The strange resilience of the UK e-borders programme

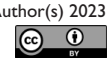
Technology hype, failure and lock-in in border control

Article

SECURITY DIALOGUE

The strange resilience of the UK e-Borders programme: Technology hype, failure and lock-in in border control

Security Dialogue
1–19


Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/09670106231182833
journals.sagepub.com/home/sdi
Sage

Christina Boswell
University of Edinburgh, UK

James Besse
University of Edinburgh, UK

Abstract

The UK government's e-Borders project presents an intriguing anomaly: despite repeated and acknowledged failings of the project over two decades, it has remained a core part of border strategy across successive administrations. This article seeks to explain the surprising resilience of this programme by developing the concept of political lock-in. We combine insights from critical security studies with science and technology studies concepts of 'tech hype' and lock-in. We apply these insights to trace how e-Borders was constructed as a compelling technological solution to pressing security issues. This created a form of political lock-in, whereby the project became impossible to abandon because of its political urgency, despite increasing awareness of its unfeasibility. With the project caught in a liminal state of non-completion, successive governments expanded the scope of the programme by attaching new security problems to it, thereby rendering it even more unviable. Our analysis thus throws up a paradox: rather than mobilizing resources to accomplish its tech vision, securitization created forms of lock-in and paralysis that made the programme more difficult to accomplish.

Keywords

European Union, identity, international security, securitization, security

Introduction

In 2003, the UK government launched an ambitious 'e-Borders' programme, designed to check all travellers arriving in the UK through a complex system of passenger data collection and screening. Eighteen years on, after considerable expenditure, swingeing criticism, successive revisions and multiple relaunches, the e-Borders programme remains unrealized. Yet, despite this failure,

Corresponding author:
James Besse, University of Edinburgh, Surgeon's Square, Edinburgh, EH1 1LZ, UK.
Email: j.w.besse@sms.ed.ac.uk

e-Borders remains a core part of the government's border strategy – indeed, the programme has increased in prominence over the years, most recently as part of a post-Brexit emphasis on digital borders. E-Borders thus appears to represent an anomaly: patently unachievable, but impossible to abandon. What explains the resilience of this project in the face of repeated setbacks?

To understand the persistence of the e-Borders project, we develop the notion of 'political lock-in': a situation in which technology hype twinned with securitarian rhetoric creates an incontrovertible political logic, making a project difficult to abandon, despite its manifest failings. In order to develop this argument, we bring together science and technology studies literature on the dynamics of technology hype and critical security studies insights into the performative power of securitizing moves. In doing so, we contribute to an emerging literature integrating science and technology studies and critical security studies to make sense of new technologies of borders and immigration control (Andersson, 2016; Bellanova et al., 2020; Bourne et al., 2015; Evans et al., 2021; Pelizza, 2021; Pollozek and Passoth, 2019; Sontowski, 2018; Valkenburg and Van der Ploeg, 2015). Through analysing successive e-Borders programmes between 2002 and 2021, we show how technology visions to address security issues can produce particularly pronounced forms of technology hype, which in turn lock policy actors into unfeasible programmes. By invoking security imperatives, visions of border technology can attain a compelling, even irrefutable logic. Such technologies become taken for granted as the political solution to security problems, buffering them from criticism in the face of operational and technical failure.

Further, we suggest that this combination of political lock-in and operational failure means that the roll-out of the technology risks being suspended in a liminal state – neither accomplished nor abandoned. The indeterminacy and fluidity of the unfinished project in turn allows new political projects to be attached to the technology, resulting in continual adjustment, and indeed expansion, of the goals of the programme. The upshot is a self-reinforcing cycle of hyped expectations, failure to complete and mission creep. The technology project is continually adapted and expanded, with the paradoxical effect that it becomes less and less feasible to operationalize. In this way, such technology visions are part of a dysfunctional 'promise–requirement cycle' (Van Lente, 2012), locking the state into undeliverable projects.

The article starts, in the first section, by locating our argument about the dynamics of political lock-in in literatures on critical border studies, security studies, and science and technology studies. In the second section, we apply these approaches to examine the evolution of e-Borders between 2002 and 2021, drawing on a range of transcripts and policy documents. The third section reflects on the lock-in effects created by the programme and the incremental expansion that rendered it increasingly unfeasible.

Technological innovation in border control

There is a growing literature on the use of technology in immigration control, much of it focused on borders. Scholars have charted the roll-out of intrusive methods of surveillance in the form of biometric identification and registration, digitalized databases, and technologies for detecting irregular migrants (Amoore, 2011; Boyce, 2015; Broeders, 2007; Broeders and Dijstelbloem, 2015; Broeders and Hampshire, 2013; Jeandesboz, 2016; Vrăbiescu, 2022; Walters, 2010). Contributions have analysed the 'surveillance assemblage' of elements and actors implicated in border control (Allen and Vollmer, 2018; Haggerty, 2006; Haggerty and Ericson, 2000) and the 'technologies of security' deployed to identify, calculate, prevent and mitigate threats (Aradau et al., 2008). These technologies have been depicted as a form of 'dataveillance' (Amoore and De Goede, 2005), an instance of biopolitics (Ajana, 2013), or as a 'superpanopticon' (Poster, 1990) with worrying ethical implications (Ajana, 2013; Metcalfe and Dencik, 2019).

However, there has been a paucity of literature in critical security studies systematically analysing how these technologies redeem their promises of surveillance and control in practice. Studies focused on the rhetoric around technological innovation can gloss over the practical complexities of implementation, overlooking the often flawed and incomplete realization of such projects. This omission is beginning to be rectified by a body of literature drawing on science and technology studies about the conflicts and compromises involved in realizing ambitious technology programmes. New technologies typically confront multiple sites of resistance, contestation and adaptation on the part of tech designers, users and intermediaries (Ciborra, 1991; Hyysalo, 2021; Stewart and Williams, 2005). Literature on border control has built on such insights to explore the messy practice of border technology, suggesting that 'biometrics is anything but an omnipotent instrument of control' (Sontowski, 2018: 2731), and is instead characterized by 'experimentation, flux and uncertainty' (Walters, 2010: 77). This literature highlights a gulf between the stated effectiveness of border control IT projects and realities on the ground.

In this article, we focus on an important but underexplored aspect of the disjunct between rhetoric and reality, showing how discursive hype around new technologies can create forms of 'lock-in': entrenchment and resistance to change, despite the manifest disfunction of such technologies. According to classic science and technology studies' accounts of lock-in, increasing returns on investment in technology create incentives to persist in favouring a particular technology over others. This occurs through four main dynamics (Arthur, 1989). First, initial fixed costs become spread across an increased number of units, creating increasing returns. Second, learning effects mean that actors accumulate specialized skills and knowledge. Third, adoption of the technology stabilizes expectations among users and producers about aspects such as performance, quality and longevity, leading to 'adaptive expectations'. And, fourth, network and coordination effects mean that advantages accrue to agents adopting the same technology as others. A good example of such lock-in is provided in Collingridge's (1982) discussion of roads and automobiles, which shows how commitment to certain technologies can, in the longer-term, create lock-in as communities of practice and new technologies build up the installed base.

While literature on border control has not explicitly deployed the concept of 'lock-in', we can identify two main (and often overlapping) approaches in the science and technology studies/critical security studies literature that trace similar social and economic dynamics that tie actors in to particular technologies. The first is literature on the economic and institutional dynamics of lock-in. Critical security studies scholars have shown how officials become committed to particular sociotechnical tools and approaches that allow them to sustain and expand their practices. The literature on private security actors in particular has argued that such actors have an interest in framing migration as a security issue with close linkages to issues such as terrorism and drug trafficking, in order to create a security problem that can be solved by their preferred technical solution (Bigo, 2002, 2014). Indeed, the rise of private security actors in migration control has diminished legal accountability and political transparency (Gammeltoft-Hansen and Nyberg Sorensen, 2013), with these actors often successfully constructing migration as a security problem in order to market their own products and services as solutions to it (Abrahamsen and Williams, 2008).

If the economic and institutional accounts focus on the strategies and vested interests of actors implicated in border technologies, a second account understands lock-in as an upshot of the performative effects of sociotechnical infrastructures and assemblages, which unleash new and self-sustaining dynamics. Science and technology studies/critical security studies literature has deployed the concept of information infrastructures to understand how new technologies can reconfigure the agency of street-level administrators and border agents (Pelizza, 2017; Trauttmansdorff and Felt, 2021), recalibrating social relations (Pollozek and Pasoth, 2019) and reconstituting subjectivities (Pötzsch, 2015). Others have developed the concept of sociotechnical

assemblages to show how border technologies become appropriated in different ways by a range of actors, generating conflict, competition and failure (Andersson, 2016).

While these accounts offer important insights into the resilience of border technologies, we develop a third account focused on the *political* dynamics of border technology lock-in. To do so, we build on science and technology studies literature on tech hype and the sociology of expectations. Scholars have revealed how sponsors of tech projects may overstate or 'hype' the potential of technology to solve problems as a means of mobilizing resources and support (Borup et al., 2006; Van Lente, 2012). Such hype can create expectations that bind technology sponsors into particular initiatives, even once they are recognized as failing to deliver or where there are demonstrably better alternatives. Studies have identified how visions of the future can motivate, inform and mobilize resources for technology development. For example, Borup et al. (2006: 290) show how sponsors of new tech have incentives to set expectations high initially, to attract resources and support, 'downplaying the many organizational and cultural factors on which a technology's future may depend'. For this reason, expectations can be distant from what can feasibly be achieved, especially in early-stage projects (Massarella et al., 2018). This allows 'innovators to take advantage of the . . . performativity of expectations in order to influence the momentum of the technology development (potentially leading to "self-fulfilling prophecies")', helping mobilize wider groups of stakeholders. Given that large tech projects are likely to require engagement across multiple organizations, social groups and practices, 'it becomes vital to mobilize the different social groups through negotiations and to form certain expectations of the future in order to reduce uncertainties' (Rolland, 2000). Indeed, Parks (2020) suggests that the main function of promises in technology projects is to coordinate the different actors necessary for the success of these projects – a function that becomes especially important where the consequences of decisions will only emerge in the longer term. Garnering commitment to such uncertain outcomes requires a form of 'promissory legitimacy' that needs to be generated by setting out a compelling vision of the future (Beckert, 2020). Political leaders sponsoring tech will need to communicate especially compelling technology visions, in a context of competitive party politics and scrutiny. High-profile tech projects may attract considerable criticism via practices of monitoring and accountability that are characteristic of the public sector: party political debate, media coverage, audit bodies and inspectors, and lobbying from business and nongovernmental organizations. Thus, governments advancing tech solutions will need to develop convincing ways of narrating the justification for such programmes.

One strategy for both winning political support and buffering technologies from scrutiny is to evoke the urgency or even existential necessity of deploying the chosen technology. As critical security studies literature has shown, by framing a policy issue as a security problem, politicians can legitimize measures that would not otherwise have been considered acceptable (Buzan et al., 1998; Vuori, 2008). As Bourne et al. (2015: 313) write, technology allows 'the fantasy of total security to flourish' by supplying the guise of 'certainty, accuracy, reliability, efficiency, and impartiality'. Once such securitized tech visions have been adopted, they can become taken for granted, creating strong pressure for consensus and shutting down robust political scrutiny (Balzacq, 2014; Neal, 2012), even once the immediate security threat has receded (Basaran, 2008; Bigo, 2008; Jeandesboz, 2016). Such visions can also render alternative (potentially more sensible) approaches undesirable or unimaginable (Van Oers et al., 2020; Vicsek, 2021). The upshot is that once tech visions are successfully attached to pressing security problems, they can shield projects from criticism and consideration of alternatives, despite the patent failure of such technologies to deliver their goals. This can create a form of political lock-in that is just as powerful in constraining change as the economic and institutional forms of tech lock-in outlined above.

This dynamic of inflated promises, muted scrutiny and political lock-in can lead to a form of paralysis in the development of technology, where sponsors recognize the deficiencies of the technology but nonetheless continue to support its roll-out. This can produce a kind of 'liminal technology', as described in Suboticki and Sørensen's (2021) account of the dysfunctional Belgrade metro project. They describe how the metro persisted over nearly a century as an idea that many key actors had bought into, despite prolonged disagreement and indecision about its design and a failure to realize the vision. The concept of liminal technologies suggests that the complexity of a technological project can not only impede its realization, but can also create the conditions for its continual adaptation. The unfinished technology creates a space onto which new and different goals can be projected, allowing for continual adjustment and adaptation of the technology vision.

The case: E-Borders in the UK

We explore the dynamics of political lock-in through the case of the UK e-Borders initiative, initiated in 2002 by the Labour government in office at that time. The aim of the programme was to screen all passengers before they travelled to the UK through gathering passenger data and checking these data against Home Office databases. However, the roll-out of the programme created considerable challenges, including how to mobilize the cooperation of hundreds of airline, train and ferry companies, and how to integrate data from multiple government agencies into a single database. Rather than abandoning the project, successive governments attempted to realize the e-Borders ambition through a series of relaunches and even expansions, including one as recently as May 2021. As of 2021, the UK government still had not reached the initial 2003 targets.

In line with the theoretical discussion above, we analyse the evolution of the e-Borders programme from 2002 to 2020, proceeding in three main steps. First, we examine how political leaders framed the e-Borders project to mobilize political support, including by attaching it to urgent security problems. Second, we examine the numerous problems that were identified in the course of implementing the project, and explore how the government and other political parties responded to and absorbed these criticisms, including through successive changes and relaunches of the project. Third, we chart how the 'problem' that was being addressed was gradually expanded in scope over the 18-year period, which had the effect of widening the ambition of the programme – making it increasingly unfeasible to deliver. The analysis is based on qualitative process-tracing and content analysis of a range of documents and transcripts: parliamentary debates; political speeches; Home Office and Border Agency reports and press releases; select committee hearings and reports; and reports from the National Audit Office (NAO), the Independent Chief Inspector and the Major Projects Authority.

The tech vision: Launching e-Borders, 2002–2009

Political discourse around the launch of e-Borders in the early 2000s eschewed overtly securitarian rhetoric, framing the approach in largely technical terms. To be sure, borders were seen as the site of a range of risks and harms (Vollmer, 2019): unauthorized immigration, international crime and terrorism, customs evasion and fraud. These concerns were heightened by fears about the UK's vulnerability to terrorism after 9/11. Yet proposals on electronic borders were not part of the immediate package of responses to the 9/11 attacks – they were not included in the controversial 2001 Terrorism Bill, but instead were set out in a far more technocratic White Paper published in 2002, under the relatively unsecuritized title *Secure Borders, Safe Haven: Integration with Diversity in Modern Britain* (Home Office, 2002). Among other proposals, the paper promised a new

tech-driven approach to border control. The cornerstone of the approach was the systematic collection of advanced passenger information (API), which would be checked against a new, comprehensive database to guide decisions on entry prior to travel.

The approach was presented in a largely dry and procedural way: as a technological solution that would modernize and increase the efficiency of the UK's borders, as a means of addressing a series of operational challenges. 'Passenger clearance is extremely staff intensive and the Government is committed to technological solutions' involving 'biometrics technology, such as iris or facial recognition or fingerprints' (Home Office, 2002: 95–96). In fact, the initiative marked a significant break with existing border control practices. Until then, all UK border checks had been carried out by border officials at the point of entry, based on information volunteered in landing cards that were checked against a 'warnings index' and, in some cases, questioning of passengers' intentions and a fraud and identity check of the passport (National Audit Office, 2015). The White Paper was proposing the collation of more extensive passenger data in advance of travel, via transport companies (carriers). These data would be checked against an integrated watchlist that included data from numerous UK agencies, allowing border officials to deny authorization to enter the UK before passengers travelled or at the border. Biometric data would enable officials to verify documentation and reliably match it to passengers. In this sense, the framing of the initiative can be seen as a low-key, 'unspectacular' introduction of security technology as described by Huysmans (2011) and Jeandesboz (2016).

Not only was the e-Borders programme unspectacular in its rhetoric, it was also rolled out in a relatively cautious and incremental way. The programme was initially trialled through Project Semaphore, a (supposedly) four-year, £15m pilot scheme launched in 2004 and run by IBM. Semaphore trialled the collection of advanced passenger information (API) from a limited list of carriers (excluding maritime and rail), with the data then checked against the watchlist prior to arrival in the UK. Once at the border, the new system would enable Border Agency officers to biometrically verify the identity of arriving passengers and base decisions on entry on the analysis of API. At the time of their departure for the UK, carriers would send details of passengers as they checked in, allowing a risk assessment and 'targeted' embarkation checks by the Border Agency (Rymer, 2008). While limited in scope, the project was seen as largely successful (NAO, 2014) and as justifying the launch of the full e-Borders programme in 2007.

Consistent with this 'resolutely low-key' approach to its launch (Jeandesboz, 2016: 297), the e-Borders programme initially attracted very little political attention: parliamentary debate and media coverage focused far more intensively on parallel government initiatives on asylum and ID cards for foreign nationals. In this relatively depoliticized setting, the dominant framing of e-Borders remained largely technocratic. For example, in its 2004 Strategic Plan, the Home Office flagged its investment in 'a major new system for tracking travellers' entry and exit at borders', emphasizing its 'technology toolbox', which played a 'significant role in protecting border security' (Home Office, 2004: 118). Indeed, the technical and operational virtues of the system were consistently foregrounded, with the security function of such technology presented almost as a positive side-effect of the programme.

However, the government began to ramp up its discourse on e-Borders in 2005–2006, in response to two episodes. The first was renewed terrorist attacks: the July 2005 London bombings, the June 2007 Glasgow Airport incident and the thwarted London attack of the same month. While these were not used as a vehicle to introduce urgent 'exceptional' responses, they prompted the government to more actively invoke e-Borders as part of the solution to the terrorist threat. Second was a scandal over the Home Office's failure to keep track of former offenders and irregular migrants, which led to accusations that the department was 'not fit for purpose' (Boswell, 2018: 67). This

episode triggered a major restructuring of border services that brought together the activities of the Border and Immigration Agency (BIA) with UK visas and the border work of HM Revenue and Customs to create a new UK Border Agency. Established in July 2007, the new agency was announced as a prominent part of the government's response to growing concerns about terrorism. As Prime Minister Gordon Brown explained in his statement to the House of Commons, tech played an important role in addressing security threats, while also rectifying the dysfunctionality of Home Office information systems:

> To protect us in routes and places where there is the greatest threat of harm, I believe that we now need to accelerate our plans, completing the move from old and ineffective paper-based systems to real-time monitoring, which will allow us to act immediately and in a co-ordinated way across immigration, police and intelligence.
>
> The way forward is electronic screening of all passengers as they check in and out of our country at ports and airports so that terrorist suspects can be identified and stopped before they board planes, trains and boats to the United Kingdom.[1]

The e-Borders project became a prominent part of this vision, as set out in the 2007 Cabinet Office paper *Security in a Global Hub: Establishing the UK's New Border Arrangements*. This document presented e-Borders as a solution to a wide range of perceived security risks – immigration control, preventing tax evasion and fraud, combating organized crime and terrorism, and controlling 'restricted goods'. The programme was presented as an ambitious, technology-driven approach, but with a clearer emphasis on its security role:

> The e-Borders programme, currently being developed by BIA, will ultimately deliver a modernised, integrated secure border control system for passengers across all modes of transport. . . . E-Borders represents a major change programme, and will transform the way data is used to support border control operations. (Cabinet Office, 2007: 40)

This language of 'transformation' and 'major change', along with the active invocation of security considerations, was a clear attempt to mobilize backing for this more ambitious phase of the programme, as anticipated in the literature on the sociology of expectations. The newly configured UK Border Agency actively embraced this more securitized framing as a key part of its strategy of legitimation. In its 2007 Business Plan justifying the e-Borders programme, the agency spoke of the 'paramount' importance of a 'modernised, effective and secure border control system' as a means of increasing border security and preventing terrorism (UK Border Agency, 2007: 16). Technology was key to this ambition: 'As other countries such as the USA, Australia and EU partners take similar measures to secure their borders, it is essential that the UK does not allow itself to fall behind if it is to avoid being seen as a soft target for immigration abuse, international crime and terrorism' (UK Border Agency, 2007: 21).

The programme was contracted to the Trusted Borders consortium led by Raytheon, a US security and defence technology company. The contract incorporated a series of targets agreed with Raytheon. Trusted Borders was to collect API from 95% of passengers (inbound and outbound) by December 2010, and 100% by March 2014. And it was to replace two existing systems with an integrated system for receiving and analysing data in advance and at the border by April 2011 (NAO, 2015). So, while the rhetoric remained focused on technology, the tech vision was increasingly attached to security needs. As we shall see, this combination of technological progress and security exigencies proved very potent in shoring up support for the programme.

Logistical and legal setbacks, 2009–2010

Already in 2009, Home Secretary Jacqui Smith was celebrating the early achievements of the programme: 'We have used the e-Borders system to screen nearly 90 million passengers, leading to more than 3,000 arrests including significant counter-terrorist interventions'[2] – a formulation repeatedly invoked by government and UK Border Agency officials around that period. This narrative of success went largely uncriticized in political debate until late 2009. The main opposition Conservative Party largely accepted the case for e-Borders, including the framing of the programme and the collection of API as a part of the solution to security problems facing the country, directing their critique to other areas of the government's record on immigration and counter-terrorism. The only potential counter-framing to e-Borders was the Conservative Party's plea for better police-led border control. Yet this alternative approach was not developed into a coherent and compelling alternative to e-Borders, and in other fora such as parliamentary select committees, Conservative MPs generally backed the case for e-Borders.[3]

Concerns about the programme were, however, being raised in venues devoted to more detailed and technical scrutiny. These concerns emanated mainly from the tourism and travel sector, which was vexed at the disruption created by new requirements for data gathering and checks. In Autumn 2008, the tourist operator TUI contacted the House of Commons Home Affairs Committee (HAC) outlining its worries, and in summer 2009 the Committee solicited written and oral evidence from a range of carrier companies and their representative bodies. These submissions all painted a picture of catastrophic failings in the design and roll-out of the programme. According to sector representatives, the programme was failing to heed the logistical challenges faced by carriers in collecting and delivering API and the other data required – challenges that, according to the sector, rendered current plans patently unfeasible. These challenges pointed to a lack of consultation and responsiveness by the supplier to the particular needs and constraints of carrier companies. The second main issue concerned the legal problems with collecting and sharing passenger data, including a lack of clarity over compliance with both national laws in countries from/to which passengers were traveling and EU data-protection laws. Further concerns were raised about whether requiring data from EU nationals was in conformity with free-movement provisions. Carriers consistently raised concerns about the Home Office's failure to provide clear legal advice on whether the collection of API and other passenger information was legal, and were anxious about the implications for their businesses of them rolling out a system that would be in breach of national and EU laws.

Intriguingly, the criticisms suggest that e-Borders had not created lock-in in the form of vested economic interests, institutional embedding or sociotechnical assemblages. Quite the contrary: the main commercial actors in this sphere – the travel and tourism operators – were actively resisting the new technology, considering it to be disruptive to their business. And rather than institutionalizing new communities of practice, these actors described a fraught and dysfunctional relationship with the company contracted to implement the programme. Indeed, the travel sector was clear that a large part of the problem lay with the supplier contracted by the UK Border Agency, Trusted Borders. The sector contrasted the generally smooth working relations and implementation of Operation Semaphore to what they saw as fundamental failings of Trusted Borders. BMI complained that Trusted Borders 'appear to be overly influenced by commercial factors and have failed to properly engage with carriers in order to fully understand our business'; they had 'maintained an inexplicable unwillingness to accommodate recognised industry-standard methods of data transmission'.[4] British Airways and Virgin Atlantic both commented that no lessons appeared to have been learnt from Project Semaphore: 'indeed the knowledge and experience gained through Semaphore seems to have been disregarded by those responsible for e-Borders'.[5] The Board of

Airline Representatives spoke of a 'great mistrust' of the supplier, which was described by TUI as 'totally inflexible to meet the needs of the industry and totally inflexible to meet international standards'.[6]

In response to this radical critique of the programme, the Home Office responded with a strong 'securitizing move'. The director general of the Home Office, Lin Homer, forcefully evoked the compelling security logic behind the programme. In her written response to the HAC, Homer immediately referenced the urgency of the programme:

> By way of background, let me explain that through the e-Borders Programme, we are targeting terrorist suspects, criminals and would be illegal immigrants before they come to the country and before they can do harm, but to do this, we need to check all cross border travel. E-Borders therefore will collect and analyse passenger and crew data provided by carriers (air, sea and rail), in respect of all journeys to and from the UK in advance of travel.[7]

Members of the Committee, from all parties, appeared to accept this security imperative. While MPs were sympathetic to the concerns of the carriers struggling with the programme, they consistently emphasized the need for these companies to accept security imperatives. Typical of this acceptance is Labour MP David Winnick's questioning of a representative from the Chamber of Shipping: 'You accept that the UK Border Agency have a very serious problem on their hands in trying to deal with terrorism and, therefore, organisations like your own are bound to be given more work than if we were living in normal times.' And again, 'does your organization accept – presumably it must do – that Britain faces an acute terrorist danger and that July 7 was not necessarily just a one-off?' (HAC, 2009).

These security considerations appear to have persuaded the HAC of the overall merits of the e-Borders programme. Thus, while the Committee recognized the deep reticence of the tourism and travel sector, and its report set out wide-ranging logistical and legal concerns raised in the evidence, the report was surprisingly anodyne in its recommendations. It appeared to accept as a given the need for the e-Borders programme to continue, with recommendations mainly relating to the need for better communications and coordination, more engaged leadership from senior officials in the Home Office and the UK Border Agency, and clarification of the legal situation. This disjuncture between acknowledged and serious flaws in the programme and the rather docile HAC response was reflected in the Committee's response to updates on progress. Following the HAC session, carrier companies did report a moderate improvement in day-to-day relations with UK Border Agency officials, and the HAC appeared satisfied that progress was being made. However, in 2010, it published a follow-up report about the programme:

> Normally, we would have published the Government's response on e-Borders, the transcript of the oral evidence from [the UK Border Agency] and the written evidence without comment. . . . However, we were struck by the fact that, despite the assurances given by the Government in their responses to our original reports, the subsequent evidence we have received reinforces and, in some areas, increases the concerns we felt at the end of last year. (HAC, 2010)

Yet again, the diagnosis from the HAC focused on relatively superficial aspects of delivery of the programme. The follow-up report reiterated its concerns about high turnover in senior Home Office staff overseeing the project and a general lack of engagement – rather than questioning the overall merits of the programme. This implied support for the project emerged despite, rather than because of, an economic or institutional lock-in: the rationale appeared to be strongly political, related to the perceived security imperatives for sustaining e-Borders.

Relaunch and 'scope creep': Digital Services at the Border after 2010

The third phase we trace saw successive relaunches of the programme, alongside a stealthy expansion in its scope. The first of these relaunches occurred in 2010 shortly after the election of a new Conservative–Liberal Democratic coalition. This might have been a chance for the government to abandon – or at least radically rethink – the e-Borders programme. Indeed, shortly after the new government came to power, the Home Office cancelled the contract with Raytheon, citing unacceptable delays in delivery. A protracted legal settlement followed, with the Home Office eventually paying Raytheon £224m in settlements plus legal costs. With the new system effectively abandoned, the UK Border Agency fell back on use of the Semaphore platform, which had originally been developed as part of the pilot (ICIBI, 2013). However, the newly named 'Border Systems' programme retained the targets on advanced passenger information and entry/exit checks, including introducing 80% exit checks on all passengers by April 2015. As well as being welcomed as a response to security problems, the focus on border control also aligned with the new administration's focus on reducing immigration. Indeed, in his announcement on the e-Borders programme in December 2010, Immigration Minister Damian Green foregrounded immigration control as the key function of electronic borders:

> The priority for the coalition remains to secure the border and to control migration. The coalition Government remain committed to the delivery of e-borders, which will help to reduce terrorism, crime and immigration abuse and to improve the productivity of border processes.[8]

This represented a greater emphasis on migration control than in previous political rhetoric on electronic borders, as well as an explicit conjoining of security and migration.

Yet criticism of the programme mounted over the ensuing months, with a number of bodies beginning to scrutinize the operation of the e-Borders programme. Much of this scrutiny revolved around operational deficiencies. In summer 2011, there was a scandal over the implementation of a pilot project to suspend border checks on some low-risk categories of entrants, which had resulted in 'chaotic scenes' at several border points (HAC, 2012). The border fiasco prompted further scrutiny of the Border Force, with the Home Affairs Committee (2012) identifying serious flaws in the Border Force's understanding and use of passenger information provided by airlines.

Alongside this critique of Border Force officials, there was also growing concern about the Home Office's approach to data collection. The cancelation of the contract with Raytheon triggered an inspection by the independent Chief Inspector of Immigration and Borders, who wrote a critical report on the operation of e-Borders, suggesting that the programme 'has yet to deliver many of the anticipated benefits originally set out in 2007' (ICIBI, 2013: 2). Among the goals that had not been delivered was the increase in passenger data collection, with only 65% of passenger movements covered. The Office for National Statistics (2012: 1) meanwhile confirmed that the promise of counting out and counting in immigrants – an objective that had become more salient given the government's target of reducing net migration – was 'some years away' from being feasible. The Chief Inspector's report called on the Home Office to 'define clearly what the aims of the e-Borders programme are ahead of the new procurement exercise, and be transparent about what e-Borders will deliver and by when' (ICIBI, 2013: 2).

The report was followed by an inquiry into the UK Border Agency by the Public Accounts Committee (PAC), which questioned the ambitious nature of the Border Agency's technology plans:

> The Department [UK Border Agency] has placed increasing demands on its IT systems. . . . The plans are very ambitious given that the specification has not been finalised for the new technology required, and the Border Force has, as yet, not issued tender documents for provision of this technology. . . . [P]rogress on introducing exit checks – and also on replacing the Warnings Index – relies heavily on the further development of the e-Borders programme, now known as the Border Systems programme, which is currently rated amber/red by the Major Projects Authority. (PAC, 2013: 4)

A report by the NAO (2014: 46) the following year expressed dismay at the UK Border Agency's continued reliance on legacy IT systems and 'multiple systems and limited integration'. The continued problems with UK Border Agency management and systems led to the decision to reintegrate the work of the agency into the Home Office, fully reversing the 2007 restructuring that had created the agency. The repeated reorganization of the Border Agency in response to high-profile political scrutiny shows how vulnerable this part of the public administration was to top-down interventions. Contrary to accounts of how security actors seek out new sites for applying their tools and practices (Bigo, 2002), the Home Office was operationg in a highly politicized environment, in which officials struggled to master the new technology – let alone roll it out to other venues.

In spring 2014, in the face of these seemingly insurmountable problems, the director general of the UK Border Agency announced to the Home Affairs Select Committee that the e-Borders programme would be terminated.[9] Yet, rather than abandoning the project, the coalition government and subsequent Conservative administrations (from 2015 onwards) launched a series of successor projects that sustained the e-Borders project. The first of these was the 2014 Digital Services at the Border initiative, which retained the core features of e-Borders, including expanding the share of passengers on whom advanced data were collected. A new Border Crossing database was to replace the Watchlist, and an Advanced Border Control system promised to replace Semaphore, with much of the work now brought into the UK Border Agency rather than outsourced to a private supplier. Again, the government framed the new Digital Services at the Border programme in explicitly securitized terms. As then Home Secretary Theresa May announced to the House of Commons in April 2014, the Home Office had 'looked to make absolutely sure that we have identified the right technology that is necessary'. She continued:

> Keeping the UK's border secure is our priority. By the end of this Parliament, we will develop replacement primary border security systems, deliver exit checks, improve resilience of all current business-critical systems, increase advance passenger information coverage, and complete implementation of second-generation e-gates.[10]

As before, House of Commons debate was focused almost exclusively on practical aspects of the implementation of this new programme, rather than questioning it more fundamentally. Questions to the home secretary focused on *when* the programme would be delivered – the notion of abandoning e-Borders was not seriously countenanced. Opposition parties were preoccupied with the government's promise to deliver all services of the programme by the next elections (in 2015). The necessity of e-Borders as a tool for addressing border security problems appeared to have been thoroughly normalized, with criticism largely focusing on delivery failures. Thus, for example, Labour MP Keith Vaz, chair of the HAC, noted that the 'e-Borders programme has been a disaster costing the taxpayer millions of pounds', but then went on to question when the programme's 'core services' would be delivered.[11] An even more excoriating appraisal emerged from the National Audit Office in its report of 2015. The NAO noted the considerable expenditure in the programme since 2003 – at least £830m – while pointing out that it still fell 'considerably short' in meeting its

original targets for collecting passenger data. Moreover, the data 'were, and remain to this day, processed on two systems that do not share data or analysis effectively. . . . Relying on legacy systems means that current processes involve extensive manual effort, duplication of effort and restrictions on the use that can be made of travel history records' (NAO, 2015: 7).

Astoundingly, despite these problems, the Digital Services at the Border programme continued to be broadly accepted in political debate. Indeed, there was a steady expansion in the range of problems it was intended to address – a tendency the NAO (2020: 6) termed 'scope creep'. Most strikingly, border checks assumed a new significance in the negotiations over the UK's departure from the European Union. In some ways, Brexit removed some of the impediments to data-sharing that had plagued early instantiations of the e-Borders programme. The UK would no longer be constrained by rules about data collection and checks on nationals of EU countries. But the UK's decision to leave the Single Market created new challenges around the control of both people and goods entering and leaving the UK from the EU. Indeed, a Public Accounts Committee enquiry found that 'around 30 of the 85 IT systems used at the border will need to be replaced or changed in some way when the UK leaves the EU' (PAC, 2017: 5). Given the Home Office's track record with replacing IT systems, the Committee was sceptical about its ability to manage the changes:

> Major changes to border management are difficult to make and will require strong coordination across government and with many stakeholders. Given the track record it seems unlikely that all the new systems needed to manage the border effectively after we exit the EU will be successfully delivered, and even if things go to plan, departments accept already that not all the systems would be ready by March 2019. Difficulties in the past with delivering improvement programmes have meant that too many border processes still rely on ageing IT systems or are paper-based. (PAC, 2017: 5)

Yet Brexit had also raised strong public expectations about border control. Politicians supporting Brexit had mobilized support around promises to 'take back control' of UK borders, with the implication that the UK would be able to exercise more robust control of who entered the country. Such expectations crept into the Digital Services at the Border programme, which was now framed as a tech solution to strengthen UK sovereign control over its borders, now unshackled by EU rules. A key part of this was a new form of electronic identification of EU/EEA nationals who had been granted settled status. Rather than take the form of physical documentation, identification would be exclusively digital, enabling border control to conduct immigration checks at or in advance of border crossing without the need for a physical document. A similar system of 'electronic visas' would be rolled out to those with other immigration statuses. The Home Office (2021: 28) described this as a radical transformation:

> Investment in border processes, biometrics and technology will result in a border that operates with a fully digital end-to-end customer journey, improving both security and the passage of legitimate travellers through the border.

In this way, the Home Office extended the UK's e-Borders programmes to solve a continually expanding range of political problems. Given its broad scope, which now included goals of supporting immigration restrictions, counting in and out, and 'taking back control' after Brexit, the goals of the Digital Services at the Border and its relationship with other projects became increasingly complicated. The changes to Digital Services at the Border included updating, rather than replacing, Semaphore. Moreover, rather than creating a single aggregated watchlist, Border Crossing would introduce technology allowing the 'simultaneous search of multiple databases' rather than integrating all data into a 'single, centrally-held watchlist' (NAO, 2020: 25). At the same time, Border Crossing was to be repurposed to enable electronic checking of the immigration

status of visitors. Deadlines for delivery were further pushed back to 2022. The NAO (2020: 37) expressed concerns about continued scope creep, noting that the Home Office had 'rated scope risk as Red, highlighting an increased likelihood of scope change'. Among the concerns were that the UK government had not worked out the implications from its anticipated exclusion from the Schengen Information System, a crucial tool for data-sharing on irregular movement in Europe.

In a pattern that was, by now, all too familiar, in March 2021 the Public Accounts Committee (2021: 3) produced a damning report on the Home Office's failure to implement Digital Services at the Border:

> The Home Office (the Department) has presided over a litany of failure in nearly 20 years of non-delivery of digital border programmes, with significant delays introducing additional costs to taxpayers, continued dependency on contractors to maintain legacy programmes, and delayed delivery of benefits to Border Force officers, other users and passengers.

The PAC (2021: 5) pointed to 'optimism bias about delivery and a failure to be open and transparent about delays', which raised concerns that the department would be unable to deliver the programme by March 2022. Yet MPs were still committed to the fundamental objectives and principles of the programme, now incorporating changed border control requirements after Brexit:

> The Digital Services at the Border (DSAB) programme is crucial to delivering the Department's overall objectives for national security at the border to protect the public from terrorism, crime, illegal immi gration and trafficking, and is vital for facilitating the legitimate movement of people across the border. (PAC, 2021: 3)

Thus, despite repeated relaunches and 'resets', the basic reconfiguration of e-Borders and its successors remained in place – indeed, with an expanded scope, to address changes to immigration and border controls after Brexit, with new deadlines set for 2022. At the same time, recent criticisms of the government's failure to deliver these programmes are evocative of concerns dating back to 2009. So, too, is the striking absence of a more fundamental questioning of the programme, creating an odd disjuncture between the profound criticisms levelled at the programme and the continued acceptance of its necessity.

Discussion

The UK's e-Borders programme has taken on a number of guises over the past 18 years: from the technocratic vision of 2002 to the relaunched, more overtly securitized Digital Services at the Border in 2014 and various successor programmes that expanded the scope of the programme, notably after Brexit. This article sought to explain why the programme was so resilient, despite repeated setbacks. We invoked literature from science and technology studies and critical security studies to elucidate how ambitious tech promises attached to security issues can create a compelling vision that locks protagonists into sustaining the programme, even once it is revealed as unfeasible. In this final section, we trace the dynamics of this form of political lock-in by exploring the main phases of the promise–requirement cycle outlined earlier: tech hype, tech disappointment and lock-in effects.

Tech Hype

The initial justification of e-Borders revolved around improving the state's technological capacity to manage risk at the border and can be characterized as largely technocratic. However, following

a spate of terrorist attacks and a scandal about Home Office failings in the mid-2000s, e-Borders was repackaged as part of a rigorous new UK Borders Agency, with a much stronger remit for tackling terrorism. This more justificatory strategy was intensified in 2009 in response to criticisms of the programme's serious deficiencies. The year 2010 saw a further shift in the vision for e-Borders, with a new government squarely aligning the programme to its goal of reducing 'net migration'. Finally, Brexit added a new set of functions to e-Borders after 2016, including ambitious goals for digitally checking the immigration status of EU nationals and providing a replacement to the Schengen Information System – all against the backdrop of strong political promises to 'take back control' of UK borders.

The capacity of e-Borders to absorb these continually shifting problem constructions is a function of its lack of completion: as long as the systems for collecting, sharing and checking data at the heart of the programme remain unfinished, their scope and objectives can be constantly adjusted. The very indeterminacy of the programme is what makes it so adept in accommodating change. Paradoxically, though, it is this constant adjustment of scope and goals that thwarts the delivery of the programme. The absorption of new goals simultaneously made the programme both more urgent to achieve and more difficult to realize.

Tech disappointment

Contrary to notions of protected spaces or niches for tech development, e-Borders and its successors were not buffered from scrutiny. On the contrary, a succession of parliamentary select committee hearings, audits and inspections set out critical failures in the ability of successive governments to deliver on their programmes. And yet, bizarrely, the overall desirability and (eventual) feasibility of e-Borders and its successors were never fundamentally questioned. Politicians were presented with wide-ranging evidence of failures, but nonetheless rallied around a shared belief in the necessity of e-Borders. This almost taken-for-granted support of the programme appears to flow from the combination of two features. First was the allure of the tech vision, with its promise to enhance efficiency and signal the modernity of the UK – a kind of performance of national sovereignty at this highly symbolic site (Meyer et al., 1997). Second was the successful 'securitizing move' of attaching this tech solution to pressing problems of national security. From combatting terrorism in the mid-2000s, to the highly charged debate on immigration control after 2010, to taking back control in 2016, border technologies became a crucial tool for providing security (Aradau and Van Munster, 2007). The potent combination of tech and security appeared to become so closely fused in the promise of e-Borders that even critics of the government were unable to step outside of this framing to query its merits or viability.

Lock-in

The analysis supports science and technology studies insights about tech hype and the promise–requirement cycle (Van Lente, 2012), showing how overly ambitious tech visions persist in spite of the complexities of delivery. We showed how such visions, initially developed to mobilize support for new projects, can produce forms of lock-in, even when technologies are revealed as defective or unfeasible. However, this binding effect needs to be discerned from the dynamics outlined in current science and technology studies/critical security studies literature. Unlike in the case of tech lock-in, electronic borders were not sufficiently embraced by users to create the increasing returns, learning effects, expectations or coordination effects anticipated in the classic science and technology account (Arthur, 1989). Nor can we find evidence of the kind of economic, institutional or sociotechnical lock-in described in accounts of border technology.

This may reflect specificities of the UK case. The highly politicized nature of border control operations afforded limited scope for border officials to entrench or expand their 'dispositions' (Bigo, 2014) in a way that could be observed in French, German or EU dynamics (Bigo, 2002; Boswell and Chabal, forthcoming). Instead, the case of e-Borders in the UK illustrates the power of *political* lock-in: the political justification of technology created a compelling logic that bound political actors to sustain and expand such projects, in the absence of – or even in conflict with – economic and institutional interests. Crucial in accounting for this political lock-in was the role of security imperatives, which trumped more mundane, technical queries raised about the viability of the proposed approaches. The labelling as a security issue buffered policymaking from serious challenges to more fundamental scrutiny.

Yet this lack of rigorous accountability also provided conditions for stasis, producing liminal technology (Suboticki and Sørensen, 2021) or proto-infrastructure (Jenkins, 2015): technology locked into a liminal state or perpetual infancy, unable to be abandoned but incapable of being fully delivered. Indeed, the persistence of successive e-Borders programmes revealed that the capacity of the project to deliver security outcomes was less important than the sociotechnical imaginary attached to these programmes. The tech vision of e-Borders showed a remarkable obduracy in the face of repeated failure. We have suggested that it was precisely this resistance to completion that permitted repeated adjustments to the scope and objectives of the proposal, in turn rendering it even more difficult to complete. Paradoxically, then, securitizing moves can be self-defeating, suppressing the political processes required to achieve the promised security goals.

Acknowledgements

The authors would like to thank the participants at the Council for European Studies 2022 annual conference, as well as Andrew Neal, the anonymous reviewers, and the editors of *Security Dialogue* for their helpful comments on earlier drafts.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This article partly builds on a project generously funded by the Economic and Social Research Council on 'Seeing "Illegal" Migrants: State Monitoring and Political Rationality', led by Christina Boswell (ES/N011171/1).

ORCID iD

James Besse https://orcid.org/0000-0001-9852-0642

Notes

1. See statement by Prime Minister Gordon Brown in the House of Commons, 25 July 2007; available at: https://publications.parliament.uk/pa/cm200607/cmhansrd/cm070725/debtext/70725-0004.htm (accessed 12 September 2022).
2. See statements by Home Secretary Jacqui Smith in the House of Commons, 2 June 2009; available at: https://hansard.parliament.uk/Commons/2009-06-02/debates/09060257000002/BordersCitizenshipAndImmigrationBill(Lords) (accessed 12 September 2022).
3. See, for example, comments in the Home Affairs Committee session on the e-Borders Programme, Session 2009/10; available at: https://publications.parliament.uk/pa/cm200910/cmselect/cmhaff/170/17002.htm (accessed 17 September 2022).
4. See 'Memorandum submitted by bmi', Home Affairs Committee, June 2009; available at: https://publications.parliament.uk/pa/cm200809/cmselect/cmhaff/817/817we10.htm (accessed 17 September 2022).

5. See ‘Memorandum submitted by British Airways’, Home Affairs Committee, December 2005; available at: https://publications.parliament.uk/pa/cm200506/cmselect/cmhaff/775/775we10.htm (accessed 17 September 2022).
6. See ‘Examination of Witnesses (Questions 69–103)’, Home Affairs Committee, 30 June 2009; available at: https://publications.parliament.uk/pa/cm200809/cmselect/cmhaff/817/9063004.htm (accessed 17 September 2022).
7. See ‘Correspondence from Lin Homer, Chief Executive, UK Border Agency, dated 1 July 2009’, Home Affairs Committee, 1 July 2009; available at: https://publications.parliament.uk/pa/cm200809/cmselect/cmhaff/817/817we15.htm (accessed 17 September 2022).
8. See statements by Minister for Immigration Damian Green in the House of Commons, 6 December 2010; available at: https://hansard.parliament.uk/Commons/2010-12-06/debates/1012067000015/E-Borders (accessed 12 September 2022).
9. See ‘Home Affairs Select Committee, Tuesday 11 March 2014’ (video); available at: https://www.parliamentlive.tv/Event/Index/5ea15cb7-a8d8-4826-97bb-96a3f0c6b69b?in=15%3A05%3A00 (accessed 17 September 2022).
10. See note 9 above.
11. See comments by Keith Vaz in ‘Home Affairs Select Committee, Tuesday 11 March 2014’, note 9 above.

References

Abrahamsen R and Williams MC (2008) Selling security: Assessing the impact of military privatization. *Review of International Political Economy* 15(1): 131–146.

Ajana B (2013) *Governing Through Biometrics: The Biopolitics of Identity*. New York: Springer.

Allen WL and Vollmer BA (2018) Clean skins: Making the e-Border security assemblage. *Environment and Planning D: Society and Space* 36(1): 23–39.

Amoore L (2011) Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society* 28(6): 24–43.

Amoore L and De Goede M (2005) Governance, risk and dataveillance in the war on terror. *Crime, Law and Social Change* 43(2–3): 149–173.

Andersson R (2016) Hardwiring the frontier? The politics of security technology in Europe’s ‘fight against illegal migration’. *Security Dialogue* 47(1): 22–39.

Aradau C and Van Munster R (2007) Governing terrorism through risk: Taking precautions, (un)knowing the future. *European Journal of International Relations* 13(1): 89–115.

Aradau C, Lobo-Guerrero L and Van Munster R (2008) Security, technologies of risk, and the political: Guest editors’ introduction. *Security Dialogue* 39(2–3): 147–154.

Arthur WB (1989) Competing technologies, increasing returns, and lock-in by historical events. *The Economic Journal* 99(394): 116–131.

Balzacq T (2014) *Contesting Security: Strategies and Logics*. London: Routledge.

Basaran T (2008) Security, law, borders: Spaces of exclusion. *International Political Sociology* 2(4): 339–354.

Beckert J (2020) The exhausted futures of neoliberalism: From promissory legitimacy to social anomy. *Journal of Cultural Economy* 13(3): 318–330.

Bellanova R, Jacobsen KL and Monsees L (2020) *Taking the Trouble: Science, Technology and Security Studies*. Abingdon: Taylor & Francis.

Bigo D (2002) Security and immigration: Toward a critique of the governmentality of unease. *Alternatives* 27: 63–92.

Bigo D (2008) The emergence of a consensus: Global terrorism, global insecurity, and global security. In: D’Appollonia AC and Reich S (eds) *Immigration, Integration, and Security: America and Europe in Comparative Perspective*. Pittsburgh, PA: University of Pittsburgh Press, 67–94.

Bigo D (2014) The (in)securitization practices of the three universes of EU border control: Military/navy – border guards/police – database analysts. *Security Dialogue* 45(3): 209–225.

Borup M, Brown N, Konrad K and Van Lente H (2006) The sociology of expectations in science and technology. *Technology Analysis & Strategic Management* 18(3–4): 285–298.

Boswell C (2018) *Manufacturing Political Trust: Targets and Performance Management in Public Policy*. Cambridge: Cambridge University Press.

Boswell C and Chabal E (eds) (forthcoming) *States of Ignorance: Governing Irregular Migrants in Western Europe*. Cambridge: Cambridge University Press.

Bourne M, Johnson H and Lisle D (2015) Laboratizing the border: The production, translation and anticipation of security technologies. *Security Dialogue* 46(4): 307–325.

Boyce GA (2015) The rugged border: Surveillance, policing and the dynamic materiality of the US/Mexico frontier. *Environment and Planning D: Society and Space* 34(2): 245–262.

Broeders D (2007) The new digital borders of Europe: EU databases and the surveillance of irregular migrants. *International Sociology* 22(1): 71–92.

Broeders D and Dijstelbloem H (2015) The datafication of mobility and migration management: The mediating state and its consequences. In: Van der Ploeg I (ed.) *Digitizing Identities*. London: Routledge, 242–260.

Broeders D and Hampshire J (2013) Dreaming of seamless borders: ICTs and the pre-emptive governance of mobility in Europe. *Journal of Ethnic and Migration Studies* 39(8): 1201–1218.

Buzan B, Wæver O and De Wilde J (eds) (1998) *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

Cabinet Office (2007) *Security in a Global Hub: Establishing the UK's New Border Arrangements*. London: Cabinet Office.

Ciborra CU (1991) From thinking to tinkering: The grassroots of strategic information systems. *The Information Society* 8(4): 297–309.

Collingridge D (1982) *The Social Control of Technology*. London: Frances Pinter.

Evans SW, Leese M and Rychnovská D (2021) Science, technology, security: Towards critical collaboration. *Social Studies of Science* 51(2): 189–213.

Gammeltoft-Hansen T and Nyberg Sorensen N (2013) The rise of the private border guard: Accountability and responsibility in the migration control industry. In: Gammeltoft-Hansen T and Nyberg Sorensen N (eds) *The Migration Industry and the Commercialization of International Migration*. London: Routledge, 146–169.

Haggerty KD (2006) Tear down the walls: On demolishing the panopticon. In: Lyon D (ed.) *Theorizing Surveillance*. Portland, OR: Willan Publishing, 23–45.

Haggerty KD and Ericson RV (2000) The surveillant assemblage. *The British Journal of Sociology* 51(4): 605–622.

Home Affairs Committee (HAC) (2009) Written evidence: The e-Borders programme. 30 June. Available at: https://publications.parliament.uk/pa/cm200809/cmselect/cmhaff/817/817we01.htm (accessed 20 October 2022).

Home Affairs Committee (HAC) (2010) Twelfth report: UK Border Agency: Follow-up on asylum cases and e-Borders programme. 23 March. Available at: https://publications.parliament.uk/pa/cm200910/cmselect/cmhaff/406/40602.htm (accessed 20 October 2022).

Home Affairs Committee (HAC) (2012) Sixth report: The work of the Border Force. 16 July. Available at: https://publications.parliament.uk/pa/cm201213/cmselect/cmhaff/523/52302.htm (accessed 20 October 2022).

Home Office (2002) *Secure Borders, Safe Haven: Integration with Diversity in Modern Britain*. London: The Stationery Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/250926/cm5387.pdf (accessed 16 October 2022).

Home Office (2004) *Confident Communities in a Secure Britain: The Home Office Strategic Plan 2004–08*. London: The Stationery Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251067/6287.pdf (accessed 16 October 2022).

Home Office (2021) New plan for immigration: Legal migration and border control – Strategy statement. May. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/988518/FBIS_Strategy_Statement_-_Web_accessible.pdf (accessed 16 October 2022).

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

Hyysalo S (2021) *Citizen Activities in Energy Transition: User Innovation, New Communities, and the Shaping of a Sustainable Future*. London: Routledge.

Independent Chief Inspector of Borders and Immigration (ICIBI) (2013) *'Exporting the Border'? An Inspection of e-Borders October 2012–March 2013*. London: ICIBI. Available at: https://www.statewatch.org/media/documents/news/2013/oct/uk-e-borders-inspection-report.pdf (accessed 1 June 2023).

Jeandesboz J (2016) Smartening border security in the European Union: An associational inquiry. *Security Dialogue* 47(4): 292–309.

Jenkins T (2015) The Internet of Things: Designing proto-infrastructures. *Paper presented at the conference 'Design Anthropological Futures' Copenhagen*, 13–14 August.

Massarella K, Sallu SM, Ensor JE and Marchant R (2018) REDD+, hype, hope and disappointment: The dynamics of expectations in conservation and development pilot projects. *World Development* 109: 375–385.

Metcalfe P and Dencik L (2019) The politics of big borders: Data (in)justice and the governance of refugees. *First Monday* 24(4). Available at: https://firstmonday.org/ojs/index.php/fm/article/view/9934/7749 (accessed 22 May 2023).

Meyer JW, Boli J, Thomas GM and Ramirez FO (1997) World society and the nation-state. *American Journal of Sociology* 103(1): 144–181.

National Audit Office (NAO) (2014) *Reforming the UK Border and Immigration System*. London: NAO. Available at: https://www.nao.org.uk/wp-content/uploads/2014/07/Reforming-the-UK-border-and-immigration-system.pdf (accessed 30 October 2022).

National Audit Office (NAO) (2015) *E-borders and Successor Programmes*. London: NAO. Available at: https://www.nao.org.uk/wp-content/uploads/2015/12/E-borders-and-successor-programmes.pdf (accessed 30 October 2022).

National Audit Office (NAO) (2020) *Digital Services at the Border*. London: NAO. Available at: https://www.nao.org.uk/wp-content/uploads/2020/12/Digital-Services-at-the-Border.pdf (accessed 30 October 2022).

Neal AW (2012) 'Events dear boy, events': Terrorism and security from the perspective of politics. *Critical Studies on Terrorism* 5(1): 107–120.

Office for National Statistics (2012) Delivering statistical benefits from e-Borders. Available at: https://www.ons.gov.uk/ons/guide-method/method-quality/imps/latest-news/delivering-statistical-benefits-from-e-borders/delivering-statistical-benefits-from-e-borders—download-file.pdf (accessed 17 April 2023).

Parks D (2020) Promises and techno-politics: Renewable energy and Malmö's vision of a climate-smart city. *Science as Culture* 29(3): 388–409.

Pelizza A (2017) Processing citizenship: Digital registration of migrants as co-production of individuals and Europe. *EASST Review* 36(3): 1–8.

Pelizza A (2021) Identification as translation: The art of choosing the right spokespersons at the securitized border. *Social Studies of Science* 51(4): 487–511.

Pollozek S and Passoth JH (2019) Infrastructuring European migration and border control: The logistics of registration and identification at Moria hotspot. *Environment and Planning D: Society and Space* 37(4): 606–624.

Poster M (1996) Databases as discourse; or, Electronic interpellations. In: Lyon D and Zureik E (eds) *Computers, Surveillance, and Privacy*. Minneapolis, MN: University of Minnesota Press, 175–192

Pötzsch H (2015) The Emergence of iBorder: Bordering bodies, networks, and machines. *Environment and Planning D: Society and Space* 33(1): 101–118.

Public Accounts Committee (PAC) (2013) Written evidence from Border Force. 23 October. Available at: https://publications.parliament.uk/pa/cm201314/cmselect/cmpubacc/663/663we04.htm (accessed 5 November 2022).

Public Accounts Committee (PAC) (2017) Brexit and the UK border: Seventh report of Session 2017–19. 4 December. Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/558/558.pdf (accessed 5 November 2022).

Public Accounts Committee (PAC) (2021) Digital Services at the Border: Forty-eighth report of session 2019–21. 4 March. Available at: https://committees.parliament.uk/publications/5024/documents/50077/default/ (accessed 5 November 2022).

Rolland KH (2000) Challenging the installed base: Deploying a large scale IS in a global organization. *ECIS 2000 Proceedings*: 192. Available at: https://aisel.aisnet.org/ecis2000/192 (accessed 17 April 2023).

Rymer T (2008) E-Borders: Friends of Presidency Group Meeting Brussels. PowerPoint presentation, 27 March. Available at: http://www.statewatch.Org/news/2008/may/uk-pnr-semaphore.pdf (accessed 15 August 2022).

Sontowski S (2018) Speed, timing and duration: Contested temporalities, techno-political controversies and the emergence of the EU's smart border. *Journal of Ethnic and Migration Studies* 44(16): 2730–2746.

Stewart J and Williams R (2005) The wrong trousers? Beyond the design fallacy: Social learning and the user. In: Howcroft D and Trauth EM (eds) *Handbook of Critical Information Systems Research*. Cheltenham: Edward Elgar, 195–221.

Suboticki I and Sørensen KH (2021) Designing and domesticating an infrastructure: Exploring the practices and the politics of an elevator for cyclists. *Urban Studies* 58(6): 1229–1244.

Trauttmansdorff P and Felt U (2021) Between infrastructural experimentation and collective imagination: The digital transformation of the EU border regime. *Science, Technology, & Human Values*. Epub ahead of print 17 November 2021. DOI: 10.1177/01622439211057523.

UK Border Agency (2007) *UK Border Agency: Business Plan*. London: Home Office.

Valkenburg G and Van der Ploeg I (2015) Materialities between security and privacy: A constructivist account of airport security scanners. *Security Dialogue* 46(4): 326–344.

Van Lente H (2012) Navigating foresight in a sea of expectations: Lessons from the sociology of expectations. *Technology Analysis & Strategic Management* 24(8): 769–782.

Van Oers L, De Hoop E, Jolivet E, Marvin S, Späth P and Raven R (2020) The politics of smart expectations: Interrogating the knowledge claims of smart mobility. *Futures* 122: 1–12.

Vicsek L (2021) Artificial intelligence and the future of work: Lessons from the sociology of expectations. *International Journal of Sociology and Social Policy* 41(7/8): 842–861.

Vollmer BA (2019) The paradox of border security: An example from the UK. *Political Geography* 71: 1–9.

Vrăbiescu I (2022) Deportation, smart borders and mobile citizens: Using digital methods and traditional police activities to deport EU citizens. *Journal of Ethnic and Migration Studies* 48(8): 1891–1908.

Vuori JA (2008) Illocutionary logic and strands of securitization: Applying the theory of securitization to the study of non-democratic political orders. *European Journal of International Relations* 14(1): 65–99.

Walters W (2010) Rezoning the global: Technological zones, technological work and the (un-)making of biometric borders. In: Squire V (ed.) *The Contested Politics of Mobility: Borderzones and Irregularity*. London: Routledge, 51–73.

Christina Boswell is Professor of Politics at the University of Edinburgh.

James Besse is a Doctoral Researcher in Science, Technology and Innovation Policy at the University of Edinburgh.