International Journal of Communication 16(2022), 1918–1939 1932–8036/20220005

A Relational Approach to Digital Sovereignty: e-Estonia Between Russia and the West

STANISLAV BUDNITSKY[1]
Indiana University-Bloomington, USA
University of Duisburg-Essen, Germany

This article explores the cultural logics underlying national digital sovereignty, defined here as statecraft relating to information and telecommunication technologies. Drawing on constructivist theories of national identity and technology, it proposes a relational approach to digital sovereignty that analytically centers national Self-Other dynamics in its development. To do this, the article traces how Estonian governing elites' constructions of Russia and the West as negative and positive Others have informed the state's digital institutions and discourses. It shows that Estonia's nationwide digitization, self-branded "e-Estonia," has been intrinsic to its existential goal of integrating into the Euro-Atlantic community and distancing itself from its Soviet past and the Russian state. Analyzed initiatives include e-government services of the 1990s, cybersecurity measures in the aftermath of the 2007 cyberattacks, and the e-Residency virtual citizenship program of the 2010s. By illuminating how sovereign powers wield digital technologies according to their national identity constructions, this study ultimately reveals the continued significance of nationalism in the digital age.

Keywords: digital sovereignty, technological nationalism, e-Estonia, e-government, cybersecurity, e-Residency, national identity, Othering, Estonia, Russia

Following Estonia's independence from the Soviet Union in 1991, the World Bank declared the country's telecommunication system deficient. Its report, "Estonia: The Transition to a Market Economy," determined that Estonia's telecommunication infrastructure was "obsolete, provide[d] a low quality of service, require[d] labor-intensive maintenance, and use[d] scarce spare parts that [could] only be purchased in Eastern Europe and ex-Soviet republics," while the sector's employees "had little exposure to the more advanced telecommunications concepts used in the West" (Rocha & Hansen, 1993, pp. 153–159). Yet, given Estonia's trying socioeconomic circumstances, the report advised against overhauling the

Stanislav Budnitsky: sbudnit@iu.edu
Date submitted: 2020-11-17

[1] Earlier versions of this article were presented at the Center for Advanced Research in Global Communication at the University of Pennsylvania, the Russian Media Lab at the University of Helsinki, and the German Historical Institute in Moscow, Russia. I thank participants of these workshops for their feedback. I'm also grateful to the three anonymous reviewers for their helpful comments.

telecommunication system with expensive Western technologies: "Though difficult, reestablishing supply ties with the East—particularly for spare parts—will be essential to the network's ongoing operations" (Rocha & Hansen, 1993, p. 154).

Estonia defied the World Bank's recommendations, which would have reinforced the republic's dependency on its former metropole (Högselius, 2005, Ch. 5–6). In fact, by the late 1980s, Soviet Estonia's Ministry of Communications had already slowed the installation of Soviet equipment in anticipation of Estonia's imminent political and infrastructural reorientation toward the West. In 1990, Tallinn seceded its telecommunication functions from Moscow to establish a mobile telephony network with Finnish and Swedish partners. Throughout the 1990s, Estonia replaced its Soviet-era information and telecommunication technologies (ICT) with Western and homegrown ones while exporting its discarded equipment to other ex-Soviet states.

Estonia's technological pivot westward was an integral part of its national ideology of "returning to Europe," an existential goal of integrating into the Euro-Atlantic community while materially and symbolically distancing from its Soviet past and the Russian state. Estonia made the digitization of its state and society a national priority. Globally, the government promoted the country's embrace of digital technologies, which it branded "e-Estonia," as epitomizing Estonia's transition from a poor postsocialist state to a full-fledged member of the developed liberal West.

This episode in Estonia's technopolitical history shows that the relationship between the state's official national identity and Others shapes its digital sovereignty. To illustrate the constitutive role of Self-Other dynamics for digital sovereignty, this article examines why and how Estonian governing elites' cultural constructions of Estonia's Russian and Western Others have informed the state's digital institutions and discourses. The proposed relational approach to digital sovereignty is contextual rather than causal. It offers the Self-Other dynamic as a sociohistorical lens through which digital sovereignty's development can be meaningfully understood in retrospect. This lens does not purport to account for the totality of the state's technopolitical decision making but illuminates their broader cultural logics.

Digital Sovereignty, National Identity, and the Other

Digital sovereignty discourses and practices have proliferated over the past decade. Broadly, digital sovereignty refers to control over respective digital domains by users, corporations, social and political movements, and national governments (Couture & Toupin, 2019; Floridi, 2020; Hummel, Braun, Tretter, & Dabrock, 2021; Pohle & Thiel, 2020). In the context of nation-states, digital sovereignty often connotes protectionist measures imposed by national governments on the operation of digital technologies within the state's physical territory, such as data localization and content filtering. By contrast, I conceptualize digital sovereignty more expansively as statecraft in the field of ICTs, including ICT-related official narratives, law and policy making, education, infrastructure, bureaucracy, diplomacy, and other institutionalized domains in domestic and foreign affairs. This conceptualization transcends the persistent analytical binary of democratic and authoritarian approaches to digital governance. It illuminates the reality that governments of all political systems and ideological persuasions deploy digital technologies to bolster sovereign power.

How national governments employ *the language* of digital sovereignty reflects their ideological commitments. Since the 1970s, countries resisting the influx of Western and especially U.S. technological and cultural products have advanced the cause of national informational and technological sovereignty (Carlsson, 2003). Continuing this tradition in the 21st century, China, Russia, and their political allies have championed the notion of sovereignty in the digital sphere to challenge perceived U.S. digital hegemony (Budnitsky & Jia, 2018). Given the term's genealogy, Estonia has shunned the rhetoric of digital sovereignty to underscore its affiliation with the Western liberal-democratic camp.

Instead, since the mid-1990s, Estonia has followed within the European Union's "information society" framework (Velmet, 2020). This liberal market-oriented vision of information society holds that digital technology heralds democratic and socioeconomic progress, while celebrating "openness" in digital networks as embodying the liberal values of governmental transparency, democratic participation, and individual empowerment (e.g., open data, open government, and open electronic borders; Schulte, 2013, Ch. 4). Estonia's information society approach has mirrored the European Union's principles expressly to "keep pace with European developments" (Estonian Informatics Council, 1998, p. 12). Tellingly, then Estonian Foreign Minister (1996–2002) and future president (2006–2016) Toomas Ilves coined the term "e-Estonia" in 2000 as a nod to the European Union's information society program "eEurope" (Ilves, 2000).

More recently, Estonia and other liberal democracies have begun reappropriating the terminology of digital sovereignty. In March 2021, the Estonian prime minister Kaja Kallas (2021–present), together with German, Danish, and Finnish leaders, proposed to accelerate strengthening Europe's autonomy and competitiveness in the digital sphere vis-à-vis the United States and China. The proposal explains that European digital sovereignty is built on "a strong transatlantic relationship" and is not about "taking a protectionist approach" (Merkel, Frederiksen, Marin, & Kallas, 2021, p. 1). It insists that Europe's digital sovereignty is "part of a global world with global supply chains" and is "committed to open markets and to free, fair and rules-based trade" (Merkel et al., 2021, p. 1). In elaborating their understanding of digital sovereignty, the proposal's signatories tried distancing digital sovereignty's liberal European conceptualization from its persistent associations with autarky and authoritarianism.

While advancing differing framings and practices of digital sovereignty, liberal and illiberal regimes are similarly guided by and committed to upholding respective national identity projects in their engagement with digital technologies. National identity discourse as propagated by the governing elite defines the nation's historical origins, membership criteria, sociopolitical values, relation to state institutions, and aspirations (Calhoun, 1997). National identities, in turn, find their reflection "in the design and fulfillment of nation-specific scientific and/or technological projects" that "at once describe attainable futures and prescribe futures that states believe ought to be attained" (Jasanoff & Kim, 2009, p. 120). Especially during the post–WWII decades of rapid technological advances and a global wave of nation-building, political leaders seeking to "refashion the identities and trajectories of their nations turned to the transformative potential of science and technology to fill out the contours of imagined futures" (Krige & Wang, 2015, p. 171). With the advent of digital technologies, governing elites discursively and materially incorporated them into their national identity projects (Dumitrica, 2015; Möllers, 2020; Schulte, 2013).

If national identity shapes the state's digital sovereignty, it follows that national Others must play a formative role in this process too. As the political philosopher Seyla Benhabib (2002) explains, "human cultures [are] constant creations, recreations, and negotiations of imaginary boundaries between 'we' and the 'other(s).' [. . .] A self is a self only because it distinguishes itself from a real, or more often than not imagined, 'other'" (p. 8; see also Triandafyllidou, 1998). For nation-states, an Other can be a historical period in the country's past, an ethnocultural minority living inside or outside the country, another and often neighboring state, and various sociopolitical phenomena (e.g., colonialism, communism, immigration) against which meaning-making elites forge national identity. In Estonia, the official national identity narrative constructs the republic's Soviet past, its Russian-speaking minority, and the Russian state as negative and, at times, threatening tripartite Russian Other whose influence upon Estonian society must be minimized (Petersoo, 2007). By contrast, the liberal West, especially Finland and Scandinavia, and Estonia's first period of national independence (1918–1940) serve as its positive Others to be emulated.

Otherness has always shaped national technopolitical histories. For example, multiple states have carried out grandiose projects that would constitute the crux of their national identity and technological sovereignty as a safeguard against U.S. dominance. Canada's perceived "threat of American expansion" into its economic and cultural space informed the government's plan for the national railway and radio systems in the late 19th and early 20th centuries (Charland, 1986). Likewise, anxiety about "economic and cultural colonization of France by the United States" served as an impetus for France's post–WWII quest to become a nuclear great power (Hecht, 2009, pp. 38–43).

In the digital era, the Self-Other binary still conditions elite thinking about technological politics. At the 2017 European Dialogue on Internet Governance in Tallinn, for example, Estonian President Kersti Kaljulaid (2016–2021) categorically depicted Internet geopolitics as a struggle of liberal democracies united by "the faith in the sanctity of the individual human spirit and freedom" against "authoritarian regimes" with "a fundamentally different value system and no regard for human dignity and freedom of speech" (Kaljulaid, 2017, paras. 1–4). Based on this dichotomy, Kaljulaid (2017) argued that democracies had to "maintain cyber space for the white powers and not abandon it to the dark forces" (para. 16).

Despite its importance for structuring digital politics, the national Self-Other dynamic in this context has received little attention. David Morley and Kevin Roberts (1995), for example, analyze "techno-orientalism"—Western construction of Japan's technological superiority in the late 1980s and early 1990s—to investigate "why, at this historical moment, this particular Other should occupy such a threatening position in the Western imagination" (p. 147). Florian Schneider's (2018) exploration of China's "digital nationalism" looks into how individual Chinese "networked actors use ICTs to shape nationalist discourse [. . .] vis-à-vis Japan as foreign Other" (p. 16). Norma Möllers (2020) considers how "Germany's Others"—China, Russia, and ISIS—inform the government's cybersecurity policy (pp. 10–17). Meanwhile, scholars of e-Estonia acknowledge the significance of Estonia's relations with Russia and the West but are yet to employ the Self-Other dynamic as their guiding analytic (for exceptions, see, e.g., Drechsler, 2018; Savchenko, 2019). My analysis draws on and contributes to these literatures on technological nationalism in the digital age and on e-Estonia as its prime example.

Methodology and Organization

This article's task is to narratively retrace how Estonian governing elites' cultural constructions of Estonia's Others have shaped Estonia's digital sovereignty. Digital sovereignty encompasses formal and informal ICT-related institutions overseen by the state. Estonia's digital sovereignty includes, for example, its cybersecurity policy framework outlined in doctrinal documents, the brick-and-mortar infrastructure of the Tallinn-based NATO Cooperative Cyber Defense Center of Excellence, and its reputation as a leading international cybersecurity norm entrepreneur.

In line with the article's focus on digital sovereignty as a state project, I view Estonian governing elites as the social agents foremost responsible for its institutional development. By governing elites, I mean representatives of the Estonian state with decision- and meaning-making powers over national identity, digital sovereignty, and their interrelationship. To be sure, Estonian and foreign private and civil society sectors have been crucial for the country's digital sovereignty via investment into the ICT sector, research and development, global promotion of e-Estonia, and in other capacities. Yet the guiding and coordinating role belongs to the state.

For Estonian elites, the existential mission of digitization as a material and discursive project is bolstering Estonian national sovereignty (Drechsler, 2018; Savchenko, 2019). Estonia's global reputation as a digital innovator, the logic goes, ensures the Western community's outsized attention on this small country. Estonian elites trust that this favorable recognition will translate into tangible foreign assistance, particularly in a confrontation with Russia.

Estonia advances a Cinderella-like story of its transformation from a poor, backward postsocialist state into a prospering Western technological trendsetter (Drechsler, 2018; Mäe, 2017). Though this account is partially justifiable, Estonian officials inflate claims about e-Estonia to attract global attention. Western journalists and politicians uncritically regurgitate these boastful claims, casting recent Estonian history as a feel-good teleological narrative of successful technological and market reforms. A typical Western media headline reads, "In Estonia, Communism's Collapse Paved the Way for Wi-Fi Everywhere" (de Pommereau, 2011).

In reconstructing elite logics and their institutional implications, I triangulate my critical reading of primary texts representing Estonian state discourses on national identity and digital sovereignty, secondary sources on e-Estonia's institutional development, such as analytical and statistical reports, and scholarship on Estonia's historical, political, and digital developments. My interpretive analysis explores meaning making by Estonian elites, mining the texts for representations of the national past, the desired future, and digital technologies' role within them (see Jasanoff, 2015, pp. 24–27; Schulte, 2013, pp. 5–10). This analysis examines the symbolic and cultural resources that speakers employ in seeking to naturalize their worldviews, including tropes, metaphors, analogies, and others. Official discourses of the state, such as policy documents and political talk, serve as particularly fruitful sites of discovery for this task.

In selecting the primary sources, I followed the dictum of casting the net widely until additional data no longer offered new insights. The primary texts came predominantly from Estonian official political and policy discourses (e.g., statements, interviews, doctrines). I located these texts through the websites

of institutions that were found to be of greatest relevance to my analytical goals (office of the president, ministry of foreign affairs, e-Estonia, and others). Because Estonia's national and digital sovereignty rely on continued symbolic recognition and material support from Western publics and especially decision-making elites, the bulk of the analyzed texts represents Estonia's foreign-facing discourse.

Since Self-Other dynamics unfold over years, decades, and often centuries, this analysis adopts a historical perspective. This long-term lens incorporates Estonia's relations with its Others in the last century and the entire three-decade span of Estonia's digital sovereignty. Although this panoramic view historicizes Estonia's digital sovereignty, its ability to closely scrutinize interactions among relevant social actors, ideas, and institutions is necessarily limited.

The empirical discussion proceeds in four parts. The first section provides an account of turning points in 20th-century Estonian history. It thus reveals the historical origins of official national identity narratives in post-1991 Estonia. The subsequent three empirical sections trace how these narratives, particularly Estonian governing elites' cultural constructions of their Russian and Western Others, have directed the development of Estonia's digital sovereignty.

An Other's influence on the national Self is most prominent during the early stages of national identity formation, acute sociopolitical change and crises, and other unsettled times (Petersoo, 2007, p. 118; Triandafyllidou, 1998, p. 603). Accordingly, each of the three empirical sections examines a turbulent moment in Estonia's history to show how Self-Other relations influenced digital sovereignty. One section analyzes the period of intensive identity- and state-formation between Estonia's independence in 1991 and its accession to the European Union and NATO in 2004, which laid the foundations of Estonia's digital sovereignty. Another examines the critical period following Russia's 2007 cyberattacks on Estonia, which triggered an overhaul of Estonia's approach to cybersecurity. The final empirical section addresses the development of the e-Residency virtual citizenship program during the European security crisis after Russia's 2014 invasion of Ukraine. The conclusion discusses the uses of the relational approach to digital sovereignty as an analytical lens beyond the Estonian case.

Estonia in the 20th Century

Estonia's cultural constructions of its Others, I contend, inform its digital agenda. These constructions have their basis in contemporary elite interpretations of Estonia's past. This section's survey of pivotal moments in Estonia's 20th-century history contextualizes Estonia's politics of memory and identity that eventually shape the development of its digital sovereignty.

The Russian Empire incorporated present-day Estonia's territory during the Great Northern War (1700–1721) with Sweden (Kasekamp, 2010). After two centuries as a Russian governorate, Estonia first attained national independence following the empire's demise in 1917. Estonia's interwar sovereignty (1918–1940) was a period of intensive state- and nation-building as, for the first time, its state borders were congruent with borders of its ethnocultural titular majority. Internationally, Estonia pivoted its export-oriented economy toward Europe and pursued geopolitical neutrality.

In August 1939, a secret pact between Nazi Germany and Soviet Russia carved Central and Eastern Europe into respective spheres of influence. The following summer, the Soviet Union annexed Estonia, Latvia, and Lithuania. Throughout the 1940s and early 1950s, Stalinist authorities imprisoned, deported, and executed tens of thousands of real and perceived political opponents among Estonians. International law never recognized the legality of the Soviet presence in the Baltics.

During the 50-year Soviet rule, Moscow integrated Estonia's economy into its centrally planned system, while imposing Russian culture and language in education, media, and other social and political spheres (Taagepera, 1993). Demographically, the ratio of ethnic Estonians to Russians shifted from 9:1 on the eve of the Soviet annexation to 2:1 by 1991. Of Estonia's 1.3 million current residents, around 70% are ethnic Estonians and around 25% are ethnic Russians. This dramatic demographic change resulted primarily from the relocation in the 1940–1960s of hundreds of thousands of Russian-speaking workers to staff the newly built industries, most of whom never integrated into the Estonian-language cultural spaces. Following independence, interethnic communication and overall integration of the Russian community increased only slightly, leading to a persistent schism in majority-minority relations (Raun, 2009).

Since 1991, Estonia's foreign relations have been characterized by its Euro-Atlantic integration, on one hand, and poor relations with Russia, on the other hand (Ehin & Berg, 2009). After independence, Western-oriented ethnocentric conservatives prevailed over moderates in the power struggle to design institutional foundations of the emerging Estonian polity (Järve, 2005). The nationalist-neoliberal governing coalition instituted preservation of the ethnic Estonian nation and culture as the state's raison d'être. Accordingly, they established a privileged relationship between the ethnocultural Estonian majority and the state while limiting ethnic Russians' participation in nation- and state-building. For example, only those who themselves had or whose families had resided in the country before the 1940 Soviet annexation were initially eligible for citizenship. Internationally, too, Estonia sought to emulate its interwar economic and political Western orientation. These early institutional frameworks delimited the range of political actors' future choices about national and digital sovereignty.

"Return to Europe" and the Invention of e-Estonia, 1991–2004

In the first independence decade, Estonian political and intellectual elites portrayed the country as a frontier of Western civilization, while depicting the Soviet past, the Estonian Russian minority, and the Russian state as alien and threatening Eastern Others (Kuus, 2012). The Estonian government identified joining the European Union and NATO as its preeminent foreign policy goals to institutionalize its proclaimed civilizational identity. Like most postsocialist European states, Estonia framed its Euro-Atlantic aspirations as a "return" to its authentic ethnocultural identity and European normalcy after the Soviet occupation (Lagerspetz, 1999). On his 1997 visit to Rome, in an address "Estonia's Return to Europe," Foreign Minister Ilves (1997a) argued that the Baltic states were "the only European countries to simply disappear off the map" during the Soviet occupation but that, nevertheless, "geographically and spiritually [Estonia's] European identity has never been in doubt" (para. 2). Ilves's positioning of Estonia as "returning" conveyed that it was always already European and therefore naturally belonged within the Euro-Atlantic institutions.

To align Estonia's political economy with the European Union, consecutive Estonian governments in the 1990s enacted ultraliberal market reforms that often exceeded those of established Western democracies (Bohle & Greskovits, 2012, Ch. 2–3). For example, Estonia was the first European state to adopt a flat tax rate. Estonian officials advertised its liberal reforms to Western decision makers as evidence of the country's cultural affinity with Europe, which the European Union and NATO membership would merely reaffirm. As Foreign Minister Jüri Luik (1994–1995) asserted at the *Wall Street Journal*'s summit in 1995, Estonia had earned "the justified reputation for free-wheeling liberalism" that "would make even Milton Friedman blush" (Luik, 1995, para. 8). At the time, digital technologies epitomized Estonia's favored libertarian ethos (Mosco, 2004). Consequently, Estonian authorities sought to move closer to the West by prioritizing the digitization of its state and society.

Reformist politicians and technologists drew on their Soviet-era technological expertise in establishing independent Estonia's digitization agenda. Within the Soviet Union, Estonia was a hub of scientific and technological education, research, and production, particularly in electronics, computer and radio engineering, and informatics (Högselius, 2005, pp. 58–71; Tyugu, 2009). While using their Soviet know-how, Estonian elites conceived of digitization emphatically as hastening Estonia's Westward transition away from the obsolete Soviet ICT systems and the Soviet past broadly (Björklund, 2016, p. 918; Drechsler, 2018, p. 8; Kattel & Mergel, 2019, p. 145; Kitsing, 2011, p. 6; Mäe, 2017, pp. 38–39; Runnel, Pruulmann-Vengerfeldt, & Reinsalu, 2009, pp. 33–34; Velmet, 2020). Estonia's inaugural information policy strategy framed digitization as supporting "the integration of Estonia into the family of developed nations" (Estonian Informatics Council, 1998, p. 15).

From the mid-1990s to the early 2000s, Estonia established the institutional foundations of its digital sovereignty in accordance with the state's broader ultraliberal frameworks (Högselius, 2005, Ch. 5–7; Krull, 2003; Rits, 2015). A permissive legal environment and the passage of ICT-specific legislation, such as the Personal Data Protection Act, Databases Act, and Digital Signatures Act, encouraged the use of digital technologies in business and public sectors. The ICT sector's privatization and liberalization, including the elimination of most import quotas and license requirements, attracted foreign telecommunication investors and triggered the early growth of e-banking, e-commerce, and mobile telecommunication. The government promoted digital access and literacy through nationwide public-private initiatives that computerized and connected the school system to the Internet, established public Internet access points, and trained thousands of Estonians in computer and Internet skills.

In the early 2000s, Estonia introduced two technologies that remain foundational for the e-government infrastructure and that few countries have been able to replicate (Vassil, 2015). The X-Road is a data exchange layer that links all public and private e-Estonia services into an interoperable environment. The Electronic ID (eID), a credit-card-sized plastic photo ID with a chip, is a national identification card that provides access to services within the X-Road environment.

Estonia's self-aggrandizing narrative about its ICT transformations became crucial in distinguishing the country from other postsocialist states vying for Western recognition and assistance (see Halliste, 2009). Even before carrying out major ICT initiatives, Estonian highest-level officials promoted to foreign audiences Estonia's plans for participating in "the high-tech revolution" (Kallas, 1996, para. 9) and "ushering Estonia

into the Information Age" (Meri, 1996, para. 12). Amid global euphoria about digital technologies, Estonia was conveying that culturally, if not yet materially, it belonged within Western technological modernity. As the Estonian government introduced new digital initiatives, such as paperless ministerial meetings, it framed them as further evidence of the country's transitional success.

Estonia's digital narrative emphasizes its existence as a productive, responsible, and self-reliant member of the Euro-Atlantic community. Anthropologist Katherine Verdery (1996) writes that Eastern European socialist regimes promoted a culture of paternalism in which the "Benevolent Father Party" gave "handouts to its children" as it saw fit, discouraging citizens from fulfilling their own needs (pp. 24–26). By contrast, the ethos of postsocialist transition privileged personal initiative and responsibility as its foundational virtues (Kennedy, 2002). Within transition culture, a society's passage from a recipient of Western aid and expertise to one that shares such expertise with others serves as a symbolic marker of the nation's success in achieving Western normalcy.

Estonia communicated its fit within the Euro-Atlantic community by assigning transitional values to its technological developments. These narratives alleged Estonia's technological ingenuity in creating and adapting digital solutions, frugality in doing that with minimal resources, and responsibility in sharing them with the world. At the 1997 Conference on Information Technology in the Baltic Sea Region, Ilves (1997b) touted the "explosive growth in Estonian participation in the global information society" (para. 3), in reference to its relatively high Internet usage, and boasted:

> [T]he Estonia [*sic*] experience in the global information revolution is something we can offer to other countries. After all, what we have shown is that even a poor country can, given the will and interest, move up to the level of the world leaders in connectedness. (Ilves, 1997b, para. 17)

As part of Estonia's discursive strategy of "returning to Europe," its officials often framed the country's technological accomplishments as evidence of ethnic Estonians' authentic Europeanness. This claim implicitly and often explicitly conveyed that Estonia's cultural affinity with Northern Europe signified its natural place within the Euro-Atlantic institutions as well. At the Conference, Ilves (1997b) argued that "something 'nordic' in the Estonian character" accounted for their supposedly natural predisposition for ICTs (para. 3). The foreign minister also delineated Estonia from the Soviet/Russian Other with an oft-used trope purporting that Estonians embraced ICTs as "a way to leapfrog over years of technical backwardness and isolation forced upon [them] by the Soviet Union" (Ilves, 1997b, para. 4).

By the time of Estonia's accession to the European Union and NATO in 2004, Estonian elites viewed their digitization program as integral for the eventual success of the country's "return to Europe." Minister of Economic Affairs and Communications Meelis Atonen (2003–2004) wrote triumphantly in Estonia's information policy strategy, "'e' has put Estonia back on the world map" (Estonian Ministry of Economic Affairs and Communications [EMoEAC], 2004, p. 2). Indeed, by the early 2000s, Western media, academic, and political circles were widely praising and tangibly supporting Estonia's digital pursuits. For example, in 2002, the United Nations, the Open Society Institute, and the Estonian government jointly launched the e-Governance Academy, a world-leading knowledge hub and training outfit on the use of digital technologies

in public administration. As the following sections demonstrate, Estonia's relations with its Russian and Western Others continued shaping the materiality and mythos of e-Estonia long after the country's initial Euro-Atlantic integration.

Memory Wars and the Cybersecurity Turn, 2007–2013

In April–May 2007, Estonia suffered a series of large-scale cyberattacks originating from Russia. The roots of the attacks and of the subsequent overhaul of Estonia's cybersecurity approach are to be found in the Estonian state's relations with the country's Soviet past, its Russian minority, and the Russian state. In Estonian historical narratives, the end of WWII signifies a return to Stalinist repressions and Soviet occupation (Onken, 2007). By contrast, most Russian-speaking Estonians and the Russian state view the Red Army as liberators of Estonia from the Nazi occupation. Since Vladimir Putin's rise to power in 2000, WWII came to dominate Russia's official national identity project, while the annual May 9 Victory Day celebration was turned into a grandiose militaristic affair signaling Russia's resurgence.

Before the 2007 Victory Day, the Estonian government announced its plan to relocate the Soviet-era WWII monument, colloquially known as the Bronze Soldier, from downtown Tallinn to a military cemetery (Brüggemann & Kasekamp, 2008). Although for Russian Estonians the statue symbolized the Red Army's heroism and sacrifice, for ethnic Estonians it represented an occupier. On the monument's relocation, this long-standing rift turned into the first violent clashes between Russian Estonians and the law in independent Estonia's history.

The controversy surrounding the Bronze Soldier instantaneously acquired an international dimension. In Moscow, protesters disrupted the Estonian Embassy's work. Russian leadership and state-affiliated media framed the incident as an assault on the memory of fallen Soviet soldiers, insinuating Estonian authorities' Nazi sympathies.

Against this contentious backdrop, Estonian governmental, telecommunications, financial, and media institutions endured several weeks of cyberattacks (Tikk, Kaska, & Vihul, 2010, pp. 14–34). Based on the geopolitical context and digital traces, it was widely presumed that the Russian government orchestrated the attacks. The incident drew colossal global coverage of Estonia, most of which sympathetically reiterated Estonia's narratives about its digital achievements and the Russian threat (e.g., Landler & Markoff, 2007).

The 2007 attacks prompted Estonian authorities to reimagine cybersecurity as a top-level political issue. Before the attacks, Estonia's cybersecurity developed incrementally as a technical issue of concern to narrow specialists (Randver, 2006, pp. 33–36). In 2005, public and private experts began drafting the principles of Estonian information security policy. The next year, the government established the Computer Emergency Response Team, the first Estonian body responsible for handling domestic cybersecurity incidents and coordinating other responsible organizations. The attacks dramatically sped up these early developments. Within several years, Estonia incorporated the issue of cybersecurity into national doctrines and adopted new cybersecurity-specific strategies and policies, amended legislation across various legal

domains to account for cybersecurity, and created new and reformed existing cybersecurity bodies (Czosseck, Ottis, & Talihärm, 2011; Kohler, 2020; Osula, 2015).

Internationally, Estonian authorities seized on their newfound legitimacy as victims of possibly the first large-scale interstate cyberattack—a status they actively promoted to emphasize Estonia's unrivaled expertise—to become a leading cybersecurity norm entrepreneur at the United Nations and other organizations (Crandall & Allan, 2015). Building on key tropes of the preceding decade, Estonian officials narrated their cybersecurity reforms to Western audiences as exemplifying Estonia's unmatched technological expertise and selflessness in sharing it. In 2008, Estonia's inaugural and one of the world's first national cybersecurity doctrines asserted: "Owing to Estonia's unique experience in dealing with cyberattacks in the spring of 2007 and subsequent policy initiatives, the international community expects a major contribution from us—and perhaps even a leadership role" (Cyber Security Strategy Committee, 2008, p. 22).

The most significant institution to emerge from the attacks arguably was the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Specializing in cybersecurity consulting, training, and research, the center is one of the Alliance's two dozen centers of excellence dealing with various security aspects. Estonia first proposed the idea of the center in 2004 and received NATO approval in 2006. Yet the parties attributed the center's expedited opening in May 2008 to Estonia's unique experience with cybersecurity. Whereas the center's staff and funding come from two dozen states, its world-class collective expertise and resources address Estonia's foremost national security threat from Russia all the while reinforcing the symbolic link between Estonia and cutting-edge digital technologies.

The center strengthens Estonia's ties with the West in several ways. Its annual Conference on Cyber Conflict, a leading discussion forum in the field, the Locked Shields, the world's largest cybersecurity exercises, and other regular and occasional events bring hundreds of security experts and policy makers to Estonia. These events allow Estonian officials to directly communicate Estonia's digital accomplishments and Russia's threat to Western military, political, and technological elites.

The center's research also attracts international attention to Estonia. For example, its most high-profile publications, the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare* and its 2017 follow-up, are the preeminent collections of expertise on the subject. Renowned Estonian legal scholar Lauri Mälksoo (2013) expressed the widespread attitude of the country's elites toward the *Tallinn Manual* as helping reaffirm Estonia's sovereign existence when he wrote that the publication further "prove[d] that Estonia as a state ha[d] really arrived in the international community" (para. 5).

Finally, the center raises Estonia's reputation as a contributing self-reliant member of the Euro-Atlantic community (Crandall, 2014, pp. 36–40). As the center's host, Estonia makes the largest annual contributions to its budget. Estonia's contribution comes from its general defense budget. In other words, Estonia's spending on the center counts toward the NATO recommendation that its members dedicate at least 2% of their GDP to defense. Since only a handful of the alliance's 30 members reach this target, Estonian officials regularly invoke that the country meets this threshold. Western officials, in turn, routinely bring up this accomplishment to praise Estonia for their responsible approach to transatlantic security.

During Estonia's second decade of independence, its relational dynamics with Russian and Western Others remained critical for its digital sovereignty. While hosting another international ICT event in Tallinn, President Ilves (2012) reiterated Estonia's existential view of ICTs as instrumental to its visibility among Western publics and thereby protection from the Russian threat: "Technology is not just an opportunity for Estonia but a necessity that allows us to maintain our state and population while remaining visible in the world" (para. 3). Russia's military invasion of Ukraine in 2014 further embedded Estonia's existential concerns into the development of its digital sovereignty.

The Ukrainian Crisis and e-Residency, 2014–2018

By the 2010s, Estonia's e-government and cybersecurity initiatives cemented the country's reputation as a digital pioneer. In 2014, on a visit to Tallinn, U.S. President Barack Obama joked that he should have called the "high-tech leader" Estonia when setting up the Healthcare.gov website, which had famously malfunctioned on its launch (Obama & Ilves, 2014, para. 14). To maintain its global innovative reputation, in late 2013, Estonia proposed a novel digital project that would make some of the e-Estonia services available remotely, particularly those relating to business conduct:

> Estonia will start offering its secure and convenient services to the citizens of other countries. Virtual residence or e-residence will be launched, meaning that Estonia will issue non-residents with electronic identity in the form of digital ID cards. The aspiration for Estonia is to become as re-known [*sic*] for its e-services as Switzerland is in the field of banking. (EMoEAC, 2013, p. 3)

E-Residency launched in December 2014 against the backdrop of Europe's then worst security crisis since WWII. Earlier that year, Russia annexed Ukraine's Russophone Crimea region and supported the separatist insurgency in Russophone Eastern Ukraine. The Kremlin alleged that its actions preempted imminent violence against Ukraine's Russian minority by the Ukrainian government and nationalist militias.

Considering Estonia's experience of Soviet annexation and that ethnic Estonians and Russians still dramatically diverged in their media consumption, collective memories, and political attitudes (see Saar Poll, 2014), the Ukrainian crisis brought new immediacy within the Estonian society to the issues of interethnic relations and national sovereignty. The government strove to minimize potential ethnic unrest and the threat of Russia's invasion. In 2015, for example, Estonia launched its first public Russian-language television channel to "create more cohesion in society and give Russian speakers in Estonia the feeling that they matter," according to its head (Deutsche Welle, 2015, para. 2). Incorporation of these extraordinary geopolitical circumstances into e-Residency's development illuminates how e-Estonia initiatives reflect Estonia's broader relational dynamics with its national Others.

As with all e-Estonia programs, e-Residency's postnational pathos of creating the new digital nation is meant to enhance Estonia's *national* image and security (Blue, 2020; Tammpuu & Masso, 2018). At the dawn of e-Residency, in a paper titled "Estonian e-Residency: Redefining the Nation-State in the Digital Era," Estonia's chief information officer Taavi Kotka (2013–2017), e-Residency Program director Kaspar Korjus (2014–2019), and others revealed how the program's portrayal of national citizenship and

territoriality as outmoded—e-Residency's main selling point—itself was rooted in considerations for Estonia's national sovereignty (Kotka, Castillo, & Korjus, 2015). The authors argued that the global network of e-residents would foster Estonians' "'soft' ties to people abroad, which may help to deter future conflicts or generate increased international support should Estonia find itself in a conflict" (Kotka et al., 2015, p. 11). For Kotka and colleagues, e-Residency would also bolster Estonia's sovereignty indirectly by advancing the country's renown as "the pioneer in the area of cyber defence" (Kotka et al., 2015, p. 12). E-Residency would do that by showing the world that "Estonia is so confident about its technical e-government platform that it is not afraid to make it publicly available to everybody everywhere" (Kotka et al., 2015, p. 12). In the end, e-Residency would "help Estonia project its transitional successes to the external world" (Kotka et al., 2015, p. 11). This positive attention, the paper argued, would increase foreign investment, trade, and tourism. Rather than redefine the nation-state, then, e-Residency has followed Estonia's official geopolitical imagination, in which its ties with Western institutions and publics helped safeguard Estonian national territorial borders from Russia's aggression.

By 2018, e-Residency acquired close to 50,000 participants, mostly from business and technology communities, and received ample praise from Western media and politicians (e.g., Pardes, 2016). In addition to marketing materials and events, e-Residency achieved this prominence by way of Estonian high-level officials touting the program during foreign visits and gifting the e-Residency card to global celebrities and political leaders as a PR stunt. Four years into the program, President Kaljulaid (2018) commended e-Residency for having brought Estonia "a significant amount of global attention and [having] helped to establish the image of Estonia as a progressive digital country" (para. 3). Yet, Kaljulaid (2018) initiated a national multistakeholder discussion to "determine what e-residency 2.0 should look like" to increase its contributions to Estonia's economy, image, and security (para. 3).

Months-long consultations on e-Residency's future involved over a hundred experts from the public, private, and civil society sectors who ranged from IT developers to the prime minister. The discussions resulted in the white paper, "e-Residency 2.0," containing 49 recommendations for improving the program. Some key suggested innovations included expanding e-Residency services beyond the business realm, engaging Estonian citizens in e-Residency alongside foreigners, and educating foreign e-residents about Estonian history and culture. While proposing structural changes to e-Residency, the white paper reaffirmed the program's ultimate mission of bolstering national sovereignty: "Through strong business and cultural ties, Estonia's importance in the world will grow. By the same means, the deterrent effect on potential aggressors and national security will also increase" (Korjus, 2018a, p. 13). The unnamed "ties" and "aggressors" implied the West and Russia, respectively.

E-Residency encapsulates Estonia's decades-long approach to digital sovereignty in the context of its relations with Russian and Western Others. In the 1990s, Estonian officials lamented the country's disappearance from the world map as a sovereign state during the Soviet occupation and viewed state digitization as a way for Estonia to "return" to the Euro-Atlantic community. Having joined Western institutions, in the 2000s, Estonia celebrated digital technologies for enhancing its defenses against Russia at the infrastructural level and, indirectly, by maintaining outsized Western attention on Estonia. In 2018,

on publication of the e-Residency white paper, e-Residency Program director Kaspar Korjus (2018b) similarly explained the significance of the program's global dissemination for Estonia's national sovereignty: "As Estonians have learnt throughout history, if more people can find our country on a map then we are more likely to remain on that map" (para. 19).

Conclusion: The Uses of the Relational Approach to Digital Sovereignty

What is to be gained from a relational approach to digital sovereignty? This article argued that centering the relationship between the national Self and its Others in the analysis of national digital sovereignty elucidates why and how it emerges and develops. This argument bridges two established claims from constructivist theories of culture and technology. One is that national identity as articulated and propagated by governing elites guides the state's technological program. Another is that identity is an inherently relational category that is maintained through continuous boundary making between the Self and its Others. Taken together, these claims indicate that it is analytically productive and sometimes imperative to attend to relational dynamics between the national Self and its Others to grasp the logics of digital sovereignty. To illustrate this proposition, this article traced how Estonia's cultural constructions of its Russian and Western Others shaped the contours of its digital sovereignty. It showed that Estonia's digital initiatives, which are often couched in technofuturistic postnational discourse, are meant to reaffirm Estonia's sovereign territorialized existence within the Euro-Atlantic community.

Whereas this article examined digital sovereignty as an elite political project manifested in high-level official discourses and institutions, the relational lens's theoretical and methodological versatility opens the door for diverse scholarly approaches to digital sovereignty. Ethnographies of infrastructure, for example, can investigate Self-Other dynamics in the everyday workings of digital sovereignty, what cultural anthropologist of technology Alix Johnson (2021) conceptualizes as the "mechanics of sovereignty." This approach treats sovereignty as a process of material construction and explores its constitutive people and practices. Lorraine Kaljund (2018), for instance, draws on participant observation and interviews with the developers of a recent e-Estonia initiative, data embassy, to explore how this team embeds ethnocentric Estonian statehood into the project's software, code, and policy.

Another dimension to consider is domestic power struggles over competing constructions of Otherness and technology. Analyses of debates and decision making surrounding digital sovereignty, particularly the use of Othering to legitimize one's technological agenda, illuminate how and why some ideas but not others become state rhetoric and policy. The official e-Estonia narrative retroactively frames Estonia's digital turn as a self-evident response to Soviet occupation and a reflection of ethnic Estonians' natural predisposition toward technology. Yet, when Estonia's ruling coalition first promoted the project of digital transformation in the early 1990s, as part of their Western-oriented ethnocentric platform, it was not uniformly supported across the political spectrum. How did e-Estonia become political dogma, the questioning of which is seen as tantamount to undermining Estonia's Euro-Atlantic credentials and benefiting Russia? Detailing national technopolitical struggles would help show digital sovereignty as always a product of political contention, including over membership in the national imagined community.

Further, sociological approaches might explore how Self-Other dynamics manifest within the circles directly involved in the making of digital sovereignty. Historically, dominant ethnic and political elites excluded their Others from creating and enjoying technological innovation on par with the privileged group (Edgerton, 2006, pp. 131–136). Scholars of e-Estonia note that the country's digital elite—entrepreneurs, developers, policy makers—remain almost exclusively ethnically Estonian (Kattel & Mergel, 2019, p. 147) and that national digitization does not benefit the social and professional standing of ethnic Estonians and Russians equally (Drechsler, 2018, p. 13). In Estonia and elsewhere, future research could employ the relational lens in examining the structural barriers to participation in the making of digital sovereignty and the consequences of such representational imbalances.

Specific manifestations of Self-Other dynamics on digital sovereignty will vary across national contexts. The analytical task of the relational approach is to discover and conceptualize Others and then empirically demonstrate their material significance for digital sovereignty. Beyond the nation-state, the relational approach potentially applies to other types of digital sovereignty conceptualized by scholars, such as municipal, personal, indigenous, corporate, and others.

References

Benhabib, S. (2002). *The claims of culture: Equality and diversity in the global era*. Princeton, NJ: Princeton University Press.

Björklund, F. (2016). E-government and moral citizenship: The case of Estonia. *Citizenship Studies, 20*(6–7), 914–931. doi:10.1080/13621025.2016.1213222

Blue, A. (2020). Evaluating Estonian E-residency as a tool of soft power. *Place Branding and Public Diplomacy*, *17*, 359–367. doi:10.1057/s41254-020-00182-3

Bohle, D., & Greskovits, B. (2012). *Capitalist diversity on Europe's periphery*. Ithaca, NY: Cornell University Press.

Brüggemann, K., & Kasekamp, A. (2008). The politics of history and the "War of monuments" in Estonia. *Nationalities Papers, 36*(3), 425–448. doi:10.1080/00905990802080646

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies, 21*(5), 594–613. doi:10.1177/1367549417751151

Calhoun, C. (1997). *Nationalism*. Minneapolis: University of Minnesota Press.

Carlsson, U. (2003). The rise and fall of NWICO. *Nordicom Review, 24*(2), 31–67. doi:10.1515/nor-2017-0306

Charland, M. (1986). Technological nationalism. *Canadian Journal of Political and Social Theory, 10*(1–2), 196–220. Retrieved from https://journals.uvic.ca/index.php/ctheory/article/download/14083/4854/0

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. doi:10.1177/1461444819865984

Crandall, M. (2014). Soft security threats and small states: The case of Estonia. *Defence Studies*, *14*(1), 30–55. doi:10.1080/14702436.2014.890334

Crandall, M., & Allan, C. (2015). Small states and big ideas: Estonia's battle for cybersecurity Norms. *Contemporary Security Policy*, *36*(2), 346–368. doi:10.1080/13523260.2015.1061765

Cyber Security Strategy Committee. (2008). *Cyber security strategy*. Estonian Ministry of Defense. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy/@@download_version/993354831bfc4d689c20492459f8a086/file_en

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. *International Journal of Cyber Warfare and Terrorism*, *1*(1), 24–34. doi:10.4018/ijcwt.2011010103

Deutsche Welle. (2015, September 28). Estonia launches own Russian-language TV channel. *Deutsche Welle*. Retrieved from https://www.dw.com/en/estonia-launches-own-russian-language-tv-channel/a-18747088

Drechsler, W. (2018). Pathfinder: E-Estonia as the β-version. *JeDEM—eJournal of eDemocracy and Open Government*, *10*(2), 1–22. doi:10.29379/jedem.v10i2.513

Dumitrica, D. (2015). Imagining the Canadian Internet: A case of discursive nationalization of technology. *Studies in Ethnicity and Nationalism*, *15*(3), 448–473. doi:10.1111/sena.12152

Edgerton, D. (2006). *The shock of the old: Technology and global history since 1900*. Oxford, UK: Oxford University Press.

Ehin, P., & Berg, E. (2009). Incompatible identities? Baltic-Russian relations and the EU as an arena for identity conflict. In E. Berg & P. Ehin (Eds.), *Identity and foreign policy: Baltic-Russian relations and European integration* (pp. 1–14). Farnham, UK: Ashgate.

Estonian Informatics Council. (1998). *Principles of Estonian information policy*. State Chancellery of Estonia. Retrieved from https://ega.ee/wp-content/uploads/2020/01/Eesti-infopoliitika-p-hialused.pdf

Estonian Ministry of Economic Affairs and Communications (EMoEAC). (2004). Estonian IT policy: Towards a more service-centred and citizen-friendly state. Principles of the Estonian information policy 2004–2006. Retrieved from https://www.digar.ee/arhiiv/en/download/23019

Estonian Ministry of Economic Affairs and Communications (EMoEAC). (2013). *Digital agenda 2020 for Estonia*. Retrieved from https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology, 33*(3), 369–378. doi:10.1007/s13347-020-00423-6

Halliste, E. (2009). How we communicated Estonia into the EU. In K. Tael & K. Sillaste-Elling (Eds.), *Estonia's way into the European Union* (pp. 132–137). Tallinn, Estonia: Estonian Ministry of Foreign Affairs. Retrieved from https://vm.ee/sites/default/files/content-editors/web-static/052/Estonias_way_into_the_EU.pdf

Hecht, G. (2009). *The radiance of France: Nuclear power and national identity after World War II* (2nd ed.). Cambridge, MA: The MIT Press.

Högselius, P. (2005). *The dynamics of innovation in Eastern Europe: Lessons from Estonia*. Cheltenham, UK: Edward Elgar.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society, 8*(1), 1–17. doi:10.1177/2053951720982012

Ilves, T. (1997a, March 20). *Estonia's return to Europe*. Presented at the Società Italiana per le Organizzazione Internazionale, Rome, Italy. Retrieved from https://vm.ee/et/node/42681

Ilves, T. (1997b, December 16). *The role of Estonia in the global information society*. Presented at the Conference on Information Technology in the Baltic Sea Region, Tallinn, Estonia. Retrieved from https://vm.ee/ru/node/42655

Ilves, T. (2000, October 25). *E-Estonia and the new Europe*. Presented at the London School of Economics, London, UK. Retrieved from https://vm.ee/et/node/42610

Ilves, T. (2012, March 14). *President of the republic at the "e-governance or e-dependence?" conference*. Retrieved from https://vp2006-2016.president.ee/en/official-duties/speeches/7193-president-of-the-republic-at-the-e-governance-or-e-dependence-conference-in-swissotel-tallinn-14-march-2012/index.html

Jasanoff, S. (2015). Future imperfect: Science, technology, and the imaginations of modernity. In S. Jasanoff & S.-H. Kim (Eds.), *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power* (pp. 1–33). Chicago, IL: The University of Chicago Press.

Jasanoff, S., & Kim, S.-H. (2009). Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea. *Minerva, 47*(119), 119–146. doi:10.1007/s11024-009-9124-4

Järve, P. (2005). Re-Independent Estonia. In S. Smooha & P. Järve (Eds.), *The fate of ethnic democracy in post-communist Europe* (pp. 61–80). Budapest, Hungary: Open Society Institute.

Johnson, A. (2021). The mechanics of sovereignty: Autonomy and interdependence across three cables to Iceland. *American Anthropologist, 123*(3), 578–589. doi:10.1111/aman.13617

Kaljulaid, K. (2017, June 6). President of the Republic at the opening of EuroDIG. Tallinn, Estonia. Retrieved from https://www.president.ee/en/official-duties/speeches/2428-president-republic-opening-eurodig

Kaljulaid, K. (2018, May 6). President Kaljulaid: We must give a new meaning to e-residency. Retrieved from https://web.archive.org/web/20210506145827/https://president.ee/en/meedia/press-releases/14458-president-kaljulaid-we-must-give-a-new-meaning-to-e-residency/

Kaljund, A. L. (2018). Restoration doctrine rebooted: Codifying continuity in the Estonian data embassy initiative. *PoLAR: Political and Legal Anthropology Review, 41*(1), 5–20. doi:10.1111/plar.12240

Kallas, S. (1996, March 12). *Statement by Minister Kallas at the Foreign Press Centre in Tokyo*. Retrieved from https://vm.ee/en/news/statement-minister-kallas-foreign-press-centre-tokyo

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation. In M. E. Compton & P. 't Hart (Eds.), *Great policy successes* (pp. 143–160). Oxford, UK: Oxford University Press.

Kasekamp, A. (2010). *A history of the Baltic states*. Houndmills, Basingstoke, UK: Palgrave Macmillan.

Kennedy, M. D. (2002). *Cultural formations of postcommunism: Emancipation, transition, nation, and war*. Minneapolis: University of Minnesota Press.

Kitsing, M. (2011). Success without strategy: E-Government development in Estonia. *Policy & Internet, 3*(1), 1–21. doi:10.2202/1944-2866.1095

Kohler, K. (2020). *Estonia's national cybersecurity and cyberdefense posture: Policy and organizations*. Zürich, Switzerland: Center for Security Studies (CSS), ETH Zürich. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf

Korjus, K. (2018a). *E-Residency white paper 2.0*. Republic of Estonia E-Residency. Retrieved from https://s3.eu-central-1.amazonaws.com/ereswhitepaper/e-Residency+2.0+white+paper+English.pdf

Korjus, K. (2018b, December 18). *Estonian President Kersti Kaljulaid reveals the future direction of e-Residency*. Retrieved from https://medium.com/e-residency-blog/estonian-president-kersti-kaljulaid-reveals-the-future-direction-of-e-residency-5b1177dfa78c

Kotka, T., Vargas Alvarez del Castillo, C. I., & Korjus, K. (2015). Estonian e-Residency: Redefining the nation-state in the digital era. University of Oxford Cyber Studies Programme. Retrieved from https://www.etis.ee/File/DownloadPublic/a25d260a-f24b-4bd0-a456-ddfd6998a68e?name=Working_Paper_No.3_Kotka_Vargas_Korjus.pdf

Krige, J., & Wang, J. (2015). Nation, knowledge, and imagined futures: Science, technology, and nation-building, post-1945. *History and Technology, 31*(3), 171–179. doi:10.1080/07341512.2015.1126022

Krull, A. (2003, April). *ICT infrastructure and e-readiness assessment report: ESTONIA*. Tallinn, Estonia: PRAXIS Center for Policy Studies. Retrieved from http://www.praxis.ee/wp-content/uploads/2014/03/2003-Ict-infrastructure-and-e-readiness-assessment.pdf

Kuus, M. (2012). Banal Huntingtonianism: Civilisational geopolitics in Estonia. In S. Guzzini (Ed.), *The return of geopolitics in Europe? Social mechanisms and foreign policy identity in crises* (pp. 174–191). Cambridge, UK: Cambridge University Press.

Lagerspetz, M. (1999). Postsocialism as a return: Notes on a discursive strategy. *East European Politics and Societies, 13*(2), 377–390. doi:10.1177/0888325499013002019

Landler, M., & Markoff, J. (2007, May 28). In Estonia, what may be the first war in cyberspace. *The New York Times*. Retrieved from https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141.html

Luik, J. (1995, April 8). *Remarks*. Presented at the *Wall Street Journal* Europe's First Annual Central European Economic Reform Summit, London, UK. Retrieved from https://vm.ee/en/news/remarks-mr-juri-luik-wall-street-journal-europes-first-annual-central-european-economic-reform

Mäe, R. (2017). The story of e-Estonia: A discourse-theoretical approach. *Baltic Worlds, 10*(1–2), 32–44. Retrieved from https://balticworlds.com/wp-content/uploads/2017/06/BW-1-2-2017-M%C3%84E.pdf

Mälksoo, L. (2013, August 8). The Tallinn Manual as an international event. *International Centre for Defence and Security*. Retrieved from https://icds.ee/en/the-tallinn-manual-as-an-international-event

Meri, L. (1996, June 25). *Remarks delivered by Ambassador Trivimi Velliste on behalf of Lennart Meri*. Presented at the IEWS-Citibank Baltic Investors Forum, New York, NY. Retrieved from https://vp1992-2001.president.ee/eng/PrinditavDokument.asp?ID=4428

Merkel, A., Frederiksen, M., Marin, S., & Kallas, K. (2021, March 1). *Letter to the president of the European Commission on digital sovereignty*. Estonian Government. Retrieved from https://www.valitsus.ee/en/media/3840/download

Möllers, N. (2020). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, Technology, & Human Values, 46*(1), 112–138. doi:10.1177/0162243920904436

Morley, D., & Robins, K. (1995). *Spaces of identity: Global media, electronic landscapes and cultural boundaries*. London, UK: Routledge.

Mosco, V. (2004). *The digital sublime: Myth, power, and cyberspace*. Cambridge, MA: The MIT Press.

Obama, B., & Ilves, T. (2014, September 3). *Remarks by President Obama and President Ilves of Estonia in joint press conference*, Tallinn, Estonia. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2014/09/03/remarks-president-obama-and-president-ilves-estonia-joint-press-confer-0

Onken, E.-C. (2007). The Baltic states and Moscow's 9 May commemoration: Analysing memory politics in Europe. *Europe-Asia Studies, 59*(1), 23–46. doi:10.1080/09668130601072589

Osula, A.-M. (2015). *National cyber security organisation in Estonia*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/CS_organisation_ESTONIA_032015_1.pdf

Pardes, A. (2016, May 5). Estonia's e-Residency program is the future of immigration. *Vice*. Retrieved from https://www.vice.com/en_us/article/avyx5a/estonias-e-residency-program-is-the-future-of-immigration

Petersoo, P. (2007). Reconsidering otherness: Constructing Estonian identity. *Nations and Nationalism, 13*(1), 117–133. doi:10.1111/j.1469-8129.2007.00276.x

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review, 9*(4), 1–19. doi:10.14763/2020.4.1532

Pommereau de, I. (2011, March 4). In Estonia, Communism's collapse paved the way for Wi-Fi everywhere. *Christian Science Monitor*. Retrieved from https://www.csmonitor.com/World/Global-News/2011/0304/In-Estonia-Communism-s-collapse-paved-the-way-for-Wi-Fi-everywhere

Randver, R. (Ed.). (2006). *Information technology in public administration of Estonia yearbook 2005*. Estonian Ministry of Economic Affairs and Communications. Retrieved from https://www.digar.ee/arhiiv/en/download/214865

Raun, T. U. (2009). Estonia after 1991: Identity and integration. *East European Politics and Societies, 23*(4), 526–534. doi:10.1177/0888325409342113

Rits, K. (2015). *EGovernment in Estonia* (No. 17). Brussels, Belgium: European Commission. Retrieved from https://joinup.ec.europa.eu/sites/default/files/document/2015-03/egov_in_estonia_-_january_2015_-_v_17_final.pdf

Rocha, R., & Hansen, J. (1993). *Estonia: The transition to a market economy*. Washington, DC: The World Bank. Retrieved from http://documents.worldbank.org/curated/en/715701468771070270/pdf/multi0page.pdf

Runnel, P., Pruulmann-Vengerfeldt, P., & Reinsalu, K. (2009). The Estonian Tiger Leap from post-communism to the information society: From policy to practice. *Journal of Baltic Studies, 40*(1), 29–51. doi:10.1080/01629770902722245

Saar Poll. (2014, March). *Public opinion and national defence, March 2014*. Estonian Ministry of Defence. Retrieved from https://www.kaitseministeerium.net/sites/default/files/elfinder/article_files/public_opinion_and_national_defence_2014_march.pdf

Savchenko, D. (2019). E-Estonia reprogrammed: Nation branding and children coding. In M. Biagioli & V. A. Lepinay (Eds.), *From Russia with code: Programming migrations in post-Soviet times* (pp. 213–228). Durham, NC: Duke University Press.

Schneider, F. (2018). *China's digital nationalism*. New York, NY: Oxford University Press.

Schulte, S. R. (2013). *Cached: Decoding the Internet in global popular culture*. New York: NYU Press.

Taagepera, R. (1993). *Estonia: Return to independence*. Boulder, CO: Routledge.

Tammpuu, P., & Masso, A. (2018). "Welcome to the virtual state": Estonian e-residency and the digitalised state as a commodity. *European Journal of Cultural Studies, 21*(5), 543–560. doi:10.1177/1367549417751148

Tikk, E., Kaska, K., & Vihul, L. (2010). *International cyber incidents—Legal considerations*. Tallinn: Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

Triandafyllidou, A. (1998). National identity and the "other." *Ethnic and Racial Studies, 21*(4), 593–612. doi:10.1080/014198798329784

Tyugu, E. (2009). Computing and computer science in the Soviet Baltic region. In J. Impagliazzo, T. Järvi, & P. Paju (Eds.), *History of Nordic computing 2* (pp. 29–38). Berlin, Germany: Springer.

Vassil, K. (2015). *Estonian e-Government ecosystem: Foundation, applications, outcomes*. Washington, DC: World Bank. Retrieved from http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf

Velmet, A. (2020). The blank slate e-State: Estonian information society and the politics of novelty in the 1990s. *Engaging Science, Technology, and Society, 6*, 162–184. doi:10.17351/ests2020.284

Verdery, K. (1996). *What was socialism, and what comes next?* Princeton, NJ: Princeton University Press.