blogs.icrc.org/law-and-policy/2021/04/08/humanitarian-duty-to-integrity>
- McDonald, S., and A. X. Mina. February 26 2019. The war-torn web. *Foreign Policy* <https://foreignpolicy.com/2018/12/19/the-war-torn-web-internet-warring-states-cyber-espionage>
- Murphy, M. 2017. *The economization of life*. Durham, NC: Duke University Press.
- ODI. 2015 September 14. Doing cash differently: How cash transfers can transform humanitarian aid. *Overseas Development Institute* <https://odi.org/en/publications/doing-cash-differently-how-cash-transfers-can-transform-humanitarian-aid/>
- Oxfam Pacific. October 22 2020. The unblocked cash project: Oxfam Pacific scales blockchain solution to revolutionize humanitarian aid. <https://medium.com/unblockedcash/unblocked-cash-oxfam-pacific-scales-blockchain-solution-to-revolutionize-humanitarian-aid-4fb7f2a14f6b>
- Parker, B., and A. Slemrod. June 17 2019. UN gives ultimatum to Yemen rebels over reports of aid theft. *The New Humanitarian* <https://www.thenewhumanitarian.org/news/2019/06/17/un-yemen-rebels-aid-theft-biometrics>
- Pasquale, F. 2018. Digital capitalism: How to tame the platform juggernauts. *Friedrich-Ebert-Stiftung - Division for Economic and Social Policy* 1–4. <https://www.fes.de/en/digital-capitalism-how-to-tame-the-platform-juggernauts>
- Pelizza, A. 2019. Processing alterity, enacting Europe: Migrant registration and identification as co-construction of individuals and polities. *Science, Technology & Human Values* 45 (2):1–27. doi:10.1177/0162243919827927.

- Peter, F. April 24 2017. Political legitimacy. *The Stanford Encyclopedia of Philosophy* <https://plato.stanford.edu/archives/sum2017/entries/legitimacy/>
- Pohle, J., and T. Thiel. 2020. Digital sovereignty. *Internet Policy Review* 9 (4):4. doi:10.14763/2020.4.1532.
- Rahman, Z. June 21 2021. The UN's refugee data shame. *The New Humanitarian* <https://www.thenewhumanitarian.org/opinion/2021/6/21/rohingya-data-protection-and-UN-betrayal>
- Rodenhäuser, T. March 16 2020. Hacking Humanitarians? IHL and the protection of humanitarian organizations against cyber operations. *EJIL:Talk! Blog of the European Journal of International Law* <https://www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/>
- Rodriguez, S. November 30 2021. Facebook's executive in charge of cryptocurrency is leaving the company. *CNBC* <https://www.cnbc.com/2021/11/30/metasp-head-of-cryptocurrency-david-marcus-resigns.html>
- Ryan, B. 2015. Security Spheres: A phenomenology of maritime spatial practices. *Security Dialogue* 46 (6):568–84. doi:10.1177/0967010615598049.
- Salesforce. 2019. First do no (digital) harm: Protecting the humanitarian mission with the cloud. <https://www.salesforce.com/blog/first-do-no-digital-harm-protecting-the-humanitarian-mission-with-the-cloud/>
- Sandvik, K. B. 2019. Making wearables in aid: Digital bodies, data and gifts. *Journal of Humanitarian Affairs* 1 (3):33–41. doi:10.7227/JHA.023.
- Scheel, S. 2021. The politics of (non)knowledge in the (un)making of migration. *Journal of Migration Studies* 1 (2):1–33. doi:10.48439/zmf.v1i2.113.
- Scott-Smith, T. 2016. Humanitarian neophilia: The 'innovation turn' and its implications. *Third World Quarterly* 37 (12):2229–51. doi:10.1080/01436597.2016.1176856.
- Serres, M. 2007. *The parasite*. Minneapolis and London: University of Minnesota Press.
- Shapin, S., and S. Schaffer. 1985. *Leviathan and the Air-Pump: Hobbes, Boyle, and the experimental life*. Princeton: Princeton University Press.
- Squire, V. 2020. *Europe's Migration Crisis: Border deaths and human dignity*. Cambridge UK: Cambridge University Press.
- Stacey, K., and H. Murphy. April 17 2020. How Facebook's Libra went from world changer to just another PayPal. *Financial Times* <https://www.ft.com/content/79376464-72b5-41fa-8f14-9f308acaf83b>
- Staton, B. May 18 2016. Eye spy: Biometric aid system trials in Jordan. *The New Humanitarian* <https://www.thenewhumanitarian.org/analysis/2016/05/18/eye-spy-biometric-aid-system-trials-jordan>
- Sturm, C. 2017. Reflections on the anthropology of sovereignty and settler colonialism: Lessons from native North America. *Cultural Anthropology* 32 (3):340–48. doi:10.14506/ca32.3.03.
- Swartz, L. 2017. Blockchain dreams: Imagining economic alternatives after bitcoin. In *Another economy is possible: culture and economy in a time of crisis*, ed. M. Castells, 82–105. Cambridge UK: Polity Press.
- Swartz, L. 2020. *New money: How payment became social media*. New Haven and London: Yale University Press.
- Taylor, L. 2016. No place to hide? The ethics and analytics of tracking mobility using mobile phone data. *Environment and Planning, D, Society & Space* 34 (2):319–36. doi:10.1177/0263775815608851.
- Tazzioli, M. September 25 2017. The circuits of financial-humanitarianism in the Greek migration laboratory. *Border Criminologies Blog* <https://www.law.ox.ac.uk/research-subject-groups/centre-criminology/centreborder-criminologies/blog/2017/09/circuits>

- Tazzioli, M. 2019. Refugees' debit cards, subjectivities, and data circuits: Financial-humanitarianism in the Greek migration laboratory. *International Political Sociology* 13 (4):392–408. doi:10.1093/ips/olz014.
- UNICEF. 2020 June 19. UNICEF cryptocurrency fund announces its largest investment of start-ups in developing and emerging economies. *UNICEF* <https://www.unicef.org/press-releases/unicef-cryptocurrency-fund-announces-its-largest-investment-startups-developing-and>
- UNOCHA. 2012 June. OCHA on message: Humanitarian principles. *UNOCHA* https://www.unocha.org/sites/dms/Documents/OOM-humanitarianprinciples_eng_June12.pdf
- UNOCHA. 2020 December 1. Global humanitarian review 2021. *ReliefWeb* <https://reliefweb.int/report/world/global-humanitarian-overview-2021-enarfres>
- van Reekum, R. 2018. Patrols, records and pictures: Demonstrations of Europe in the midst of migration's crisis. *Environment and Planning, D, Society & Space* 37 (4):625–43. doi:10.1177/0263775818792269.
- Vigneswaran, D. 2020. Europe has never been modern: Recasting historical narratives of migration control. *International Political Sociology* 14 (1):2–21. doi:10.1093/ips/olz025.
- De Vries, Gerard. 2016. Bruno Latour. Cambridge: Polity Press.
- Weitzberg, K., M. Cheesman, A. Martin, and E. Schoemaker. 2021. Between surveillance and recognition: Rethinking digital identity in aid. *Big Data & Society* January-June:1–7. doi:10.1177/20539517211006744.
- WFP. 2019a February 5. Palantir and WFP partner to help transform global humanitarian delivery. *World Food Programme* <https://www.wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery>
- WFP. 2019b June 20. World Food Programme begins partial suspension of aid in Yemen. *ReliefWeb* <https://reliefweb.int/report/yemen/world-food-programme-begins-partial-suspension-aid-yemen>
- WFP. 2020. Building blocks project overview. *World Food Programme Innovation Accelerator*. <https://innovation.wfp.org/project/building-blocks>.
- Winner, L. 1980. Do artifacts have politics? *Daedalus* 109 (1):121–36.
- World Vision/Nepal Innovation Lab. 2018. *Sikka: A digital asset transfer platform designed for the financially marginalized*, 1–11. Nepal: World Vision international.
- Zetter, K. 2014. *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. New York: Crown Publishing Group.
- Zook, M., and J. Blankenship. 2018. New spaces of disruption? The failures of Bitcoin and the rhetorical power of algorithmic governance. *Geoforum* 96 (August):248–55. doi:10.1016/j.geoforum.2018.08.023.
- Zook, M., and M. Graham. 2018. Hacking code/space: Confounding the code of global capitalism. *Transactions of the Institute of British Geographers* 43 (3):390–404. doi:10.1111/tran.12228.
- Zuboff, S. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Public Affairs.