Digital Nationalisms: Identity, Strategic Communication, and Global Internet Governance

by

Stanislav Budnitskiy

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Communication

Carleton University
Ottawa, Ontario

Abstract

A growing number of states in the twenty-first century have reimagined and rearticulated the role of digital technologies as indispensable to the nation's economic, cultural, and political success—and sometimes survival—under the conditions of digital globalization. Digital nationalism refers to this shift in the national state's imagination of digital technologies vis-à-vis their national Selves, as well as attendant discursive and material efforts at constructing and strategically communicating their national digital identities. On the one hand, this is a global trend, which is rooted in the rationalist imaginary and posits digital technological development as critical to economic growth and overall national well-being. On the other hand, and this is the crux of the argument underlying this dissertation, national cultural identities shape the specific logics and language of respective national digital rhetoric and policies.

To illuminate the workings of digital nationalism, the dissertation examines how Estonia's and Russia's conduct in the domain of global internet governance—the design and administration of legal and technological architectures of the global internet and surrounding geopolitical debates—reflect their national identity visions. The dissertation argues that Estonia's championing of the "internet freedom" narrative is meant to bolster its central identity aspiration of symbolically and institutionally "returning to Europe" after half a century of the Soviet rule, while Russia's championing of "internet sovereignty" contributes to its identity narrative of a resurgent great power following its geopolitical decline in the first post-Cold War decade.

The dissertation offers a critical cultural approach to the study of digital technological politics and aims to contribute to our understanding of the logics of digital

globalization and global internet governance, contemporary nationalism, and socio-

political trajectories in post-socialist Europe.

Acknowledgements

No other undertaking in my life has been at once as isolating and collaborative as this dissertation. For helping me not only endure but also enjoy this arduous and rewarding journey I am thankful to many individuals and institutions.

I owe my greatest intellectual debt to my academic advisor, Melissa Aronczyk, whose scholarship was critical in first sparking the idea to one day pursue doctoral studies and whose encouraging reply to my introductory email convinced me definitively to embark upon something as reckless. Between our initial correspondence seven years ago and the panicky emails in the last days of dissertation writing, I received nothing but the kind of intellectual and personal support that a graduate student can only hope for.

Every faculty and staff member I have met in the Communication program at Carleton University has been incredibly generous with their time and expertise. In particular, thank you to Ira Wagman and Dwayne Winseck for helping me mold this project from its embryonic stage through its completion and for valuable insights into subjects beyond my dissertation work. I am also thankful to Chris Russill for his teaching and advising over the years. I am indebted to the always kind and patient Graduate Administrator Coleen Kornelsen for helping me navigate university bureaucracy, and to Melanie Leblanc who so aptly succeeded her.

I would not have been able to pursue my doctorate at Carleton without the leadership of the Communication program securing the Ontario Trillium Scholarship on my behalf. I thank the program and the Ontario Trillium Foundation for their generosity. I am also grateful for the dissertation funding provided by the Center on Public

an attentive friend and an inspiring scholar who could have written another dissertation of his own in the time we spent discussing mine. I am especially grateful to Britt Tevis for her incisive critique and loving encouragement in working on this dissertation and beyond.

This monograph would not have seen light without the emotional and material support of my family who made sure I was able focus on the studies first and foremost throughout these years. A heartfelt thank you to grandma Maya, Mama, Papa, my brother Zhenya, my sister-in-law Yulia, and my niece Alexandra, who was not yet born when this project began but who has been a source of indescribable joy for all of us ever since – СПАСИБО! I dedicate this dissertation to them.

Table of Contents

List of Tables

List of Figures

Introduction

Over the course of the past two decades, particularly since the late 2000s, a fast growing number of states have reimagined the role of digital technologies vis-à-vis their national Selves as indispensable to their nation's existential success, or even survival. Governments frame their official embrace of digital technologies as the sole conceivable response to the pressures of what they view as an increasingly globalized and competitive world. While this trend can be observed across dozens of countries, national identity narratives rooted in local cultural repertoires underlie the logic and language of individual national digital identities and account for cross-country differences among them. This shift in the national state's vision for digital technologies, attendant state-led discursive and material efforts at constructing national digital identities, and the strategic communication of both to global audiences is the crux of what this dissertation refers to as *digital nationalism*.

This dissertation is centrally concerned with the relationship between identity narratives and state digital rhetoric and policy. It asks: *Why and how does national identity relate to digital communication technologies and by extension the workings of digital globalization?* I explore this question by examining identity narratives and digital policies of Russia and Estonia, champions of the internet sovereignty and internet freedom narratives respectively, in the ongoing normative debate about the future configuration of the global internet.[1]

---

[1] I use lowercase "internet" to refer to the global digital network in its contemporary usage and understanding and uppercase "Internet" (found mostly in the respective section on the history of this technology) to refer to the original project under the auspices of the U.S. Department of Defense before the mid-1980s, when what would eventually become the mass medium of today was but one of many small-scale experimental projects in computer networking. The language pertaining to the internet, as this

While rulers have always sought to harness communication technologies to bolster their powers domestically and internationally, the concept of digital nationalism invokes more than power politics by digital means. Rather, the notion of digital nationalism illuminates a co-constitutive cultural process. At one level of this process, national self-identification contributes to shaping the logic and language of the state's digital discourse and policy, while at another, the bureaucratic state comes to envision digital technologies as critical to the cultural nation's interests and values that the state professes to represent.

A passage from the introduction to France's inaugural International Digital Strategy, issued in 2017 by the country's Ministry of Foreign Affairs, conveys some of the logics that underlie digital nationalism as a national project:

> Digital technology is now a key issue for France's foreign policy and public action as a whole, be it for the success of France's economy in the global competitive sphere or for conditions of stability, security and power on a global scale. … [I]t is time for France to define the principles for digital technology that it wishes to see succeed around the world. To achieve this, France must promote a model which is faithful to its values. (French Ministry of Foreign Affairs, 2017)

Three logics of state digital nationalism can be distinguished. First, digital nationalism is part and parcel of globalization. Digital nationalism emerged out of governments' growing anxiety that in the context of global competition they ought to develop national competitive identities in order to secure the benefits of globalization. As both an icon and an enabler of globalization, digital technologies and their integration into national life has come to be perceived by political and business elites worldwide as expressive of a country's readiness for the global age. Second, the state considers that

---

dissertation shows, is itself a highly political matter. For an interesting discussion of politics surrounding the spelling of the internet/Internet, and an argument *for* treating the internet as a proper noun, see Bay (2017).

digital technologies necessarily need to reflect and advance national values. These values, in turn, form the basis for the state's understanding of what its economic and security interests are, including in the digital realm. Third, each country's digital nationalism seeks to strategically promote in the global political and informational arena its own digital identity and its normative vision of the global digital order.

Illustrative of the increasing rhetorical and institutional entwinement of digital technologies and nationalisms, since the late 2000s, France has established the French Digital Council, a government-affiliated advisory body; appointed a Secretary of State for Digital Affairs; introduced a Digital Diplomacy section of the Ministry of Foreign Affairs, which suggests that "[d]igital technology offers many opportunities to promote the 'French brand' against a background of increasingly stronger power plays" (French MFA, 2018);[2] helped launch La French Tech, a global network of French startups boasting a tagline "Disruptive since 1789: Join the New French Revolution" (La French Tech, n.d.); and adopted the Digital Republic bill, a multipronged program of the country's digital development, which states that "[t]wenty-first century France must embrace digital technology, prepare for future developments, take up all the opportunities and shape a society that embodies the principles of liberty, equality and fraternity" (French Government, 2016).

Identity narratives that underlie the state's digital rhetoric and policy, in line with Clifford Geertz's understanding of the role of culture, should be viewed not as a power, "to which social events, behaviors, institutions, or processes can be causally attributed," but a context "within which they can be intelligibly—that is, thickly—described"

---

[2] Here and in the rest of the document, I shorten "Ministry of Foreign Affairs" to "MFA" within in-text references. In bibliographic references at the end of this document, respective bodies appear under their full titles, e.g., French Ministry of Foreign Affairs.

(Geertz, 1973, p.14). This relationship has been referred to as "constitutive causality," which "seeks to explain events in terms of actors' understandings of their own contexts, rather than in terms of a more mechanistic causality" (Schwartz-Shea & Yanow, 2012, p. 52). This core proposition of the dissertation is a complement to, rather than a replacement for, existing approaches to the study of digital technologies. It is intended as an alternative analytical approach, not in the sense of being "mutually exclusive" with other approaches, but of being "available as another possibility" (Oxford Dictionaries, n.d.).

From Identity Narrative to Digital Policy

The national state's ambition to reimagine the nation for the digital age is a testament to nationalism's enduring relevance "as the fundamental organizing principle of the interstate order, as the ultimate source of political legitimacy, as the taken-for-granted context of everyday life and as a readily available cognitive and discursive frame to make sense of the world that surround us" (Ozkirimli, 2017, p. 5). Diverse accounts of nationalism have emphasized varying historical circumstances and socio-political factors as critical to its origins and ensuing development (see Hearn, 2006; Hutchinson & Smith, 1995; Ozkirimli, 2017). This dissertation understands nationalism historically as a modern socio-political principle emanating from late eighteenth-century Europe, which posits the nation to be the natural and preeminent form of collective self-organization and argues that borders of the cultural nation and the state must be congruent (Breuilly 1994; Gellner, 2009; Hobsbawm, 2012).

After Benedict Anderson's canonical definition, I treat the nation as an *imagined*

political community.[3] The nation is imagined because each of its members will never meet all of her fellow co-nationals, but she goes through life imagining a national body that occupies a certain physical space and moves in unison through time. The national imagination, according to Anderson, considers the nation as (a) *limited* in a sense that, no matter how elastic its imagined boundaries, the national community does not think itself congruent with the entire mankind, but imagines there to be a symbolic border beyond which another national community lays; (b) *sovereign* in a sense of being imagined as independent from the divine force, other national communities, and any outside influences to chart collectively its own existential path, and where the national state serves as the ultimate manifestation of sovereignty, and (c) *communal* in the sense that no matter the real structural inequalities within the community, its members imagine relations among themselves to be inherently egalitarian and horizontal.

National imagination depends on the persistence of the rhetoric of nationhood, the ways of talking about the nation, and of articulating human action in national terms (Benhabib, 2002, pp. 5-8; Billig, 1995, p. 8; Calhoun, 1997, p. 5; Hall, 1996, pp. 4-5; Wodak et al., 2009, p. 22). Characteristics of each collective national identity present a particular constellation of cultural repertoires—socially constructed, preexisting, and readily available constitutive components of culture, such as symbols, stories, rituals, and world-views—from which people draw selectively to construct their strategies of action (Corse, 1996, pp. 156-161; Lamont & Thevenot, 2000, pp. 8-10; Swidler, 1986, p. 273). Understanding national identity as a constellation of cultural repertoires mandated and institutionalized by the state "allows us to consider both the systematic variations in

---

[3] Anderson's conceptualization in part draws upon Seton-Watson's suggestion that "a nation exists when a significant number of people in a community consider themselves to form a nation, or behave as if they formed one" (Seton-Watson, 1977, p. 5 cited in Anderson, 2006, p. 6).

national culture and the complexity of the link between culture, nation, and individual action" (Corse, 1996, p. 161). In other words, individual action does not follow a script predetermined by national identity but is restricted, to a degree, by local cultural norms that favor certain words and behaviors while deeming others impossible or improper.

The state's continuous codification of select cultural repertoires into an official national identity through various systems of symbolic propagation, such as education, literature, and media, makes particular cultural repertoires widely taken-for-granted. This, in turn, renders certain individual and collective human action more imaginable and, as a result, materially possible than others within a given national context. The constant flux and malleability of the precise repertoires that constitute the national identity at any given moment in history is well-captured with Rogers Brubaker's suggestion that we treat national identity not as a fixed category but a process of self-identification based on one's self-understanding and manifested in outwardly self-representation (Brubaker, 2004, pp. 41-48).

In line with the culture-oriented analytical framework of this dissertation, I approach the state as a cultural formation (see Steinmetz, 1999). This approach does not negate the more traditional understanding of the state as a compendium of actors, institutions, material resources, and internal power dynamics. This lens, rather, means *analytically* viewing culture, and specifically national identity, as forming the broader context for and underlying the logics of state rhetoric, policy, institutional arrangements and dynamics, relations with internal non-state actors and external significant others—as opposed to treating culture in a narrower sense of one of many governmental concerns, alongside education, healthcare, defense, and other traditional realms of state

policymaking. Specifically, the two interrelated assumptions of this approach that I borrow are first, that "[t]he state still has crucial advantages over other actors in the effort to construct hegemonic identities and to unify the centripetal identifications within any given territory along nationalist lines," and second, that "states are not 'autonomous' from extrastate cultural forces, but are shot through with circuits of meaning that cut across the state-society frontier" (Steinmetz, 1999, pp. 11-12). Clifford Geertz thus writes that "[o]ne of the things that everyone knows but no one can quite think how to demonstrate is that a country's politics reflect the design of its culture" (Geertz, 1973, p. 311). This dissertation is one such attempt to illuminate how underlying cultural meanings inform the workings of state policy by examining the state's rhetoric and policy in the realm of global internet governance.

When a polity envisions its digital philosophy, it reaches for the logic and language found in the most prominent national cultural repertoires in order to imagine, talk about, and justify its digital agenda to its citizens and the world. As outlined in the French bill of the Digital Republic, "As Internet access for all epitomizes the Republican notions of solidarity and the inclusion of citizens, it will be one of the mainstays of the Digital Republic bill" (French Government, 2016). Russia's advocacy of digital sovereignty is meant to bolster the country's resurgent great power self-identification (see Ch. 3-4), while Estonia's e-Estonia national digital vision views digital technologies as means to escape the Soviet legacy and join the West (see Ch. 5). It is in this sense of allowing to think, talk, and act with regards to digital technologies in certain ways as opposed to others, rather than in a sense of mechanistic causality, that national identity structures digital discourse and policy.

Methodological Nationalism

The focus on the national poses a potential theoretical-methodological research trap:

> Much of social science has proceeded on the explicit or implicit assumption of the nation-state as container and as representing a unified spatio-temporal unit. Most of history has not corresponded to these putative conditions; and even the modern nation-state failed to instantiate them fully. (Sassen, 2006, pp. 397-398)

This unreflexive research assumption about the nation-state as the natural socio-political unit of the modern world has been critiqued as *methodological nationalism* (Chernilo, 2011; Wimmer & Schiller, 2002). Ulrich Beck is one of the most vocal critics of what he terms the "zombie science of the national": "Just as nation-based economics has come to a dead end, so too has nation-based sociology" (Beck, 2006, p. 23). Beck attributes to methodological nationalism "the insistence that the meta-game of global politics is and always will be a national game," and a view that "the nation-state, as the source of legitimacy for supranational norms and organizations, is constant and absolute" (Ibid, pp. 5-41).

Milton Mueller (2017, Ch. 6, n.p.) applies the critique of methodological nationalism to those researchers of internet and its governance who

> assume that the nation-state must be the primary agent for local control. They uncritically assume that territorial governments are the most appropriate units, if not the only units, to make decisions about information policy, and that they must make the same decisions for everyone in their territory and embed them directly in the operation of the network itself.

Critics of methodological nationalism are correct to point out that much scholarship in the social sciences approaches research with the *assumption* of the nation-state's naturalness, primacy, and timelessness. In contrast with such assumptions, critical

theories of nationalism, which form the theoretical foundation of this project, bring to digital nationalism reflexive awareness of the socially constructed nature of the national identity and polity as a product of a particular juncture in world history, not a force outside of history and politics. The project *self-consciously* takes the national as its *object of investigation* to think about the peculiar ability of nationalism to adjust to various historic circumstances and pressures, such as digital globalization. Digital nationalism as an analytical lens is not a prescriptive concept, in that it does not offer to privilege the national over the global in policymaking or any other social arena.

While methodological nationalism as an unreflexive practice is to be avoided, some scholars have noted the resilience of national-level politics in the context of global media policy to suggest that "the national level remains a hegemonic site for the organization of politics" (Carpentier, 2011, p. 122) and, in particular, recognized the national level's importance to analyzing digital globalization:

> The epochal transformation we call globalization is taking place inside the national to a far larger extent than is usually recognized. It is here that the most complex meanings of the global are being constituted, and the national is also often one of the key enablers and enactors of the emergent global scale. (Sassen, 2006, p. 1)

Sassen is not talking about the relative significance of the national vis-à-vis the global in the contemporary world, but rather suggests that *both* are crucial to the analysis if we are to comprehend the dynamics of globalization. Her notion of analytic borderland, which I consider in the next section, is helpful in bridging the national-global nexus.

Digital Nationalism as an Analytic Borderland:

Between the National and the Digital/Global

In conceptualizing the interplay between the national and the global spatio-temporal orders and organizational logics in the context of digital nationalism, I employ Saskia Sassen's notion of an *analytic borderland*, "a heuristic device that allows one to take what is commonly represented as a line separating two differences, typically seen as mutually exclusive, into a conceptual field—a third entity—that requires its own empirical specification and theorization" (Sassen, 2006, pp. 379-386). This national-global dynamic "is not simply a zero sum where either the national loses at the hands of the global or vice versa," but a mixed order where each force at once reconstitutes the other and is reconstituted by it (Ibid.). An analytic borderland approach helps to view in-between social phenomena as malleable "frontier zones" rather than a binary or a spectrum between two distinct poles. Examples of such frontier zones that exist at once in the national and global dimensions include global networks of financial centers that are based in specific locations (such as London's City and New York's Wall Street) but deal with cross-border financial flows, and global networks of localized environmental activists, who often address local issues but share globally expertise and resources with each other toward a common goal of global environmental well-being.

Sassen offers foundational principles for researching analytical borderlands. At its broadest, "[t]he theoretical and methodological task entails detecting the social thickness and specificity of these various dimensions and intersections so as to produce a rich and textured understanding" (Ibid.). Drawing on William Sewell's notion of "thickening the social," Sassen argues for "a thickening of the global that … [would] bring social thickness to our analysis of globalization" (Ibid.). The three specific elements of this research agenda include (a) examining the actual practices (material, organizational,

discursive) involved in making the shift in the preexisting orders, (b) empirical specificity in detecting concrete interactions where actors or entities from two putatively different orders intersect, and, (c) scrutiny of analytic borderlands not as anomalous or accidental formations but a product of specific, complex, and consequential deliberate action that captures the making of a structural shift.

Digital nationalism is an example of a third entity, or a frontier zone, that exists at the intersection of national identity and digital globalization, and to which the lens of an analytic borderland can be productively applied. At one end, national digital visions and projects are a function of centrifugal globalizing forces as "[w]orldwide models define and legitimate agendas for local action, shaping the structures and policies of nation-states and other national and local actors in virtually all of the domains of rationalized social life" (Meyer et al., 1997, p. 145). States thus constitute what Alasuutari has termed "the global tribe of moderns," in that they mimic and synchronize each other's policies (Alasuutari, 2015).

Discursive and policy frameworks for information and communication technologies spread across the world from the leading global organizations and powerful framework-setting states. For example, the United Nations Educational, Scientific, and Cultural Organization (UNESCO) issued in 2009 *National Information Society Policy: A Template* (UNESCO, 2009) and in 2016 an updated version *Knowledge Societies Policy Handbook* (UNESCO & UN University, 2016). These detailed manuals for the development of national ICT institutional and policy frameworks target countries that do not possess necessary resources to develop their own, with the ultimate goal to universalize global ICT development.

While digital visions on one end originate in a handful of global institutions and are, in this sense, exogenous to national states, on the other end of this recursive process, national states and societies not only variously adapt such global templates in accordance with their cultural and political-economic circumstances—if they choose to consult global templates at all—but also shape these very global frameworks. For example, governance of the global internet in the past decade and a half has acquired near universal legitimacy as a field of highest-level international diplomacy. There is widespread agreement among governments on the significance of issues pertaining to the global internet that require discussion and decision-making, from cybersecurity and protection of local languages online to child safety and e-commerce. One tangible manifestation of this trend is a quickly increasing number of dedicated national bodies and posts around the world that deal with matters of internet governance. At the same time, national governments promote divergent rhetorical and policy frameworks for the global internet, such as those of internet sovereignty and internet freedom that are at the center of this dissertation's investigation. Even when governments find themselves on the same side of the ideational camp, the logics of their support vary; in their advancement of the internet freedom narrative the rationales of the United States, Estonia, and Mongolia certainly differ among themselves. While being mindful of the inherently recursive nature of global digital politics, the focus of this dissertation is limited to investigating how the national logics adapt and contribute to shaping digital globalization.

Relying on Sassen's research principles, the goal of this dissertation is to bring social thickness to the analysis of digital nationalism by examining the discursive and material practices of the state (e.g., strategic construction and communication by the state

of its internet narrative and institutionalization of the digital vision – and how they relate

to respective national cultural repertoires), detecting concrete interactions between

national and global digital actors and entities (e.g., the relationship between national

governments and the internet's global management institutions, such as the Internet

Corporation for Assigned Names and Numbers), and capture the making of a structural

shift in the relationship between the state and digital technologies by examining the

deliberateness of state action in fostering digital nationalism (e.g., out of what political

considerations and under what sociohistorical circumstances did Estonia come to

envision itself as e-Estonia and how has this vision been upheld intact for nearly two

decades).

A state's digital agenda may encompass a diverse range of activities. Some of the

more common ones include: provision of e-services by the federal and local government

(e.g., online health records, taxing, voting), computerization and internetization of the

educational system, legislation of the national cyberspace segment, and fostering of the

startup system (e.g., opening of startup clusters, hosting of international startup events,

issuance of startup visas). The domain of digital nationalism that this dissertation

examines in detail is global internet governance.

Global Internet Governance as Digital Nationalism

The definition of internet governance has been subject to much scholarly debate.[4]

The difficulty of narrowing the definition of internet governance lays in part in the

astonishing diversity of issues this arena encompasses at is broadest: from e-commerce

---

[4] For discussions focused on the definitions of the internet and internet governance, see Abbate, 2017; Drake, 2004; Haigh, Russell, & Dutton, 2015; Hofmann, Katzenbach, & Gollatz, 2016; Mathiason, 2009, Ch. 1; Miao & Ang, 2016; van Eeten & Mueller, 2013; Wilson, 2005; Ziewitz & Pentzold, 2014.

and cybersecurity to protection of children online and censorship.[5] Laura DeNardis provides a useful starting understanding of global internet governance as a network of state and non-state actors, bodies, issues, and processes concerned with the "design and administration of the technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies" (DeNardis, 2014, p. 6). Milton Mueller in one instance stresses a particular dimension of global internet governance as "the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies" (Mueller, 2010, p. 9), which is also the focus of this study.

Nazli Choucri notes that since around the mid-2000s, as major economic, social, and political issues became inextricably bound to the workings of online technologies, from obscure technical bodies and forums "issues connected to cyberspace and its uses have vaulted into the highest realm of high politics" (Choucri, 2012, p. 3). In a similar vein, Laura DeNardis points out how conflicts over internet governance have become "the new spaces where political and economic power is unfolding in the twenty-first century" (DeNardis, 2014, p. 1). Monroe Price aptly describes global internet governance as "a quasi-Olympic sport" (Price, 2015, p. 130), emphasizing the intensity of the global competition among states over the internet's management. Adopting cyberstrategies and addressing issues of internet governance at high-profile international gatherings became a new marker of modernity for nation-states. Why and how internet governance came to be the expression of digital nationalism is the overarching story I tell in this dissertation.

---

[5] For categorizations of internet governance issues, see DeNardis & Musiani, 2016; Kurbalija, 2016; Mueller, 2007.

Global internet governance is an analytic borderland that features the three characteristics that underlie digital nationalism as I operationalize it. First, global internet governance is part and parcel of digital globalization, as its mandate encompasses legal and technological architectures of the global internet. Second, national cultural repertoires shape how states imagine and articulate their internet governance agendas. Third, states strategically communicate their normative visions of global internet governance to domestic and international audiences—through political rhetoric, organization of relevant diplomatic events, dissemination of circumvention or blocking software, endorsement of publications, funding of digital rights organizations, and other ways—in the name of the nation's best interests and bolstering of national identity.

Accordingly, in this dissertation, I operationalize global internet governance as:

A geopolitical debate in which states draw upon national values and interests to strategically communicate normative visions of technological and administrative internet configurations.

The dissertation examines digital nationalism in Russia and Estonia by investigating the relationship between respective identity, strategic communication, and internet governance in each case.

Case Studies: Russia and Estonia

In examining how identity narratives infuse national digital identities and global digital governance, I employ a case study approach. Gerring defines a case study method as

an intensive study of a single case (or a small set of cases) with an aim to generalize across a larger set of cases of the same general type. If the inference

pertains to nation-states, then a case study would focus on one or several nation-states. (Gerring, 2006, p. 65)

The two nation-state cases that I focus on are Russia and Estonia, where Russia serves as the primary case and Estonia as a secondary illustrative case for limited comparison. The cases illustrate empirically the theoretical proposition of the dissertation about the co-constitutive relationship between national identity narratives and the state's digital discourse and policy.

Russia has employed global digital technologies to assert its resurgent great power identity. After a brief period of officially embracing Western liberalism in the early- to mid-1990s, Russia has been increasingly opposed to the West and has relied on traditional conservative cultural repertoires. Under Vladimir Putin, Russia has advanced the notion of sovereignty, including in cyberspace, as the overarching focus of its discourse and ideology, in opposition to the normative liberal rhetoric of open offline and online borders. Russia's internet governance discourse uses the language of territorialized sovereignty, which bounds a cultural and national space that tolerates no foreign interference.

After the ethnic Estonian majority shrank from 90 to 60 percent of the population during successive Nazi and Soviet rule in 1940-1991, the re-independent Estonian state in 1991 set as its main priority the preservation of Estonian ethno-cultural identity and language. Estonia has viewed institutional and symbolic turning to the West as key to its economic prosperity and security. Estonia's strategy of digital innovations and support for internet freedom, known as e-Estonia, was meant to serve as tangible evidence of its readiness for joining the Euro-Atlantic community and belonging in the Western high-tech modernity. While the discourse surrounding e-Estonia is couched in the language of

post-national Western liberal globalism, its logics and goals are rooted in Estonian nationalism.

The key difference here between the primary Russian case and the secondary Estonian case lays in the number and extent of primary and secondary sources consulted for the purposes of this comparison. While the number of such sources in the Russian context is greater than of those in the Estonian context, the volume and depth of engagement with the Estonian sources allows for the claims made in this dissertation. The main methodological limitation in accessing the Estonian socio-cultural context is that I do not possess knowledge of the Estonian language and my lived experience with the Estonian context is limited to a research trip in June 2017; thus, no scholarship and primary sources in the Estonian language were consulted. Comparatively, I speak Russian natively and have lived most of my life in Russia, and was therefore readily able to consult primary documentation from Russia.

Several reasons, however, allow me to productively include the Estonian case for limited comparison in this dissertation. First and foremost, I conceptualize the Estonian case not as fully comparative, but illustrative. It is meant to illustrate the workings of digital nationalism in a setting where the strategic narrative differs from Russia's, but the identity-based logic and language are also present and can be shown. Second, I have experience in researching the Estonian context beyond this project. In 2012, I defended a Master's thesis on Estonia's strategic communication and majority-minority relations, have since published Estonia-related research, and presented it at several academic conferences. This research has received awards for best conference papers and funding from academic institutions. Third, the Estonian state provides English translations of key

strategies, speeches, news, and others sources of political discourse under analysis. Thus there was no issue in accessing and assessing Estonia's strategic narrative of the Self and its significant Others and of global internet governance. Lastly, my specific focus in this dissertation is on how the state externally communicates its national identity in the context of internet governance. In other words, I make no claims about the nuances of Estonia's internal political and identity developments *per se*, but rather about how its official identity narratives—which can be traced with scholarship and primary sources available in English—relate to the Estonian national digital vision.

There are several reasons why Russia and Estonia were chosen as cases, which pertain to the three key pillars of this project: identity, strategic communication, and global internet governance.

Pillar I: Identity

In Russia and Estonia, the adoption of digital technologies by the society and the state has taken place contemporaneously with intensive nation- and state-building following the dissolution of the Soviet Union in 1991.[6] The historical accident, in which formerly socialist republics of Central and Eastern Europe attained independence from Moscow's direct and indirect control coincided with the beginning of the internet's rapid globalization, makes this part of the world particularly interesting and illustrative of how identity and digital technologies interact.

In addition to Russia and Estonia serving as pertinent illustrative cases *individually*, their nearly three centuries-long *relationship*, during most of which the

---

[6] For example, Members of the Kurchatov research institute outside of Moscow established Soviet Russia's first international internet connection with Finland—via a node in Estonia—and registered the Soviet Union's domain *.su* in 1990, while *.ru* was registered in Russia in 1994. Estonia connected to the global internet in 1992 also through academic institutions and registered its country-code domain *.ee* the same year.

territories of contemporary Estonia were subjugated to the Russian rule, makes them a particularly apt pair for this study. The territory of contemporary Estonia was conquered by the Russia Empire in the early eighteenth century during the Great Northern War. Estonian cultural and then political nationalism arose since the 1850s, in part in response to the Russian imperial rule. After the collapse of the Russian Empire in 1917, Estonia attained independence for two decades in the interwar period before it was forcefully occupied by the Soviet Union in 1940, and remained so until 1991. The Soviet rule at various points was characterized by mass deportations and executions of ethnic Estonians, state-led cultural-linguistic Russification and political Sovietization, and the resettlement into Soviet Estonia of hundreds of thousands of Russian-speakers. All of this fundamentally changed Estonia's ethnic composition: from 90 percent ethnic Estonians in the late 1930s to 60 percent Estonians and 30 percent Russians at the time of the Soviet Union's dissolution. Owing to this complicated legacy of their intertwined histories, post-Soviet relations between Estonia and other Baltic states of Latvia and Lithuania, on the one hand, and Russia, on the other hand, have been "remarkably poor" (Ehin & Berg, 2009, p. 1).

The Estonia-Russia national identity dynamic has directly affected the digital relations between the two countries. Most famously, the 2007 cyberattacks on Estonia's critical infrastructure are widely perceived to have been sanctioned by the Kremlin in retaliation for the removal of the commemorative Soviet World War II monument from downtown Tallinn, which Russian state media and officials framed at the time as an assault on Russia's history.

Pillar II: Strategic Communication

The second domain underlying this dissertation, in which Russia and Estonia have been prominent actors, is that of global strategic communication. Since the early 2000s, the countries' governments have engaged in concerted and ever-expanding institutionalized efforts to narrate their interests and values to foreign audiences. The national strategic communication has pursued tangible (e.g., membership in regional and global organizations, foreign direct investments, tourists, students) and intangible gains (e.g., respect for Russia's self-identification as a great power from the world's major powers and recognition of Estonia's self-identification as an inherently Western nation and state by the Euro-Atlantic community of states).

Russia first officially proclaimed its intention to engage with mediated public diplomacy as a matter of state policy in 2000 and has since grown a sizeable strategic communication apparatus. For example, Russia's international television broadcaster RT boasts channels in Arabic, English, French, and Spanish, while the radio and online publication Sputnik News has editions in dozens of languages.

Much of Estonia's strategic communication has been coordinated by Enterprise Estonia, a government-affiliated institution founded in 2000 whose self-professed "long-term goal is to help Estonia become one of the most competitive countries in the world" (Enterprise Estonia, n.d.-d). Enterprise Estonia's program of Brand Estonia has been communicating Estonia's identity narrative to global audiences through multiple media platforms and channels. One of Brand Estonia's core pillars is that of *e-Estonia: The Digital Society*, which promotes the narrative of "Estonia's emergence as one of the most advanced e-societies in the world – an incredible success story that grew out of a partnership between a forward-thinking government, a pro-active ICT sector and a

switched-on, tech-savvy population" (Estonian MFA, 2016). This strategic narrative, as the quote above from the website of Estonia's Ministry of Foreign Affairs illustrates, permeates not only strictly branding and promotional materials, but has long become a staple of Estonia's political and identity narrative of the highest level.

Pillar III: Global Internet Governance

Estonia and Russia are among the leading voices in the global internet governance debate. Estonia is an advocate of the internet freedom agenda, while Russia, alongside China, is the leader of the internet sovereignty agenda. Both countries' representatives are actively involved in the most important venues and processes of global internet governance. Estonia, for example, is a founding member of the Freedom Online Coalition, the preeminent intergovernmental body of internet freedom supporters; is host to the Tallinn-based NATO Cooperative Cyber Centre of Excellence, which publishes an authoritative *Tallinn Manual* on international cyber law and annually hosts high-profile CyCon conferences; and to the e-Governance Academy, a research hub of digital expertise with wide-ranging training programs across the Eurasian region. Since the late 1990s, Russia has been advancing the narrative of the global internet based upon the trope of sovereignty, and since the late 2000s has played a key role in building a coalition of internet sovereignty supporters through organizations like the Shanghai Cooperation Organization (SCO) and BRICS (a coalition of Brazil, Russia, India, China, and South Africa).

While there are many structural similarities between Estonia and Russia that make them a particularly suitable pair for analytical juxtaposition, this cross-country analysis is conducted in the spirit of "contextualism," which "aims to understand the meaning of an

idea or practice in its context and uses comparison to examine the mechanisms or principles that unify or differentiate cases" (Powers & Vera-Zambrano, 2018, pp. 2-5). Contextualism is thus antithetical to "universalism," which "examines similarities and differences in journalism and political communication by analyzing variables (e.g., professionalism, commercialism) that are assumed to have similar (i.e., universal) meanings across the cases analyzed." The analysis of Estonia's and Russia's digital nationalisms should then be carried out with due attention to the particularities of their respective national media, social, and political systems – without universalist presumptions.

Methodology

The dissertation's theoretical underpinnings are rooted in social constructivist ontology, which deems "human 'knowledge' [to be] developed, transmitted and maintained in social situations" (Berger & Luckman 1966, p. 15). From the social constructivist perspective, identity—the central analytical category of the project—is "a key element of subjective reality and, like all subjective reality, stands in a dialectical relationship with society. Identity is formed by social processes. Once crystallized, it is maintained, modified, or even reshaped by social relations" (Ibid., p. 194). As the primary concern of the sociology of knowledge is with understanding the social construction of reality, the methodological task of this project is to excavate and examine Russian and Estonian state identities and illuminate how their underlying cultural repertoires shape the logics of respective official digital narratives and policies, in particular those relating to internet governance.

The methodological design of this project draws on classic and contemporary accounts of the interpretivist tradition (Geertz, 1973; Hopf, 2002; Rabinow & Sullivan, 1988; Shwartz-Shea & Yanow, 2012). The purpose of cultural interpretive analysis is the search for meaning, as opposed to a strict law and/or hard causality, its data is "our own constructions of other people's constructions of what they and their compatriots are up to," and its method is analyzing the "flow of social discourse" among local actors and "guessing at meanings, assessing the guesses, and drawing explanatory conclusions from the better guesses, not discovering the Continent of Meaning" (Geertz, 1973, pp. 5-21). In addition to attentive observation of the "subject's intentions or preferences or interests," Ted Hopf suggests, there "must always be an accompanying account of the relevant sociohistorical context. Evidence does not consist of the actor's words alone" (Hopf, 2007, p. 62).

In excavating national identity narratives, I share Charlotte Epstein's approach to state discourse: "A state is what it says it is and how it performs itself in its relations with other states" as a reflection of the "inherently fluid and performative nature of state identities" (Epstein, 2008, p. 254). I do not seek to discover and expose the actor's supposedly true identity and motivations in their self-serving calculated rhetoric. All outwardly self-presentation of one's internal self-understanding is performative. There is no essential identity to be discovered behind the public façade: whatever the actor chooses to communicate publicly about themselves is what they deem as best representing their nature and advancing their interests, while also illuminating their perceived limits of the doable and sayable.

This, of course, does not mean uncritically accepting state rhetoric. Rather, this

means interrogating state rhetoric not for the supposedly hidden objective and observable

truth obscured by ephemeral words so as to measure and expose the gap between reality

and rhetoric, but interrogating state rhetoric for its underlying logics and language. For

example, an assertion of Estonia's official self-promotion that "[i]t is not accidental that

Estonians are eager Internet surfers and keen mobile phone users" (Allsalu, 2005) should

be measured against the statistics of internet and mobile use in Estonia. This is, however,

only the first, albeit necessary and informative, step. The more fundamental analytical

task lays in understanding and explaining *why* Estonia's strategic communication deems

it crucial to project an image of the Estonian nationals as avid tech-users. To do this, in

line with Hopf's abovementioned imperative that evidence must include the actors'

words *and* respective sociocultural contexts, I go beyond verification of official claims

and situate them within the sociocultural circumstances of the given national context as

well as within the broader global developments.

Research Method

Drawing on social constructivism and interpretive cultural analysis, the method of

this project consists of three consecutive steps: excavation of the national Self's

identification from official discourse, excavation of the national Self's vision of the

internet and its governance, and intertextual analytical juxtaposition of the two narratives

in order to establish the relationship between the Self's identification and internet

governance.

National self-identification here is understood "as intersubjective beliefs about the

national self in relation to others, conceptualize[d] as embedded in a society's shared

stock of knowledge, operationalize[d] as a set of texts" (Allan, 2016, p. 21). The texts I

focus on primarily relate to policy discourse and encompasses both state law and policy documents *per se*, as well as articulations of the state's normative visions of the Self and ensuing political strategies found in, for example, official media commentary, press-releases, addresses, state media content, official social media accounts, and promotional materials. This is because, as Stephanie Schulte's study of cultural constructions and representations of the internet demonstrates, policy documents and debates render visible "rhetorical and political shifts in national priorities" and, particularly relevant for this study, "the nationalist characteristics of visions of the internet" (Schulte, 2013, pp. 11-15).

In operationalizing the diverse set of texts to excavate and illuminate national priorities and visions of the internet, I view all types of documents as articulations of the society's shared stock of cultural repertoires. This does not mean that I attribute equal political weight to, for example, a national strategic doctrine and a tweet from a ministerial account. It is well understood that a national strategy is a product of years-long coordination among multiple actors within the state, approved by the country's highest-level leadership, and guides a country's policy in a certain area over the course of several years; a tweet could be posted by an intern in charge of social media management. What I mean by analytically treating all texts as equal is that I do not view them as arranged in a normative hierarchy of reliability and trustworthiness. That is to say, while certainly applying an understanding of the peculiarities of each text's format, I do not perceive, for instance, a law or a policy document as supposedly hard evidence that should be taken for granted as compared to the supposedly weak evidentiary value of

political speech due to the fact that there is potentially more room for rhetorical manipulation.

This is because, to reiterate, the interpretive orientation that this dissertation subscribes to does not search for an objective rational essence of the nation's identity and its internet policy, but instead looks for the nation's own understandings as expressed in *all* kinds of texts, from strategic doctrines to tweets. Additionally, I do not analyze various kinds of evidence in isolation but do so systematically: e.g., I include in the corpus of data not one brochure of Estonia's *e-Estonia* promotional campaign, but dozens of nation branding items that allow to make claims about Estonia's strategic national narrative. This approach is borne out by the results of the study: in both Estonian and Russian cases, I found *stylistic* differences in *how* the national narrative is expressed (e.g., media appearances allowed for sarcasm and humor as compared to official policy documents) but the content remains fundamentally consistent across various types of texts.

Step I: Contextualization of the National Self

The first step excavates Estonian and Russian official identity discourse to illuminate *who the (hegemonic) national Self and the Other is.* Secondary literature on Russian and Estonian histories, societies, and politics informs my understanding of their socio-historical contexts, while thick narrative analysis of primary texts by Estonian and Russian elites reveal what national cultural repertoires underlie official identity discourse.

Primary sources include, for example, major annual national addresses by the country's leadership (e.g., Anniversary of the Restoration of Estonian Independence; Russian Presidential Address to the Federal Assembly), leadership speeches at major

international political fora (e.g., Munich Security Conference, UN General Assembly), national doctrines and strategies (e.g., foreign policy concepts, national security strategies), and state strategic communication (e.g., Estonia's Brand Estonia initiatives, ERR news agency; Russia's RT, Sputnik News). In order to immerse myself into the cultural, political, and media environments of my case study countries, I spent September 2016-July 2017 living in and visiting Russia and Estonia.

An important caveat is in order. The focus of this dissertation is limited to the hegemonic national Self—a prevailing official self-identification as expressed by individuals and institutions speaking on behalf of the state—as the most directly impactful in terms of state policymaking. At the same time, this analysis is carried out with full understanding of and attention to the multifaceted nature of any national identity discourse and the internal power struggles among groups representing these differing identity visions and narratives. While I do not myself detail these internal dynamics, scholarly and expert sources on Estonia's and Russia's domestic socio-political life inform my writing. I address internal struggles to the extent that they explicitly pertain to my argument: for example, how the tension between the ethnic Estonian majority and Russian-speaking minority has bolstered Estonia's official Western-oriented identity, including its support for the internet freedom agenda, and, to take another example, how the anti-regime oppositional movement in Russia in 2011-12 turned the official state identity narrative increasingly anti-Western, including its reinforced support for internet sovereignty.

Acknowledging the internally diverse, conflictual, and contradictory nature of any national identity and socio-political life allows to mitigate at least partially the danger of an analytical pitfall that Rogers Brubaker terms "groupism":

> [T]he tendency to take discrete, bounded groups as basic constituents of social life, chief protagonists of social conflicts, and fundamental units of social analysis. … [T]he tendency to reify such groups … as if they were internally homogeneous, externally bounded groups, even unitary collective actors with common purposes. … [T]he tendency to represent the social and cultural world as a multichrome mosaic of monochrome ethnic, racial, or cultural blocs. (Brubaker, 2004, p. 8)

Step II: Contextualization of the National Internet Governance

The second step analyzes Estonia's and Russia's engagement with the internet at the domestic and international levels to illuminate *what the Self's normative understanding of the internet and its governance is.* The primary method is thick narrative analysis of political statements, policy documents, and media commentary by Estonian and Russian officials pertaining specifically to their discursive construction of the internet and its governance. This step illuminates how major themes are constructed to create the overarching discourse, and which symbolic resources are drawn upon to make arguments.

Primary sources include, for example, speeches and statements by country representatives at international internet policy events (e.g., ICANN conferences, Internet Governance Forum, NATO International Conference on Cyber Conflict), national and collective digital development doctrines and strategies (e.g., Digital Estonia 2020, OECD Principles for Internet Policy Making; Strategy of Information Society Development of Russia in 2017-2030, BRICS Communications Ministers Communique), media articles

and interviews relating to the internet by top officials, and coverage of internet governance by respective state media outlets.

In addition to textual analysis, as part of the second step that analyzes the state's engagement with internet governance, I conducted participatory observation at several high-profile international Internet and media governance events, including the United Nations Internet Governance Forum (2014), Freedom Online Coalition (2015), and European Dialogue on Internet Governance (2017). This allowed me to witness speeches by and informally converse with Estonian and Russian representatives, taking note of their themes, framing, language, tone, setting, and reception, as well as to obtain a more nuanced understanding of internet governance as a diplomatic and policymaking process.

Step III: Intertextualizaiton of the National Self and National Internet Governance

Thick contextualization of the first two steps is followed by thick intertextualization in the third step, whereby I analytically juxtapose excavated national visions and digital visions in order to address the overarching research question posed by this project: *How does national identity relate to global digital politics*?

Organization of the Dissertation

The dissertation consists of three parts. Part I, Digital Nationalism, outlines the theoretical and analytical foundations of the digital nationalism framework, and then applies it to the case of global internet governance to illustrate how identity narratives relate to internet governance. Part II, The Narrative of Internet Sovereignty, and Part III, The Narrative of Internet Freedom, illustrate the workings of digital nationalism by examining empirically the logics and language of internet governance in Russia and

Estonia, where Russia serves as the primary country case study and Estonia is a secondary illustrative case for limited comparison.

Chapter 1, *Digital Nationalism: A Framework*, elaborates the concept of digital nationalism as an analytical orientation and a social phenomenon. The chapter first situates digital nationalism within existing literature on the relationship between technologies and the internet in particular on the one hand, and the administrative state and the cultural nation on the other. The second part of the chapter elaborates digital nationalism as an analytical lens and a social phenomenon. The analytical lens of digital nationalism refers to self-conscious analytical understanding of the nation's sociocultural identity narratives as structuring the state's digital discourse and policy.

The discussion of digital nationalism as a social phenomenon applies Craig Calhoun's three-part framework of nationalism as discourse, project, and evaluation to the relationship between nationalism and digital technologies to elaborate a three-pronged understanding of digital nationalism as discourse, project, and evaluation. Digital nationalism as discourse refers to how nationalism as an all-permeating discursive framework of modernity shapes the imagination behind some material digital artifacts and practices, while these practices, in turn, reproduce the discursive framework of nationalism. Digital nationalism as project refers to concerted state efforts at engaging with digital technologies domestically and internationally in the name of the nation's self-proclaimed interest, identity, and image. Digital nationalism as evaluation refers to the global competition among national digital projects, whereby states promote their national digital identities to global audiences and attempt to shape the global digital order in their favor.

Chapter 2, *Global Internet Governance*, applies the framework of digital

nationalism to the case of global internet governance—an international process of

policymaking surrounding the legal and technological architectures of the global internet.

The chapter first discusses how global internet governance is an analytic borderland that

lays at once in both national and global spaces by depicting briefly its rise from an

experimental scientific project to geopolitical prominence. Illustrating the dissertation's

key proposition about the co-constitutive relationship between nationalism and digital

technologies, the second part of the chapter then focuses on how identity narratives

underlie the logics and languages of national internet governance visions of the global

internet.

Part II, The Narrative of Internet Sovereignty, consists of Chapters 3 and 4 that

illustrate how Russia's narrative of internet sovereignty is underlain with its national

identity narratives. Chapter 3, *Re-Making of a Great Power Identity: Russia's Identity*

and Strategic Communication from the End of the Cold War to Renewed Confrontation,

focuses on how Russia's gradually changing official identity narratives from a Western

liberal democracy, to a normal power, to a great power have shaped its domestic media

policy and external strategic communication. This discussion illuminates the several

interconnections that are foundational to my understanding of digital nationalism: those

between Russian national cultural repertoires and state identity, between domestic

identity and foreign policy, and between identity narratives and the logic and language of

external strategic communication.

Chapter 4, *A Digital Sovereign: Russia's Internet Governance at Home and*

Abroad, draws on Chapter 3 to examine Russia's digital nationalism as application of its

identity logics to its domestic and foreign policy of the internet. The chapter shows how Russia's increasingly assertive identity narrative of a self-professed global counter-hegemonic great power, and the specific cultural repertoires that underlie this narrative, form the meaningful context for understanding the logics and language of the Russian state's engagement with digital technologies. Thus, Russian sovereigntist identity narrative is shown to infuse its identity and associated rhetoric and policy of internet sovereignty.

Part III, The Narrative of Internet Freedom, consists of Chapter 5, *Re-Making of a Western Identity: Estonia's "Return to Europe" as an e-State*. The case study of Estonia's digital nationalism project branded as *e-Estonia: The Digital Society*, which includes vocal support of the internet freedom agenda, illustrates how these efforts are underlain with the identity narrative of Estonia's cultural and institutional returning to the Euro-Atlantic community after the Soviet occupation.

By analytically synthesizing Russian and Estonian efforts in identity building, strategic communication, and internet governance, the dissertation ultimately reveals why and how nationalism continues to play a critical role in the age of digital technological globalization.

PART I – DIGITAL NATIONALISM

Chapter 1: Digital Nationalism: A Framework

1.1 Introduction

This chapter elaborates the concept of digital nationalism as an analytical lens and a social phenomenon. The basis of digital nationalism as an analytical lens is to take seriously national socio-historical contexts and group identities anchored in them in the study of everyday practices and politics of digital technology. In addition to self-conscious attention to cultural specificity of each national sociocultural context under analysis, digital nationalism theorizes why and how identity narratives structure national digital rhetoric and policy and accounts for their cross-national variations.

The discussion of digital nationalism as a social phenomenon applies Craig Calhoun's three-part framework of nationalism as discourse, project, and evaluation to the relationship between nationalism and digital technologies to elaborate a three-pronged understanding of digital nationalism as discourse, project, and evaluation. Digital nationalism as discourse refers to how nationalism as an all-permeating modern discourse shapes the imagination behind some material digital artifacts and practices, while these practices, in turn, reproduce the discursive framework of nationalism. Digital nationalism as project refers to concerted state efforts at engaging with digital technologies domestically and internationally in the name of the nation's interest, identity, and image. Digital nationalism as evaluation refers to the global competition among national digital projects, whereby states advance their national digital identities and attempt to shape the global digital order in their favor.

The first section of this chapter reviews existing literature on the relationship between technology, the state, and the nation to situate the concept of digital nationalism within the longer tradition of scholarly thinking about these issues. The second part of the chapter elaborates digital nationalism as categories of analysis and practice.

1.2 From Technological Nationalism to Digital Nationalism

In conceptualizing digital nationalism, I draw on existing scholarship in the spirit articulated by Clifford Geertz:

> Studies do build on other studies, not in the sense that they take up where the others leave off, but in the sense that, better informed and better conceptualized, they plunge more deeply into the same things.
>
> …Theoretical ideas are not created wholly anew in each study; as I have said, they are adopted from other, related studies, and, refined in the process, applied to new interpretive problems. (Geertz, 1973, pp. 25-27)

Broadly understood, communication technologies have for thousands of years contributed to shaping the workings of societies, while in turn being shaped by social forces themselves. In line with the dissertation's focus on national identity and digital technologies, I limit the following overview to studies that address the relationship between technology and nationalism/globalization as central to their analysis.

Technological Nationalism and Globalism

The concepts of technological nationalism and globalism—and their shortened versions of techno-nationalism and techno-globalism—have populated scholarly and intellectual discourse since around the mid-1980s. Though not addressing digital communication technologies *per se*, and laying mostly outside of media and communication discipline, this strand of scholarship nevertheless offers some useful insights about the relationship between the technology, the polity, and the nation.

Maurice Charland critically examines the concept of *technological nationalism* in the context of Canadian government's historical efforts at nation- and state-building (Charland, 1986). For Charland, technological nationalism is the governmental rhetoric of technology as constitutive of the nation. Charland critiques technological nationalism as a top-down political project void of cultural meaning besides the pathos of technological prowess itself, which is therefore unable to genuinely reflect the national experience. In contrast with Charland, I examine precisely how cultural meanings in specific national contexts inform the state's rhetoric of digital prowess. Yet Charland offers several useful insights for the study of digital nationalism. I borrow from Charland's discussion of technological nationalism a critical distinction between the state's claims in the name of the nation and the national experience, as well as an understanding of "rhetoric [as] a constitutive component of the social application of technology, for it guides its possible applications" (Ibid, p. 198).

Robert Reich, then-Professor at Harvard and 1993-1997 U.S. Secretary of Labor, discussed the notions of *techno-nationalism* and *techno-globalism* in a defense of the latter in an opinion piece, "The Rise of Techno-Nationalism," in *The Atlantic Monthly* magazine (Reich, 1987). Reich defines techno-globalism as a view that technological development is an inherently multinational endeavor, the processes and products of which should be freely shared between nations. Techno-nationalism, then, is a protectionist sentiment that technology should be developed and consumed within respective nations. According to Reich, techno-globalism had traditionally prevailed as a norm in the American context, but toward the late 1980s, anxiety over superiority of the Japanese technologies spurred the rise of techno-nationalism of the Reagan

administration.

While Reich advances a techno-globalist industrial policy of knowledge exchange, the logic and language of the article perpetuate the discourse of nationalism through naturalizing the world as a world of nations. This seeming paradox illuminates one manifestation of digital nationalism as a discourse: even when one argues against nationalist technological policy, one's ways of thinking and speaking about the world are cognitively and linguistically entrapped, to great extent, within nationalism as a hegemonic discourse of modernity. As a result, arguments in favor of the global often end up reproducing the national framework.

The article's concluding passage, for example, employs binary categorizations of "us" and "them" to refer to nations, assigns nationality to businesses ("Japanese companies") and social classes ("American workers"), as well as puts forth the notion that a state-based nationwide policy should be implemented to the benefit of a geographically bounded national citizenry:

> *Japanese* companies like Fujitsu can help *American* workers discover how to transform research findings into practical innovations of all kinds. *Our national* policy goal should be to ensure that *they* do indeed teach *us*, and that *we* do in fact learn. (Reich, 1987, n.p.; emphasis added)

Several common traits in the literature on technological nationalism and globalism can be distinguished. First, unlike Charland's and Reich's distinctly negative connotations assigned to technological nationalism, much of academic discourse on techno-nationalism in later years employed the concept to signify in neutral terms a holistic technological state policy pursuant of national goals. Illustrative of this understanding, in examining China's post-WTO accession technology policy, University of Oregon political scientists Suttmeier and Xiangkui define techno-nationalism as "a

commitment to use political means to secure technological progress in the interests of national defense and economic advantage for Chinese industry" (Suttmeier & Xiangkui, 2004, p. 9). Shigeru Nakayama, a preeminent Japan-based scholar of Asian scientific and technological history, similarly defines technological nationalism as "the state of affairs in which technology is promoted by a nation-state and for the sake of national interest" (Nakayama, 2012, p. 11). My employment of digital nationalism as a state project is related to this understanding as it refers to the state commitment to use digital technologies in the name of advancing national interest, identity, and image.

Second, while techno-nationalism and techno-globalism have often been set up as opposites (e.g., Nakayama, 2012; Ostry & Nelson, 1995), a new concept of *neo-techno-nationalism* emerged to account for the increasing confluence of national and global logics,

> in which one sees both 'expanded state commitments' to technological development (in keeping with techno-nationalist assumptions), but also active public-private partnerships, a more welcoming openness toward foreigners in national technology programs, and greater commitment to international rule-making and policy coordination." (Suttmeier & Xiangkui, 2004, p. 17; see also Shim & Shin, 2016)

This is a crucial trait for digital nationalism as a state-based project, since it was born out of and is fostered by the logic of global competitiveness.

The third trait is that even though developed Western nations are arguably the most technologically nationalist in the sense of advancing their technological goals through political means, studies of techno-nationalism by both Western and Asian scholars focus overwhelmingly on Asian countries, most notably Japan, China, and Korea. Besides these Asian countries' objective political-economic challenge to the West

due to their technological prowess, this kind of Othering has decades-long cultural roots in the phenomenon of *techno-Orientalism*, whereby literary, cinematic, and new media representations of Asia and Asians in hyper-technological yet intellectually primitive terms express Western anxiety over Asia's potential cultural and economic dominance (Roh et al., 2015). This is an explicit example of how preexisting cultural frameworks directly shape technological analysis and policymaking.

Two studies of techno-nationalism and techno-globalism stand out as particularly relevant to my conceptualization of digital nationalism, as they address the relationship between technology and the socio-cultural contexts. Economist Sandro Montresor of the University of Bologna approaches the issue from the perspective of Science and Technology Studies with a particular focus on innovation, yet offers a taxonomy of techno-nationalism that is sensitive to the cultural dimension (Montresor, 2001). Montresor breaks the concept of techno-nationalism into two constituent parts: *techno-statism*—signifying "the technological relevance of the *state* as a formal institution and as a policy authority"—and *techno-nationality*—"the implications that the *nation*, meant as the social-cultural basis of a state, has for the actors that are involved in the innovative process" (Ibid., 2001, p. 401; original emphasis). Techno-nationality matters to technological politics, in that "history, culture and social relationships still provide elements of strong differentiation of the innovative process [among nations], [including] within a context of increasing international integration" (Ibid., p. 407). The distinction between the nation and the state and attention to historical, cultural, and social contexts in the construction of national digital visions are central to digital nationalism as an analytical approach.

The second study that explicitly addresses the national logics of technological development is by King's College historian of science and technology David Edgerton is *The Shock of the Old: Technology and Global History Since 1900* (2006). The chapter on "Nations" places the concepts of techno-nationalism and techno-globalism under critical socio-historical scrutiny that aligns closely with my treatment of digital nationalism, and offers several crucial insights applicable to my framework. For Edgerton, techno-nationalism as an analytical category refers to an uncritical assumption that the nation is a natural unit for the study of technology, while techno-nationalism as practiced by national intellectuals and policymakers means normatively linking the well-being of the nation to the reality and/or claims of its technological prowess. For instance, celebration of the inventive national citizen and claims to having invented or implemented a technology first and/or most widely—an instance of techno-nationalism Edgerton calls *invention-chauvinism*—has been central to nationalism. Techno-globalism, according to Edgerton, is the opposite extreme, which analytically takes the globe as the unit of analysis and proclaims technologies, especially communication technologies, to be inherently internationalizing forces destined to make the nation-state obsolete. Despite their fundamental normative differences, techno-nationalism and techno-globalism share *innovation-centrism* – the conviction that technological innovation and dissemination are key to their respective goals, such as national economic growth or global peace.

Edgerton illuminates the intertwined relationship between the national, the global, and the technological – the work that digital nationalism aims to do as applied to digital technologies. First, technological exchange between states blurs the national-global distinction. For example, the politically and culturally isolated Soviet Union in the 1920s-

1930s imported U.S. technologies and specialists to build entire industries *en masse*.

Second, at the non-state level, the nation-state's technological borders are made porous

through activities of individuals and multinational corporations. For example, some

production and/or research hubs serving the global market may be more logistically

integrated into global technological production chains than they are into national

economy. Third, and a rarity for scholarship on techno-nationalism and techno-globalism,

Edgerton addresses the ethnic and racial dimensions of technological politics by

illustrating how access to and benefits of technological development are often unevenly

distributed along ethnic and racial lines as opposed to national borders.

Having overviewed scholarly approaches to the relationship between technology,

nationalism, and globalization, the next sections turn to literature that focuses specifically

on the internet and its governance in the context of contemporary digital globalization.

Global Internet and the State

Novelty of the information space in the early twentieth-century stems from the

qualitatively unprecedented potential of digital communication technologies to infiltrate

national public spheres (Price, 2002; Rantanen, 2005). Some scholars have proposed that

digital globalization fundamentally undermines state power over domestic informational

space (Appadurai, 1996; Beck, 2006; Castells, 2009; Owen, 2015). The appropriate role

of state sovereignty vis-à-vis the global internet has thus become a key question of global

internet governance (DeNardis, 2014, p. 24; Mueller, 2010, p. 60).

Scholarly responses to the issue predominantly in the legal field have proposed

that (a) the internet is its own sovereign that cannot and/or should not be subjected to

traditional state sovereignty (a less techno-deterministic version of this claim proposes

that, at the very least, the internet poses an unprecedented challenge to the state's

informational hegemony); (b) the internet is the latest instantiation of a global technology

can, and likely will, be fully subjected to state sovereignty – like all preceding

technologies in their day; (c) technological malleability of the internet allows for

technology itself to become the regulator. The proposed taxonomy of approaches, to be

sure, does not imply ideological unity among authors *within* each of the three groupings,

only their broadly similar suggestions about the nature and the future of the global

internet vis-à-vis existing state order.

The first group of scholars treat the internet as an exceptional technology for its

unprecedented transnational reach to propose that the cyberspace is deserving of its own

law outside of traditional legal frameworks. In an article that has since become the

scholarly canon of what is often referred to as cyberlibertarianism, "Law and Borders:

The Rise of Law in Cyberspace," David Johnson and David Post argue: "Just as a

country's jurisprudence reflects its unique historical experience and culture, the law of

Cyberspace will reflect its special character" that "will not, could not, and should not be

the same law as that applicable to physical, geographically-defined territories" (Johnson

& Post, 1996, pp. 1401-1402; see also Post, 1995). Scholars of this persuasion propose

self-regulation by the diverse internet community of internet-related businesses, digital

rights-focused and other internet-related civil society organizations, and users as their

ideal model of internet governance. As the state's increasing involvement in internet

governance rendered these propositions obsolete in a practical sense by the late 1990s,

Post and others have remained committed to cyberlibertarianism as a self-professed

normative ideal (Mueller, 2010, 2017; Post, 2009).[7]

The second group of scholars have challenged the notion of cyberspace's ability to escape traditional state-based institutions and to fundamentally reshape the international order (Goldsmith, 1998a, 1998b, 1998c; Goldsmith & Wu, 2006; Wu, 1997). The central thesis of this school of thought is authoritatively summed in the following passage from Jack Goldsmith's tellingly titled article, "The Internet and the Abiding Significance of Territorial Sovereignty":

> The Internet is not, as many suggest, a separate place removed from our world. Like the telephone, the telegraph, and the smoke signal, the Internet is a medium through which people in real space in one jurisdiction communicate with people in real space in another jurisdiction. Territorial sovereignty supports national regulation of persons within the territory who use the Internet. It also supports national regulation of the means of communication—Internet hardware and software—located in the territory. Finally, a nation's prerogative to control events within its territory entails the power to regulate the local effects of extraterritorial acts. (Goldsmith, 1998, p. 478)

The third line of thinking about the relationship between existing state power structures and the internet, represented most notably by Joel Reidenberg and Lawrence Lessig, has emphasized the governing power instilled in the digital technology. Reidenberg, in a non-celebratory way, thought traditional lawmaking institutions to be undermined by the advent of networked borders and communities (Reidenberg, 1996). As a response to the technological challenge, Reidenberg offered the concept of *Lex Informatica*, "the set of rules for information flows imposed by technology and

---

[7] For example, in the introduction to the *Networks and States*, a study of the relationship between the global internet and the nation-state published in 2010, Milton Mueller writes: "The author's normative stance is rooted in the Internet's early promise of unfettered and borderless global communication, and its largely accidental and temporary escape from traditional institutional mechanisms of control" (Mueller, 2010, p. 5).

communication networks" (Reidenberg, 1998, p. 556), to suggest that law- and policymakers across the world could use technology's inherent flexibility and customizability to adjust technological design to their respective local contexts and needs. Lex Informatica is *not* meant as a way to circumvent state regulation, which Reidenberg critically refers to as "the technological assault on state jurisdiction" by "Internet separatists" who work to divorce internet activity from democratic institutions answerable to the public (Reidenberg, 2005).

Lawrence Lessig similarly stresses the regulatory power vested in the technological design. Lessig's treatise *Code and Other Laws of Cyberspace* (Lessig, 2006) put forth the famous dictum of Code is Law. The theoretical idea underlying the notion of Code as Law is that programming code has the ability to embed into the technology's core design the values of those who control the code-making. As coding of major technological systems has aligned increasingly with corporate and state actors, Lessig warns, the original internet's egalitarian promise is being eroded by powerful interests. For example, from a space of anonymity in the 1980s, the internet was fast becoming a space of corporate and state surveillance by the late 1990s. Unlike Reidenberg, who offers to utilize technology as a way to accommodate diverse sovereign state jurisdictions, Lessig's ultimate goal is precisely the opposite – to distance the internet community from the rule of the existing offline institutions: "if cyberspace wants to be considered its own legitimate sovereign, and thus deserving of some measure of independence and respect, it must become more clearly a citizen-sovereignty" (Lessig, 2006, p. 290). To that end, Lessig encourages the transnational community of likeminded users to actively engage in shaping the regulation in the *offline* world in order to preserve

the *online* world's liberties (Lessig, 2006, p. 336).

Global Internet and the Nation

Global internet governance debates reflect the diversity of cultural values and political ideologies of their participants (DeNardis, 2014, pp. 15-16; Mueller, 2010, Ch. 11). The tension between the global reach of the internet and the diversity of national values was recognized as a major policy issue from the early days of the mass internet. For example, an edited volume *Governance of Global Networks in the Light of Differing Local Values* from 2000 contemplated how and whether legal, technological, and policy mechanisms could accommodate cultural difference within digital globalization (Engel & Keller, 2000). The concern for local values has since remained central to discussions of internet governance. Thus, arguing for possible virtues of a bordered internet, Goldsmith and Wu propose that it would allow "people of different value systems to coexist on the same planet" (Goldsmith & Wu, 2006, p. 152). In contrast, in arguing strongly against a bordered internet, David Post nevertheless recognizes that "[c]ountries have different laws because people have different histories, different cultures, different customs, and different views on important matters," and the key question of global internet governance remains in "how to bring law to the inter-network while preserving the diversity of values and viewpoints that characterize the global community" (Post, 2009, p. 170).

Multiple scholars have anticipated that the internet would foster the spread of liberal-democratic values across various national sociocultural contexts. Writing in 1997 on the relationship between cultural sovereignty and global technologies, Ingrid Volkmer envisioned that the global internet would foster "an increasingly homogenized world in which modern liberalism, values and ethics are spread globally" (Volkmer, 1997, pp. 50-

51). Around the same time, Henry Perritt was less deterministic in his predictions, as he believed that "[c]yberspace has not escaped the vortex of politics at the domestic or international level," yet considered the internet to be a natural ally in strengthening the global liberal order:

> Liberalism gives a vision of cyberspace that is fitting not only because of the global spaces for individual freedom of expression the Internet provides but also because the liberal tradition gives meaning and purpose to cyberspace that resonates with the better angels of human nature. (Perritt, 1998, pp. 441-442)

The notion of the internet as a promoter of liberal values has persisted to our days, albeit in a more restrained fashion, as by the mid-late 2000s liberal and illiberal governments alike exhibited their mastery in shaping the online environment (Deibert et al., 2008, 2010; Giacomello, 2005; Goldsmith & Wu, 2006). Philip Howard, a leading scholar of the liberalizing effects of digital technologies upon state governance, describes the use of information and communication technologies by oppositional movements as "a necessary but not sufficient causal condition for contemporary regime change" (Howard, 2010, p. 4). Larry Diamond suggests that digital "liberation technology" is particularly conducive to advancing liberal democracy but acknowledges the barriers that governments are able to put in its way: "the struggle for electronic access is really just the timeless struggle for freedom by new means. It is not technology, but people, organizations, and governments that will determine who prevails" (Diamond, 2010, p. 82).

While some scholars have attributed the universalizing capacity to mold local values in a particular way to the internet, others have emphasized an inverse dynamic of how preexisting national sociocultural order shapes peoples' views on and employment of the internet. Lyombe Eko's scholarship since the early 2000s has addressed explicitly

the fact that "the political, linguistic and cultural differences between the nations of the world render a single global Internet regulatory regime unsuitable and even undesirable despite several proposals to that effect" (Eko, 2001, p. 448; see also Eko, 2012, 2013). For example, the "self-regulation model of the United States and the United Kingdom is rooted mainly in Anglo-American socio-political and commercial culture" (Ibid., p. 448), while France's traditional cultural protectionism meant that "laws and policies that have regulated French culture, media and society, some for more than 100 years, have been transferred wholesale to the Internet" (Ibid., p. 470). Eko's work offers a nuanced examination of how local socio-cultural contexts shape varying national interpretations of international legal-political frameworks, such as freedom of expression, intellectual property, surveillance, human rights, and others.

Abundant scholarship has examined the influence of historical and contemporary strands of a national culture—for instance, 1960s communalism, romantic individualism, libertarianism, neoliberalism—upon the U.S. internet (e.g., Friedman, 2005; Schulte, 2013; Streeter, 2010; Turner, 2006). Given the overwhelming U.S. impact on the internet's development in the 1980s-90s, much of popular and media discourse equated American internet culture with *the* internet culture. However, studies of national internet contexts outside of the United States have demonstrated that local internet usage and policy from the beginning have reflected local cultures. Canadian policymakers in the second half of the 1990s engaged in "discursive nationalization" of the internet, whereby "[t]he transformation of the Internet from an unknown and potentially unruly technology into an enabler of Canadian exceptionalism [was] achieved discursively by delimiting it as a national infrastructure, space, and tool" (Dumitrica, 2015, p. 468). In one of the first

major ethnographies of the internet based in Trinidad and Tobago, Daniel Miller and Don Slater found that "Trinidadians' national identity and culture [was] central to their use of the Internet. Contrary to all the predictions about a new global medium, they anchor[ed] their encounter with the Internet in their specific place" (Miller & Slater, 2000, p. 24).[8] Rafal Rohozinski arrived at similar conclusions with regards to the internet's use and policymaking in the Russian context in the 1990s (Rohozinski, 1999).

Bottom-Up Internet Nationalism

Another strand of literature emphasizes the bottom-up use of the internet by the population for distinctly nationalist purposes.

In *Cyber Nationalism* (2007), Xu Wu examines the origins and characteristics of Chinese cyber nationalism, which he understands as a non-governmental grassroots ideology and networked movement that uses online technologies to propagate nationalistic causes among Chinese people worldwide. The primary focus of the Chinese cyber nationalist movement is on international issues relating to China, while its ultimate goal lays in bolstering China's global status of a major power. This brand of nationalism is independent from the official patriotism of the Chinese Communist Party and situationally overlaps and conflicts with state nationalism.

Ying Jiang (2012) also employs the term "cyber nationalism" in her monograph *Cyber-Nationalism: Challenging Western Portrayals of Internet Censorship in China*. Jiang uses the concept of cyber nationalism to connote broadly the Chinese online users' emotionally charged refutations of Western media coverage of the Chinese internet

---

[8] Miller and Slate (2000, p. 84) offer a broader point: "there is no reason to suppose that [internet] encounters dis-embed people from their particular place; or that they come to treat their real-world locations as less relevant to their encounters or identities; or that they construct new identities in relation to 'cyberspace' rather than project older spatial identities through new media and interactions."

environment and, in particular, state controls over freedom of expression online. Using

Foucault's theory of governmentality as her central analytical framework, Jiang

illuminates how the Chinese state maintains popular nationalism through fostering

consumerism.

Florian Schneider's *China's Digital Nationalism* (2018) examines how a diverse

range of stakeholders in China—from the ruling Communist Party to online activists

filling nationalist forums—strive to shape the meaning of Chinese nationalism through

digital networks. I share Schneider's central concern with the continued relevance of

nationalism in the digital age. By engaging with theories of strategic communication and

the concept of nationalism as evaluation (discussed below), this project additionally

examines how state-led digital nationalism is implicated in the neoliberal logics of global

competitiveness.

As online activists and social movements continue to operate within the national

framework, Shawn Powers and Michael Jablonski (2015) in *The Real Cyber War: The*

Political Economy of Internet Freedom conclude that the popular political demands

> almost always fall within the framework of the existing nation-state system;
> relatively few call for the end of state sovereignty or for the creation of regional
> or global governance structures. … Although connective technologies allow for
> the creation of new and nontraditional communities and governance structures,
> nationalism is alive and well. Confronted with the complexities of an
> interconnected world, citizens clamor for more and better governance. (Powers &
> Jablonski, 2015, p. 156)

Top-down and bottom-up employment of the internet in distinctly national ways

and for national purposes has led many to suggest the internet's imminent fragmentation

along national cultural-linguistic and socio-political lines. Most scholars agree that this is

a key trend in the internet's contemporary development but put forward differing

responses to the issue.

Fragmentation of the Global Internet

In a white paper, "Internet Fragmentation: An Overview," by William Drake and Wolfgang Kleinwächter, prominent scholars of internet governance, and Vint Cerf, inventor of the TCP/IP protocol and Chief Internet Evangelist at Google, the World Economic Forum's (WEF) Future of the Internet Initiative takes a stand against fragmentation (Drake, Cerf, & Kleinwächter, 2016). Noting their self-admittedly "strongly held views about the importance of promoting a secure, stable and integrated Internet consistent with the values of open economies and societies as well as fundamental human rights and freedoms," the authors warn that the "open global Internet" is facing the danger of "splintering" into "loosely coupled islands of connectivity."

Cyrus Farivar, veteran technology journalist, contextualizes internet development in Estonia, Iran, Senegal, and South Korea in *The Internet of Elsewhere: The Emergent Effects of a Wired World* (2011). My project shares the basic premise of Farivar's study: "when the Internet arrives in any country, it bumps up against various preexisting political, economic, social, and cultural histories and contexts," and, consequently, "all countries' online applications and cultures are inevitably distinct, with differences derived from very local characteristics" (Ibid., pp. 11-13). However, Farivar interprets the interplay between the global internet and local contexts from a decidedly West-centric perspective.

According to Farivar, the internet "can be co-opted and/or fought against by regimes that are not ready for it to be used freely. Other developing societies, too, may

not be completely ready to use the Internet effectively. This is why manifestations of the Internet remain so varied in different corners of the globe" (Ibid., p. 16). Accordingly, Farivar celebrates Estonia and South Korea as success stories of emulating Western-style internet use, while political authoritarianism in Iran and low socio-economic development in Senegal are said to have hindered similar developments there. Farivar's implicit suggestion that runs through the book is that the internet has one particular effective use intended by its Western progenitors, and deviation from this is due to the underdeveloped regions being "not ready" to make the most of the Western technology. *The Internet of Elsewhere* thus comes across as an exploration of why and how the non-Western Others were successful (or not) in reinventing themselves as model global citizens.

Ethan Zuckerman, Director of the MIT Center for Civic Media, in *Rewire: Digital Cosmopolitans in the Age of Connection* (2013) bemoans the missed opportunity of the global internet to foster a global conversation and human connection, and encourages global curiosity, serendipity, and intellectual risk-taking in our online conduct. While "it's easier than ever to share information and perspectives from different parts of the world," Zuckerman writes, we don't take advantage of the unprecedented opportunities offered by the global internet (Zuckerman, 2013, p. 19). Zuckerman calls upon the internet community to "rewire" our relationship with the internet in the spirit of cosmopolitanism, where instead of mimicking their offline realities, users would seek new knowledge, people, and experiences online.

Milton Mueller in *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace* (2017) examines the legal-political aspect of fragmentation. Mueller

criticizes growingly forceful attempts by state sovereigns to align internet borders with borders of their respective national jurisdictions. True to his self-professed cyberlibertarian normative stance, Mueller offers a radical solution in forming Net Nationalism, a transnational collective of actors committed to the egalitarian and emancipatory promise of the early internet, who would conduct governance of global communication. This grouping would consist of at least four types of actors: the technical community, the digital rights civil society organizations, the online businesses, and those states supportive of the multistakeholder governance model.

Eli Noam (2013, pp. 10-13) is among a few prominent scholars to endorse fragmentation. Noam argues against "the internet purists, who long for the golden days in which a bunch of computer scientists got together and changed the world[,]" and suggests instead that we "embrace the emergence of diversity" in cyberspace in a new networked constellation of the Federated Internet: "An internet of internets … a system of federated internets working together in some form of technological coexistence of interoperability." According to Noam, decades after the internet was founded and developed through efforts of a small group of pioneers with a common "non-profit, sharing ideology and a libertarian philosophy of minimal government," the internet community has grown into a global multifaceted populace and the internet's architecture should reflect this fundamental change "since governments around the world diverge widely."

1.3 Digital Nationalism as an Analytical Orientation

Digital nationalism as a mode of analysis refers to the self-conscious attention to the role of culture, and in particular national identity, in interpreting the co-constitutive relationship between nationalism and digital technologies. As such, digital nationalism

calls for greater analytical recognition of national cultural-historical contexts and the

national framework as important to our understanding of the workings of digital

technologies. Digital nationalism proposes that historically grounded national cultural

repertoires and identities inform the underlying logic and language of digital

communications policy and discourse domestically and, taking foreign policy to be a

reflection of domestic identity, internationally. In so doing, they reinforce the very

national world order. Digital nationalism thus highlights the national logic at work in the

domain of digital technologies and attendant discourses and policies.

Digital nationalism understands technology as socially constructed (Bijker et al.,

2012; MacKenzie & Wajcman, 1999). While the relationship between society and

technology is mutually constitutive, as they "communicate constantly through the

realization of values in design and the impact of design on values," *analytically* digital

nationalism pays particular attention to why and how society influences technology as the

latter is "always biased to some extent by the values of the dominant actors" (Feenberg,

2010, p. 68). The dominant cultural values that underlie social imaginaries, or widespread

taken-for-granted discourses about how the world ought to work, guide the development

of digital technologies and the internet in particular (Flichy, 2007; Mansell, 2012).[9]

Digital nationalism analytically targets that link between the cultural matrix expressed by

dominant national actors, on the one hand, and digital technologies, on the other.

Two studies of the cultural logics behind digital technologies, *The Cultural Logic*

of Computation by David Golumbia (2009) and *Cached: Decoding the Internet in Global*

---

[9] Charles Taylor describes the social imaginary as "the ways people imagine their social existence, how they fit together with others, how things go on between them and their fellows, the expectations that are normally met, and the deeper normative notions and images that underlie these expectations" (Taylor, 2004, p. 23) and posits that the nation and the state have been its central loci in modern times (Ibid., p. 178).

Popular Culture by Stephanie Schulte (2013), offer crucial insights that the analytical approach of digital nationalism draws upon. Noting that "[w]e are always talking about cultural politics, even when we appear not to be doing so," David Golumbia argues that "computers can only be understood productively when they are seen as part of the cultural and historical contexts out of which they emerge—when … they are read like texts" (Golumbia, 2009, pp. 2-7). In discussing the changing imagination of the internet over time and across various national contexts more categorically, Stephanie Schulte proposes that "culture determines policy. Cultural values and not an objective reality outside of culture set policy agendas, shape policy debates, and help determine policy outcomes" (Shulte, 2013, p. 170). In particular, Shulte proceeds, "representations of the internet produced by a number of agents for diverse purposes were (and are) intricately linked with national identity even as they grapple with a 'global' technology" (Schulte, 2013, pp. 170-171).

Relying on this analytical orientation, the next section employs Craig Calhoun's three-part framework of three dimensions of nationalism as discourse, project, and evaluation to discuss digital nationalism as a social phenomenon that can be observed and studied.

1.4 Digital Nationalism as Discourse, Project, and Evaluation

In thinking about the cultural relationship between nationalism and digital technologies, I employ Craig Calhoun's three-pronged framework that highlights three modalities of nationalism as discourse, project, and evaluation:

> First, there is nationalism as discourse: the production of a cultural understanding and rhetoric which leads people throughout the world to think and frame their aspirations in terms of the idea of nation and national identity, and the production

of particular versions of nationalist thought and language in particular settings and traditions. Second, there is nationalism as project: social movements and state policies by which people attempt to advance the interests of collectivities they understand as nations[.] … Third, there is nationalism as evaluation: political and cultural ideologies that claim superiority for a particular nation; these are often associated with movements or state policies, but need not be. (Calhoun, 1997, p. 6)

I employ Calhoun's framework of nationalism as discourse, project, and evaluation to the study of digital nationalism not as separate lenses but as a three-part whole. Each of the three dimensions serves a specific purpose in framing the project's central argument that identity narratives structure national digital discourse and policy and, by extension, international politics of the digital.

Nationalism as discourse offers an understanding of nationalism as a hegemonic referent of modernity, where discourse is

[W]ays of constituting knowledge, together with the social practices, forms of subjectivity and power relations which inhere in such knowledges and the relations between them. Discourses are more than ways of thinking and producing meaning. They constitute the 'nature' of the body, unconscious and conscious mind and emotional life of the subjects which they seek to govern. Neither the body nor thoughts and feelings have meaning outside their discursive articulation, but the ways in which discourse constitutes the minds and bodies of individuals is always part of a wider network of power relations, often with institutional bases. (Weedon, 1987, p. 107)

The relationship between materiality and discourses, in turn, is mutually constitutive (Carpentier, 2017; Schmidt, 2008). Ruth Wodak explains this dynamic as

a dialectical relationship between particular discursive practices and the specific fields of action (including situations, institutional frames and social structures), in which they are embedded. On the one hand, the situational, institutional and social settings shape and affect discourses, and on the other, discourses influence discursive as well as non-discursive social and political processes and actions.

(Wodak, 2001, p. 66)

In line with this dialectic approach, digital nationalism as discourse refers to how digital artifacts and practices are at once expressive of nationalism as a hegemonic discourse and contribute to its reproduction. For example, the technological design of Facebook that allows users to indicate their country of origin in their profile is only imaginable within the national discourse that constructs the world as a world of nations. At the same time, users' widespread employment of this function reproduces the naturalness of the national discourse in a way that is not readily noticeable and even less so thought of as nationalist.

To be sure, I do not propose that *all* digital practices and rhetoric reproduce the national discourse, but that many of them could be analytically interpreted in this way— even when they are not generally construed as such or thought of as exemplifying *de*nationalization. The analytical task of digital nationalism is to illuminate the *nationalizing* logics of such digital practices and rhetoric.

Digital nationalism as project refers to concerted state-based rhetorical and material efforts that attempt to advance the interests of collectivities they understand as nations through engagement with digital technologies. This modality helps bring to light the central argument of the dissertation about the influence of identity narratives upon digital politics. I view digital nationalism as project as the most explicit instantiation of digital nationalism as discourse. Popular legitimacy of the state rests upon the degree to which it is perceived as successfully defending the interests of the entire nation, and therefore the state overtly constructs all of its efforts as aimed at achieving this goal. For this reason, this dissertation is primarily concerned with state-based digital nationalism as its object of analysis.

Digital nationalism as evaluation refers to states' claims to digital prowess and to the global competition among such strategic narratives. State-led digital nationalism efforts may be domestic, such as the development of the national governmental e-services system or internetization of schools, and international, such as advocacy of the state's normative vision of the global internet's legal and technological architecture in international diplomatic venues. The modality of digital nationalism as evaluation helps to bridge the national-global nexus and illuminate digital nationalism as what Saskia Sassen terms analytic borderland, an entity that operates simultaneously in national and global registers. Digital nationalism as evaluation illuminates how identity narratives underlie the state's foreign policy and strategic communication of the digital.

The following three sections discuss in greater detail each of digital nationalism's three modalities of discourse, project, and evaluation as derived from Calhoun's framework.

Digital Nationalism as Discourse

Nationalism as a discursive framework refers to the ways of acting, thinking, and talking about the world that largely unreflexively and unproblematically assume one's belonging to a national ethno-cultural collective and envisions the world as consisting of such collectives contained within the boundaries of national states. Nationhood as a social category is naturalized through manifold practices that are discursive (Anderson, 2006), material (Zubrzycki, 2017), ritualistic (Hobsbawm & Ranger, 2012; Tsang & Woods, 2014), and routine (Billig, 1995; Edensor, 2002; Fox & Miller-Idris, 2008; Skey, 2011; Skey & Antonsich, 2017), as well as private and public, elite and lay, individual and collective, commercialized, consumptive and productive, and in numerous other

ways. Digital nationalism as discourse then refers to the artifacts and practices, in which

digital communication technologies are imbricated in

> the production of a cultural understanding and rhetoric which leads people
> throughout the world to think and frame their aspirations in terms of the idea of
> nation and national identity, and the production of particular versions of
> nationalist thought and language in particular settings and traditions. (Calhoun,
> 1997, p. 6)

The number of ways in which artifacts and practices relating to digital

technologies contribute to reproducing the discourse of nationhood is too great to attempt

their exhaustive mapping, but a sample of illustrative examples helps to convey their

diversity. Some of these practices are self-consciously nationalist, in that engagement

with digital technologies is driven primarily out of national sentiment. For example, so-

called patriotic hackers may disrupt online activities of the state they perceive as hostile

to their nation, while patriotic users vehemently engage in online discourse in supposed

defense of their nation's history and honor (see, e.g., the discussion of Chinese cyber

nationalism above).

Representatives of national minorities and diasporas use nationalism to advance

their rights and maintain identity over distance (Saunders, 2010). The double-bind of

linguistic and geographic proximity results in users' privileging of websites in national

online segments, regardless of the restrictiveness of national online environment (Taneja

& Webster, 2016). Nationalism is reproduced online through pre-internet practices, like

the all-permeating use of national symbols and language in online content, and some

inherent features of the global internet's architecture, such as the division of cyberspace

into national domain zones like *.ca* (Szulc, 2017).

Many digitally-related practices that are at once structured by nationhood and serve to reproduce it may seem obscure and inconsequential, yet it is precisely their mundanity that reinforces nationalism's naturalness. Facebook often commemorates tragic events, such as the Paris terrorist attack in November 2015, by introducing an option to veil one's profile picture with the national flag of the country where the event took place. While this option's cross-border availability and outpouring of support from around the world may be read as a sign of interconnected digital cosmopolitanism, the framing of tragedies in such distinctly national terms by a powerful meaning-making institution like Facebook and its consumption by thousands of people reproduces nationhood as a natural symbolic resource that makes the social world legible.

While the state is the ultimate manifestation of the national order, as the examples above demonstrate, the state is only one of many social actors that take part in the self-conscious and unselfconscious reproduction of the discourse of nationhood alongside the business, the media, civil society organizations, individuals, and others. The next section focuses on the second pillar of Calhoun's three-pronged framework of nationalism as a project, which, in the context of digital nationalism, refers to concerted state-based employment of digital technologies for the benefit of the nation.

Digital Nationalism as Project

Calhoun understands the dimension of nationalism as project as "social movements and state policies by which people attempt to advance the interests of collectivities they understand as nations" (Calhoun, 1997, p. 6). I operationalize this definition to the view state-based digital nationalism as a concerted government-led effort to utilize digital technologies domestically and internationally in order to bolster the

national interest and identity.

The project of digital nationalism encompasses official rhetoric pertaining to digital technologies by those mandated to speak on behalf of the state—in media articles, commentaries, interviews, official press-releases, websites, speeches, and elsewhere—and attendant official institutions, strategic documents, legal and policy frameworks, bureaucracies, diplomacy, lingo, rankings and indices, imagery, and infrastructures.

For example, Estonia's government's project of *e-Estonia: The Digital Society* is a wide-ranging program that encompasses the national digital infrastructure (e.g., e-taxing, e-health records, e-voting, e-parking), numerous policy documents specializing in digital matters (e.g., Digital Estonia 2020) as well as the diffusion of the digital imperative across policy discourse, political rhetoric by state representatives about Estonia's digital prowess in global media and political venues, a host of promotional materials of Estonia's digital practices (e.g., websites, brochures, videos, exhibitions), and Estonia's own cyber rankings.

The central proposition of this dissertation about how identity narratives underlie the state's digital discourse and policy manifests itself particularly prominently within the register of digital nationalism as a state project. Culture infuses national identity and ultimately state identity by affording a broad, yet not unlimited, range of national cultural repertoires from which people draw selectively to construct their action (Corse, 1996, p. 156-161; Lamont & Thevenot, 2000, pp. 8-10; Swidler, 1986, p. 273). This proposition is rooted in the critical distinction between the nation's cultural identity and the state's political identity.

The hyphenated concept of the "nation-state" is made up of two distinct, albeit

historically intertwined, concepts of the administrative statehood and cultural nationhood. On the one hand, nations seek to attain and then maintain state sovereignty (Anderson, 2006, p. 6; Calhoun 1997, Ch. 4); on the other hand, institutions and practices of the state reproduce the nation across time and space (Hobsbawm, 2012, p. 10). As Ernest Gellner suggests (1983, p. 4),

> nationalism emerges only in milieu in which the existence of the state is already very much taken for granted. The existence of politically centralized units, and of a moral-political climate in which such centralized units are taken for granted and are treated as normative, is a necessary though by no means a sufficient condition of nationalism.

The relationship between the nation and the state is characterized by perpetual tension rather than harmony. Arjun Appadurai describes this relationship as "everywhere an embattled one" to suggest that "while nations (or more properly groups with ideas about nationhood) seek to capture or co-opt states and state power, states simultaneously seek to capture and monopolize ideas about nationhood" (Appadurai, 1996, p. 39). Charles Taylor similarly notes the imperfect overlap between the political identity of the state and the richer and more complex cultural identities of its national citizenry (Taylor, 2004, p. 192). The greater the overlap between the two, the greater the social cohesion within the state; yet even the most cohesive societies will naturally feature a diversity of views on domestic affairs, the nation's core values, and the state's standing in the world.

State digital rhetoric and policy reflect collective culturally established meanings. State officials and policymakers, being members of the national community, draw from the pool of everyday discourses and taken-for-granted knowledges about the world that are rooted in domestic political and cultural contexts (Hopf, 2009, p. 284; Weldes, 1999, p. 9). Erik Ringmar captures the relationship between self-identification and political

action:

> The pursuit of interests is indeed an important reason for action … but in order to
> answer a question regarding an interest we must first be able to answer a question
> regarding who or what we are. It is only *as some-one* that we can want *some-*
> *thing*, and it is only once we know who we *are* that we can know what we *want*.
> (Ringmar, 1996, p. 13; original emphasis)

Thus, for example, the Estonian state's digital nationalism is the function of the

identity narrative about the Estonian nation's inherent cultural Europeanness and the need

to rejoin the Euro-Atlantic community symbolically and institutionally. This widely

shared identity narrative was institutionalized as the highest state interest at the moment

of Estonia's regaining of independence from the Soviet Union in 1991 and has guided its

foreign policy since, including its digital foreign policy.

Digital Nationalism as (Global) Evaluation

The third dimension of nationalism in Craig Calhoun's three-part framework,

alongside nationalism as discourse and project, is that of nationalism as evaluation:

"political and cultural ideologies that claim superiority for a particular nation; these are

often associated with movements or state policies, but need not be" (Calhoun, 1997, p. 6).

Nationalist expressions of superiority in the broadest sense may be carried out by state

and non-state actors and may lead to nationalist excesses of symbolic and physical

violence towards the nation's internal and external Others. As applied to the realm of

digital politics, nationalism as global evaluation means strategic communication by states

of their digital identities and the global competition of such claims, in which states (a)

promote their national digital projects as being on par with or superior to the perceived

global norms of digital development, and (b) strive to shape global political and

technological configurations regulating the development of digital technologies in line

with respective national ideas about who they are and what digital order benefits their national destiny.

It has been asserted widely from both critical and celebratory perspectives that globalization of financial, informational, and human flows and emergent supra-national governing regimes have undermined, or, at least, reconfigured, state sovereignty and national identity (e.g., Beck, 2006; Held, 2004; Owen, 2015; Price, 2002; Sklair, 2002; Urry, 2002). Much evidence can be legitimately put forth in support of this claim. Since the late 1970s-early 1980s, cross-border mobility of all flows grew steadily until the financial crisis of 2007-08, while digital bandwidth flows alone grew 45 times in 2005-2014 (McKinsey Global Institute, 2016, pp. 23-41). State autonomy can be seen as having been partially circumscribed by binding norms and regulations of regional and global intergovernmental bodies, such as the European Union and the World Trade Organization, as well as by transnational corporate and civil society organizations. For example, in May 2018 the European Union introduced the General Data Protection Regulation, a major update to its pan-European digital governance regime containing stringent rules about the treatment of users' personal digital data, which apply universally to jurisdictions of all EU member states, as well as to any non-EU entity whose activities pertain to personal data of EU subjects.

Globalization, however, is a multifaceted process that has had vastly uneven and often internally contradictory manifestations across time, space, and particular areas of human activity. Any categorical claims about the overarching nature of the global-national dynamic are bound to be oversimplifications, and instead the study of

globalization should be approached with critical caution (Hay & Marsh, 2000; Scholte, 2005).

Leslie Sklair (1999) groups the multitude of understandings of globalization and respective scholarly approaches into four clusters: (a) *the world-systems approach* based on the distinction between core, semi peripheral, and peripheral countries in terms of their changing roles in the international division of labor dominated by the capitalist world-system (pp. 149-151); (b) *the global culture approach* focused on the problems that a homogenizing mass media-based culture poses for national identities (pp. 151-154); (c) *the global society approach*, which partially overlaps with the global culture approach, but is centrally concerned with the idea that the concept of world or global society became a believable idea in the modern age, and, in particular, science, technology, industry and universal values are increasingly creating a world that is different from any past age in its self-consciously global awareness (pp. 154-156); and (d) *the global capitalist approach*, which locates the dominant global forces in the structures of an ever-more globalizing capitalism (pp. 156-159).

Within the global culture approach Sklair identifies a subset approach of *globo-localism*, which unites scholars of different disciplines and theoretical positions with a shared "urge to theorize and research questions of what happens to *territorial identities* (within and across countries) in a globalizing world. … The main research question for all these writers is the autonomy of local cultures in the face of an advancing 'global culture'" (pp. 153-154; original emphasis). My approach shares the central interest of globo-localism—with necessary attention to other schools of globalization studies—in the relationship between territorial identities and globalization, namely in the realm of the

digital. There is a crucial caveat, however: I do not think of the national and the global as autonomous and mutually exclusive entities, where one substitutes the other, but rather as mutually constitutive dynamics (Aronczyk, 2017; Castells, 2009; Kraidy, 2005; Sassen, 2006, Ch. 7-8; Steger, 2009).[10]

I view nationalism and globalization as inherently bound. Nationalism as a political project is global and competitive: nationalist ideology views the world as consisting of nations and considers its own brand of nationalism as superior to those of its significant others. Calhoun notes that "[t]he idea of nation is also inherently international and works partly by contraposition of different nations to each other" (Calhoun, 1997, p. 93). Liah Greenfeld similarly points out nationalism's globally competitive nature:

> Nationalism and globalization are often considered to be processes leading to opposite poles in cultural, economic, and political history. In fact, the relationship between them has been far more complex than this and in the past century and a half they may be said to have worked in tandem. … Nations, communities constituted by the nationalism of its members, are inherently competitive. … Since the dignity of the individual identity is derived from the membership in the nation, one becomes necessarily invested in the collective dignity of the nation, sensitive of the nation's standing among other nations, and committed to preserving and augmenting its prestige. Thus, national populations, relative to populations of other types of society, are remarkably easy to mobilize for collective effort. … The decision as to which sphere to choose as the arena for international competition depends on the nation's particular strengths, weaknesses, and values. (Greenfeld, 2011, pp. 5-6)

---

[10] Castells (2009, p. 30): "The age of globalization is also the age of nationalist resurgence, expressed both in the challenge to established nation-states and in the widespread (re)construction of identity on the basis of nationality, always affirmed against the alien."
Sassen (2006, p. 381): "The specificity of the global does not necessarily reside in being mutually exclusive with the national. The strategic spaces where many global processes are embedded are often national; the mechanisms through which new legal forms, necessary for globalization, are implemented are often part of state institutions. … But the processes that constitute this insertion partly denationalize the national."
Steger (2009, p. 194; original emphasis): "The transformation of the national imaginary is a slow and messy business, hardly a matter of either national or global, but of both national *and* global. Both formations will continue to coexist uneasily for the next decades."

The neoliberal globalization of the past forty years has not done away with nationalism but made nations "consumable" more than ever—not least due to the dissemination of digital communication technologies—by global investors, tourists, students, skilled workers, and media audiences (Urry, 1995). David Harvey identifies this as a central paradox of the current epoch:

> The image of places and spaces becomes as open to production and ephemeral use as any other. … The active production of places with special qualities becomes an important stake in spatial competition between localities, cities, regions, and nations. … [T]he less important the spatial barriers, the greater the sensitivity of capital to the variations of place within space, and the greater the incentive for places to be differentiated in ways attractive to capital. (Harvey, 1989, pp. 293-296)

The purpose of national competitive differentiation is not solely economic, or at least not always expressly so. While some state efforts explicitly pursue quantifiable targets, such as the number of incoming tourists and financial direct investments, many others fall within the much less tangible territory of national reputation or soft power, where a direct causal material benefit is nearly impossible to assess. Throughout history, polities have been concerned with the recognition and respect they received, or not, from their significant Others (Lebow, 2009; Renshon, 2017). Since around the early 2000s, however, there has been a noticeably reinvigorated awareness among states about their status in the world community (Paul et al., 2014). This has been particularly true for great and middle powers like China, Brazil, France, Germany, India, the Netherlands, Russia, South Korea, and Turkey, which individually and collectively have tried to steer globalization in the direction congruent with their national interests, but also for smaller states, even if their ambitions have been proportionally limited.

Since the late 1990s, objective globalizing trends and state governments'
subjective perception of the need to bolster its global political-economic standing and
reputation within the community of nations has led to concerted state efforts at defining
and strategically communicating national identity to global audiences (Aronczyk, 2013;
Browning & Ferraz de Oliveira, 2017; Comaroff & Comaroff, 2009; Volcic &
Andrejevic, 2016). Whereas mediated governmental propaganda surely is not a novel
phenomenon (Jowett & O'Donnell, 2014; Taylor, 2003), these objective and subjective
imperatives of globalization and media-technological affordances of the early twenty-first
century have spurred a new wave of state-led informational initiatives targeted at foreign
audiences (Hayden, 2012; Miskimmon et al., 2013; Price, 2015).[11]

Viewing a state partly as "a collection of stories connected to power" and
narratives as partly constituting "the mythic architecture of the state," Monroe Price
argues that under pressure from globalizing information flows and empowered by digital
communication technologies, over the past two decades, many states have allocated
increasing resources to crafting national *narratives of legitimacy* (Price, 2015, p. 41).
Narratives of legitimacy are highest-level justifications for the existence of the state and
its ruling regime that encompass the nation's historical mythology, contain present-day
ideologies, and delineate the boundaries of its desired identity. Fundamentally differing

---

[11] Numerous new state-run strategic communication media outlets and promotional campaigns have
launched since the early 2000s. International television news channels include, for example, China's CGTN
launched in 2000, Iran's Press TV in 2007, France's France 24 in 2006, Turkey's TRT World in 2015,
Qatar's Al Jazeera English in 2006, and others. U.S.-funded Current Time, a Russian-language TV channel
aimed at the post-Soviet space, launched in 2017 specifically to counter Russia's media influence across
the region.
The content of such state-affiliated media producers may differ greatly in terms of production and
journalistic quality. These disparities, while an important issue for media and communication studies, are
outside of this dissertation's specific focus. What matters most for my purposes is that these initiatives
illustrate an argument about how identity logics and narratives underlie global strategic communication,
including about digital technologies: that is, regardless of available media resources, countries pursuing
mediated strategic communication share a common goal of narrating their normative version of world
politics based on their respective domestic identities.

national visions of how society should be organized and what purposes drive it that underlie narratives of legitimacy have led to the global narrative competition of "the great clashing narratives" (Ibid., p. 251).

Digital nationalism as global evaluation, or a global competition of national digital projects, expresses the dynamics of narratives of legitimacy and the great clashing narratives. In propagating the national mythology of the French state, for example, France's Ministry of Foreign Affairs proposes that "[d]igital technology offers many opportunities to promote the 'French brand' against a background of increasingly stronger power plays" (French MFA, 2018). Accordingly, France has been actively promoting its national identity brand of a startup nation explicitly within the logic of global competition among digital nationalisms. For example, speaking of the need to overhaul France's digital strategy, President of France Emmanual Macron said: "We will drive through these transformation [sic] without delay. You do not wait, because your competitors do not wait" (Vey & Kelly, 2017).

1.5 Conclusion

This chapter elaborated digital nationalism as a mode of analysis and a social phenomenon. Digital nationalism as a mode of analysis refers to the self-conscious attention to the role of culture and specifically identity narratives in interpreting the co-constitutive relationship between nationalism and digital technologies. Digital nationalism as a social phenomenon—following Craig Calhoun's three-part framework of nationalism as discourse, project, and evaluation—refers to (a) how nationalism as a hegemonic modern discourse serves as the meaningful context for the construction of digital artifacts and processes and how digital technologies, in turn, reproduce the

national framework; (b) state-led agendas that use digital technologies in the name of advancing national interest, identity, and image and the logics of which are underlain with respective identity narratives; and (c) the logic of global competitiveness that encourages states to strategically propagate their digital identities to global audiences and seek to shape global digital economic and political conditions in their favor.

The next chapter illustrates how the framework of digital nationalism can be used in the study of the relationship between nationalism and digital technology by applying it to the domain of global internet governance. Global internet governance is a constellation of governmental and non-governmental actors, bodies, and processes concerned with the administration of the internet as a technology and development of related principles, norms, and policies. This dissertation is particularly interested in the discursive dimension of global internet governance, viewing it as a geopolitical debate in which states draw upon national values and interests to strategically communicate normative visions of technological and administrative internet configurations. As major economic, social, and political issues became inextricably bound to the workings of online technologies, global internet governance has come to the fore of international relations over the course of the last decade. Why and how internet governance came to be the expression of digital nationalism is the story the next chapter tells.

Chapter 2: Global Internet Governance

2.1 Introduction

The previous chapter outlined the framework of digital nationalism as three interrelated dimensions. Digital nationalism as discourse refers to the dialectic where, on the one hand, the modern discourse of nationalism enables thinking about digital technology in national terms and how, on the other hand, digital artifacts and practices contribute to the reproduction of the cultural understanding of nationalism as the preeminent discursive socio-political framework. Among the many public and private ways of the cultural reproduction of nationalism through digital technologies, digital nationalism as project is arguably the most explicit one and refers to state employment of digital technologies in order to bolster national interests and values. These efforts encompass digitally-related rhetoric and attendant institutions, strategic doctrines, legal and policy frameworks, bureaucracies, diplomacy, lingo, rankings and indices, imagery, and technological solutions. The logic and language of such state-led efforts, as I argue, is underlain with identity narratives. Lastly, digital nationalism as evaluation refers to how the state strategically promotes its digital identity and seeks to shape the global digital order congruent with its national interests and values.

This chapter frames global internet governance—policymaking surrounding the legal and technological architectures of the global internet—as an expression of digital nationalism. Digital nationalism here is understood narrowly as a state-led effort to strategically communicate its digital identity to global audiences and shape the global

digital order. I argue in particular that the logic and language of such efforts derives from respective national identity narratives.

The purpose of this chapter is two-fold as it relates to the preceding chapter and the following chapters. The first goal is to demonstrate why and how global internet governance came to be an arena of global affairs that is expressive of digital nationalism. This discussion illuminates how the framework of digital nationalism outlined in Chapter 1 applies to specific areas of digital politics. The second goal is to set the framework of global internet governance in order to study its specific strategic narratives of internet sovereignty and internet freedom as advanced by Russia and Estonia in Chapter 3-5. I thus outline some of the key rhetorical and institutional structures of the global internet governance, within which Russian and Estonian narratives are situated in the remainder of the document.

Global internet governance is a preeminent arena of global communication policy that has become a contentious domain of global affairs broadly (Bradshaw et al., 2015; Choucri, 2012; Costigan & Perry, 2012; DeNardis, 2014). With the rise of global politics of the internet, literature on the subject has proliferated accordingly and has predominantly focused on the internet governance's institutional, infrastructural, political-economic, international relations, and legal dynamics.[12] Some scholars have addressed ideational and ideological differences among key actors of global internet governance—most often national states—as crucial to understanding the field's dynamics (e.g., Kiggins, 2012; Mueller, 2010, Ch. 11; Powers & Jablonski, Ch. 6; Price, 2015, Ch.

---

[12] E.g., Carr, 2016; Choucri, 2012; Brousseau, Marzouki, and Méadel, 2012; Bygrave & Bing, 2009; DeNardis, 2014; Goldsmith & Wu, 2006; Lessig 2006; McCarthy, 2015; Mueller, 2010; Musiani et al., 2016; Post, 2009; Powers & Jablonski, 2015; Radu et al., 2014.

6) and thought of global internet governance as being structured by competing normative narratives (e.g., Chenou, 2014; Pavan, 2016; Pohle et al., 2016).

However, no major study thus far has applied fully a cultural framework to the examination of global internet governance and employed national identity narratives as its *central* analytical lens. Addressing this omission, in this dissertation I conceptualize global internet governance as

> *A geopolitical debate in which states draw upon national identity narratives to strategically communicate respective normative visions of technological and administrative internet configurations.*

This approach contributes to self-conscious investigations of the relationship between context-specific identities, socio-political values, and cultural histories, on the one hand, and information policy, technological systems, and the internet, on the other hand – an approach that still warrants greater scholarly attention (e.g., Braman, 2009, p. 354; Medina, 2011, p. 215; Oates, 2013, p. 8; Peters, 2016, p. 192). In a revealingly titled article, "Can we write a cultural history of the Internet? If so, how?," Fred Turner appeals: "We need local studies of the Internet and cultural change, conducted in different locations around the world, with sufficient respect for and understanding of the local cultural histories that precede the Internet's arrival" (Turner, 2017, pp. 44-45). The central promise of applying the analytical lens of digital nationalism to the study of global internet governance is to deliver such local studies of the internet with broader theoretical implications.

This chapters consists of two parts. The first part, Internet Governance from ARPANET to WCIT, briefly overviews some fundamental institutional developments of global internet governance from its emergence within the U.S. military to currently a

preeminent arena of global affairs. The historical trajectory and the present-day

governing architectures of the internet have been abundantly documented and analyzed.[13]

Reiterating this detailed history lays outside of the scope of this dissertation. The purpose

of following limited discussion instead is to (a) illuminate how internet governance came

to be inherent to state-based digital nationalism as a project of national development and

the nation's global competitive identity; (b) relatedly, illuminate how global internet

governance is an analytic borderland that occupies a national-global nexus; and (c)

introduce some of the foundational institutions and concepts of the global internet

governance (e.g., ARPANET, ICANN, multistakeholderism) that national narratives of

global internet governance incorporate as symbolic resources (e.g., a rhetorical appeal to

ARPANET history in support of non-state-based internet governance model in

contemporary debates).

The second section, Strategic Narratives of Internet Freedom and Sovereignty,

examines the rhetorical and institutional foundations of the central narratives about global

internet governance that consolidated in the 2010s, when internet governance definitively

came to be an expression of digital nationalism. Having conceptualized the field through

the lens of strategic communication, the section then examines three key normative

narrative approaches to governance of the global internet: American, European, and

---

[13] For historical accounts of the internet and its governance, see Abbate, 1999; Greenstein, 2010; Rosenzweig, 1998. For mappings of the stakeholders, bodies, issues, lingo, and venues central to contemporary global internet governance, see DeNardis, 2014; Domanski, 2015; Balleste, 2015; Bygrave & Bing, 2009; Glen, 2017; Mathiason, 2009; Radu et al., 2014.
The discourse of digital technologies and the internet in particular is often strategically forgetful and couched in the language of novelty (Flichy, 2007, p. 1; Golumbia, 2009, pp. 3-4; Mosco, 2005, p. 8). Some of global internet governance's most powerful actors thus argue that the internet's technological novelty must also be accompanied by a novel multistakeholder arrangement, which benefits their interests. However, some of the major issues in the current debates, such as globalization and national sovereignty, echo concerns of decision-makers and audiences of electronic networks since the second half of the nineteenth century (Marvin, 1988; Mattelart, 2000; Mathiason, 2009, Ch. 2; Standage, 1998; Wenzlhuemer, 2013; Winseck & Pike, 2007).

Sovereigntist. The section illuminates the central argument by demonstrating how each approach—regardless of its rhetorical framing of the internet as either global and borderless or national and sovereign—is underlain with national identity narratives. This discussion also preempts the following three chapters on Russian and Estonian internet governance narratives, since they are related back to the limited typology this section offers.

2.2 Internet Governance from ARPANET to WCIT-2012

The internet, like any complex technology, is the product of collaborative and conflicting, yet always collective, intellectual efforts that cross the public-private divide and national boundaries. No single individual, government, enterprise, or even epoch can be said to have invented the internet when it is understood broadly as a complex multi-layered system of physical infrastructure, networking protocols, applications, and social behaviors that they engender.[14] For example, undersea cables, without which intercontinental internet connections would be impossible, have their origins in the nineteenth-century telegraph era, while personal computing, which fostered mass dissemination of the internet, would unlikely see light without the theoretical work of Alan Turing in the 1940s-1950s and the industrial drive of the Silicon Valley in the 1980s-1990s. The following brief account, needless to say, has no pretense of telling this story exhaustively. What follows is only one of multiple internet histor*ies*, as there is not, and should not be, one canonical history of the internet.

I offer a brief chronological reconstruction from today's vantage point of the architecture of the global internet governance and its attendant debates. The key task of

---

[14] On the conception of the internet as interconnected layers, see Benkler, 2006, Ch.11; Solum & Chung, 2004; Schewick, 2010, pp. 83-90.

this story is to convey why and how current internet governance arrangements came into being: for example, what the Domain Name System is, why it is so central to the internet's functioning, why consequently its supervising organization, the Internet Corporation for Assigned Names and Numbers, plays a critical role within global internet governance, and why it is the subject of heated geopolitical debates. As a result of this admittedly limited retrospective focus, this story leaves out many individuals and organizations that contributed to the internet's technological emergence and development, particularly those outside of the United States.

At the same time, the role of the public and private sectors in the United States was critical in the internet's development. The U.S. administration surely was not the sole actor involved in the internet's development, as American and foreign private sectors, research institutions and universities, and individual engineers and entrepreneurs made indispensable contributions to this process in direct and indirect ways. For example, the rise of the private microcomputer industry in the 1980s allowed millions of users to establish internet connections at home. However, without the decades-long funding of the internet research and critical infrastructure by the U.S. government, such as the ARPANET initiative of the U.S. Department of Defense in 1969-1983 and the National Science Foundation network backbone in 1985-1995, as well as crucial executive decisions along the way, like the U.S. military directive that *all* ARPANET users must adopt the internet's underlying TCP/IP protocol suite by 1984, it is unlikely that the internet would have surpassed its many competing networks to emerge by the early 1990s as the preeminent global digital network.

It is then with appreciation for the role of many international individuals and organizations involved in the building of the internet, yet with a self-consciously limited focus outlined above, that this section should be read.

A Military Internet, 1970s

The internet—a computer network interconnected through the TCP/IP protocol—originated in the 1970s as ARPANET within the U.S. Department of Defense Advanced Research Projects Agency (ARPA), a body mandated with experimental scientific and technological projects in the context of the Cold War (Abbate, 1999, Ch. 2-4). The internet was one of several networks that were being developed around the world, with varying rationales and levels of dissemination in the 1970s-1980s alongside. Other networks included, for example, the All-State Automated System of Management (OGAS) in the Soviet Union (Peters, 2016), CYCLADES (Pouzin, 1973) and Minitel (Mailland & Driscoll, 2017) in France, and Project Cybersyn in Chile (Medina, 2011).[15] In particular, CYCLADES lent some crucial technical design features to ARPANET. The Internet, however, was the first network to adopt an internetworking principle, which allowed for interconnection among devices and networks from different manufacturers and of varying physical properties. The internet thus became the first and has since grown into the world's largest digital *network of networks*.

The internet's governing community at the time was essentially synonymous with its user community, which consisted of several dozen people and famously boasted a collegial horizontal working ethos. Actors in contemporary global internet governance

---

[15] In line with the intentionally retrospective approach to this section discussed above, I leave out the histories of other computer networks, not because they don't matter in the history of networked computing, but because they were either never widely adopted or ultimately were overwhelmed by the internet—and thus their histories are less relevant to the study of today's internet governance arrangements.

debates, particularly those advancing non-state-based governance models, regularly discursively employ the mythology of the internet's early history as a symbolic resource in support of present-day normative visions (Haigh, Russell, & Dutton, 2015, p. 146).[16] For example, Vinton Cerf, co-founder of the TCP/IP protocol underlying internet communication and currently Google's Chief Internet Evangelist, argues that "the multistakeholder, cooperative, and collaborative nature of the Internet's development has been a major source of its resilience and its ability to absorb new applications and players since its conception 40 years ago and should form the basis for its future evolution" (Cerf, 2014, p. 7).

When the U.S. military voluntarily seized its monopoly over the development and use of the internet in the 1980s, the internet's user base and governing community greatly expanded and began its institutionalization.

A Civilian Internet, 1980s

Throughout the 1980s, the internet underwent fast popularization, although predominantly still within the United States (Abbate, 1999, Ch. 6). Governance of the internet, still at the time outside of explicit involvement of national governments, was primarily concerned with its technical development. A small institutional grouping of interconnected non-profit bodies founded between the late 1980s - early 1990s by key figures of the 1970s ARPANET community came to be in charge of the short- and long-term research and development of internet standards and associated policies (Figure 1; DeNardis, 2014, Ch. 3; Galloway, 2004, Ch. 4). This technical community, particularly

---

[16] "Aligning oneself with the soul of the Internet has become a powerful—albeit often flawed—way of advancing one's positions. Tracing a particular practice back to its prehistory in the ARPANET or arguing that a certain philosophy was clearly formulated in the creation of the Internet and has guided it ever since is a way of giving oneself the moral high ground and casting one's opponents as enemies of one of humankind's most successful recent creations" (Haigh, Russell, & Dutton, 2015, p. 146).

the Internet Engineering Task Force, has since retained the ultimate technological

authority over the internet's foundational protocols.

Figure 1. Internet Standards Development Community.
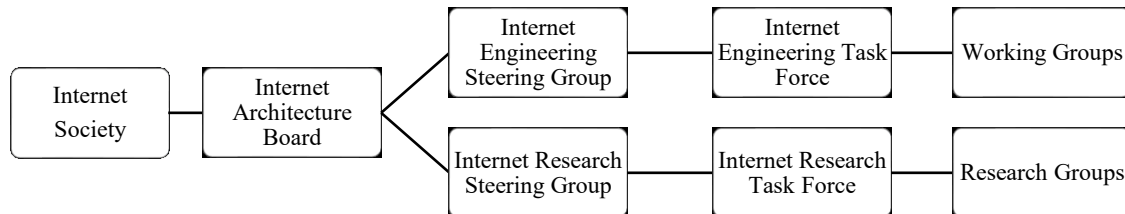
Despite their indispensable role for the functioning of the global internet, and

thereby having a major effect upon public policy issues, internet standards organizations

are non-profit non-governmental entities that are not answerable to traditional state

authority other than the U.S. law. This has made the technical community's critical role

in global internet governance subject to criticisms from the international community and

critical scholars (Froomkin, 2003; Russell, 2014, Ch. 8).[17] Some critique this self-

professedly egalitarian and radically democratic group and its practices as, for example,

"internally self-appointed wise men" (Noam, 2013, p. 13) and "a self-selected oligarchy

of scientists" (Galloway, 2004, pp. 122-123).

---

[17] Membership in the developers' community is voluntary and informal, participation in standards-setting is nominally open to anyone, discussions take place via a mailing list and three conferences a year, and final decisions are made through a deliberative procedure known as rough consensus, where not the precise vote count matters but a sizeable majority. This is because (a) the technical community's detachment from traditional institutions means a lack of democratic oversight by the public and (b) there are, in fact, numerous structural barriers to participating, such as technical, linguistic, time, and financial resources one needs to participate. This means that participants often represent corporations or states. The organization's own structure, as Figure 1 illustrates, is also not entirely non-hierarchical, with various internal administrative, gatekeeping, and technical review stages. All of these factors have contributed to the fact that, contrary to the myth of non-state-based internet governance as inherently egalitarian and global, it is an elite enterprise skewed overwhelmingly in favor of developed countries, and in particular the United States. For example, at the IETF triannual conferences, close to ninety percent of participants come from developed countries supportive of the internet freedom policy framework, while U.S. citizens constitute between a third and a half of all attendees (Internet Engineering Task Force, n.d.).

In the 1990s, particularly the second half, the internet turned from a niche into a mass medium in the United States and more developed countries of the world. The self-regulatory model of governance by the community of the internet's developers and users gave way to major corporate and state powers.

A Commercial Internet, 1990s

In the second half of the 1990s, the internet transformed from a place for hobbyists into a major political-economic domain and increasingly expanded beyond North America.[18] While the number of internet users remained relatively small and the space was closed to commercial activity before the mid-1990s, administration of the internet's Domain Names System (DNS), known as the Internet Assigned Numbers Authority (IANA), was logistically manageable, economically unattractive, and politically uncontroversial.[19]

The Domain Name System is often described as the address book of the internet (DeNardis, 2014, pp. 41-45). The function of the DNS is straightforward: to translate user-friendly alphabetic host names (e.g., google.com), which humans use, into respective numerical identifiers (216.58.210.14), which internet-connected devices use to exchange data. Atop the DNS pyramid is the *root zone file*, a single master file with an authoritative list of generic top-level domains (e.g., .com) and country code top-level domains (e.g., .ca) stored at *root name servers*. Delete a certain entry from the root file

---

[18] Between 1995 and 2017, the number of users rose from 0.4 percent of the world's population to nearly 55 percent (Internet World Stats, 2018). Against the decline in global economic flows since 2007, in 2005-2014 cross-border digital bandwidth flows have grown 45 times and are projected to grow another nine times by 2021 (McKinsey Global Institute, 2016). Six of the world's ten most valuable corporations, including the top four, are digital technologies and internet companies, most of which are barely twenty years old (Forbes, 2018). User base of the most popular social media and communication services, such as Facebook, WhatsApp, and Instagram, rivals the world's most populous countries (Taylor, 2016).

[19] There are thirteen root name servers, eight of which are located in the United States and one in Hong Kong, Japan, Netherlands, Sweden, and the United Kingdom, with multiple mirror servers across the world for expediency and efficiency (Internet Assigned Numbers Authority, n.d.).

and it is no longer easily or not at all accessible to an average user. In this way, management of the DNS/root file provides ultimate technological and therefore geopolitical authority over the global internet.

Commercialization of the internet's domain namespace, whereby registering a domain name turned from a free to paid service, and an influx of businesses online turned this essentially bookkeeping function of administering the DNS into a seat of immense political-economic authority over the global internet.

In light of the tectonic shift in the nature of DNS management, the U.S. administration forcefully moved to initiate a new governing system that would ensure its control of the DNS and the internet's overall development (Carr, 2016, pp. 54-60; Mueller, 2002; Paré, 2002).[20] This resulted ultimately in the establishment of the Internet Corporation for Names and Numbers (ICANN) as a California-based non-profit. Since its establishment in 1998, ICANN has occupied the central place in the political-economic system of global internet governance through its oversight of IANA. Until October 2016, ICANN's administration of IANA was under contract with the U.S. Department of Commerce, thus ensuring American control of the system not only *de facto* but also *de jure*.

Mounting pressure from the international community to address the issue of power imbalances in the emerging global internet governance system led to the UN resolution to hold a two-part World Summit on Information Society (WSIS) in Geneva in

---

[20] Three normative government documents issued in 1997-98 and relating to internet governance outlined this vision: The Framework for Global Electronic Commerce (Clinton & Gore, 1997), Improvement of Technical Management of Internet Names and Addresses (known as the "Green Paper**";** U.S. Department of Commerce, 1998a), and the Management of Internet Names and Addresses ("White Paper"; U.S. Department of Commerce, 1998b).

2003 and in Tunis in 2005.[21] The next section traces how internet governance rose to the forefront of global politics.

A Geopolitical Internet, 2000s

Global internet governance first came to be an explicit expression of digital nationalism in the 2000s, as a large number of states increasingly asserted their authority in governing the internet domestically and internationally (Deibert et al., 2008, 2010, 2011; Drezner, 2004; Giacomello, 2005; Goldsmith & Wu, 2006, Ch. 5; Mueller, 2010). Alongside the private sector, which collectively possesses awesome governance powers over the global internet (DeNardis, 2014, Ch. 7; Tusikov, 2016), the state is a key stakeholder in internet governance in its overt role as a policymaker and covert ways of influencing the private sector. States "can and do shape Internet technology" in a direct policymaking way (Carr, 2016, p. 10), while additionally "state control of Internet governance functions via private intermediaries has equipped states with new forms of sometimes unaccountable and nontransparent power over information flows" (DeNardis, 2014, p. 15). Accordingly, scholars have suggested that "only by giving the great powers pride of place is it possible to ascertain the conditions under which nonstate actors will exercise their influence" over global internet governance (Drezner, 2007, p. 118), while "failure to account for the importance of state interests in shaping future policy ignores the different geopolitical interests at stake in debates over internet freedoms and governance" (Powers & Jablonski, 2015, p. 19).

The World Summit on Information Society first elevated internet governance as a key issue of global communication politics, and by the close of the decade internet

---

[21] For the range of criticisms of ICANN, see Abbate, 1999, p. 208; DeNardis, 2014, pp. 227-228; Goldsmith & Wu 2006, pp. 169-170; Mueller, 2010, pp. 57-62; Powers & Jablonski, 2015, p. 49; Sassen, 2006, p. 333.

governance definitively ascended to the forefront of national foreign policies and global

politics (Choucri, 2012; DeNardis, 2014; Mueller, 2010).

World Summit on Information Society

The World Summit on Information Society, consisting of forums in Geneva in

2003 and in Tunis in 2005 and a set of associated events and processes, inaugurated

internet governance as an explicitly geopolitical domain (Mueller, 2010, Ch. 3; Raboy,

Landry & Shtern, 2010). WSIS produced three major lasting outcomes for global internet

governance. First, WSIS signaled the expansion of internet governance from the technical

niche into a standalone public policy domain. This shift was reflected in the first widely

accepted definition of internet governance adopted by the Summit as "the development

and application by governments, the private sector and civil society, in their respective

roles, of shared principles, norms, rules, decision-making procedures, and programmes

that shape the evolution and use of the Internet" (International Telecommunication

Union, 2005, p. 75). Second, WSIS established the UN Internet Governance Forum

(IGF), an annual multistakeholder gathering with no binding policymaking powers, as the

main venue for discussing global internet governance issues (Ang & Pang, 2012; Epstein,

2013; Malcolm, 2008; Mueller, 2010, Ch. 6).[22] Third, as reflected in the definition, WSIS

enshrined into the understanding of internet governance the principle of

multistakeholderism—participation in the decision-making process by all relevant state-

and non-state stakeholders, including IETF, ICANN, the private sector, governments,

users, and others.

---

[22] A sign of fast institutionalization of internet governance, a plethora of national and regional forums
would spring up over the following years, such as, for instance, the European Dialogue on Internet
Governance and the German IGF in 2008, the Russian IGF in 2011, the South East European Dialogue on
Internet Governance in 2015, and others.

Multistakeholderism has since become at once the hegemonic understanding of how internet governance should operate and the greatest point of contention among stakeholders with different normative visions. Multistakeholderism, as applied to the internet, is a policymaking model that involves multiple parties from the public, private, and civil society sectors in governance (Raymond & DeNardis, 2015; Radu, 2014, Part II). The reality of multistakeholderism in global internet governance, however, diverges from the ideal. While a variety of non-state actors partake in decision-making deliberations in online and offline fora, powerful actors, such as major geopolitical powers and digital corporations, are able to exert much greater policymaking authority (Carr, 2015; Drake & Wilson, 2008, Part III; Hofmann, 2016; Powers & Jablonski, 2015, Ch. 5). As opposed to leveling the field of internet policymaking, multistakeholderism as currently practiced rather reflects and reinforces structural inequities within and between countries.

A Fragmented Internet, 2010s

While the first decade of the twenty-first century exposed major and increasing cleavages among varying visions of who and how should govern the internet, in the 2010s they have become fully intertwined with the broader and increasingly antagonistic geopolitical process. Rising powers, notably Brazil, China, India, and Russia, have individually and collectively challenged the global political-economic hegemony of the Euro-Atlantic community, including in the domain of internet governance and infrastructure (Ebert & Maurer, 2013; Winseck, 2017). The unprecedented intensity of the conflict in the post-Cold War era put into question the very future of the post-WWII

international liberal order (Ikenberry, 2018).[23] Growing divergence in approaches to internet governance domestically and internationally raised fears that the global internet order was also under threat (Chander & Lê, 2015; Force Hill, 2012; Mueller, 2017; Drake et al., 2016). Arguably the single most emblematic event of global internet governance entering a new level of geopolitical contention, as well as being illustrative of the workings of digital nationalism, was the World Conference on International Telecommunications that occurred in 2012.

World Conference on International Telecommunications-2012

The World Conference on International Telecommunications (WCIT-2012) took place in Dubai under the auspices of the International Telecommunication Union (ITU), a specialized agency of the United Nations focused broadly on the technical standards for information and communication technologies (ICT). The meeting was organized to renegotiate the outdated 1988 International Telecommunication Regulations (ITR), a binding ITU treaty of general principles for the provision of international telecommunication services, and became one of the most contentious and widely covered episodes in the history of global communication policymaking.[24]

---

[23] Many in the post-2012 period have employed the Cold War metaphor, though often with a hesitant question mark, to characterize the state of global affairs (e.g., Legvold, 2016; Lucas, 2014) and communication and internet governance (e.g., Blau, 2012; Economist, 2012; Mueller, 2013; Thussu, 2015, p. 247; Van Gelder, 2012). Metaphors of the Cold War and of fragmentation, especially its more problematic synonyms like "Balkanization," particularly when coming from powerful voices in the debate, are not merely descriptive; they shape the internet governance discourse from normative positions and need to be considered critically, or best abandoned (for critique, see Brown, 2013; Maurer & Morgus, 2014; Musiani & Pohle, 2014).

[24] Headlines in mainstream English-language publications included, for example, "The plot against the Internet" in *Politico* (Krigman, 2012), "The U.N. Fought the Internet – and the Internet Won" in *Forbes* (Ackerman, 2012), "The fight to keep a state-free Internet" in *The Financial Times* (Goldstein, 2012), "Beware a Sleeping Godzilla: The UN's Internet Treaty Fiasco" in *Wired* (Weinstein, 2012), "Would you trust Vladimir Putin with the keys to the web?" in *The Guardian* (Naughton, 2012), "Hands Off the Internet!" in *The New York Times* (Brooks, 2012), and "Will Thugs Rule the Web?" in *The New York Post* (Herman, 2012).

Since late 2011, predominantly Western activists, corporations, civil society organizations, media outlets, and liberal governments vocally opposed what they framed as an imminent threat of authoritarian countries using WCIT-2012 to secretively plot an internet takeover.[25] The wave of criticism, in which even esteemed internet figures and journalists sometimes resorted to vile rhetoric, ushered ITU to craft a counter-narrative—including blog posts, official statements, FAQ pages, and an unequivocal "WCIT Myth Buster" PowerPoint presentation—refuting the charges of nefarious scheming (Conneally, 2012; International Telecommunication Union, 2012c, 2012d).

Concerns of the internet freedom advocates were not entirely unfounded. Certain proposals from authoritarian governments, some of which were enshrined in the final version of the ITR, had the potential to legitimize unduly restrictive and sometimes repressive domestic online regimes (Kleinwächter, 2012; Winseck, 2012). At the same time, the public relations campaign waged against the WCIT-2012 was by and large alarmist (Hill, 2014; Mueller, 2012). In the case of major corporate and state powers, forceful criticism of the ITU was also self-serving, meant to preserve the technological hegemony of the American polity and private sector (Powers & Jablonski, 2015, pp. 118-128).

After two weeks of heated debates at WCIT-2012, the ITR passed with a majority of votes but no consensus: 89 states signed the updated ITR; 55 states did not

---

[25] E.g., Criticism came from major corporate and state representatives in the United States, including then-Executive Chairman of Google Eric Schmidt and then-Commissioner of the Federal Communications Commission Robert McDowell (Hill, 2014, pp. 35-47); Google launched a Take Action initiative that encouraged users to sign a petition against allegedly looming efforts by some governments "to increase censorship and regulate the Internet" in order to preserve the "free and open" internet (Google, n.d.; Google, 2012); Vint Cerf, co-inventor of the TCP/IP protocol suit and Google's Chief Internet Evangelist, published a host of op-eds (e.g., Cerf, 2012); European Parliament issued a warning against the possible expansion of the scope of international telecommunication regulations to include the internet in its ambit (European Parliament, 2012).

(International Telecommunication Union, 2012a, 2012b). Reflecting the ideational divide in internet governance debates, the signatories consisted mostly of developing and/or illiberal countries in Africa, the Middle East, Central Asia, South-East Asia, and Latin America, including China and Russia, while those who voted against were predominantly Western liberal democracies and their allies.

WCIT-2012 is expressive of digital nationalism in that states draw upon the logics and languages of respective identity narratives to strategically communicate their digital Selves, digital significant Others, and the global digital order they want. For example, representatives of various branches and bodies of the U.S. state communicated their position regarding the WCIT-2012 through a set of shared long-standing cultural repertoires of the American identity narrative rooted in the discourse of political and economic liberalism—what the U.S. Congress resolution lauded as a "consistent and unequivocal policy of the United States to promote a global Internet free from government control and preserve and advance the successful multistakeholder model" (Rubio, 2012, n.p.; for other examples of the U.S. narrative pertaining to WCIT-2012, see Kramer, 2012; McDowell, 2013; Strickling, 2012).

The next section illuminates how identity narratives underlie visions and policies of global internet governance by examining in greater detail the two key strategic narratives of the global internet governance debate that institutionalized throughout the 2010s: internet freedom and internet sovereignty.

2.3 Strategic Narratives of Internet Freedom and Sovereignty

I approach global internet governance as a discursive competition of normative strategic narratives about who and how should govern the global internet. Drawing on Miskimmon et al., I conceptualize a strategic narrative as

> a means for political actors to construct a shared meaning of the past, present, and future of international politics to shape the behavior of domestic and international actors. Strategic narratives are a tool for political actors to extend their influence, manage expectations, and change the discursive environment in which they operate. They are narratives about both states and the system itself, both about who we are and what kind of order we want. (Miskimmon et al., 2013, p. 2)

Strategic narratives in the case of global internet governance are expressed through an array of texts, where text is understood broadly as all forms of articulations across law and policy documentation, political speech, news media, promotional materials, scholarship, software code, and other discursive environments. My analytical focus in this and remaining chapters is predominantly on strategic policy documents (e.g., U.S. International Strategies for Cyberspace) and public statements by officials at political venues and in the media (e.g., "Remarks on Internet Freedom" by Hillary Clinton in 2010, which launched the Internet Freedom program of the U.S. State Department).

The two main strategic narratives of global internet governance that I focus on in this dissertation are those of internet freedom and internet sovereignty. The camps are divided over the central question of global internet governance about whether information flows are to be regulated by a global community of state and non-state actors or by national governments (Goldsmith & Wu, 2006, p. 150). The narrative of internet freedom, espoused largely by developed liberal states and their allies, asserts that the internet presents a unique technological and governance arrangement, in which state

governments historically have not and should not have a privileged role, as compared to other non-state stakeholders. The main self-professed task of the multistakeholder governance community is to facilitate the global flow of online information and eliminate barriers that states may erect to information flows across their territories. The narrative of internet sovereignty, advanced mostly by illiberal state governments, asserts that global internet governance should be state-based, with input from other stakeholders in consultative secondary roles.

The following excerpts illustrate key tropes of the two strategic narratives. The Group of Seven (or G7), an alliance of the most economically advanced liberal democracies consisting of Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States, states in its 2017 *G7 ICT and Industry Ministers' Declaration: Making The Next Production Revolution Inclusive, Open, and Secure*:

> Openness is a key feature of the digital transformation, stemming from basic principles such as the global nature of the Internet and the free flow of information. To this effect, we reaffirm support for ICT policies that preserve the global nature of the Internet, promote the free flow of information across borders[.]
> … [W]e strongly believe that freedom of expression and the free flow of information, ideas and knowledge are essential for the digital economy and beneficial to development. We are aware that in contemporary society, the free flow of information helps to generate confidence and plays a central role in cultural, economic and inclusive growth. (G7, 2017, p. 8)

Advocates of internet sovereignty, in contrast with the G7 narrative of informational borderlessness, emphasize the right of states to govern nationally the incoming digital flows. The 2015 *Communique of BRICS ICT Ministers on Results of the Meeting "Expanding of Collaboration in Spheres of Telcom and Infocommunications"* by members of BRICS, an alliance of Brazil, Russia, India, China, and South Africa,

confirmed the right of all States to establish and implement policies for

information and communication networks in their territories in accordance with

their respective history, culture, religion and social factors. Other States should

understand and respect this right to self-determination.

…This will in turn promote universal access to the Internet for everybody,

participation of States in governing the Internet infrastructure, the sovereign

rights of States to participate in governing the Internet in their respective

jurisdictions in accordance with international law and the adherence to

fundamental human rights and freedoms. (BRICS, 2015)

The distinction in policy and rhetoric between the camps advancing internet

freedom and internet sovereignty narratives is often blurred, and the normative labels

associated with these groups will be critically interrogated in this dissertation. Yet I

preserve the *analytical* division of the freedom/sovereignty camps for two reasons. First,

this dissertation relies on the interpretive tradition that "seeks to explain events in terms

of actors' understandings of their own contexts" (Schwartz-Shea & Yanow, 2012, p. 52).

Actors in the global internet governance debate themselves overwhelmingly portray the

field as being divided into two camps. The rhetoric of each state individually and of

intergovernmental organizations exposes *their* view of world politics through the lens of

the us/them binary and as populated by aligned and oppositional significant Others – a

view that is also characteristic of the nationalist framework. The second reason to

analytically employ the freedom/sovereignty binary as an entry point into the discussion

is that the actors' own rhetorical framing has materialized into observable institutions and

practices of global internet governance that both uphold and perpetuate the divide. Thus

while government representatives of the two groups often populate the same

policymaking and discussion venues, their institutionalized groupings (e.g., BRICS,

Freedom Online Coalition, OECD, Shanghai Cooperation Organization) and voting

patterns (e.g., for/against ITRs at WCIT-2012) differ consistently enough to speak of two distinctive camps.

The following sections examine the institutional arrangements and rhetorical tropes behind key strategic narratives of the global internet governance debate. I aim to demonstrate that identity narratives underlie the logic and language of these narratives, irrespective of whether a state argues for full preservation of the existing multistakeholder governance model, its partial rebalancing in favor of state authority, or a move toward fully state-based governance. Advocates of all strategic narratives in this debate pursue technological closure, a normative consensus around a technological configuration of the internet that meets their aims (McCarthy, 2015, Ch. 5; Price, 2018).

Internet Freedom

The rhetoric of internet freedom posits that the global flow of online information carries universal liberal-democratic freedoms of expression, assembly, and elections, among other freedoms. The policy implication is that the principles and institutions associated with Westphalian state sovereignty, such as the primacy of national governments, laws and borders, international state-based organizations, and international treaties are not appropriate for the governance of the internet. Internet freedom employs metaphors such as "free," "open," "global," "interoperable," and "borderless" for the internet, while using tropes such as "fragmentation," "splinter-net," and "sovereign," to imply the threat of increased differentiation of the internet along national lines with a more central role for states and state-based organizations in internet governance.

Supporters of the internet freedom agenda encompass a diverse and loose coalition composed of predominantly developed liberal-democratic governments (e.g.,

Australia, Estonia, the USA) and their less economically developed geopolitical allies (e.g., Ghana, Georgia, Mongolia), major digital corporations (e.g., Facebook, Google, Microsoft), digital rights advocacy groups (e.g., Access Now, Article 19, Electronic Frontier Foundation), academic and research institutions (e.g., Centre for International Governance Innovation, Citizen Lab at the University of Toronto), the internet standards community (ICANN, IETF, ISOC, W3C), and individuals with varying affiliations whose voices have come to have particular prominence and resonance in the debate (e.g., Ronald Deibert, Vinton Cerf, Milton Mueller).

There is variance of beliefs, motivations, and histories among those who share the basic ideational and rhetorical tenets of the internet freedom agenda. While the private sector may have a genuine concern for human rights online, the free flow of information with minimal barriers to entry and operation in national markets also directly benefits financial interests of global digital companies like Google and Facebook. Non-profit digital rights advocacy groups, even though their work is often financed by state and corporate donors, have no direct financial incentive in promoting internet freedom, and many are highly critical of governments and corporations for their violations of users' digital rights. Organizations and individuals who approach digital politics from a libertarian perspective, historically a powerful ethos within the internet freedom camp, oppose what they perceive as an excessive role that liberal and illiberal states alike play in internet governance but often align with liberal-democratic governments and West-based corporations in their opposition to illiberal states.

At the state level, which is the explicit focus of this project, governments of the internet freedom agenda operate through several internet-specific and general political

institutional venues. Traditional intergovernmental organizations that advance the

internet freedom narrative include, most prominently, the European Union, the

Organization for Economic Co-Operation and Development, the Group of 7, and NATO.

The preeminent intergovernmental body dedicated to promoting internet freedom is the

Freedom Online Coalition (FOC). Founded in 2011 by fifteen original member states, the

FOC currently includes thirty governments that are developed Western liberal

democracies and their allies in the developing world. The Coalition strategically

communicates the internet freedom narrative in three primary ways: (a) annual

ministerial-level meetings of member governments that are also attended by numerous

private and civil society actors; (b) an FOC-funded Digital Defenders Partnership grant

program for individuals and organizations to build a global "digital emergency sector"

able to expediently respond to threats to internet freedom worldwide; and (c) regular

political statements that range from stating general normative principles of internet

freedom to applying these principles in addressing specific issues (e.g., Joint Statement

on Restrictive Data Localization Laws; see Freedom Online Coalition, 2017).

While institutions supportive of the foundational liberal principles behind the

internet freedom narrative include the United States and their Western European allies,

American and European approaches to global internet governance diverge in their views

on some aspects of global internet governance. As the global digital and internet

hegemon, the United States administration argues for the full preservation of the

multistakeholder status quo. Both the European Union collectively and key European

powers individually wish to see a greater role for governments and more protection of

user rights against corporate exploits and argue for certain organizational changes while

preserving core values of internet freedom. The next two sections detail the similarities and differences between these two subnarratives of the internet freedom agenda.

U.S. Approach to Internet Governance

The U.S. state power historically has been singularly instrumental, as compared to other countries, in the shaping of the global internet's institutional, legal, and technological architecture and continues to exert unparalleled influence over their configurations (Carr, 2015; McCarthy, 2015; Powers & Jablonski, 2015). The United States is the greatest beneficiary of the global internet governance status quo, in which unelected U.S.-based non-governmental organizations, foremost ICANN and IETF, occupy the central place in the global internet's political economy, while other governments do not possess comparable authority over their decision-making. The United States government, accordingly, has championed what can be called a maximalist internet freedom narrative that promotes preservation of the existing internet governance arrangements, without any major structural changes to the power balance between the non-governmental organizations and national governments in favor of the latter. This section illuminates why and how cultural repertoires central to the American identity discourse have constituted the basis for imagining and narrating the U.S. policy framework for the global internet.

Core normative tropes of the U.S. internet governance narrative are summed, for example, in the bipartisan Cyber Diplomacy Act of 2017 passed in the U.S. House of Representatives in 2018:

> [I]t is the policy of the United States to work internationally with allies and other
> partners to promote an open, interoperable, reliable, unfettered, and secure
> internet governed by the multistakeholder model which promotes human rights,

democracy, and rule of law, including freedom of expression, innovation,

communication, and economic prosperity, while respecting privacy and guarding

against deception, fraud, and theft. (Royce, 2018, p. 30)

Although the United States government was central to the invention,

development, and dissemination of the internet and formation of its governance model

from the late 1960s onwards, until the late 1990s, the White House abstained from heavy-

handed micro-management of the internet progenitors' community and exercised its

influence rather through structural support and macro-level decision-making. After

several decades of supporting the internet's development without officially imagining and

framing it as inherent to the nation's destiny, since the late 1980s-early 1990s, the U.S.

government has incorporated the discourse and policy of the internet into the broader

national discourse and policy.

In 1997-1998, the White House played an instrumental role in fostering the

establishment of the non-state-based architecture of global internet governance with

ICANN at its center. When a major challenge to the ICANN-based status quo arose from

the international community in the 2000s, the United States began to engage in a

concerted effort to institutionalize and promote the internet freedom agenda (Powers &

Jablonski, 2015). Since the second half of the 2000s, and particularly after 2010 when the

Internet Freedom program of the U.S. State Department was inaugurated, the U.S. state

has allocated close to $150 million globally toward the development of anti-censorship

software, digital safety training programs for activists and journalists, civil rights groups

funding, and research and publication advocating internet freedom (see Internet Freedom

Project, n.d.; Open Technology Fund, n.d.; U.S. Agency for Global Media, n.d.; U.S.

Department of State, n.d.).

The U.S. strategic narrative of the global internet has been consistent since the early 1990s and is anchored in the cultural repertoires underlying American identity narrative based on the idea of freedom articulated through the tropes of democracy and free markets. This narrative has "discursively constructed the Internet as a free and open domain to counter the global community vision of the Internet that relied on robust government involvement in defense of community" (Kiggins, 2012, p. 195).

One of the early examples of the U.S. strategic narrative about the global digital communication that conveys these key cultural repertoires is a speech delivered in 1994 by then-U.S. Vice President Al Gore at the inaugural World Telecommunication Development Conference under the auspices of the UN International Telecommunication Union (Gore, 1994). Gore proposed five principles upon which to found the emerging global information infrastructure and which illuminate the logic and language of the virtually unchanging U.S. narrative of the global internet.

The principles called upon national governments to advance (a) *private investment* into telecommunications "to obtain the benefits and incentives that drive competitive private enterprises, including innovation, increased investment, efficiency and responsiveness to market needs"; (b) *market competition* as "the best way to make the telecommunications sector more efficient, more innovative and more profitable"; (c) *flexible regulatory framework* that "fosters and protects competition and private sector investments, while at the same time protecting consumers' interests"; (d) *open access* for users to global communication that is unrestricted in content and non-discriminatory in pricing while also protecting intellectual property, as "[t]he countries that flourish in the twenty-first century will be those that have telecommunications policies and copyright

laws that provide their citizens access to a wide choice of information services"; and (e) *universal service* to means of communication for all, irrespective of their location and income, whereby the ultimate "goal is a kind of global conversation, in which everyone who wants can have his or her say."

Gore's rhetoric conflated ideas of political liberalism and economic liberalism – a strategic communication tactic at the center of the U.S. internet freedom narrative (Kiggins, 2015; McCarthy, 2015). Gore suggested that the opening of national societies and economies to unrestricted informational and financial flows would foster a planetary communion based upon liberal-democratic values:

> … [Global Information Infrastructure] will greatly promote the ability of nations to cooperate with each other. I see a new Athenian Age of democracy forged in the fora [that] the GII will create.
> …To promote; to protect; to preserve freedom and democracy, we must make telecommunications development an integral part of every nation's development. Each link we create strengthens the bonds of liberty and democracy around the world. By opening markets to stimulate the development of the global information infrastructure, we open lines of communication.

While rooted in liberal U.S. cultural repertoires of democracy, freedom, and openness, Gore's speech emphasized their supposed universality in order to discursively legitimize U.S. interests and values by framing them as a common global good and destiny—another common tactic of the U.S. strategic communication of the global internet: "Are these principles unique to the United States? Hardly. Many are accepted international principles endorsed by many of you." This proposition illustrates an inherent paradox in the U.S. discourse of the global internet: while the United States benefits from the internet's global expansion and therefore advance the narrative of an "open," "global," and "interoperable" cyberspace, the internet's genuine

internationalization—whereby states and societies worldwide shape the internet in accordance with their cultures, interests, and values—undermines the ability of the U.S. government and the private sector to steer the global internet's development. U.S. discourse of internet governance rarely explicitly reveals the national logic, but it is found elsewhere in the official U.S. political discourse. For example, the 2017 U.S. National Security Strategy states: "The Internet is an American invention, and it should reflect our values as it continues to transform the future for all nations and all generations" (Trump, 2017, p. 13).

The U.S. internet governance narrative seeks to delegitimize other countries' challenge to the perceived U.S. internet hegemony by framing them as undermining not U.S. national interests but universal democratic principles. The 2017 U.S. National Security Strategy, for instance, portrays international multilateral institutions as a legitimate instrument of international relations when employed by the United States to advance their sovereign interests and values, but is is reduced it to a kind of a nefarious authoritarian ploy when used by other states to advance theirs:

> As we participate in [multilateral institutions], we must protect American sovereignty and advance American interests and values. … The flow of data and an open, interoperable Internet are inseparable from the success of the U.S. economy. … Authoritarian actors have long recognized the power of multilateral bodies and have used them to advance their interests and limit the freedom of their own citizens. (Trump, 2017, p. 40)

European Approach to Internet Freedom

The European strategic narrative of global internet governance is supportive of the liberal-democratic values underlying the internet freedom agenda but places greater

emphasis, compared to the U.S. approach on the responsibility of national governments, to protect their citizens' civic rights from corporate exploitation (Christou & Simpson, 2011; Schulte, 2013, Ch. 4). The European Union's (EU) stance on internet governance can be summarized with an excerpt from the European Commission's 2014 communique *Europe's role in shaping the future of Internet Governance*:

> The Internet should remain a **single, open, free, unfragmented** network of networks, subject to the same laws and norms that apply in other areas of our day-to-day lives. Its governance should be based on an inclusive, transparent and accountable **multistakeholder model** of governance, without prejudice to any regulatory intervention that may be taken in view of identified public interest objectives such as to ensure the respect for **human rights, fundamental freedoms** and **democratic values as well as linguistic and cultural diversity and care for vulnerable persons**. (Buttarelli, 2014, p. 11; original emphasis)

While the European Union's fundamental principles on internet governance greatly overlap with those professed by the United States, there are long-standing differences between the two approaches in their understanding of the nature and purpose of the internet in relation to the state and society. The European Union—like the United States and unlike countries of the internet sovereignty camp—believes that internet governance does not require new binding international regulations for the global internet and a structural oversight of an intergovernmental international body, such as the UN International Telecommunication Union. The EU thus gives partial credence to the notion of the internet's exceptional nature, in that its governing infrastructure is unique and should not fall fully within traditional mechanisms of international governance.

However, unlike the United States and like countries of the internet sovereignty camp, the EU considers the current institutional and procedural configuration of the multistakeholder system to be (a) favoring the United States through their historic

influence over ICANN and other key nodes of the global internet and (b) lacking full

legitimacy due to insufficient transparency and accountability of the global internet's

technical standards-setting community to democratic elected institutions. Recognizing

that formal openness to participation in the work of core standards-setting organizations

has not provided for *actual* inclusiveness, the EU has proposed to globalize internet

governance by granting governments of the world greater leverage in the decision-

making of ICANN and other non-state-led institutions and processes that are critical for

the global internet.

The European Union's *supranational* rhetoric and institutions of internet

governance are the outcome of internal struggles among Europe's diverse *national*

interests and identities. For example, debates about the creation of Europe's borderless

digital commercial space pit countries with large self-sufficient national markets against

smaller European states that would benefit from the loosening of digital trade barriers

within Europe. Thus, while the European Union as a collective rhetorically supports the

notion of a single, open, and un-fragmented global internet (depending on their own

national political-economic circumstances), member states of the Union have divergent

ideas about how freely digital flows should be allowed to traverse Europe's physical

borders.

From the perspective of digital nationalism, which employs national identity as its

central analytical category, European countries' varied normative visions for digital

Europe reflect their divergent identities. A European identity, understood as a shared

cultural sense of the European "we" as the preeminent basis of lay self-understanding and

elite justification for political action, has not emerged, despite the ever-increasing

commonality of the European economic, political, and regulatory space (Checkel & Katzenstein, 2009). This is seen not only in the rise of formerly fringe Eurosceptic and parochial right-wing forces to the political mainstream across the continent in the 2000s-2010s, but also in the distinctly national imaginary and rhetoric of some of the EU's most prominent champions. A look at the internet governance stance of France, continental Europe's geopolitical and technological leader alongside Germany, illuminates national identity narratives as underlying regional and global dynamics of internet governance.

Since the late 2000s-early 2010s, France has been actively engaged in developing digital nationalism as a state project with the proclaimed goal of bolstering the national competitiveness and prestige in the global arena. Global internet governance has occupied an important part of these efforts. In the last decade, France has been involved in the work of intergovernmental and multistakeholder internet governance fora, published the inaugural Cybersecurity Strategy in 2011 and its update Digital Security Strategy in 2017, established the French Digital Agency in 2015 charged with coordinating digital development efforts, institutionalized Digital Diplomacy as an official facet of its foreign policy ("Global governance of the Internet" is one of its sections), passed the Digital Republic bill in 2016, and in 2017 issued France's International Digital Strategy that maps France's diplomatic efforts in the digital realm.

France has been among the world's leading advocates of global internet freedom as one of the fifteen founding members of the Freedom Online Coalition, a Sponsoring Nation of the NATO Cooperative Cyber Defence Centre of Excellence, and an official cyber-partner of the United States. The digital relationship with the United States was reaffirmed in two high-profile bilateral meetings of cyber-diplomats in Paris in 2016 and

Washington in 2018, which reiterated key principles of the internet freedom agenda "based on the applicability of existing international law, adherence to non-binding peacetime norms of state behavior, and implementation of practical confidence building measures" (U.S. Department of State, 2018; see also U.S. Embassy & Consulates in France, 2016).

While staying committed to the shared Euro-Atlantic internet freedom agenda and its core ideational principles, France's efforts have been driven by its own interests and values that do not fully overlap with those of even its closest political allies in the EU. France has consistently advocated a greater role in internet governance decision-making for democratically elected governments vis-à-vis non-governmental institutions like ICANN and, at times, has been vocally critical of the GAFA grouping (Google, Apple, Facebook, and Amazon) for their overwhelming influence over internet governance outside of the purview of any traditional democratic institution. France's criticism of ICANN in 2014, for example, was ignited by its concern over the registration of new domains of *.wine* and *.vin*, an industry foundational to France's national economy, culture, and identity, which France wished to maintain control over in the digital sphere as well as in the offline sphere (Lee, 2014). This debate exemplifies how the distinctly national values are projected into cyberspace.

French digital nationalism is seen as well in how French national cultural repertoires implicitly and explicitly inform the logic and language of its digital policy. For example, the Digital Security Strategy frames France's involvement in contributing to *global* stability of cyberspace through the perspective of its *national* imperative: "France owes it to itself to assist in reinforcing the capabilities of countries that would

like to increase the resilience and security of their information systems[.] … This action should also enable France to reinforce its own cybersecurity" (National Cybersecurity Agency of France, 2015, p. 40).

In another example, the rationale the Government of France provides for its Digital Republic program explains: "Twenty-first century France must embrace digital technology, prepare for future developments, take up all the opportunities and shape a society that embodies the principles of liberty, equality and fraternity" (French Government, 2016). Accordingly, one of the three pillars of the Digital Republic, Fraternity through an inclusive digital society, states: "As Internet access for all epitomizes the Republican notions of solidarity and the inclusion of citizens, it will be one of the mainstays of the Digital Republic bill" (Ibid.). Foundational cultural pillars of the French Republic thus form the meaningful context, within which it becomes possible to imagine and implement digital solutions as benefiting the French state and nation.

Sovereigntist Approach to Internet Governance

The concept of digital nationalism suggests that states self-consciously use digital technologies in pursuit of national sovereign interests and values. In this sense, all states in the global internet governance debate are internet sovereigns. The designation of the "internet sovereignty" camp, then, does not suggest that its members are uniquely acting upon their sovereign logics. The suggestion rather is that that the notion of sovereignty and its attendant concepts are *central* to their strategic communication and normative policy frameworks of global internet governance, and that their employment of sovereignty directly challenges the U.S.-led geopolitical and technological world order seen as infringing upon their sovereign affairs.

The strategic narrative of internet sovereignty stresses the primacy of Westphalian state sovereignty as the normative underlying principle for global internet governance. While recognizing the global reach of the internet, proponents of internet sovereignty emphasize that, as with preceding communication systems, national governments and national laws should guide domestic internet governance, while intergovernmental organizations and international law should underlie global internet governance. This approach, known as multilateralism, is formally not opposed to multistakeholderism but interprets it differently. Whereas internet freedom rhetoric frames multistakeholder governance as equal participation in policymaking by all stakeholders from the public, private, and civil society sectors, internet sovereignty rhetoric recognizes the legitimate right to participation in the deliberations by non-state actors but considers binding policymaking to be the exclusive prerogative of national governments.

Advocates of internet sovereignty, the central normative claim of which is about the state's exclusive right to internet policymaking, are unsurprisingly predominantly national governments and state-affiliated organizations. The majority of prominent state supporters of internet sovereignty are illiberal regimes with limited or no history of democratic governance. China and Russia are the leading advocates of the internet sovereignty agenda (on Chinese internet governance, see Mueller, 2011; Negro 2014; Shen, 2016; Zeng et al., 2017). Brazil and India are generally supportive of this approach as well but usually in less confrontational terms. Other states that have co-authored internet sovereignty proposals and/or are members of organizations that support this agenda are found among Central Asian and Middle Eastern autocracies (e.g., Iran, Saudi Arabia, Tajikistan) and other illiberal regimes worldwide (e.g. Cuba, Venezuela).

Advocates of internet sovereignty since the late 2000s have developed collective and individual institutions and initiatives that advance their key ideas. In 2009, members of the Shanghai Cooperation Organization (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) signed an Agreement on Cooperation in the Field of International Information Security. The Agreement includes a commitment to "internationalization of global Internet governance" and, alluding to the United States and other technologically developed states, names the "[u]se of dominant position in the information space to the detriment of the interests and security of other countries" as one of the key threats to international informational security (Shanghai Cooperation Organization, 2009, p. 203). In 2010, China issued its first white paper on the internet, articulating its philosophy of the internet's economic and political development nationally and globally based unequivocally on the principle of state sovereignty: "Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected" (Chinese State Council, 2010). In 2011, in the first joint effort of this kind at the highest level of diplomacy, China, Russia, Tajikistan, and Uzbekistan proposed a resolution on the International code of conduct for information security to the UN, which conveyed core pillars of the internet sovereignty discourse of the primacy of state sovereignty and international law (Li et al., 2011).

After 2012, when Xi Jinping came to power in China and Vladimir Putin returned to presidency in Russia, these champions of internet sovereignty amplified nationalist and statist ideologies domestically (Chen, 2016). The changing self-identification has, in turn, shaped their domestic and global internet policies. Guobin Yang writes that the Chinese

internet since 2012 has been characterized by "an increasingly visible ideological thread vying to give coherence to an expanding system of internet control" (Yang, 2014, p. 109). A similar trend has characterized Russia's post-2012 approach to internet governance, in which traditionalist discourse served to legitimize an unprecedented level of new restrictive internet regulations (Asmolov & Kolozaridi, 2017, pp. 74-76). China and Russia have institutionalized their shared normative understanding of the basic principles of internet governance through bilateral initiatives like the 2015 cooperation agreement on information security and the 2016 Chinese-Russian high-level forum on cybersecurity.

Internationally, China and Russia have reinforced their efforts at internet sovereignty advocacy, in which SCO (India and Pakistan joined in 2017) and BRICS have come to play an increasingly prominent role. In 2015, for example, an updated version of the International Code of Conduct for Information Security was resubmitted to the UN; this time, however, the initiative came from the SCO as a single multilateral organization opposed to several of its individual members. BRICS became another major vehicle of challenging the status quo in internet governance. Since 2015, BRICS communication ministers gather annually, sometimes in conjunction with SCO, to collectively promote internationalization of internet governance and the global ICT market more broadly against the proclaimed monopoly of the United States. Rivaling numerous Western-based fora of internet governance, in 2015 China launched the annual World Internet Conference (also known as Wuzhen Summit) attended by, among other high guests, then Prime Minister of Russia, Dmitry Medvedev.

The speech by President of China Xi Jinping delivered at the opening of the World Internet Conference in 2015 illustrates key tropes of the sovereigntist internet

governance narrative (Xi, 2015). Xi celebrates the internet as an open global space that

benefits human civilization and encourages the world's furthering interconnectedness, of

which China is an eager participant:

> The Internet has turned the world into a global village where distance no longer
> prevents people from interacting with each other. … With the deepening of world
> multi-polarity, economic globalization, cultural diversity and IT application, the
> Internet will only play a bigger role in the progress of human civilization. … All
> countries should advance opening-up and cooperation in cyberspace and further
> substantiate and enhance the opening-up efforts. … China's door of opening-up
> will never close.

Unlike in the internet freedom narrative, however, metaphors of an open, global,

and borderless internet imply affordances of global economic liberalism rather than

signaling commitment to a liberal-democratic political order: "Through the development

of cross-border e-commerce and the building of information economy demonstration

zones, we will be able to spur the growth of worldwide investment and trade, and

promote global development of digital economy" (Ibid.). In this framing, the internet

does not by default carry the liberal value of individual freedom; instead, freedom is

conditioned upon the value of collective order: "Like in the real world, freedom and order

are both necessary in cyberspace. Freedom is what order is meant for and order is the

guarantee for freedom" (Ibid.).

The way to uphold internal order with due respect to the cultural diversity of the

world, Xi argues, is by recognizing the principle of "cyber sovereignty" as foundational

to the global internet governance system:

> The principle of sovereign equality enshrined in the *Charter of the United
> Nations* is one of the basic norms in contemporary international relations. It
> covers all aspects of state-to-state relations, which also includes cyberspace. We
> should respect the right of individual countries to independently choose their own

path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security. (Ibid.)

Xi's reference to "cyber hegemony," often used interchangeably with "monopoly" in the internet sovereignty discourse, and to outside interference in a country's internal affairs is a thinly veiled allusion to the role and actions of the United States vis-à-vis cyberspace. Accordingly, Xi points out the key gap from the perspective of internet sovereignty between the internet as a common global good shared by all countries and the imbalance of the existing internet governance model that favors the United States and their allies. The proclaimed penultimate goal of the internet sovereignty agenda, then, is to "build an Internet governance system to promote equity and justice":

> There should be no unilateralism. Decisions should not be made with one party calling the shots or only a few parties discussing among themselves. All countries should step up communication and exchange, improve dialogue and consultation mechanism on cyberspace, and study and formulate global Internet governance rules, so that the global Internet governance system becomes more fair and reasonable and reflects in a more balanced way the aspiration and interests of the majority of countries. (Ibid.)

2.4 Conclusion

This chapter framed global internet governance as an instantiation of digital nationalism to illustrate the relationship between national identity narratives and the state's digital rhetoric and policy. Global internet governance broadly refers to policymaking surrounding the legal and technological architectures of the global internet and is operationalized in this dissertation more narrowly as a geopolitical debate in which

states draw upon national identity narratives to strategically communicate normative visions of technological and administrative internet configurations.

Global internet governance is neither exclusively national nor global in its actors, issues, institutions, and infrastructures, but is a third entity at the national-global nexus where state-led digital national narratives about the global internet's architecture are conveyed. The chapter categorized several key normative approaches to global internet governance, such as the maximalist internet freedom approach advocated by the United States in defense of the status quo, the European approach to internet freedom that shares with the United States principal internet values but advocates greater accountability of the current mutistakeholder model to democratic public policy institutions, and the sovereigntist approach that challenges alleged internet hegemony of the United States and argues for the primacy of state governments in regulating the global internet.

By linking each approach to its respective underlying identity narratives, I illuminated the dissertation's central argument that differing national rhetorical and policy agendas of states are underlain with the logic and language of respective identity narratives. The following three chapters illustrate this proposition in greater depth. Chapters 3 and 4 examine how Russia's identity narrative of sovereignty in the context of its resurgent identity of a great power has underlain the logic and language of its digital and internet sovereignty advocacy. Chapter 5 illuminates how Estonia's championing of the internet freedom narrative expresses its identity imperative of joining the Euro-Atlantic community symbolically and institutionally.

Chapter 3: Re-Making of a Great Power Identity: Russia's Identity and Strategic Communication

3.1 Introduction

This and the following chapters together tell the story of Russia's digital nationalism: how the Russian state has come to view digital technologies as indispensable to its national development at home and advancement of its geopolitical interests abroad. While the increasing legitimization of digital technologies as simultaneously enabling and embodying national competitive identity is a global trend, this dissertation illuminates how varying national identity narratives underlie the logics and language of respective digital nationalisms and account for their differences. I examine this co-constitutive dynamic between the national and the digital in the context of debates surrounding global internet governance.

One of the first sociological studies of the Russian internet covering its nascent development in the 1990s, *Mapping Russian Cyberspace: Perspectives on Democracy and the Net*, concluded that the digital network's development in Russia was inextricably embedded within its national socio-cultural context and encouraged future research to pay due attention to this co-constitutive relationship:

> [T]he Russian Net's scope and character, and that of its attendant cyberspace, are strongly embedded in its specific socio-cultural context, bounded by language and the specific needs of its users. The Russian case reminds us to be cautious in our tendency to conceptualize networks as a universal social technology, unbounded by the norms of human societies and behaviour. Perhaps we need to adopt an anthropological approach to cyberspace, which is as much defined by culture, language and circumstance as any other area of human endeavour. (Rohozinski, 1999, p. 24)

Rohozinski's early observation has become increasingly apt as the Russian state and society have embraced digital technologies over the past two decades (Gorham et al., 2014; Gorham, 2014, Ch. 6; Oates, 2013; Schmidt et al., 2006). The following example illustrates how identity narratives and the broader socio-cultural environment serve as the constitutive context for national digital rhetoric and policy. At the Internet Entrepreneurship in Russia Forum in June 2014, President Vladimir Putin addressed Arkady Volozh, the head of Yandex, Russia's largest digital technologies company:

> [Y]ou said only three or four countries have their own search engines, and the countries that do have them have a special mission. I hope you will agree with me that the experiment will work only if each one of these missionaries has pure sovereignty. As you see, if there is one owner behind all four, this is not a mission any more, but a monopoly[.]
>
> Thus, our mission is to help you, help our national segment and the people who work in this very promising sphere to become independent, if not from the viewpoint of the state and society, then at least in terms of their ability to express their views and to formulate them in the way they find necessary. Whenever this happens on a national basis, this always benefits the state. (Putin, 2014)

Putin's remarks and the setting of the conversation, when situated analytically within Russia's socio-cultural and digital contexts, reveal much about Russia's digital nationalism. In terms of the geopolitical context, the event took place only several months after Russia's military incursion into Ukraine in spring 2014, which triggered the beginning of the worst crisis in Russia-West relations since the end of the Cold War. The financial and technological sanctions imposed by the United States, the European Union, and several others countries upon Russia, as well as the perceived threat of being disconnected from global digital systems like SWIFT, heightened Russia's rhetorical and institutional stress on digital sovereignty (see Connolly & Hanson, 2016). For example, the Government Import Substitution Commission was established, the then Minister of

Telecommunications Nikiforov called for "full informational sovereignty" by switching to homegrown digital companies and educating a million programmers over the coming years (Russian Ministry of Digital Development, Communications and Mass Media 2014), and a plan for import substitution of software for 2015-2025 was adopted (Russian Ministry of Digital Development, 2015a).

Another important contextual piece of information is that the Internet Entrepreneurship in Russia Forum was organized by the Internet Initiatives Development Fund (IIDF), a state venture capital fund established a year prior at Putin's public suggestion and which, at the time, was Russia's biggest and one of Europe's most active funders (Dow Jones, 2014). Activities of the IIDF, including the gathering of Russia's top digital elite to meet with the President, speaks to the unprecedentedly high place that digital technologies have come to occupy in Russia's state building and political imaginary, as well as to the role of the state in Russia's digital development vis-à-vis the private sector.

The broader political logic of Putin's words about the internet is also revealed through their analytical juxtaposition against Russia's identity discourse of the 2000s-2010s. Putin's appeal to sovereignty as the highest normative ideal—which in Russian political discourse stands for independence of the state's conduct from outside (particularly Western) influences—is in line with the increasingly central place that such understanding of sovereignty has gained in Russia's political imaginary since the late 1990s. Another core trope of Russia's identity discourse invoked in Putin's remarks is that of a monopoly, which refers to—without calling it by name—the supposed geopolitical and technological hegemony of the United States and which stands in the

way of an equitable world order based on genuine state sovereignty and independence. Lastly, in his exchange with Volozh at the Forum, Putin refers to Russia's digital industry as "our national segment" and suggests that if the private sector acts "on a national basis," this "always benefits the state" (Putin, 2014). This framing conveys the statist logic of the Russian government that views the global digital realm as divided into sovereign national segments, in which interests of domestic digital actors should align with state interests, or, at the very least, maintain independence from foreign influence.

This brief episode illustrates how digital governance rhetoric and policy are embedded in multiple overlapping contextual layers, which necessarily must be taken into consideration in the analysis. Following Sarah Oates' observation that "[t]he internet in the post-Soviet sphere shows us that while the online world offers essentially the same opportunities to different countries, national media and political systems themselves are key factors in shaping and constraining the internet within country borders" (Oates, 2013, p. 26), this and the next chapter limit their scope to jointly illuminating the role of Russia's national media and political systems as forming the constitutive context, which has framed the development of Russia's digital nationalism and internet governance. Accordingly, this chapter outlines the trajectories of the first two formative pillars of this dissertation of identity and strategic communication, while the next chapter builds on this discussion to demonstrate how the changing logics of identity narratives and their strategic communication have shaped Russia's participation in the global internet governance.

Organization of the Chapter

The chapter consists of three sections. The first section, National Identity, reveals two arguments: first, how cultural repertoires that underlie the official identity narrative inform state policy; and second how domestic identity relates to state foreign policy. To illustrate these points, I offer a historical overview of Russian national identity and foreign policy narrative from the fall of the USSR in 1991 until the present. This section illuminates why Russia finds itself, in matters of internet governance and beyond, opposed to the West, even though in the early 1990s the ubiquitous presumption of ruling elites in the West and Russia itself was that the country was on a path to becoming a Western-style liberal democracy and joining Western institutions.

The next two sections illuminate how the Russian state's changing identity since 1991 has informed its domestic and external media spheres. The second section, Identity and Domestic Media, stems from an understanding that the materiality, discourse, and policy of the internet need to be understood within the country's broader media landscape. This section details media practices and policies from the emergence of independent Russia in 1991 to the present day to trace how Russian media, and ultimately the internet, regained a state-centric character.

Whereas the second section juxtaposes domestic identity and media, the third section, Identity and Strategic Communication, investigates the relationship between identity, foreign policy, and international broadcasting infrastructure. This section traces the resurgence of Russia's external communication apparatus to illustrate two developments: first, the rise of reputation and attendant strategic communication industries as geopolitical factors in the Russian context; and second, how the country's domestic self-understanding as a resurgent great power has been translated into an

assertive foreign media policy. If global internet governance is viewed in terms of a competition of national strategic narratives about the internet, as this dissertation proposes, it is indispensable to place Russia's active participation in those debates in the context of its broader soft power advance.

The vision of what the Russian nation is and ought to be held by the governing elite has practical policymaking implications domestically and internationally (Tolz, 2001, p. 236). Accordingly, I divide the discussion into periods that follow the terms of Russian presidency or their combinations (1991-1996, 1996-1999, 2000-2004, 2004-2008, 2008-2012, 2012-present) to indicate not a clear-cut break, but a meaningful pivot. There is both change within each presidential term and continuity among them. In order to better illustrate changes and continuities in Russia's post-Soviet history, each of the three sections in the chapter begins with the discussion of the respective developments in the 1990s, even though by 2000, less than two percent of Russians were online, compared to 28 percent in Estonia and 43 percent in the USA (International Telecommunication Union, 2015). Nevertheless, this essentially pre-internet decade is crucial for understanding the roots of political and specifically informational developments since 2000. This is because, first, post-2000 political-ideological framework under Vladimir Putin's and Dmitry Medvedev's presidency rhetorically constructs itself *in contrast* to the 1990s—and thus should be juxtaposed against it. Secondly, and more specific to informational developments, certain elements of Russia's domestic and international internet governance, discussed below, were put in place in the 1990s even in the absence of the mass online audience as such, so understanding their surrounding political and media context is essential.

The discussion draws on two types of sources: scholarship on Russian domestic and foreign developments and primary data from the field of official Russian discourse gathered from strategic policy documents, including speeches and media interviews by officials. This discussion is not intended as an exhaustive account of Russia's identity trajectory in its own right, but is offered as meaningful background that contextualizes the changing nature of Russia's digital nationalism.

3.2 National Identity: "Russia was and will remain a great power."

Russia's digital nationalism—how the state has utilized digital technologies to bolster the national identity and image—has changed with the state's understanding of the Self and consequently the Self's interests. In line with the dissertation's cultural interpretive approach to the political, I treat states as discursive cultural formations and thus trace the change in Russia's identity through the analysis of cultural repertoires, which the state draws upon in constructing and propagating the official national Self and can be excavated from state discourse.

The Russian state's political system has been characterized by increasing authoritarianism since the early 2000s (Gel'man, 2015; Gill, 2015, Greene, 2014; Koltsova, 2006; Ledeneva, 2013; Levitsky & Way, 2010, pp. 186-201; Taylor, 2011). This is evidenced, for example, in the essential control by the executive branch of the legislative and judiciary branches of the state, formal and informal pressures placed upon oppositional political parties and movements, increasing control of the communication system by the state, restrictions of the civil society sector to conform to the official discourse, severe limitations put upon the work of foreign governmental and non-governmental organizations in Russia, and numerous other ways that have enhanced the

role of the state as the key decision- and meaning-making actor. While the increasing authoritarian tendencies of the past two decades are obvious, it is crucial to recognize that, as Levitsky and Way note, "[p]ost-Soviet Russia was never a democracy. … Nevertheless, the regime was quite open in the early and mid-1990s" (Levitsky & Way, 2010, p. 191). The Russian case reminds us, then, that it is important to be attentive to the continuities as much as the changes in national political systems and narratives. In many ways, Putin's regime is part and parcel of Yeltsin's regime, and thus framing the discussion as a sharp change from democracy in the 1990s to authoritarianism is 2000s is potentially misleading. This can be seen in particular in Russia's digital nationalism, which has relied on the notion of state sovereignty in its narrative of the international informational sphere since at least the late 1990s.

Whereas much scholarship has examined the change that the Russian regime has undergone from political-economic, institutional, and legal perspectives, I look to the political discourse and the cultural repertoires it draws upon in determining and illustrating the shifts and continuities in the Russian state's construction of the national Self. Two threads run through Russia's political discourse and my discussion: the notion of the strong state and Russia's relations with the West.

The notion of the strong state implies the power of the ruling elite to authoritatively control the country's borders, economy, regional elites, state institutions, and to conduct independent foreign policy (Tsygankov, 2014). From the 13-14th centuries until 1991, such autocratic rule was the norm rather than exception for Russia, even during more liberal periods in imperial and Soviet history (Suny, 2006; Zimmerman,

2014).[26] By noting the long history of the autocratic rule and the rhetoric of the strong

state in Russia's political discourse, I, of course, do not suggest that Russian elites and

populace are somehow psychologically more predisposed towards authoritarianism as

supposedly innate to their nature. Rather, the deep roots of authoritarianism make it more

easily and readily available to the meaning-making elites as a cultural repertoire in the

Russian context, similar, for example, to the availability of the cultural repertoire of

individual liberty in the American context.

Post-Soviet Russian elites have internalized and reproduced the binary of the

strong/weak state in official political discourse, framing weakness of the state as a

temporary crisis to be overcome in pursuit of strengthening the state. In contemporary

Russian political discourse, the notion of "sovereignty" is often used interchangeably

with the notion of the "strong state." When applied to digital politics, the lens of the

strong state helps to situate Russia's discourse of digital sovereignty within the broader

context of its pursuit of the strong—sovereign—state.

The second long-standing attribute of Russian political imaginary is that,

historically, Russia has constructed its self-understanding and international behavior in

relation to the Western Other (Tsygankov, 2012; Neumann, 2016a; Tolz 2001, Ch. 3).

Since at least the early eighteenth century, Western Europe and, since the twentieth

century, also the United States have played the role of Russia's significant Other, from

which Russia has sought recognition and respect. Over centuries, a cyclical pattern has

emerged: periods of rapprochement—when Russia saw its status of a great power as

recognized by the West—have been followed by periods of confrontation when Russia

---

[26] My own employment of the notion of the strong state is not normative but analytical: it is meant not as an
endorsement of autocratic rule but a useful lens in understanding and analyzing Russian history and
identity.

thought itself as not recognized by the West. This pattern is present in the Russia-West relations after 1991: from seeing Russia (by both Russia itself and the West) as part of the liberal West in the early 1990s to the rising tensions since the late 1990s and particularly after 2012, when, in the view of the Russian leadership, the West did not accommodate Russia's resurgent great power aspirations. The analytical lens of the West as Russia's historical significant Other is particularly pertinent to understanding the logic of Russian foreign policy and outward-oriented strategic communication.

1991 – 1999: From Western Liberalism to Liberal Statism

At the time of its emergence as an independent state in late 1991, Russia's official identity discourse was aligned with Western liberalism. Over the course of the decade, while retaining its rhetorical commitment to democracy and market economy, Russia's identity increasingly drew on more traditional cultural repertoires, such as Russian language, Orthodox religion, and socialist past. Russia's understanding of what defines the nation, what role the state plays vis-à-vis society, and what place Russia as a country occupies within the international order have changed accordingly: from Western liberalism at the opening of the decade to what I shall call *liberal statism* toward its close, an interim identity discourse between preceding liberalism of the early 1990s and increasing statism beginning in the early 2000s.

In the aftermath of the Soviet Union, around 1991-1993, official Moscow enthusiastically embraced the liberal-democratic transition of the economy and polity, and saw the country as being on a path to joining the West. In line with liberal nationalism, the concept of national identity in 1991-1992 was explicitly non-ethnic and devoid of either imperial or Soviet legacy. Only Russian citizenship—not ethnicity,

culture, or language—was to be the marker of belonging in the nation. Around thirty

million ethnic Russians, who found themselves a minority in the newly independent post-

Soviet republics outside Russia, were thus not included within the nation.

The purely liberal identity, however, was soon abandoned. The severe socio-

economic crisis brought on by the shock therapy, supervised and encouraged by Western

financial institutions, discredited the notions of democracy and capitalism in the eyes of

the population and parts of the political class within the very first years. In the changing

socio-political climate, the state abandoned the strictly civic-liberal understanding of the

nation. In 1993-1994, its definition expanded to include the knowledge of Russian

language as a marker of national belonging, thus extending the boundaries of the nation

to Russian-speakers across the former USSR. In 1995-1996, the conception of the nation

began to include both imperial and Soviet elements at once. In addition to the continued

promotion of the post-Soviet concept of civic identity with loyalty to the new democratic

Russia, the state now also sought to incorporate closer ties with the former Soviet space

and eastern Slavic nations (Belarusians and Ukrainians) as elements of Russia's self-

understanding.

In the second half of the 1990s, after Boris Yeltsin's reelection for the second

four-year presidential term in 1996, Russia's identity discourse continued to move away

from its liberal beginnings of the early years of independence. In 1996, Russia adopted its

first Concept of the State Nationalities Policy, a doctrinal document outlining Russia's

normative vision for regulating inter-ethnic relations within the country and with the

Russian diaspora abroad. The Concept institutionalized Russia's official self-

understanding by advocating "the cultivation of Russian patriotism" around a civic non-

ethnic identity (Yeltsin, 1996, n.p.). At the same time, Russians as an ethnic group are distinguished as playing a "uniting role" in the multi-ethnic Russian nation spread across the "Eurasian national-cultural space." The Concept states: "Interethnic relations in the country will depend on the national well-being of the [ethnically] Russian people, the backbone of the Russian state." Over the second half of the 1990s, Russia's self-understanding as a multiethnic nation with the leading role of the ethnic Russian people united around the civic state became hegemonic across the mainstream political spectrum.

Foreign Policy

1991 – 1995: "The struggle of ideologies has come to an end. Now we have to take care to meet Russia's needs."

As a nuclear power and a permanent member of the UN Security Council, Russia remained an important geopolitical actor after the fall of the USSR. At the same time, Russia's strongly pro-Western identity in the first half of the 1990s and its extreme economic weakness limited Russia's involvement in global affairs mainly to participation in the resolution of numerous interethnic conflicts around its borders (Tsygankov, 2016, Ch. 3). The logic and language of the first post-Soviet Foreign Policy Concept, signed into law in April 1993, are telling of Russia's transitional self-understanding in the period that the Concept itself characterizes as a "post-totalitarian social rearrangement" (Yeltsin, 2005, p. 31).

The overarching idea of Yeltsin's regime in the early years was to discursively delineate independent Russia from the Soviet times and signal the country's belonging in the liberal-democratic West. The Concept is thus explicit about the Soviet Union's

shortcomings, such as alleged "imperial arrogance and egocentrism," "ideological narrow-mindedness," and "'messianic' communist ideology and expansionism" (Yeltsin, 2005, pp. 45-50). In contrast to the Soviet times, echoing Francis Fukuyama's end of history thesis, the Concept considers the post-Cold War as the beginning of a liberal-democratic post-ideological age: "The struggle of ideologies has come to an end. Now we have to take care to meet Russia's needs" (Yeltsin, 2005, p. 28). The Concept proposes that what drives Russia's foreign policy is the desire for the world to "acknowledge Russia's leading role as the engine for market reform and guarantor of democratic transition within the post-Soviet space" (Yeltsin, 2005, p. 43) and hails cooperation with the World Bank, the International Monetary Fund, and the USA.

1996-1999: Geopolitical Fault Lines Reemerge

During Yeltsin's second presidential term, the etatization of identity with ethnic elements informed foreign policy (Tsygankov, 2016, Ch. 4). In a telling sign of the times, the seat of the Minister of Foreign Affairs went from a staunchly liberal Andrey Kozyrev, who the left-wing opposition derided as "Mister Yes" for allegedly being overly yielding to the West, to Yevgeny Primakov, previously the head of the Foreign Intelligence Service of much more centrist-conservative persuasion, who would go on to serve as the Prime Minister in 1998-1999.

Different strands of Russia's identity informed various aspects of its foreign policy. Cultural-linguistic markers of Russian identity manifested themselves in Moscow's increasingly vocal support of the ethnic Russian diaspora, particularly in the Baltic states. Reflecting Russia's strengthening nostalgic Union identity, from 1996-2000

Russia and Belarus were working on the creation of the federative Union State of Russia

and Belarus.[27]

While Moscow embraced the West in the early 1990s, divisions in Russia-West

relations began to re-emerge prominently in the second half of the 1990s. Arguably the

lowest point in the Russia-West relations in the first post-Cold War decade came in 1999

and related to the NATO-led bombings of Yugoslavia during the 1998-1999 Kosovo

War. Many Western powers supported the Kosovo Albanians' state-seeking nationalist

aspirations for independence from Yugoslavia, while Russia supported Belgrade's state-

led nationalism of preserving Yugoslavia's territorial sovereignty. This episode is

illustrative of how preexisting, readily available cultural repertoires underlie

contemporary identity narratives of the national Self and the Other and ultimately inform

policymaking. In its support of the Yugoslav regime and opposition to NATO, the

Russian government drew upon such varied repertoires as, for example, (a) Russia's

historic role as a defender of Slavic Orthodox peoples, (b) post-WWII repertoire of the

primacy of the United Nations in the international order, and (c) the Soviet-era anti-

Americanism. These socially widespread repertoires did not *determine* state action, in a

direct causal sense, but made certain political choices more obvious and others more

politically challenging. The NATO bombings of Yugoslavia itself became a repertoire

within Russia's socio-cultural context as a symbol of an alleged quintessence of

American—and broadly Western—disregard for international law, hypocrisy, and

hostility toward Russia and its partners. Russian political elites have since drawn upon

---

[27] The Union State of Russia and Belarus, founded in 1996, nominally exists to this day but never came close to its original vision of a federative political entity. Interest in the idea subsided dramatically after Vladimir Putin's coming to power in 2000 and briefly reignited several times throughout the 2000s. With the creation of the Eurasian Economic Union in 2014-2015, which includes Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia, the project of the Union state is likely to become more obscure.

this repertoire in legitimation of their contemporary actions, such as involvement in the Syrian War.

Although recovering from the socio-economic crisis of the first post-Soviet years, Russia was still too weak economically to fully profess a great power status but began to promote the normative notion of a multipolar world, as opposed to the U.S.-led unipolar liberal order. The vision of the polycentric world, however, was not culturally anti-Western, as it would increasingly become in the 2000s, particularly after 2012-2014. Instead, Russia still saw itself as part of the West, albeit a distinct part that no longer wished to uncritically mimic Western models and was more assertive in standing up to what it perceived as threats to its identity.

2000 – 2008: Building a Sovereign Democracy

Official narrative of the nation and the country during Vladimir Putin's first two presidential terms focused centrally on the need to strengthen the state after its weakening in the 1990s. A few months before being elected President, then Prime Minister Putin detailed his political philosophy in a programmatic newspaper article, "Russia at the Turn of the Millennium" (Putin, 2005b). Over the next eight years, much of Russian official discourse and policy followed within the framework outlined in the article, so it could be read analytically as a primer on the logics of Russia's national identity during that period.

"Russia at the Turn of the Millennium" proposes three lessons from Russia's past and three recipes for its future success. The first lesson is that the Soviet political-economic model was "moving along a path that was a dead-end and that ran clear of the highway of civilization" (Ibid., p. 225). This assertion reaffirms the incoming elite's commitment to democratic and market principles by reiterating the discursive boundary

between the Soviet and post-Soviet projects. The second lesson is that Russia has used up its limit for political and socio-economic upheavals, cataclysms and radical reforms. This lesson serves as a promise of stability after a tumultuous decade. The flipside of the normative rhetoric of stability would come to manifest itself through the Kremlin's intolerance of domestic dissent and protest, as well as opposition to pro-Western popular uprisings across its borders. The third lesson is that Russia needs to combine the principles of a market economy and democracy with Russia's realities. The lesson signals Russia's deviation, evident since the second half of the 1990s, from the Western liberal-democratic framework toward an increasingly hybrid model.

Building on the three historical lessons, Putin proposes three strategic developments: Russian Idea, Strong State, and Efficient Economy. The Russian Idea should be understood as the normative articulation of the national identity, which the polity, Strong State, and economy, Efficient Economy, institutionally embody. The Russian Idea, as Putin underscores, is not a mandatory top-down state ideology, but rather a set of traditional cultural repertoires, upon which social consolidation and political process should take place. The four ideational pillars of the Russian Idea include Patriotism ("The sense of pride in the Homeland, its history and achievements."), Great Powerness ("Russia was and will remain a great power."), Statism ("Our state and its institutes and structures have always played an exceptionally important role in the life of the country and its people."), and Social Solidarity ("It is a fact that in Russia a striving towards collectivism has always prevailed over individualism."). The cultural pillars of patriotism, great powerness, statism, and collectivism would come to increasingly populate Russian domestic and foreign policy narrative—including of internet

governance—in 2000-2008 as a reflection of Russia's growing self-understanding as a resurgent Strong State.

In Putin's framework, cultural repertoires of the Russian Idea underlie the concept of the Strong State polity. Rhetorically contrasted with the weakened state apparatus of the 1990s, which faced economic, legal, and territorial separatism of regional elites, the Strong State here alleges potent state institutions able to enforce constitutional rule across the country, not a dictatorial rule: "*A strong state power in Russia means a democratic, constitutional, competent federative state*" (Putin, 2005b, p. 229; original emphasis).

The economic vision, Efficient Economy, also reflects the cultural underpinnings of the universal-particular dialectic Putin puts forth.[28] On the one hand, it proposes to draw upon the Western experience of building market economy through liberal economic policies and integration into global economy, including membership in the World Trade Organization. On the other hand, national historical traditions color the implementation of the liberal economic course. Putin suggests the time has not yet come to leave the economy to the proverbial invisible hand of the market. The dual liberal-statist approach to the economy after 2000 would manifest itself in a combination of, on the one hand, liberal domestic reforms (e.g., Russia introduced the lowest flat income tax in Europe of 13 percent in 2001) and foreign economic policy (e.g., the joining of WTO and rhetorical support of economic globalization) and, on the other hand, the state capitalism built around state corporations as expressive of national identity (e.g., the input of state companies into the economy increased from 35 percent in 2005 to 70 percent in 2015).

---

[28] On post-Soviet Russia's political-economic developments, including their relation to the nation- and state-building process, see Lane, 2008; Makarychev & Mommen, 2013; Müller, 2011; Rutland, 2013.

The notion of "sovereignty" as a euphemism for domestically strong state institutions and the ability to conduct independent national foreign policy arose as central to Russian political discourse and imaginary in the 2000s and has since maintained its centrality in Russia's political imaginary (Deyermond, 2016; Morozov, 2008; Ruutu, 2017; Ziegler, 2012). For example, at the meeting of the Valdai Club in 2007, Putin posited sovereignty as indispensable to the very survival of Russia—a change towards greater assertiveness from the discourse of the early 1990s when economic revival of the impoverished post-Soviet Russia was considered essential for its survival:

> Sovereignty is … something very precious today, something exclusive, you could even say. Russia cannot exist without defending its sovereignty. Russia will either be independent and sovereign or will most likely not exist at all. (Putin, 2007b)

Vladislav Surkov, Deputy Chief of Staff of the President in 1999-2011 and seen as the main ideologist of Putin's era, captured the zeitgeist with the notion of "sovereign democracy" (for explication in his own words, see Surkov, 2009; for liberal critique of the notion, see Petrov, 2005). Although introduced around 2005, sovereign democracy has become a commonly used analytical shorthand to describe the political system of the 2000s by its proponents and opponents alike. The core idea of sovereign democracy, as advanced by its supporters, is that Russia should not uncritically transpose Western liberalism onto its own experience, but independently build democratic institutions at its own pace and with accommodation of local cultural, social, and political norms and traditions.

Foreign Policy, 2000-2008: From Post-9/11 Engagement to Challenging Liberal Order

National identity discourse based on the notions of patriotism, great power

aspirations, strong state, and social collectivism informed Russian foreign policy in the first decade of the 2000s (Tsygankov, 2016, Ch. 5). The normative concept of multipolar/polycentric world—an international order founded upon the principle of state sovereignty as outlined here and with the United Nations at its center—that appeared in Russia's foreign policy imaginary and discourse in the late 1990s was reinforced beginning in the 2000s and ultimately became central to the country's construction of the world order (Chebankova, 2017; Miskimmon & O'Loughlin, 2017).

Illustrative of this shift in Russia's foreign policy logic, the 2000 Concept of Foreign Policy in stark contrast with the 1993 Concept's transitional post-ideological sentiment expressed disillusionment in Russia's Western partners: "Some of the expectations for the emergence of new, equitable and mutually beneficial partnerships between Russia and the rest of the world have not materialized" (Putin, 2005a, p. 89). Instead of propagating a full embrace of the liberal-democratic paradigm and institutions, the 2000 Concept advanced the notion of a multipolar world order that questions legitimacy of the unipolar U.S.-led world, argues against the resolution of global issues exclusively through Western institutions and forums of limited membership, and pledges to promote collective resolution of key problems through the United Nations. Russia's logic and rhetoric of global digital governance reflects the normative notion of multipolarity founded upon the principle of state sovereignty: Russia's strategic narrative of global internet governance frames the global digital order as monopolized by the United States and portrays Russia's goal as rearranging the global digital architecture in an allegedly more equitable way.

Russia's foreign policy discourse clearly distinguishes between economic and

political globalization. Benefits of economic globalization are meant to bolster, not undermine, the sovereign national order. The 2000 Concept thus promotes Russia's aspiration to play a full and equal part in the global financial-economic system and the country's integration into the global economy. While lauding economic globalization, the Concept stresses the idea of "a sovereign state as the fundamental component in international relations" and speaks out against "outside influences" and "arbitrary interference in internal affairs" (Putin, 2005a, p. 92).

Russia's digital narrative preserves the delineation of economic globalization, on one hand, and cultural and political globalization, on the other hand. Russia embraces economic digital globalization but alleges that the United States are skewing the fair competition through active measure to maintain the global leadership of American digital products and services. Russia's economic strategy in the digital realm is to promote its ICT sector internationally and benefit from the opportunities of digital globalization. At the same time, Russia has been increasingly opposed to the cultural and political effects of digital globalization that it perceives as elements of outside influence and interference in its internal affairs by digital means that challenge its national sovereignty. Example of such perceived outside influence include, for instance, the accessibility of foreign content, the use of foreign IT products by the state apparatus, ownership of Russian citizens' personal data by foreign online services, and lack of legal-political mechanisms at Russia's disposal to influence the workings of key digital governance institutions, like the Internet Corporation for Assigned Names and Numbers.

Relations between Russia and the West deteriorated significantly during Vladimir Putin's second presidential term of 2004-2008. Russia's disillusionment with the West,

expressed already in the 2000 Concept, was exacerbated by what the country's leadership saw as hostile acts towards Russia and the multipolar UN-based international order it has come to vocally advocate. These actions included, most notably, the 2003 invasion of Iraq in circumvention of the UN decision, NATO's continued eastward expansion (Bulgaria, Romania, Slovakia, Slovenia, and Russia's immediate neighbors Estonia, Latvia, and Lithuania became members in 2004), and overwhelming Western support for pro-Western uprisings that brought down regimes broadly aligned with Russia in Georgia in 2003, Ukraine in 2004, and Kyrgyzstan in 2005.

As Russia's economy continued its growth (Trading Economics, n.d.) and the country's leadership perceived the actions of its Western Significant Other as increasingly hostile, the identity narrative domestically and internationally became more assertive and confrontational in Putin's second term (Tsygankov, 2016, Ch. 6). Russia's self-understanding in the world was pronouncedly communicated in Putin's speech at the Munich Conference on Security Policy in early 2007. This arguably most important and telling text of Russian foreign policy under Putin's first two terms unequivocally conveyed Russia's dissatisfaction with what it framed as the U.S.-led unipolar world order and Russia's intention to challenge it:

> [W]hat is a unipolar world? However one might embellish this term, at the end of the day it refers to one type of situation, namely one centre of authority, one centre of force, one centre of decision-making.
> It is [a] world in which there is one master, one sovereign. And at the end of the day this is pernicious not only for all those within this system, but also for the sovereign itself because it destroys itself from within.
> … One state and, of course, first and foremost the United States, has overstepped its national borders in every way. This is visible in the economic, political, cultural and educational policies it imposes on other nations. Well, who likes

this? Who is happy about this? (Putin, 2007a)

2008 – 2012: Putin-Medvedev Tandem and Failed Modernization

From 2008-2012, formerly First Deputy Prime Minister Dmitry Medvedev served

as Russia's President, while Vladimir Putin assumed the position of a Prime Minister.

With Putin's popularity still high, the question was whether Medvedev would conduct

independent policy and whether it would thaw Russia's increasingly chilly political

climate.[29] Medvedev and Putin ruled in a tandem with ambiguously delineated power

sharing arrangements. The two-pronged regime created greater ambiguity in the official

identity narrative, yet its core pillars set in place in the early 2000s remained unchanged.

This also held true for Russia's digital nationalism as the overarching course toward

digital sovereignty domestically and a challenge to the international digital status quo

remained at its core. The ICT sector's growth and Medvedev's personal enthusiasm for

digital technologies provided additional impetus for the state's further embrace of digital

technologies as critical for its national interest, identity, and image.

Medvedev's political record was mixed in its ideational orientation and tangible

results (Black, 2014). On the one hand, Medvedev's term was characterized by a degree

of liberalization inside Russia and rapprochement in its relations with the West, while the

overarching trope of Medvedev's single-term presidency was "modernization," which

was to encompass institutions, infrastructure, innovations, and investments (Medvedev,

2009a). On the other hand, Russia under Medvedev stayed within the framework set in

---

[29] Clearly, this question was on the minds of several international leaders. "The Medvedev Thaw: Is It Real? Will It Last?" is the title of a June 2009 statement to the U.S. Commission on Security and Cooperation in Europe delivered by the Director of the Human Rights and Security Initiative, Sarah Mendelson, who is also a Senior Fellow of the Russia and Eurasia Program at the Center for Strategic and International Studies (Mendelson, 2012).

place by Putin over the previous years. By the beginning of Medvedev's term, the normative concepts of sovereignty and strong state had become an unquestioned ideational pillar of the regime and maintained their crucial place within identity discourse in 2008-2012, if slightly less centrally. As one scholarly assessment summed, "Medvedev's modernization, then, was an attempt to *strengthen* the regime through a mixture of fake reforms and half-measures, not to *reform* it" (Wilson, 2015, p. 154; original emphasis).

Foreign Policy, 2008-2012: U.S.-Russia Reset and (Briefly) Moving Beyond Cold War Mentalities

Russia's liberalized identity discourse under Medvedev, as compared to Putin's rule in 2000-2008, precipitated a détente in the relationship between Russia and the West (Pacer, 2016). The beginning of Medvedev's presidency, however, gave good reason for caution to those Western observers who saw in him potential for a thaw. In August 2008, only a few months into his term, Russia entered into a five-day armed conflict with Georgia—a close ally of the EU and the USA—over the status of South Ossetia, a pro-Russian breakaway region of Georgia. Russia's relations with the West soured precipitously over the following months, but the chill did not last long. Already in March 2009, U.S. Department of State Secretary Hillary Clinton and Russia's Minister of Foreign Affairs Sergey Lavrov officially launched a so-called "Reset" policy intended to normalize the relationship. Soon after, then-U.S. President Barack Obama and Dmitry Medvedev released a joint statement indicating that they were "ready to move beyond Cold War mentalities and chart a fresh start in relations between [the] two countries" (Obama & Medvedev, 2009).

Russia updated its Concept of Foreign Policy in the wake of Medvedev's presidency. The Concept shares ideological foundations with its predecessor from 2000, but also reflects changes to the country's self-understanding that had taken place since. The 2000 Concept portrays Russia as only beginning to gradually recover its economic strength and international weight it lost after the breakup of the USSR. After eight years of booming economic growth, the 2008 Concept portrays Russia as possessing "significant resources in all spheres of human activities" and having "acquired a full-fledged role in global affairs" (Medvedev, 2008, n.p.).

The 2000 Concept speaks disapprovingly yet rather cautiously of the emerging fault lines between Russia and the West. By 2008, Russia was more vocal about its opposition to international trends deemed unfavorable to the country's interests. On the one hand, the Concept commends the post-Cold War environment for overcoming historical prejudices and stereotypes. At the same time, the Concept also notes a growing "civilizational dimension" to contemporary international relations, where the competition is turning to "value systems and development models" (Ibid.). The Concept speculates that it is the prospect of losing their global hegemony that led the West to return to an alleged policy of political and psychological containment of Russia.

Domestic liberalization and relative international normalization came to an end with Medvedev's presidential tenure. In its last half a year, December 2011-May 2012, Russia witnessed a series of the largest anti-governmental rallies in post-Soviet history, sparked by the announcement in September 2011 of Vladimir Putin's wish to run for presidency and widely reported fraud at the parliamentary elections in early December 2011 (Gabowitsch, 2017; Gel'man, 2015, pp. 115-123). Russia's official state identity

narrative was challenged by a multifaceted oppositional identity coalition and affected its self-understanding and self-presentation over the coming years. Russia's ruling elite perceived the crisis as a consequence of the weakening of the state during Medvedev's limited liberalization. Consequently, after Putin's return to presidency in the spring of 2012, Russia's official identity narrative shifted dramatically to cultural repertoires associated with social conservatism and anti-Western illiberalism as central to its construction of the Self and its significant Other. This post-2012 identity turn has impacted Russia's media and digital visions, as discussed in sections on media and strategic communication in this chapter and in the next chapter devoted fully to Russia's internet governance at home and abroad.

2012 – Present: From Sovereign Democracy to Sovereign Morality

Following the illiberal identity pivot under Vladimir Putin's third presidential term, there has been a qualitatively different approach in the regime's internet-related rhetoric, norms, and policies at home and abroad. Domestically, the conservative turn has informed mounting restrictive regulation and practices applied to the online sphere. For example, users have been fined and jailed for posting, sharing, and "liking" information deemed morally inappropriate. Internationally, as Russia's relations with the West reached their lowest point since the end of the Cold War, Russia's long-standing normative emphasis on digital sovereignty has become substantially more assertive.

In response to the protests of 2011-2012 that challenged Russia's official identity, beginning in early 2012 the Kremlin initiated a move toward illiberal traditionalist identity discourse and increasingly autocratic governance (Gel'man, 2015, pp. 123-128; Petrov & Lipman, 2015; Sakwa, 2014, Ch. 7-9). The conservative turn from "sovereign

democracy to sovereign morality" (Sharafutdinova, 2015) was a departure not only from the more liberal-technocratic rhetoric of Medvedev's modernization discourse, but from the trajectory of Russia's post-Soviet identity course altogether. If the proclaimed goal of the Kremlin before 2012 was to rebuild a strong state while drawing on civic cultural repertoires of patriotism, great powerness, statism, and collectivism, after 2012, Russian identity discourse took on distinctly moral, religious, and civilizational dimensions (Makarychev & Medvedev, 2015; Østbø, 2017; Stepanova, 2015).[30]

As part of the general insistence on appreciation of a nation's heritage, the focus on the Russia's own history, identity, and destiny has become one of the core pillars of official identity discourse. For example, Vladimir Putin authored an op-ed "Russia: The National Question" in 2012 (Putin, 2012a) and the following year devoted his keynote address at the meeting of the Valdai Club to Russian identity (Putin, 2013b), while Russia updated its State Strategy on Nationalities Policy for the first time since 1996 (Putin, 2012b). Russia's long-standing commitment to articulating the nation as a community of many ethnicities and cultures united by common history, Russian language, and civic state patriotism has remained unequivocal. Within this accommodating and inclusive rhetorical framework, however, there has been an unprecedented ethno-nationalist emphasis on the ethno-culturally Russian (*russkii*) core of the civic Russian nation and the wider civilizational concept of the Russian World (*Russkii Mir*), which transcends the

---

[30] Three legislative initiatives from 2013-2014 are particularly illustrative of the new identity and policy paradigm: the law banning the propagation of nontraditional sexual relations to minors, the law banning profanity in arts and media, and amendments that harshen punishment for offending religious believers. In passing these laws—all of which apply to online speech—the state and state media discursively delineated heteronormativity, religiosity, and adherence to traditional morality as markers of belonging in the Russian nation, in contrast with the allegedly morally corrupt liberal West.

Russian state borders through Russian language and culture, Orthodoxy, and the diaspora (Blakkisrud, 2015; Laruelle, 2015; Tsygankov, 2014, Ch. 13).

The concept of "sovereignty," which partially lost its primacy during Medvedev's rule, returned to centrality in official discourse and was discursively incorporated into the national identity itself, as Vladimir Putin made clear in his speech at the meeting of the Valdai Club in 2013:

> [T]he desire for independence and sovereignty in spiritual, ideological
> and foreign policy spheres is an integral part of our national character.
> … Russia's sovereignty, independence and territorial integrity are unconditional.
> These are red lines no one is allowed to cross. For all the differences in our
> views, debates about identity and about our national future are impossible unless
> their participants are patriotic. (Putin, 2013b)

Renewed emphasis on sovereignty was institutionalized, for example, in the founding in the upper house of the Russian parliament of the Temporary Committee to Protect State Sovereignty and Prevent Interference in Russia's Internal Affairs (Russian Federation Council, n.d.).

Foreign Policy, 2012 – Present: Political Chilling with the West, Warming with the East

The geopolitical orientation of state-led digital nationalism is reflective of the respective state's construction of the Self and its significant Others in the international system, as well as of the system as such. Since 2012, Russia's foreign policy of the internet, underlain by its national identity narrative, has become more assertive and anti-Western (Legvold, 2016; Tsygankov, 2016, Ch. 8; Zevelev, 2016), while its cooperation in the field of internet governance with the BRICS and China has intensified. This section provides an overview of key rhetorical and policy pillars of Russia's foreign policy after

2012 to contextualize the discussion of its strategic narrative of internet sovereignty in Chapter 4.

Although throughout the 2000s Russian foreign policy discourse increasingly noted emerging fault lines, including civilizational, between Russia and the West, it is only after 2012 that the diplomatic discord was framed explicitly and primarily in civilizational terms. In what is among the most expressive statements of Russia's post-2012 foreign policy rhetoric, Putin in his address at the meeting of the Valdai Club in 2013 drew a direct link between the West's alleged rejection of traditional values and the unipolar world order:

> We can see how many of the Euro-Atlantic countries are actually rejecting their
> roots, including the Christian values that constitute the basis of Western
> civilisation. They are denying moral principles and all traditional identities:
> national, cultural, religious and even sexual. They are implementing policies that
> equate large families with same-sex partnerships, belief in God with the belief
> in Satan.
> … At the same time we see attempts to somehow revive a standardised model
> of a unipolar world and to blur the institutions of international law and national
> sovereignty. Such a unipolar, standardised world does not require sovereign
> states; it requires vassals. In a historical sense this amounts to a rejection of one's
> own identity, of the God-given diversity of the world. (Putin, 2013b)

Illustrative of how quickly and dramatically the Russia-West dynamic deteriorated after 2012, the Concept of Foreign Policy passed in February 2013 to replace the 2008 version adopted under Medvedev was supplanted by the new version already in December 2016 to reflect Russia's much more assertive anti-Western stance. The deterioration of Russia-West relations after 2012 unfolded in several stages. In the first period of 2010-2012, in parallel to Russia-U.S. cooperation under the Reset policy, discord in the Russia-West relations began to re-emerge in their different approaches to

the Arab Spring. While the West supported revolutions across the Middle East as popular democratic uprisings, Russia perceived the events as a continuation of U.S. regime change strategy that undermines national sovereignty and reinforces the unipolar world order. In the second period of 2012-2014, after Russia's identity discourse turned increasingly illiberal under Putin's third presidency, relations took a sharp turn for the worse as the West was openly critical of Russia's new domestic discourse. The third period of 2014-2016 was arguably the single lowest point in the Russia-West relations in the post-Soviet times. Amid the political crisis in Ukraine, which Russia framed as another example of Western meddling in sovereign affairs, Russia annexed the Crimea region of Ukraine in February-March 2014 and has allegedly aided the separatist movement in Eastern Ukraine since that spring. The West, in turn, imposed sanctions on Russian economy and industry, as well as individual sanctions on members of the Russian elite. Anti-Western rhetoric in Russian political discourse reached its peak during this time. The fourth and current period began in mid-late 2016, when Western governments and media accused Russia of influencing elections in the United States, France, Germany, and generally attempting to undermine the liberal world order.

At the same time as Russia's relations with the West plummeted, Moscow's relations with the BRICS, and in particular China, entered a new phase of proximity (Rozman, 2014). For example, in 2015, BRICS countries launched the New Development Bank, a multilateral development bank with a starting capital of $50 billion with 20 percent provided by each member state. The same year, China and Russia signed a major bilateral agreements package of over thirty individual documents that encompass a wide variety of areas of cooperation from economy to cybersecurity. Russian foreign policy

discourse has narrated the country's BRICS and China relations in terms of constructing a multipolar world and challenging the U.S. hegemony—the same rhetoric Russia has relied on in advancing the strategic narrative of internet sovereignty multilaterally through BRICS and bilaterally with China.

3.3 National Media System

As noted in the introduction to this chapter, I view national media and political systems as shaping the contours of specific digital nationalisms. For example, many of the practices that were applied to the internet were first developed and normalized in the realm of the offline media (e.g., top-down censorship, journalistic self-censorship, control through ownership, and others). Whereas the previous section discussed key pivots in Russia's domestic and foreign policy, this and the next section build on that discussion to illuminate how Russia's shifting official self-understanding has impacted its state media policy pertaining to domestic audiences and external strategic communication. The relationship between identity and the media landscape is not causal but contextual: the historically informed identity does not strictly define media systems but broadly delineates discursive possibilities of its development. In the Russian media context, the state has historically played the central role in shaping the Soviet and Russian media landscape (Richter, 2011, p. 201; Vartanova, 2012, p. 122). This section focuses on the relationship between the media sector and the state.

1991-1999: Transition to Capitalism

Privatization of the media sector and retreat of the state as the primary actor in the meaning-making arena were the two key systemic changes that Russia's media sphere underwent in the 1990s (on Russian media in the 1990s, see Belin, 2002; McNair, 2001;

Price et al., 2002). While the digital media in the 1990s played a marginal role in Russia's socio-political life—the first political online media were founded only in the late 1990s—this decade is critical to understanding the Russian media system and therefore the context within which Russia's digital nationalism developed around statist principles in the 2000s-2010s.

The collapse of the Soviet Union in late 1991 saw end of the system of state support of the media sector with the, and news media organizations became fully dependent upon market forces. In the context of a profound socio-economic crisis in Russia in the first half of the 1990s—including a barely existent advertising market, collapse of reliable mail and transportation networks, and a sharp decline in the population's purchasing power—the class of nouveau riche media owners of the country's major media held overwhelming influence upon the national media system. The compendium of conflicting oligarchic interests collectively allowed for a degree of media pluralism unprecedented in Russian history. However, such instrumentalization of journalism throughout the 1990s undermined the fledgling opportunity for the media sector to develop into a democratic civic institution serving the public interest (Roudakova, 2017, especially Ch. 2-3).

The cultural construction of the media as serving special interests took root as a widespread cultural repertoire in Russian society. This allowed the state in the 2000s to force major privately owned mass media outlets under its direct and indirect control, with little resistance from the journalistic community and the public writ large, and in the 2010s to apply these logic and methods to the digital media with equally little opposition. The next section overviews etatization of the Russian media sphere in the 2000s.

2000 – 2012: From Media Oligarchy to Media Statism

The central media development of the 2000s was the state's becoming the ultimate authority over Russia's information space (see Becker, 2004; Beumers et al., 2009; Gehlbach, 2010; Koltsova, 2006; Oates, 2007). The Kremlin framed its increasing authoritarian approach to the media within the broader narrative of establishing a strong, functional, and orderly state after the alleged chaos of the 1990s. In institutionalizing the strong state identity, throughout the 2000s the Kremlin oversaw the creation of a legal and policy framework, as well as a political culture, that made the post-2012 state's offensive on the internet easily implementable by the state and readily accepted by the population. For example, the Kremlin's practice of replacing undesirable media owners with regime loyalists, which was applied to major television, radio, and newspaper outlets in the 2000s, was transferred to internet-related businesses (Pallin, 2017).

The Kremlin outlined its strategic vision for the information space in the Doctrine of Information Security of the Russian Federation in September 2000, the first such document in post-Soviet history (see Carman 2002). The Doctrine guided the state's information policy in the 2000s. The Doctrine's framing of information through the lens of national security and threats to the country and its people was a departure from the Kremlin's substantially more liberal media philosophy of the preceding decade. The Doctrine posits the state as the key producer of cultural knowledge and protector against hypothetical threats to its information sovereignty. The Doctrine, for example, warns against the informational threats to "the spiritual rebirth of Russia" that could come from, among others, "increasing the spiritual, economic, and political dependency of Russia on Western information structures" (Putin, 2000a, n.p.).

In the 2000s the Kremlin's information policy strove for control not over the totality of mass media's political economy and discourse but over select strategic outlets that were influential enough to potentially undermine the very essence of the political and cultural project of the strong state. Thus, since the Kremlin deemed the online environment to not yet possess the kind of socio-political influence that warranted immediate attention, its focus fell primarily on the offline media—first and foremost: television (Oates, 2006). For example, in addition to the historically state-owned RTR television channel, by 2001 the Kremlin already pressured the oligarch owners of NTV and ORT, the only other two television stations with nationwide coverage, to relinquish control to the state-affiliated media groups. The Kremlin then applied the same tactic to print media, as when businesses close to the state acquired some of the most influential national dailies, for example, *Izvestiya* in 2005, *Kommersant* in 2006, and *Komsomolskaya Pravda* in 2007.

Like his presidency overall, the four years of Medvedev's rule left an ambiguous record in terms of the state vis-a-vis the media environment (Jackson, 2016, pp. 362-363; Wilson, 2015, pp. 151-152). There was a degree of symbolic and regulatory media liberalization. For example, in 2009 Medvedev gave his first interview as president to *Novaya Gazeta*, a liberal newspaper traditionally highly critical of Putin's regime, and in 2011 visited the studios of *Dozhd'*, then a newly launched liberal television channel. At the same time, key pillars of the media framework established over the course of Putin's presidency did not change: through its direct and indirect control of the mainstream media, the Kremlin maintained its dominance over the national discourse, while strategically allowing a degree of oppositional rhetoric. The next section addresses the

shift in the state's media policy that followed the turn of identity narrative towards greater statism and its application to the online sphere.

2012 – Present: The State Extends Control Over National Dsicourse

The conservative pivot in Russia's national identity following Vladimir Putin's return to presidency in 2012 manifested itself in the media realm in the furthering of state control over national informational space. The change was not only in the degree of control, but also its kind. The changing official identity narrative altered the limits of the doable and sayable—the type of cultural repertories that could be drawn upon in legitimating political action. For example, as anti-Western sentiments became increasingly salient to Russia's self-presentation, members of parliament advancing a legislative initiative to limit further foreign ownership of Russian media argued that their initiative intended to counter the "informational Cold War" the West was allegedly waging against Russia, in which foreign-owned media might aid the enemy (Zhegulev, 2015).

At least three qualitatively new features of media policy after 2012 as compared to the preceding decade can be observed.

First, media law has become substantially more regulated with a dramatic increase in restrictive regulation related to media and national discourse broadly, including the soaring authority of the Russian government media watchdog Roskomnadzor (DLA Piper et al., 2016; Gorbunova, 2017). Regulation pertained to the political economy of the media sector as well as media content. In line with the overall approach to informational policy since 2000, the end purpose of the latest wave of the restrictive media laws is not total control over national discourse but the spreading of a broad chilling effect, which is

achieved through selective application of each law to a handful of cases meant to serve as a cautionary precedent.

Second, if the Kremlin's informational policy previously pertained largely to overtly political discourse, after the moral turn of 2012, high and quotidian culture also fell under the ambit of the state's concern and regulation. In the 2000s, the state advanced a mildly conservative statist cultural agenda, but it did not identify as a defender of traditional values domestically and the bastion of conservatism internationally. Once this identity vision came to the fore, it informed the media landscape. If previously the state was principally concerned with the media challengers to its *political* project, it now explicitly turned attention to *cultural* discourse as well. The laws regarding, for example, propagation of homosexuality to minors, profanity in arts and media, and offence to religious believers all apply to offline and online media space and serve as some of the examples of this trend.

Third, whereas in the 2000s the state did not actively engage in trying to control online discourse, after 2012 the state turned rhetorical and regulatory attention to the networked public sphere by applying preexisting restrictive laws to online conduct and, for the first time, passed a host of new internet specific laws. The next chapter discusses these developments in detail.

3.4 External Strategic Communication

National media and political systems, this chapter argues, contribute to shaping state-led utilization of digital technologies for advancing its interests, identity, and image, which constitutes digital nationalism. The values underlying each individual state-based digital nationalism are strategically communicated to domestic and foreign audiences

through narratives about the state's digital identity and the global digital order. This section illuminates in particular how national strategic narratives of internet governance are embedded within the logics and rhetoric of the country's strategic communication writ large.

I view national visions of internet governance, such as Russia's advocacy of internet sovereignty, as strategic narratives. After Miskimmon et al. (2013, p. 2), I understand strategic narrative as

> a means for political actors to construct a shared meaning of the past, present, and future of international politics to shape the behavior of domestic and international actors. Strategic narratives are a tool for political actors to extend their influence, manage expectations, and change the discursive environment in which they operate. They are narratives about both states and the system itself, both about who we are and what kind of order we want.

Global internet governance as a compendium of strategic narratives about national digital identities and the global digital order, then, is understood as a geopolitical debate, in which states draw upon national values and interests to strategically communicate normative visions of technological and administrative internet configurations.

The concurrent rise of global strategic communication and Russia's resurgent great power identity since the early 2000s have led Russia to take its international reputation seriously and allocate substantial resources toward creating a multifaceted sector tasked with advancing Russian soft power. This section's tracing of Russia's methodical building up of its strategic communication apparatus in the last decade and a half as a matter of highest-level national vision helps to illuminate Russia's communicative logics and—central to the aims of this dissertation—the roots of Russia's becoming a leading voice in the global internet governance debate. The discussion also

shows how these narratives relate to Russia's changing vision of the Self and its significant Others.

This discussion relies on scholarship on Russian strategic communication and soft power, as well as Russian policy documents and policy discourse that pertain to strategic communication.[31]

1991 – 1999: Post-Cold War Triumphalism and Strategic Communication Hiatus

The Russian state in the 1990s did not undertake a concerted effort to rebuild the collapsed Soviet-era strategic communication apparatus due to ideational and material circumstances. The first factor lay in the particular geopolitical context of the immediate post-Cold War period. Alongside most Western powers, Moscow indulged in the idea that liberal democracy was the final form of governance, and no further global ideological competition would take place. It was therefore widely assumed in Washington and major capitals around the world that the very *raison d'être* for maintaining costly international propaganda infrastructures was largely passé as there was no longer the need to convince non-Western regions of the benefits of liberal democracy and market economy (see, e.g., Cull, 2012).

The second factor was Russia's material weakness. The socio-economic upheaval that accompanied Russia's economic restructuring from socialist to capitalist principles made international image-making low on the list of national priorities. Official rhetoric of the time conveys the government's concern not with Russia's positive perception by the rest of the world but with its very existential perseverance. For example, the 1993 Concept of Foreign policy names economic revival "the key condition for the survival of

---

[31] See Feklyunina, 2008, 2016; Larson and Shevchenko, 2010, 2014; Kiseleva, 2015; Laruelle, 2015; Miskimmon & O'Loughlin, 2017; Rawnsley, 2015; Sergunin & Karabeshkin, 2015; Simons, 2014; Taras, 2014; Wilson, 2015.

the country and the salvation of the nation" (Yeltsin, 2005, p. 38).

Even as Russian identity and foreign policy discourse in the second half of the 1990s became more assertive and showed signs of growing discord between Russia and the West, there was yet no state information policy and tangible initiatives aimed at building infrastructure to communicate Russia's changing self-understanding. In this respect, Vladimir Putin's coming to presidency in 2000 marks the beginning of a new approach to Russia's strategic communication.

2000 – 2008: Rebuilding Strategic Communication Infrastructure

This section traces the logics, rhetoric, and key material steps in the reemergence of modern Russia's strategic communication infrastructure. At least three domestic and international factors shaped the rise of Russia's strategic communication during Putin's two presidential terms. First, the rebirth of U.S. public diplomacy as part of the Global War on Terror following the attacks of 9/11 renewed global competition of national strategic narratives. The geopolitical imperative to tell the world about one's country was supported by the quickly expanding affordances of information and communication technologies. Second, the Russian leadership's political vision began to deviate from that of its Western partners. Russia perceived its story to be intentionally distorted by Western media and wished to gain greater agency in projecting its vision to the outside world. Lastly, due to high economic growth, Russian government was, for the first time, able to allocate sufficient resources toward rebuilding strategic communication activities.

Putin articulated the logic of Russia's strategic communication, which, broadly, has not changed since then, in his first Annual Address to the Federal Assembly in 2000:

> [I]n the conditions of a new type of external aggression – international terrorism
> and the direct attempt to bring this threat into the country – Russia has met with

a systematic challenge to its state sovereignty and territorial integrity, and found

itself face to face with forces that strive towards a geopolitical reorganization

of the world.

Our efforts to save Russia from this danger are often interpreted in a subjective

and biased manner, and serve as the occasion for various types of speculation.

An important area of foreign policy activity should be ensuring objective

perception of Russia. Reliable information on the events in our country is

a question of its reputation and national security.

A response to this and many other challenges are impossible without

strengthening the state. Without this, it is impossible to solve another national

task. And although strengthening the state has for some years been proclaimed

as the goal of Russian policy, we have not moved beyond declarations and empty

talk. (Putin, 2000b)

The passage conveys core pillars of Russia's strategic narrative that also underlie

its internet sovereignty narrative. State sovereignty is proclaimed as the highest

overarching normative ideal. Russian sovereignty and broadly the geopolitical order

based on the principle of sovereignty is said to be threatened by nefarious Others. In this

case, they are international terrorists, but since 2007, the Western sovereign Others,

foremost the United States, would be named as challenging the UN-based order that

Russia favors. Putin alleges that the global media sphere is skewed intentionally against

Russia, as its actions are supposedly reported in a subjective, biased, and speculative

manner. Putin proposes strengthening of the state as the solution to this alleged

misrepresentation. Specifically, this means strengthening Russia's strategic

communication capabilities to ensure its "objective perception" and "reliable

information" abroad. Strategic communication thus is elevated to the status of the highest

state priority.

Strategic policy documents passed in 2000 reflect the new regime's heightened

attention to communication and image. The Doctrine of Information Security is

concerned principally with informational protectionism of the domestic sphere, while the 2000 Foreign Policy Concept introduces external strategic communication as a matter of foreign policy. The Concept's designated section on Information Support for Foreign Policy Activities prescribes several specific goals: (1) objectively and accurately communicating Russia's political stance and actions; (2) informing the outside world of Russia's accomplishments in culture, science, and intellectual pursuits; and (3) shaping a positive perception and a friendly attitude towards Russia (Putin, 2005a). These objectives, the Concept proposes, dictate a pressing need for Russia to develop its own effective apparatus to influence public opinion abroad.

It took several years to begin the implementation of the public diplomacy prescriptions put forth in 2000, but in 2004-2008, Russia eventually undertook an expansive host of initiatives to develop multifaceted strategic communication. The Russian Information Agency "Novosti" (RIAN), successor to the Soviet international broadcasting bureau, was chosen as a platform for resurrecting Russia's global media outreach: a new management team was appointed and funding increased. RIAN established the Valdai International Discussion Club, Russia's main annual political forum that brings together hundreds of top-level Russian and international scholars, pundits, and politicians to discuss contemporary Russian affairs, and features Vladimir Putin as a keynote speaker. In 2005, the Russian Presidency also took under its auspices the Saint Petersburg International Economic Forum (held from 1997). The Forum quickly became another key annual event attended by global political and business elites, which shines the global media spotlight on Russia. In 2005, RIAN oversaw the establishment of Russia Today, an international TV network broadcasting in English (since 2005), Arabic

(since 2007), and Spanish (since 2009). Russia Today's original editorial policy in 2005-2008 centered around telling the world about events *in* Russia, but, starting in 2009, changed to covering international news from the Russian perspective (more on this below). In 2006, Russia signed a contract with the U.S.-based PR firm Ketchum that was tasked with liaising with Western financial and media sectors to attract investment and positive coverage to Russia. In 2007, Russia launched the Russkiy Mir (Russian World) Foundation to promote Russian language and culture abroad, as well as liaise with the Russian diaspora (Klyueva & Mikhaylova, 2017). Led by prominent conservative figures and with close ties to the Russian Orthodox Church, the philosophy of Russkiy Mir is rooted in cultural traditionalism and opposition to Western values—reflecting the growing socially conservative strands of Russian identity toward the end of the decade. In 2007, Russia successfully bid to host the 2014 Sochi Olympic Games.

The vast array of strategic communication initiatives across the entire spectrum of conventional public diplomacy methods—from international broadcasting to sporting mega events—that Russia launched within only a few years conveys the utmost seriousness of the government's approach to how it is perceived in the world and how it wants to propagate its domestic identity. These efforts were further institutionalized and expanded in the following years under President Dmitry Medvedev.

2008 – 2012: Institutionalization and Expansion of Strategic Communication

Under the four-year presidency of Dmitry Medvedev, Russian national identity narrative stayed within the ideational framework of a resurgent great power, though relied on a more liberal and less culturally traditionalist rhetoric. After Russia's global image suffered a major blow in the aftermath of the conflict in Georgia in August 2008,

Russia's external communication strategy focused on further institutionalization and legitimization of strategic communication as an instrument of foreign policy, which this section traces.

Western media's unfavorable coverage of Russia in the course and aftermath of the five-day Russia-Georgia war of August 2008 prompted some Western observers to suggest at the time that Russians "have not yet learned how to play the media game. Their authoritarian government might never do so" (Reynolds, 2008; see also Levy, 2008). Moscow's failure to convey its version of events to international audiences signaled to the Kremlin the need to reinforce and revamp its strategic communication. In fact, the new iteration of the Concept of Foreign Policy introduced several months before the conflict already outlined some of these changes (Medvedev, 2008).

The 2008 Concept introduces the notion of "public diplomacy" (*publichnaya diplomatiya*) as an overarching framework for Russia's strategic communication activities, thus instituting the concept as part of the highest-level foreign policy thinking and lingo. In international communication, the Concept proposes to pursue several paths: (1) promote an "objective" perception of Russia as a democracy with a market economy and an "independent foreign policy"; (2) communicate "full and accurate" information about Russia's stance on major international issues, foreign policy initiatives, and domestic reforms and developments; (3) direct state funds into enhancing Russia's international broadcasting capabilities and thus develop effective means to influence public opinion abroad; and (4) take steps to repel informational threats to Russia's sovereignty and security (Medvedev, 2008).

The Concept advocates a more assertive approach to cultural diplomacy in order to promote the Russian culture's "unique contribution to the cultural and civilizational diversity of the contemporary world and to the development of an intercivilizational partnership" (Medvedev, 2008, n.p.). The Concept reframes Russian diasporic populations from agentless victims in need of protection into subjects that extend the "Russian World" and "partners" in spreading and strengthening Russia's international positions.

Strategic vision for Russia's external communication materialized in a number of major initiatives over the course of Medvedev's presidency. In 2008, Medvedev established *Rossotrudnichestvo* (Federal Agency for the Commonwealth of Independent States, Compatriots Living Abroad and International Humanitarian Cooperation), Russia's first designated public diplomacy agency (Rossotrudnichestvo, n.d.). *Rossotrudnichestvo*'s broad mandate encompasses, for instance, overseeing academic exchanges, diaspora relations, Russian language popularization, sister-cities program, coordination of Russia's regions' cooperation with the world, and targeted humanitarian aid and development programs.

After Russia Today failed to adequately defend the country's position in the Russia-Georgia conflict, its editorial approach underwent a major change. Rebranding itself into RT (akin to the British Petroleum's name change to BP in an attempt to substitute the national connotation with a global one), the channel began to portray Russia's perspective on the world instead of telling the world *about* Russia and its domestic developments. RT's coverage grew increasingly critical of Western liberal

elites. RT expanded its operation by launching Spanish-language broadcasting as RT en Español in 2009 and a U.S.-based RT America in 2010.

Continuing its sport diplomacy effort after winning the right to host Sochi 2014 Olympics, in 2009, Russia successfully bid to host the 2018 FIFA World Cup. In 2010, delivering on the Concept's promise of "support to national nongovernmental organizations interested in promoting Russia's foreign policy interests," the Kremlin established two academic and diplomatic think tanks that would come to serve as the intellectual backbone to Russia's soft power push: Russian International Affairs Council and the Gorchakov Foundation for Public Diplomacy.

2012 – Present: Strategic Communication by "Patriotically Minded People"

The period since 2012, when visions of the global internet clashed resoundingly in December 2012 at the ITU World Conference on International Telecommunications, has been the most contentious in the communicative struggle over global internet governance. Russia's assertive advocacy of internet sovereignty at WCIT-2012 and elsewhere should be viewed as an integral part of its overall turn to more forceful strategic communication.

During Putin's third term, Russian national identity has been characterized by a sharp pivot towards cultural and political anti-liberal conservatism. After Russia's annexation of Crimea in early 2014 and the sanctions that were imposed on Russia thereafter, the Russia-West relations have reached their lowest point since the end of the Cold War. Official identity discourse reflected in political speech and strategic documents passed since 2012—the 2016 Doctrine of Information Security (Putin, 2016b), the 2013 (Putin, 2013a) and 2016 (Putin, 2016a) Concepts of the Foreign Policy, and the

2015 National Security Strategy (Putin, 2015)—reaffirms the need for Russia to promote

its vision to foreign audiences and defend its own society from informational hostility

allegedly aimed at Russia from abroad.

The proposed methods for Russia's strategic communication have remained

largely unchanged, but the framing of their purpose shifted from the language of raising

Russia's geopolitical status and striving for positive perception in the 2000s to portraying

strategic communication in the context of clashing civilizational values after 2012. For

example, during his 2013 visit to RT headquarters in Moscow, Vladimir Putin noted that

RT was created in 2005 as "a player that wouldn't just provide an unbiased coverage

of the events in Russia but also … try to break the Anglo-Saxon monopoly on the global

information streams" (President of Russia, 2013).

Putin's remark the same month, voiced at the annual end-of-year news

conference, suggested that "there should be patriotically minded people at the head

of state information resources, people who uphold the interests of the Russian

Federation" (Putin, 2013c), signaling a wholesale restructuring of the international

broadcasting infrastructure in order to align it institutionally and ideationally with the

post-2012 identity narrative of traditionalist statism. Russian Information Agency

"Novosti" (RIAN)—a key node of Russia's public diplomacy infrastructure through the

hosting of RT and Valdai Club—was restructured into the International Information

Agency Rossiya Segodnya.[32] After its initial post-Soviet revamping in 2004 and until

2014, RIAN had come to represent a measured voice among state-owned outlets amid the

increasingly uncritical coverage—a stance no longer tolerable within the post-2012

---

[32] Rossiaya Segodnya translates from Russian as Russia Today. The agency should not be confused with
RT, the television network formerly known as Russia Today and, since the restructuring of 2013-2014, part
of Rossiya Segodnya.

conservative paradigm. The RIAN reform saw the merger of the information agency itself, the RT channel, and the Voice of Russia radio broadcaster in early 2014. Rossiya Segodnya united all of Russia's international broadcasting outlets, except RT, under a new brand, Sputnik News.

Both political-economically and ideologically, the new international broadcasting behemoth of Rossiya Segodnya fits into Putin Russia's practice of creating state-owned national champions infused with the mythology of national identity, prosperity, and stability (Backes, 2014). Within just several years of existence, *Sputnik News* expanded its operations to include news wires, websites, and radio programming in nearly forty languages targeting dozens of countries. Now under the umbrella of Rossiya Segodnya, RT also continued its expansion with the launch after 2014 of RT UK, a designated UK-oriented television channel with an office in London, RT Deutsch, a German-language news website, and the French-language RT France channel based in Paris. Sputnik News' and RT's editorial stance, which often relies on intentional distortions and conspiracy theories (Yablokov, 2015), is derisive of Western liberal establishment and world order.

The openly anti-Western narrative of Russia's strategic communication since 2012, and especially since 2014, has attracted much criticism from Western media and governments (France24, 2017; Jackson, 2015; Wilson, 2017). Russian leadership, in turn, has interpreted Western hostility towards its strategic communication as further evidence of the alleged civilizational strategy of containing Russia. The 2016 Doctrine of Information Security, for example, states:

> One can observe a trend towards an increased volume of biased coverage of
> Russia's state policy in Western mass media.

Russian mass media abroad are often being openly discriminated against, [while] Russian journalists are made to face obstacles in carrying out their professional duties.

There is a growing informational pressure on the Russian population, foremost the youth, with the goal to dilute traditional Russian spiritual and moral values. (Putin, 2016b)

3.5 Conclusion

The state's digital vision is entangled with the logics and trajectories of its national media and political systems. Accordingly, this chapter investigated the relationship between Russian national identity, Russian domestic media environment, and Russian external strategic communication—divided into the three respective sections—since the inauguration of modern Russian independence in December 1991 and until the present. In line with the dissertation's cultural studies approach, I examined the discourse of the actors through analysis of key policy documents and political statements, as well as tracing the logics of institutional and infrastructural changes in these domains.

The logics of Russian political and media developments can be analytically divided into three terms: 1991-1999, 2000-2012, and from 2012 until the present. In the 1990s, under the presidency of Boris Yeltsin, Russian identity was predominantly liberal, though incorporated statist elements in the second half of the decade. Accordingly, in foreign policy, Russia at first imagined itself as part of the liberal-democratic West but grew increasingly disillusioned with what it perceived as lack of equal treatment and respect from its Western Significant Others. In the domestic media environment, the new class of oligarchic capitalists that emerged under market economy came to own the country's key mass media outlets that reflected their private interests and worldviews. Taken together, however, this provided a healthy degree of media pluralism in the

absence of systemic state censorship. As per external strategic communication, Russia's pro-Western identity and lack of resources meant that reputation management was not yet among the foreign policy priorities.

In the long 2000s decade that encompassed two presidential terms of Vladimir Putin (2000-2008) and one term of Dmitry Medvedev (2008-2012), Russia's identity centered around the notion of rebuilding the strong state after its economic and institutional weakening in the 1990s. Under Putin, this project drew on the cultural tropes of patriotism, great powerness, statism, and social solidarity. Under Medvedev, the key trope was modernization through technological innovation. Despite somewhat differing rhetoric, the proposed goal of both was strengthening Russia's sovereignty—a notion that in the 2000s came to the fore of political imaginary and discourse to propagate Russia as an assertive and self-sufficient great power.

This period was one of steadily shrinking media freedoms as the state methodically purged non-loyal voices from the public sphere. The ultimate goal of state media policy was not total control of the national discourse, but informational hegemony and marginalization of oppositional voices. The online public sphere remained largely outside of the state's concern as the internet's dissemination was still significantly lower compared to offline media and the state considered the online environment to not possess significant political weight.

In foreign policy, after a brief period of rapprochement and cooperation following 9/11, tensions with the West grew over what Russia perceived as continued misrepresentation of and disrespect toward its sovereign politics. To correct the allegedly biased coverage of Russia, the Kremlin instituted strategic communication within

Russia's foreign policy documents and discourse. Russia rebuilt, virtually from scratch, a vast strategic communication infrastructure encompassing various strands of international broadcasting and public diplomacy.

Russian official identity narrative since 2012 has taken a sharp turn toward illiberal traditionalist conservatism, which has informed changes in the country's domestic and foreign policy. The state rearticulated its role vis-à-vis society from the arbiter of the political domain to the ultimate moral authority. The Kremlin used the notion of protecting traditional cultural values (such as, for example, heteronormativity and religious beliefs) to rationalize a new restrictive legal framework pertaining to the national discourse. Mainstream media, almost all of which were already directly and indirectly controlled by the state prior to 2012, followed the state's conservative turn in their rhetoric, while several prominent remaining critical outlets were brought under state control through various mechanisms.

Relations between Russia and the West in the period since 2012 have reached their lowest point in the post-Cold War period over the Ukrainian crisis and the Syria War. Russian foreign policy discourse adopted traditionalist rhetoric. The normative narrative of a multipolar world, central to Russian foreign policy discourse since the late 1990s, assumed a civilizational dimension: global political competition began to be explained increasingly not through the language of rational interests but that of a clash of identities. In this competition, Russia has articulated its Self as the defender of traditional European values, while the liberal West as morally corrupt. To propagate its new identity, Russia has reinforced its strategic communication effort both in terms of infrastructure and the anti-Western sentiment.

The post-2012 identity turn has had a major impact on Russian domestic and foreign internet governance. The Russian state explicitly turned its regulatory and rhetorical attention to cyberspace in an effort to attain similar influence over the online discourse that it had successfully imposed over the offline media discourse in the 2000s. In global internet governance, in the context of direct confrontation with the West, the centrality of the notion of sovereignty to Russia's identity discourse has translated into Russia definitively establishing itself as a leading proponent, alongside China, of the internet sovereignty narrative.

The chapter can be understood analytically on at least three levels.

At the first analytical level, each of the chapter's sections—National Identity, National Media System, and External Strategic Communication—on its own illustrates a contained theoretical argument pertaining to the respective social domain. National Identity shows, first, how official identity draws on historically grounded cultural repertoires existing within national discourse and, second, how the dominant domestic identity institutionalized by the state informs national foreign policy. The section on National Media System illustrates the relationship between the media sector and the state, in which the latter increasingly asserts its role as the preeminent meaning-maker. The section on Strategic Communication illustrates how, since the early 2000s, concern of national governments over how they are perceived globally and ensuing strategies of reputation management have been increasingly incorporated into national foreign policies and, by extension, global politics.

At the second analytical level, the chapter can be read as a conversation between its three sections. National Identity outlines the evolution of Russia's self-understanding

after 1991 and then illustrates how these developments have informed, first, its domestic media environment (National Media System) and, second, its foreign media policy (External Strategic Communication). Drawing on the discussion of the Russian state's pursuit of the identity of a strong state and a great power in the National Identity section, the National Media System section emphasized how these changes in the official identity narrative have impacted Russia's media environment. Drawing on the National Identity section's discussion of Russia's relations with its historic Western Oher after 1991, the External Strategic Communication section illustrated how post-Soviet Russia's foreign policy trajectory—from enthused embrace of Western liberalism in the early 1990s to extreme anti-Western illiberalism since 2012—has informed the organizational structure and messaging of its external strategic communication.

At the third level, this chapter is a prelude to the next chapter's discussion of the internet-specific developments in Russia's domestic and global affairs as it grounds the next chapter's discussion of internet-related discourse and policy within respective socio-historical circumstances. In conjunction, this and the following chapters, then, illustrate how national identity narratives underlie national digital visions, which is the core proposition of digital nationalism as an analytical lens.

Chapter 4: A Digital Sovereign: Russia's Internet Governance at Home and Abroad

4.1 Introduction

In August 2017, *The Guardian* reported that after thirteen years of negotiations aimed at forging an international legal framework governing cybersecurity, a "[d]ispute along cold war lines led to collapse of UN cyberwarfare talks" (Bowcott, 2017). The central disagreement among national delegates at the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security unraveled around the notion of the right to self-defense against cyberattacks. Western states supported the legal adoption of this clause. A few other states, reportedly including Russia, China, and Cuba, counter-argued that the introduction of the right to self-defense would legitimize the use of force by states claiming to be victims of a cyberattack. The dispute ended in a stalemate.

In their analysis of the UN incident, "International Cyber Law Politicized," cybersecurity experts Michael Schmitt and Liis Vihul hypothesize that Russia, China, and Cuba "perhaps … want to avoid the perception that 'the West' gets to dictate the rules of the game for cyberspace" and propose that the situation "may reflect the current dismal state of relations outside the cyber realm" (Schmitt & Vihul, 2017).

The UN episode and its diagnosis reveal several themes with which this dissertation is centrally concerned in line with its three pillars of identity, strategic communication, and global internet governance. First, there is a contentious debate at the highest level of international diplomacy surrounding the "rules of the game for cyberspace," or global internet governance. Second, the countries' normative positions on

cyberspace reflect politics *outside* of the cyber realm that relate to their respective

identity narratives. Third, countries care about the *perception* of their actions in global

politics to the extent that it informs their behavior and policy in international relations,

highlighting the critical role that strategic communication and national image have come

to play in global politics. This attention to the reputational side of informational

geopolitics is partly due to the fact that mainstream media now routinely cover the

intricacies of internet governance.

These circumstances at the intersection of identity, strategic communication, and

global internet governance offer an entry point into this chapter, which examines the

logics and language of Russia's digital nationalism—state-based engagement with digital

technologies meant to advance its material conditions at home and great power identity

internationally. Drawing on the discussion in Chapter 3 of the trajectories of Russia's

official identity discourse and strategic communication since 1991, the chapter addresses

the central question of this dissertation about the relationship between national identity

and digital communication technologies by investigating Russia's participation in the

domain of global internet governance. This chapter illuminates the reiterative global-

national dynamic underlying digital nationalism by examining Russia's strategic

narrative of internet sovereignty in the field of global internet governance.

Organization of the Chapter

The chapter is divided into two main sections. The first section, Constructing

Runet, addresses how Russia's identity has shaped its social construction of and policy

engagement with the internet domestically. The second section, Championing Internet

Sovereignty, focuses on Russia's international advocacy of the notion of internet

sovereignty by examining the institutionalization of its internet diplomacy and key themes of its strategic narrative—and how these developments relate to Russia's self-identification.

The distinction in the discussion between Russia's domestic and foreign governance of the internet is analytical rather than practical, as most issues pertaining to digital communication technologies operate at both national and global levels at once. For example, Russian data localization laws, which prescribe that foreign online services store personal data of Russian citizens on servers within Russia's territorial borders, directly implicate domestic and foreign companies and politics. While the law was part of Russia's domestic move toward increasingly restrictive online regulation and passed by the national parliament, it resulted in the blocking of access in Russia to the U.S.-based service LinkedIn.

This chapter should necessarily be read in conjunction with the previous chapter's detailing of Russia's post-Soviet identity and media trajectories. While the *previous* chapter addresses Russia's identity and media policy without touching deeply on the internet-related developments, *this* chapter only briefly reminds the reader of pivotal moments in Russia's national identity discourse and foreign policy, but otherwise focuses almost exclusively on internet-related issues. This proposed analytical juxtaposition follows the interpretive theoretical-methodological underpinning of this dissertation, which views culture (i.e., identity discourse) as forming the constitutive context for socio-political institutions and processes (i.e., digital governance).

The two sections within this chapter about Russia's domestic and global internet governance should also be read in relation to each other in line with the dissertation's

approach that views domestic identity as informing foreign policy. This approach does

not suggest that Russia's internal and external construction and communication of

internet governance are identical in their rhetoric and dynamic, but that the two realms

are mutually constitutive and operate according to the overarching national identity logic.

Method and Data

The primary method used in this chapter is textual analysis of materials that

reflect official Russian understanding of the purpose of the internet and its governance in

relation to the Russian nation and the global political order. Most materials were located

at the websites of the Russian Presidency, Government, Ministry of Digital Development,

Communications and Mass Media, Ministry of Foreign Affairs, and the Security

Council.[33] Relying on secondary literature and my own early exploratory research, I

determined these bodies to be most immediately involved in the discursive and

institutional construction of Russia's internet governance.

The types of texts under analysis include chiefly transcripts of internet-related

events with official participation (e.g., Internet Entrepreneurship in Russia Forum), media

articles and interviews by representatives of the state in state and non-state media (this

function at the websites of official bodies allows to account for officials' media

appearances without the need to search individual media outlets), officials' addresses at

international events (e.g., address of a Deputy Minister of Telecom and Mass

Communications at the opening ceremony of the 2014 Internet Governance Forum;

similar to media appearances, this function allows to account for most texts presented by

---

[33] Illustrative of the increasing integration of digital technologies into official state discourse and vision that this dissertation is centrally concerned with, in May 2018 Russia's Ministry of Telecom and Mass Communications was restructured and renamed into the Ministry of Digital Development, Communications and Mass Media. To refer to the Ministry and its head prior to May 2018, I use the shorthand Ministry/Minister of Telecom.

Russian officials at global internet governance fora, such as UN and ITU conferences, Internet Governance Forum, WSIS, Netmundial, ICANN conferences), ministerial annual reports of their activities, and relevant strategic-level policy documents (e.g., Doctrine of Information Security, Strategy of Information Society Development).

Specific materials were located through search at the websites of official bodies for relevant keywords (e.g., "internet," "digital" – in Russian) and/or exploration of relevant website sections in full (e.g., a section on "Participation in International Organizations" at the website of the Ministry of Digital Development). Overall, close to 120 items were located and surveyed through systematic analysis of said websites. Up to 30 other items were located through secondary literature and primary materials. For example, if an annual ministerial report pointed to an event and/or initiative that previously was not located but was deemed relevant, I added this item to the corpus of texts under analysis.

Statistics on Russia's digital sector are widely available from official and analytical sources. On its website, the Ministry of Digital Development provides information on several key indicators of digital development since 2004 (e.g., the number of broadband subscriptions per 100 people by Russian regions, the volume of communication traffic, see Russian Ministry of Digital Development, 2018). The Federal State Statistics Service provides varied statistics in a designated section on Science, Innovation, and Information Society (Russian Federal State Statistics Service, n.d.-b). This includes, for example, a joint report of over 300 pages by the Ministry of Digital Development, the State Statistics Service, and Higher School of Economics, *Information Society in the Russian Federation*, with highly detailed internet and telecommunications

statistics for 2014-2017 (Laikam, 2017). Illustrative of how geopolitical and ideational coalitions pertain to digital statistics, since 2010 BRICS countries have been publishing joint annual statistical reports, which include a section on Information and Communication Technology (Russian Federal State Statistical Service, n.d.-a). Numerous internet-related indictors (e.g., the proportion of internet-connected libraries among all libraries) are available at the Integrated Interdepartmental Informational-Statistical System, a government-run multi-sectoral database that is searchable online (Russian Ministry of Digital Development & Russian Federal State Statistics Service). Data on Russian internet is additionally available from Russian and foreign private research and polling firms (e.g., GfK, 2018; Russian Association of Electronic Communication, n.d.). Lastly, scholarly research and writing serve as another sources of data (e.g., Vartanova, 2016).

The Russian-language websites of federal bodies (e.g., Presidency, Government, ministries, legislature) are detailed, up to date, well-structured, searchable, and easy to navigate, and offer a full range of materials pertaining to the respective body's activities (e.g., strategies, transcripts of meetings, news, media appearances of representatives). This kind of transparency and availability is in line with the imperative of the Russian state's e-government program and is itself illustrative of how the state has come to view digital technologies as integral to advancing its agenda and communication with the domestic public.

The English-language versions of official websites vary in their content. For example, the Russian- and English-language versions of the websites of the Presidency and the Government offer similar content in that full English translations are available for

most Russian content, while the minority of content is only partially translated or unavailable in English. The English version of the website of the Ministry of Digital Development, on the other hand, has not been updated since 2015, while the website of the Russian Security Council only has a Russian-language version. Given the discrepancy between Russian- and English-language versions of official websites and in order to consult documents in their original language, I used materials in Russian and, where available, provide here links their official translations or, if those were unavailable, translate them into English myself.

4.2 Constructing *Runet*

1991-1999: Encountering Runet

Despite the prowess of the Soviet Union's scientific-technological complex, the Soviet regime never developed a homegrown computer industry and network (Gerovitch, 2002, 2008; Peters, 2016; Strukov, 2014, pp. 11-21; Wilson, 2009). The genesis of the Russian internet can be situated in 1990, when employees of an academic research institute incorporated the first private computer network, linked it to the global internet via Helsinki, and registered the Soviet Union's country code top-level domain, *.su* (Asmolov & Kolozaridi, 2017, p. 65; Konradova & Schmidt, 2014, p. 39). In 1994, Russia's national domain registry introduced the country code top-level domain *.ru*, marking the birth of what came to be referred almost exclusively as *Runet*, the Russian segment of the internet.[34] Between the late 1980s and late 1990s, the internet in Russian

---

[34] *Runet* is sometimes understood as including all Russian-language online activity, incorporating online activity inside Russia, by Russian-speaking populations in Russia's neighborhood, and by diasporic Russian-speakers abroad (e.g., Germany, Israel, United States). For my purposes, I understand *Runet* as any internet-related activity pertaining to the Russian socio-political context. This activity largely encompasses websites registered at .su, .ru, and .рф (the Cyrillic .rf domain launched in 2010). However, it also includes

spread from the academic-scientific community to the wider society but was still limited

largely to the capital-based, upper middle-class stratum (Asmolov & Kolozaridi, 2017, p.

65-69; Bulashova et al. 2012; Perfiliev, 2002).

Table 1. Internet use in Russia, 1995-2016.

Year	1995	2000	'02	'04	'06	'08	'10	'12	'14	'16
Individual using the internet (% of pop.)	0.15	1.98	4.13	12.86	18.02	26.83	43	63.8	70.52	76.41
Fixed broadband subscriptions (per 100 people)	N/A	N/A	0.01	0.47	2.02	6.46	10.9	14.6	17.5	19.47

Source: World Bank (International Telecommunication Union, World Telecommunication/ICT
Development Report and database).[35]

The Russian state's relationship with the internet in the 1990s reflected the

internal tensions between identity narratives of Russia as an aspiring Western-style

liberal market democracy and a historically statist great power that saw its interests

increasingly diverge with those of the West. The two positions were articulated and

enacted by various institutions within the Russian political system. On one hand, the state

pursued a hands-off approach towards the internet aligned with its overall laissez-faire

media policy (Ellis, 1999, Ch. 5). On the other hand, some elements within the state

---

foreign domains and their activities that explicitly pertain to the Russian socio-political context. For
example, I do not incorporate into analysis the Russian-language version of Latvia's leading media outlet
Delfi (http://rus.delfi.lv), which addresses local Latvian issues and targets the Latvian Russian-speaking
minority, but I do incorporate one of Russia's leading liberal news outlets Meduza (http://meduza.io),
which is registered as a media organization and physically located in Latvia, but which is run by some
leading Russian journalists and focuses on Russian issues and audiences.

[35] I draw this statistical information from the World Bank, which provides information from the
International Telecommunication Union's annual World Telecommunication/ICT Development Report and
database for free that is otherwise only available for purchase. The ITU database serves as official UN data
on telecommunications and is arguably among the world's most authoritative sources of statistical
information on the sector. The World Bank's website makes this information easily searchable over several
decades and allows for easy cross-country and/or region comparison. For these reasons, I deem this
statistical source as pertinent for my purposes.

system exhibited early "interest in defining, dividing and controlling a corner of Russian cyberspace" (Rohozinski, 1999, p. 24). For example, representatives of the Russian intelligence services in 1997 warned parliamentarians that the developed countries, first and foremost the United States, were working against Russia by means of ICT and suggested that Russia should build a closed governmental intranet impenetrable to adversaries, as well as introduce some online restrictions for the general public (Kondratyev, 1996; Neskromny, 1997).

The country's executive branch largely did not act upon propositions to impose heavy-handed restrictions upon online activities due to the Russian state's liberal self-identification at the time. A notable exception to this approach was the System for Operation-Investigative Activities (SORM), a system of telecommunications surveillance introduced in 1995 that provided the Federal Security Service (FSB) with access to users' communication (Soldatov & Borogan, 2015, Ch. 4; Strukov, 2009, p. 214). Internet service providers were made to install costly devices provided by the FSB that essentially created a backdoor for the intelligence service to access users' personal data. An updated SORM-2 in 1998 expanded the system's surveillance capabilities. After Vladimir Putin's coming to power in 2000, a new state order allowed the FSB to access personal data *without* informing internet service providers about the specific targets prior to carrying out surveillance—signaling a new phase in Russia's self-identification, in which the balance in the state-individual relations increasingly tilted in favor of the former.

Another illustrative example of Russia's changing self-identification is the state's relations with the civil society in the context of the internet, in which the state grew increasingly uncomfortable with what it perceived as interference into its sovereign

167

affairs. Foreign civil society organizations—activities which, in the 1990s, were often

rooted in the deterministic teleological belief that technological progress would foster

democratic change—were instrumental in the early development of Russia's

technological infrastructure (Bulashova et al., 2012; Graham, 2006, Ch. 22; Konradova &

Schmidt, 2014, p. 38-41). Among the most consequential such initiatives for the

development of *Runet* was George Soros' Open Society Foundation's $100-million

program that established 33 university-based internet-connected computer centers in

1996-2001 (Peterson, 2005, pp. 70-71; Rohozinski, 1999, pp. 10-11; Strukov, 2014, p.

22). Russia's official stance toward Soros-funded activities in the country has changed

dramatically over the course of three decades in line with Russia's changing self-

identification: from state collaboration and endorsement in the 1990s, to growing

criticism for alleged interference in Russia's internal affairs in the 2000s, and finally to

banning Soros' foundations for their purported threat to the state's constitutional order

and security in the 2010s.[36]

---

[36] George Soros' organizations cumulatively spent around a billion dollars on support for Soviet/Russia's intellectual and civic life in 1987-2003, which was in a dire state, due to economic hardships. In the 1990s, the country's highest-level leadership—including President Yeltsin, Prime Minister Chernomyrdin, and the State Duma—publicly defended Soros' philanthropic work from vocal criticism of oppositional conservative identity coalitions, whose ranks included such prominent figures as the Nobel Laureate writer Alexander Solzhenitsyn, and who viewed Soros' advancement of Western liberal-democratic and market principles as undermining traditional Russian values (Chernykh & Polous, 2015; Soyfer, 2015). With the shifting of Russian official identity discourse toward increasing statism and anti-liberalism beginning in the early 2000s, officials more often began to frame foreign aid to Russian organizations as ideologically-driven interference in the country's sovereign affairs. For example, Viktor Chernomyrdin, who, as a Prime Minister in the 1990s, co-sponsored Soros' internetization initiative and personally refuted Soros' critics, chastised Soros in his new role as an Ambassador to Ukraine in 2004: "He is… a marauder! Where his billions come from, we roughly know. But who gave him this right [to comment on everything and evaluate everyone]? Or did he grant himself the right to meddle in everything?" (Rudenko, 2004). Another decade later, when Russian identity as a champion of traditional Christian European values was in a self-described civilizational conflict with the liberal West, the Russian Prosecutor General's office banned the Open Society Foundations and the OSI Assistance Foundation as "undesired organizations" that allegedly posed "a threat to the foundations of the constitutional system of the Russian Federation and the security of the state" (Russian Prosecutor General's Office, 2015).

The Russian state's limited engagement with the internet throughout the 1990s was in large part because of the internet's then minimal dissemination due to the population's low financial resources, and therefore marginal significance in Russia's socio-political life. As this section argues, however, the logic of this approach to internet governance should also be understood in relation to Russia's then rather liberal self-identification, in particular with regards to freedom of expression and media policy. While most countries in the 1990s practiced a relatively lax approach to the internet as governments were only beginning to grapple with legislative implications of the new digital technology, examples of China's and Vietnam's early restrictive online controls show that different approaches to the internet were possible from the beginning.

At the same time, calls for greater state involvement with the internet from members of the intelligence community and some ministers, as well as the adoption of an electronic surveillance system by the Federal Security Service, indicate that the statist cultural repertoires, which privilege state interests over individual rights, still held potency within Russia's political imaginary. Over the course of the following decade, the trend toward increasingly statist self-identification would coincide with the global trend toward institutionalization of internet governance within the political system.

2000 – 2008: A Normal Digital Power

During Vladimir Putin's first two presidential terms, the internet in Russia evolved from a marginal elite medium into a networked communication platform used by over a quarter of the population. Russia's identity discourse in the same period transformed from substantially liberal with statist elements in the late 1990s to predominantly statist with some cultural repertoires of liberalism. The concept of

sovereignty rose to prominence within identity and political discourse to signify Russia's reassertion of the self as a normal great power, in which state institutions were to be consolidated after their weakening in the 1990s and which were to reassert its role as an important geopolitical actor (Tsygankov, 2005).

The Kremlin saw media and communication as central to the task of institutionalizing its understanding of sovereignty. Several months into Vladimir Putin's presidency in 2000, Russia adopted the Doctrine of Information Security, the first comprehensive information strategy in its post-Soviet history, which outlined Russia's vision of information sovereignty that has guided its information policy since. Reflecting a newly statist identity discourse, the Doctrine clearly indicates the state's vision of the information sphere as crucial to the production of national identity and the state as the primary actor in the realm of meaning-making (Carman, 2002). Following this new approach, key offline media outlets came under the influence of the state by the end of Putin's second term (Gehlbach, 2010; Oates, 2007).

While the state's influence over television, print, and radio grew, the online sphere developed relatively autonomously in the same period. Though a few short-lived state-linked initiatives were launched to challenge the oppositional narrative online and high-level state officials occasionally spoke in favor of stricter state control over the internet, no concerted effort was undertaken to substantially limit online freedoms or take over the online economy (Deibert & Rohozinski, 2010). I propose that the difference between the state's approach to offline and online media for much of the 2000s should be viewed not as a deviation from Russia's identity vision of a normal great power, but rather as a tactic pursued for at least several reasons.

The internet's development at this stage in no way conflicted with Russia's official identity discourse of a normal great power and, arguably, only bolstered it precisely because of the state's liberal approach to internet governance. First, even though access to the internet grew from under two to over twenty-five percent of the population in 2000-2008, it remained quantitatively a secondary source of news and public debates. The internet thus posed a comparatively limited potential threat to the regime as an alternative space of meaning-making. Second, whereas some scholars attribute a democratizing potential that is conducive to fostering anti-authoritarian dissent to the internet, the specific circumstances of the internet's dissemination in Russia in the 2000s were not necessarily prone to igniting anti-regime opposition. This is because the first eight years of Putin's presidency, during which the percent of internet penetration grew by hundreds annually, saw unprecedented economic growth in Russia's post-Soviet years, thereby maintaining Putin's popularity at a consistently high level. Thirdly, those dissenting publics across the political spectrum that *were* actively using the internet for online communication failed to transfer their online activity into any meaningful offline action (Fossato et al., 2008). Fourth, as until the end of Putin's second term Russia was communicating to foreign audiences an image of a normal great power rather than a major challenger to the existing system, the Russian leadership employed genuine freedoms enjoyed in *Runet* as a rhetorical resource in support of its self-presentation as a normal power. For example, at the Q&A session during Putin's official visit to the Netherlands, a journalist asked Putin whether he thought it was "necessary to support democratic establishments and independent mass media"; Putin was able to reply:

> Let me remind you that in Russia today more than three thousand radio
> and broadcasting corporations, along with more than 47 thousand printing houses

are functioning. Internet is developing very quickly and absolutely freely,

something which causes certain problems and raises certain issues, and I think

not only in our country, but also in western European countries. But despite these

questions, Russia is not undertaking any steps to restrict the freedom

of the Internet. (Putin, 2005c)

While refraining from overtly regulating the internet at this stage, Russia's digital

nationalism took root through a number of early steps toward discursive and institutional

nationalization of *Runet*. Russia adopted several major national strategies pertaining to

various aspects of internet development: for example, e-government strategy Electronic

Russia 2002-2010 (Russian Government, 2014a), the Development in Russian Federation

of High Technology Parks (Russian Government, 2014b), and the first Strategy of

Information Society Development (Putin, 2008). Russia cooperated with various

international organizations on the internet development and was in early talks with the

Internet Corporation for Assigned Names and Numbers about creating a Cyrillic country

code top-level domain name (Twomey, 2007).

These early efforts are important to note here, since much academic and media

discourse has contrasted Dmitry Medvedev's enthusiastic embrace of the internet during

his presidency in 2008-2012 (see below) with the seemingly minimal engagement with

the internet during Putin's first two terms (2000-2008) and overtly restrictive approach

during Putin's third term (2012-2018). This framing, however, obscures continuity in

Russia's digital nationalism beginning from the early 2000s, which has been consistent

with the state's view of digital technology as serving the national purpose at home and

abroad. For example, the 2008 Strategy of Information Society Development, adopted

toward the very end of Putin's second presidential term, states that one of the goals

information and communication technologies should serve is the "preservation of the

culture of the multiethnic Russian nation, strengthening of moral and patriotic principles within the public consciousness, development of the system of cultural and humanitarian education" (Putin, 2008).

2008 – 2012: A Modernizing Digital Power

Official domestic and foreign policy discourse during Dmitry Medvedev's single-term presidency is associated with the notion of modernization, a term popularized by Medvedev that connoted an innovative overhaul of Russia's economy and society, with reliance on the latest technological solutions (Black, 2012; Freire & Simão, 2015; Wilson, 2015). In contrast with Putin, who famously does not personally use the internet, then President Medvedev started a video blog and a Twitter account, visited Silicon Valley on his official trip to the United States in 2010, oversaw the establishment of the preeminent techno park Skolkovo outside of Moscow, and overall boasted an image of a technophile and a champion of Russia's ICT modernization. While Medvedev's personal habits contributed to elevating the significance of the internet within Russia's official discourse and policy, this vector remained embedded firmly within the broader ideational framework of Russia's self-identification as a resurgent sovereign great power set in the early 2000s – modernization of the economy and society with reliance on digital technologies was meant to bolster Russia's strong state identity.

In the several years of Medvedev's presidency, internet uptake in Russia more than doubled to reach over sixty percent, and the internet definitively entered the country's socio-political life. For example, in May 2012 it was reported that the daily audience of *Runet*'s most popular online news aggregator, Yandex.News, exceeded for the first time the audience of any one television network (BBC News, 2012). Medvedev's

presidency illustrates well this dissertation's understanding of the dynamic between individual agency and ideational structures in the operation of digital nationalism. The discursive and policy options of statesmen are limited by the preexisting understandings of the nation and its place in the world that is only partially malleable in the short-term, such as a single presidential term. At the same time, within the given cultural and ideational framework, a country's leader and other high-level officials may choose their own tactics. The overarching goal of re-building a sovereign great power in Russia remained intact between Putin's and Medvedev's presidency, but Medvedev's circle was more proactively and explicitly engaged with digital technologies in conducting this project. Russia's digital nationalism under Medvedev developed along the lines of further institutionalization, intensification of the public-private relations with the internet industry, and globalization of Russia's growing digital prowess.

In line with both the global trend toward greater institutionalization of digital governance within traditional national political apparatuses and Russia's internal logic of technological modernization as key to bolstering sovereignty, Russia at this time implemented a number of steps to further integrate digital technologies into the project of constructing and communication an identity of a great digital power. For example, in 2010 Russia passed a new strategy of Information Society for the period of 2011-2020, established the Presidential Council for Modernization and Technological Development of Russian Economy and Council for Information Society Development in 2009, and became a co-founder of the public-private Russian Internet Governance Forum, the Russian branch of the UN Internet Governance Forum, held since 2010.

While the state's engagement with digital technologies grew in breadth and depth under Medvedev, there was fundamental continuity in the cultural construction of the internet and its governance with the previous years. For example, in addressing the 2009 Russian Internet Forum for the second year in a row—itself a sign of unprecedented engagement by the country's leadership with the internet—Medvedev restated the core pillars of Russia's view of the internet:

> The Internet should not be an environment dominated by rules set by one country alone, even the strongest and most advanced country. There should be international rules drawn up through collective effort, and the worldwide web should continue to develop as it has done so far – as a common environment. Only this way can we counter terrorism, xenophobia, and other unlawful activity on the Web. Finally, only through collective agreements can we protect copyright. (Medvedev, 2009b)[37]

This passage communicates several key repertoires underlying Russia's digital identity. First, Russia's opposition to the alleged U.S. dominance over internet governance. Based on its advocacy of state sovereignty as the foundational principle of international relations and international law, Medvedev proposes an alternative of bringing the internet under the ambit of the international community. Second, references to terrorism, xenophobia, and other unlawful activities connote Russia's long-standing construction of the internet as a potential threat to Russia's state order and traditional cultural values (recall, for instance, Putin's abovementioned remarks in 2005 that the internet "causes certain problems and raises certain issues" [Putin, 2005c]). The tension between framing the internet as a threat, often coming from the West, and a source of national progress and sovereignty is inherent to Russia's digital nationalism. The state

---

[37] Russian Internet Forum (RIF) is distinct from the Russian Internet Governance Forum. RIF was first held in 1997 and is the longest-running major professional forum of the internet industry in Russia. Since 2009, RIF has been held together with the Internet and Business annual conference.

mobilizes the framing of the internet as a threat, particularly in times of introducing restrictive regulations. Lastly, Medvedev's defense of copyright signals Russia's commitment to the logics of global capitalism and of Russia as a reliable economic partner.

Public-Private Dynamic in Russia's Digital Nationalism

During Medvedev's presidency, the Russian state engaged more actively than ever with the country's bourgeoning private digital sector. Unlike China, Russia did not ban major foreign online companies, yet Russia's homegrown search engines, social media networks, e-mail services, and other online products came to dominate the domestic market; by the late 2000s, they became an economically and politically strategic actor with multibillion capitalization and a multimillion daily audience. Two forms of incorporating the private sector into Russia's state-led digital nationalism can be distinguished: economic and discursive.

Toward the late 2000s, the Russian state began to apply the tactic of gaining indirect influence over private outlets by way of Kremlin-loyal businessmen acquiring major digital companies (Nocetti, 2011, pp. 19-20). The Kremlin has employed the same approach of influence through ownership toward legacy media outlets since the early 2000s, which illustrates how the broader state media strategy has come to ultimately infuse the online sphere. Another state tactic of indirect influence upon the private sector can be seen, for example, in 2009 when Yandex, Russia's largest digital company, presented Sberbank, the largest state-owned bank, with the right to veto a sale of over 25 percent of its shares – a move guaranteeing the state's ultimate control over the fate of a strategic national asset (Golitsyna & Glikin, 2009). Some of these Kremlin-loyal digital

media conglomerates have since invested substantially into the world's foremost digital companies, including, for instance, the purchase of up to ten percent of Facebook shares by the Russia-based Digital Sky Technologies (later renamed Mail.ru Group) (Nocetti, 2011, pp. 19-20).

Alongside political-economic nationalization, discursive nationalization of Russian digital champions occurred through state representatives' rhetorical entanglement of the interests and achievements of the private sector and the nation via various symbolic acts (Budnitsky & Jia, 2018). In one prominent example, in 2011 Dmitry Peskov, Press Secretary to then Prime Minister Putin, promoted Russia's identity as innovative in the New York Times by referring to Yandex's public offering at Nasdaq that took place the same year:

> [A] pertinent representative of today's Russia is Yandex, which recently enjoyed a wildly successful initial public offering. Yandex is but one example of the sort of home-grown Russian innovation that is beginning to thrive here. … These companies are flourishing here because they recognize the remarkable and positive changes in Russia over the last 20 years. (Peskov, 2011)

The public-private dynamic here illuminates two aspects of digial nationalism. First, the market logic of the private sector is not antithetical to the logic of digital nationalism. The state possesses a range of material and symbolic options for including digital champions into the ambit of state-led digital nationalism. The nature of this relationship varies by each individual national context. In some cases, this dynamic may negatively impact private actors. For example, in its annual shareholder report, Yandex has to disclose the possibility of a hostile governmental takeover as a potential risks. On the other hand, the private sector often stands to benefit from this symbiotic relationship,

such as when Russian leadership contributes to raising Yandex's global profile or Estonian leadership promotes Skype.

The second point regarding digital nationalism is that a country's self-promotion as a sovereign digital power does not necessarily imply resorting to protectionism or isolationism in the digital realm in either policy or rhetoric. As the above mentioned case illustrates, in advancing its national digital prowess, the Russian state—either directly or via support for its digital champions—enthusiastically used global capital and information flows, from the Silicon Valley to the New York Times.

Under Medvedev's presidency, Russia became a pioneer of a particular manifestation of digital nationalism. Although talks about this began under President Putin several years prior, in 2009-2010 Russia introduced a Cyrillic top-level country code domain of ".рф" (.rf) in addition to the Latin-based ".su" and ".ru" extensions. A Cyrillc domain zone allows website names to be spelt in Cyrillic: for example, "президент.рф" (president.rf) in place of "kremlin.ru," while both lead to the official website of the Russian Presidency. Official discourse framed the Cyrillic domain pragmatically as a helpful tool in narrowing the digital divide within Russia by allowing those unfamiliar with the Latin alphabet to go online, but also in a symbolic sense as "an important instrument in supporting and developing the national identity and widening of the Russian-speaking internet audience" (Russian Ministry of Telecom, 2012, p. 74; see also Russian Ministry of Telecom, 2010). Some representatives of the political and business elites, however, reportedly were concerned that introduction of a Cyrillic domain would foster ghettoization of the Russian cyberspace and ease governmental censorship, or were simply irritated by the additional spendings this would require (Levy,

2009)—a reminder of the persistent cleaveages in the digital visions of the state and the corporate sector that need to be taken into consideration.

While bolstering Russia's digital nationalism, the adoption of the Cyrillic domain was only possible with the authorization from the Internet Corporation for Assigned Names and Numbers (ICANN)—the U.S.-based private non-profit in charge of the internet's naming and addressing space—even as the crux of Russia's global internet governance vision is to replace the ICANN-based governance system with the UN-based one. Moreover, at the inaugural 2010 Russian Internet Governance Forum in Moscow, then CEO of ICANN Rod Beckstrom attended to officially present the certificate for the Cyrillic domain to the Russian side, with then Russian Minister of Telecom Igor Schegolev taking part in the ceremony. The episode illustrates how the logics and political-technological infrastructures of digital nationalism and digital globalization are interdependent, and often mutually reinforcing, rather than exclusive.

The Russian state's significantly increased engagement with the internet in the production and promotion of national identity did not substantially curtail the online public sphere before 2012, especially when compared with the progressively growing state influence upon the offline media space in the same period. The oft-cited study "Control and Subversion in Russian Cyberspace" by Ronald Deibert and Rafal Rohozinski, the very name of which suggests the intent on the part of the state to sway the online narrative in its favor, nevertheless refers to *Runet* as a "relatively free … wild hive of buzzing online activity" (Deibert & Rohozinski, 2010). A three-year study of the Russian networked public sphere by Harvard's Berkman Klein Center for Internet and

Society, published in early 2012, came to a similar conclusion (Alexanyan et al., 2012).[38]

During the next presidential term, however, when Vladimir Putin returned to presidency after serving in 2008-2012 as a Prime Minister under President Dmitry Medvedev, a substantial shift in Russia's identity discourse signified a turn toward an increasingly restrictive governance of the public sphere and the networked public in particular.

2012 – 2018: A Conservative Digital Power

Following a swift conservative turn in Russian self-identification, the period after 2012 in Russia's domestic internet governance has been characterized by rapid introduction of restrictive laws, policies, and practices pertaining to the internet. The rather sudden change in the Russian state's approach to the online public sphere began soon after a series of the largest anti-governmental mass protests in the country's post-Soviet history in 2011-2012, which were sparked by Vladimir Putin's decision to return to presidency and evidence of parliamentary election fraud in late 2011 (Asmolov & Kolozaridi, 2017, pp. 74-76; Franke & Pallin, 2012; Klyueva, 2016; Nocetti, 2015, p. 113; Oates, 2013, Ch. 7; Soldatov & Borogan, 2015, Ch. 7-8).[39] After Russia's military incursion into Ukraine in 2014 and the ensuing deterioration of relations between Russia

---

[38] The authors note "the emergence of a vibrant and diverse networked public sphere that constitutes an independent alternative to the more tightly controlled offline media and political space, as well as the growing use of digital platforms in social mobilization and civic action. Despite various indirect efforts to shape cyberspace into an environment that is friendlier towards the government, we find that the Russian Internet remains generally open and free, although the current degree of Internet freedom is in no way a prediction of the future of this contested space" (Alexanyan et al., 2012, p. 2).

[39] While many Western leaders celebrate digital technologies as tools of democratic empowerment and liberation, including for their role in fostering popular uprisings, Russian authorities have always been highly critical of such revolutions and the perceived role the internet played in many of them. Moscow views the uprisings as imposed by the West and, when they take place in Russia's neighborhood—as in Georgia, Kyrgyzstan, and Ukraine in the 2000s-2010s—as directly aimed at undermining Russia's international influence. As in the case of the Arab Spring, organizers and participants of protests in Russia certainly employed digital tools for coordination and dissemination of information, but it is impossible to determine the internet's precise role. Nevertheless, the *discursive construction* of the internet by the state and state-controlled media during and after these events framed the internet as threatening to the nation and in need of harnessing.

and the West to their lowest point since the Cold War, Russia's identity moved further along the trajectory of anti-Western illiberalism.

The double-shock to the socio-political system's stability from within and from the outside in 2012-2014 triggered a reassessment of the Russian official identity narrative toward explicit incorporation of culturally conservative elements. The foundational cultural repertoires underlying Russia's self-identification as a modern but traditional strong state at home and a challenger to the alleged U.S.-led liberal international order abroad have remained consistent since at least the early 2000s. However, Russian official self-presentation acquired a rhetorical layer—accompanied by attendant policymaking—that has incorporated repertoires of traditional spiritual-moral values (e.g. Christian Orthodoxy, traditional family values) that have been alleged to form a civilizational divide between the Russian nation and the liberal West (Linde, 2016; Makarychev & Medvedev, 2015; Østbø, 2016; Sharafutdinova, 2015; Stepanova, 2015).

The culturally conservative identity turn has underlain a new approach to media and internet governance. The updated 2017 Information Society Development Strategy for the period of 2017-2030, for example, sets as one of its principles "the priority of traditional Russian spiritual-moral values and adherence to norms based on these values in the use of information and communication technologies" (Putin, 2017, p. 2). Accordingly, Russia in the recent years has passed an unprecedented number of laws that seek to align the norms of internet use with the new cultural paradigm (DLA Piper et al., 2016; Tselikov, 2014; Nocetti, 2015; Soldatov, 2015; Savelyev, 2016). Some of the new initiatives include, for example, the blacklist of websites maintained by Roskomnadzor, a

media watchdog agency under the auspices of the Ministry of Telecoms, to which sites can be added without a court order for alleged unlawful activities; the requirement for bloggers with over 3,000 daily visitors to register with the state as mass media organizations; data localization requirements for foreign online services to keep personal data of Russian citizens on servers based in Russia, and others.

Restrictive internet governance laws are applied selectively, which is in line with the Kremlin's long-standing media strategy of promoting internalization of restrictions, such as, for instance, self-censorship by journalists. For example, access to LinkedIn— one of the less popular foreign online services in Russia as compared to Facebook and Twitter—was blocked in Russia for failing to move data to Russia, while other major Western social networks continue to operate and are reportedly in talks with Russian authorities about the situation.

The change in Russia's self-identification and the ensuing deteriorating relationship with the West, which have included financial and trade sanctions that challenged the Russian IT industry, have also affected Russia's approach to the internet as source of its digital power. The internet's institutionalization and integration with the state has continued. For example, since 2012 Russia has updated its Information Security and Information Society strategies and introduced the first Digital Economy strategy, while in 2014 the Kremlin inaugurated the post of the Presidential Internet Advisor and established the Internet Development Institute policy think tank.

What differentiated these initiatives from the pre-2012 period is the ever more forceful overarching rhetorical and policy framing of such efforts in terms of bolstering Russia's sovereignty and reducing dependence on the West. The notion of "import

substitution" of foreign digital technologies with the Russian ones, which previously was restricted to professional discourse, has entered high-level political and media discourse. In 2015, the Government established the Council on Import Substitution and the Ministry of Telecoms adopted the Software Import Substitution Plan for 2015-2025. The need for homegrown digital technologies has been couched implicitly and explicitly not solely in economic terms but in the context of information sovereignty and sovereignty more broadly. For example, Minister of Telecoms Nikolay Nikiforov, addressing a youth summer camp in the recently annexed Crimean Peninsula in August 2014 (itself a symbolic act meant to communicate Russia's full embrace of the new territory in the face of the international outcry), stated:

> We stand for full information sovereignty of Russia. It's highly possible, because Russia has always been known for the high qualification of its programmers. We have worldwide famous IT companies, such as "Yandex", Mail.ru and others. We are preparing a complex of measures on substituting imported software with domestic one. It means that Russian IT companies will require at least one million programmers, able to complete such a large-scale task. (Russian Ministry of Digital Development, 2014)

This first section of the chapter addressed the state's discursive and policy engagement with the internet in accordance with the continuities and changes of Russia's official identity narrative based around the normative notion of sovereignty. The remainder of the chapter addresses Russia's advocacy of the principle of internet sovereignty in global debates about internet governance.

4.3 Championing Internet Sovereignty

Alongside China, Russia is the world's leading advocate of internet sovereignty. Internet sovereignty in rhetoric and practice places the state and state-based international

system at the top of the internet governance hierarchy above non-governmental actors, such as corporations, advocacy groups, engineering collectives, user associations, and others. While studies of the Russian internet are voluminous, few scholarly works have addressed Russian politics of global internet governance. Nathalie Maréchal (2017) and Julian Nocetti (2015) offer two differing, if partially overlapping, interpretations of the logic behind Russia's foreign policy of the internet.

Nathalie Maréchal frames global internet governance as a binary of illiberal authoritarian states supportive of internet sovereignty and liberal democracies supportive of internet freedom to propose that Russia's political authoritarianism serves as a key explanation of its internet governance logic:

> The key to understanding Russian internet policy is that it is part and parcel of an overall information control policy, the goal of which is the accumulation of power and wealth for Russia's kleptocratic elites.
> … At the international level, Russia is normalizing and helping to spread networked authoritarianism through various strategies in internet governance fora[.] (Maréchal, 2017, pp. 36-37)

Like Maréchal, Julian Nocetti recognizes the Russian regime's authoritarian tendencies, yet does not view this as the sole explanation for Russian internet policy. More broadly, he does not subscribe to the authoritarianism/democracy binary as the exclusive structuring principle behind the internet governance debate:

> [T]he battle over the vision of internet governance cannot be characterized entirely accurately as between authoritarian, undemocratic states and liberal, freedom-loving states; it is also, and indeed more centrally, a conflict between long-established, cosmopolitan states and newer states that do not yet feel safe in their sovereignty. Russia fits into the latter category, as a relatively young nation-state that has been experiencing, since the chaotic 1990s transition to a free market economy and pluralism, a potent feeling of insecurity. (Nocetti, 2015, p. 129)

While concurring with Nocetti's argument that authoritarian and corrupt traits of the Russian regime alone are not sufficient in explaining the logic of Russian internet policy at the international level, I diverge from his proposition that Russia's global internet governance stance could be attributed to its sense of insecurity as a newer state. This explanation implies a teleological evolution from a new state's original sense of insecurity about its sovereignty, supposedly resulting in support for the rhetoric and policies of internet sovereignty, into a long-established cosmopolitan state that is secure in its sovereignty and therefore pursues liberal internet governance.

Nocetti's framing is problematic in several interrelated respects. First, the post-Cold War quarter-century, and in particular since 2014, have demonstrated that states do not necessarily follow the path from existential insecurity supposedly associated with authoritarianism to liberal cosmopolitanism. The case of Russia in 1991-2018 illustrates, rather, the opposite trend, in which official identity narrative has turned increasingly less liberal cosmopolitan and more statist as Russia came to feel more secure about its sovereignty. Secondly and relatedly, the implied universality of the teleological path from insecurity of new states to cosmopolitan security of long-established states does not account for the different internet governance models pursued by new states. For example, Estonia and Russia both attained independence in 1991 and yet have developed along different socio-political trajectories and have found themselves on the opposite sides of the internet sovereignty/freedom debate. Moreover, Russia's "chaotic 1990s" were arguably its most existentially insecure period, and yet it was the period of closest ideational alignment with Western liberalism. Conversely, once Russia reached political and economic stability in the 2000s, it increasingly returned to its historic self-

understanding of a great power, while its internet policy also became increasingly assertive and antithetical to liberal norms. At the same time, as Chapter 5 discusses, it is precisely Estonia's openly expressed insecurity about its ethno-cultural identity and state sovereignty that has driven its advocacy of internet freedom. Third, characterization of Russia as "a relatively young nation-state" suggests a strictly legal-political view of the country's emergence with the disintegration of the Soviet Union in 1991. This approach does not consider fully the much richer and older pool of preexisting cultural repertoires that post-1991 Russia, as well as Estonia, draw upon to construct and communicate their contemporary identity and internet governance narratives.

While not disputing Maréchal's and Nocetti's suggestions that Russia's authoritarian system accounts for certain logics of its internet governance advocacy, it is important to emphasize that key principles underlying Russia's vision of the global internet's techno-political architecture based around the primacy of state sovereignty have remained virtually unchanged between 1998-2018. Russia began advocacy of the centrality of national sovereignty to international informational governance at least in 1998-1999—prior to its widely acknowledged turn to authoritarianism in the early 2000s. This fact is often overlooked in contemporary analysis of Russia's internet governance, which views it through the lens of the ongoing acute conflict between Russia and the West and reduces the logic of Russia's digital governance to politics of the day without due analytical attention to their more systemic and historically informed logics. This section offers an alternative understanding of Russia's global internet governance that places a country's national identity at the center of analysis.

The following discussion consists of two parts. The first part, Institutionalizing Internet Sovereignty, illuminates the rise of global internet governance within Russia's political imaginary and strategic communication by tracing the institutionalization of this domain within Russia's foreign policy. The second part, Narrating Internet Sovereignty, illuminates how key themes of Russia's strategic narrative of internet sovereignty relate to its identity narrative. This account is meant to illustrate that, while Russia's foundational approaches to internet governance have remained virtually unchanged from 1998-2018, with the intensification of the global ideological competition and the changing of Russia's self-identification, its strategic communication of internet sovereignty has also shifted toward more assertiveness—and often confrontation—with the West and toward alignment with other supporters of internet sovereignty.

Institutionalizing Internet Sovereignty

Russia was among the first countries to enter the debate about global internet governance in the late 1990s and has remained consistent about its core normative propositions based on the privileging of the state-based international system. As has been the case with Russia's domestic governance of the internet, however, the past two decades saw the Russian state increasing assertiveness in rhetoric and institutionalization of its digital vision. The shape of Russia's global push for internet sovereignty has been congruent with its broader ideational and geopolitical framework, which has gone from alignment with the Western liberal paradigm in the early 1990s to pragmatic cooperation in the 2000s, and to an open challenge to the liberal world order in the 2010s.

Russia's early engagement with global internet governance came in 1998 when it became the first country to place the issue of international information security on the UN

agenda. Russia introduced a proposal on "Developments in the field of information and

telecommunications in the context of international security" and has put forth this

resolution to the UN vote every year since (United Nations General Assembly, 1999).

The resolution promotes Russia's identity in that (a) the text of the resolution advances

Russia's vision of the international information order based on the principles of state

sovereignty and multilateralism and (b) annual replies to the resolution by other countries

have institutionalized the resolution into a discussion platform of global internet

governance, which, in turn, contributes to Russia's image of one of the preeminent actors

in this domain.[40] Russia and other countries self-consciously view the resolution as an

element of their internet diplomacy.[41] For example, annual reports by the Russian

Ministry of Foreign Affairs note the number of votes and replies the resolution receives

as evidence of the country's diplomatic success (Russian MFA, 2008).

     Throughout the 2000s, Russia continued to advance its digital vision through

major platforms of global internet governance and regional intergovernmental

organizations. The 2000 Doctrine of Information Security, the first highest-level

---

[40] Replies by other countries to Russia's resolution are published collectively (United Nations Office for Disarmament Affairs, n.d.). In 2017, for instance, twenty three countries replied to the proposal (United Nations General Assembly, 2017). The resolution offers countries an opportunity to advance their views on global internet governance. For example, in its reply to the Russia-proposed resolution ,Canada, among leaders of the internet freedom agenda, argues: "Existing international law is applicable to the use of information and communications technology by States" (Ibid, p. 7). In the same document, Cuba, an ally of China and Russia in advancing internet sovereignty, defends the opposite claim: "We consider it necessary to establish a legally binding international regulatory framework which is complementary to existing international law but applies to information and communications technologies" (Ibid, p. 9).

[41] Estonia, for example, uses the resolution to advance the country's digital achievements and normative positions. Estonia lists among its achievements its national cybersecurity strategy as well as the hosting in Tallinn of the NATO Cooperative Cyber Defence Centre of Excellence. Estonia encourages countries to "seek ways to better formulate, disseminate and promote responsible and active cyberpolicies, narratives and argumentation." Explicit reference to narratives and argumentation suggests Estonia's self-conscious approach to global internet governance as a site of strategic communication and identity promotion. Estonia thus uses this communicative opportunity to promote the normative internet freedom rhetoric of "openness, accountability and other democratic values in cyberspace" (United Nations General Assembly, 2017, p. 11).

information-specific strategy in Russia's post-Soviet history, conveyed the logic of this engagement that has guided Russian internet diplomacy since. The Doctrine alleges "the objective of a number of states to dominate and infringe upon the interests of Russia in the world information space, to dislodge it from foreign and domestic information markets" (Putin, 2000a, n.p.). It then proposes that the "participation of Russia in the processes of development and utilization of global informational networks and systems" could serve as a counter tactic to these external threats. Accordingly, over the following two decades Russia has worked actively to promote its identity and to institutionalize its own values and interests into the legal and institutional architectures of global internet governance by participating in nearly all major processes and venues of global internet governance.

For example, at the 2003 UN World Summit on Information Society, the Minister of Communication and Information, Leonid Reiman, promoted Russia's digital image as, first, a digitally advanced country willing to share its experience with others and, second, a proponent of the international state-based system of internet governance:

> [W]e are realizing the concept of "electronic government," computerizing schools, libraries, and post offices to minimize the digital divide among various regions of our country.
> …We are ready to share [with other countries] the experience in developing and implementing complex information and communication technologies [and] the narrowing of the "digital divide" among various social groups.
> … For Russia, the leading role of international organizations of the United Nations system is obvious – of course, in close coordination with the private sector and other stakeholders. (Reiman, 2005)

By the beginning of the 2010s, questions of internet governance have reached unprecedented heights within global affairs. For example, in 2010 China and the United

States institutionalized for the first time their normative visions for the global internet into official national programs. In line with the global trend of further intensification and institutionalization of the global internet governance debate and congruent with Russia's growing opposition to the U.S.-led political order broadly, Russia amplified its efforts at internationalizing global internet governance under the auspices of the UN and at communicating its identity of a digital power in this decade.

Several novel developments took place in the 2010s. First, global internet governance reached the highest echelons of Russia's political system and therefore has been more explicitly intertwined discursively and institutionally with Russia's self-identification. For example, in 2014, the Kremlin created a position of a Special representative of the President on international information security who is also responsible for issues of internet governance, while in 2015 then Prime Minister Dmitry Medvedev became the highest ranking official to address specifically the questions of who and how should govern the global internet in his remarks at the inaugural World Internet Conference in China (Medvedev, 2015).

Internet governance rose further within Russia's foreign policy framework when it was included in its own right in the 2016 version of Russia's Foreign Policy Concept, which states that Russia "seeks to devise, under the UN auspices, universal rules of responsible behavior with respect to international cyber security, including by rendering the internet governance more international in a fair manner" (Putin, 2016a, n.p.). The following year, the Ministry of Telecom and Mass Communications published a draft of the "Concept of the UN Convention (or the Concept of Secure Functioning and Development of the Internet)," which is the most comprehensive official document to

address specifically the domain of global internet governance and is likely to underlie in the coming years Russia's proposals for shaping the system of global internet governance (Russian MFA, 2017). Other highest-level strategic documents, such as the 2016 Doctrine of Information Security (Putin, 2016b) and 2017 Information Society Development Strategy (Putin, 2017), also explicitly address the issue of global internet governance and profess the need for Russia to defend its sovereign right to govern the national online segment.

The second distinctive development in Russia's approach to global internet governance in the 2010s has been in line with the global trend toward formalization of intergovernmental efforts at advancing normative views about the global internet. The alliances formed in support of either stance about the global internet reflect their member-states' ideas about who they are as a nation and with whom their values align. For example, in 2011, predominantly Western liberal democracies and their allies in the developing world formed an intergovernmental organization Freedom Online Coalition to advance the internet freedom narrative. Since the early 2010s, Russia has also become much more actively involved in coordinating its advocacy of internet sovereignty in alliance with countries that similarly challenge the existing political and technological order, such as BRICS (Brazil, Russia, India, China, and South Africa), the Shanghai Cooperation Organization (SCO), and the Regional Commonwealth in the Field of Communication (RCC; a specialized telecommunication body of the Commonwealth of Independent States).

In 2015, the SCO put forth a joint proposal to the United Nations of the International Code of Conduct for Information Security (Liu et al., 2015), which

advocates core pillars of the internet sovereignty view, while in 2015 BRICS Ministers of Communication gathered for their first annual meeting upon Moscow's initiative (Russian Ministry of Digital Development, 2015b). The Ministers' Communique issued after the meeting "confirmed the right of all States to establish and implement policies for information and communication networks in their territories in accordance with their respective history, culture, religion and social factors" (BRICS, 2015).

The third development in Russia's foreign policy of the internet in the 2010s is its significantly more forceful and tangible attempts to shape the global internet's architecture. This shift, particularly evident after 2012, reflects Russia's changing self-identification over the course of the past two decades toward increasing antagonism vis-à-vis cultural and political values of Western liberalism. For example, in 2010 at the ITU quadrennial plenipotentiary Russia initiated the first resolution in ITU's history that strengthened the role of ITU in global internet governance, while in 2012 at the ITU World Conference on International Telecommunications-2012 Russia lobbied for changes to the ITU's International Telecommunications Regulations that would institutionalize key tenets of internet sovereignty into the organization's governing principles.

This section outlined the institutional development of internet sovereignty within Russia's foreign policy over the past two decades to illustrate how continuities and changes in Russia's self-identification have resulted in, on the one hand, persistence of normative principles underlying Russia's advocacy of internet sovereignty and, on the other hand, ascent in significance of internet sovereignty in Russia's foreign policy. The

next section focuses on Russia's strategic communication of the internet sovereignty and its constitutive themes.

4.4 Narrating Internet Sovereignty

This section examines Russia's strategic narrative about global internet governance to illuminate how Russia's understanding of the Self expressed in official identity narratives underlies its self-presentation of the national digital identity and normative view of the global digital order. This approach draws on the understanding of strategic narrative offered by Miskimmon et al. (2013, p. 2):

> [A] means for political actors to construct a shared meaning of the past, present, and future of international politics to shape the behavior of domestic and international actors. Strategic narratives are a tool for political actors to extend their influence, manage expectations, and change the discursive environment in which they operate. They are narratives about both states and the system itself, both about who we are and what kind of order we want.

National strategic narratives are not discursively limitless but rather draw upon cultural repertories available to them in given socio-historical circumstances. The following analysis deconstructs Russia's strategic narrative of internet sovereignty into its core themes and explains their logic by relating them to Russia's official identity narrative.

State Sovereignty

The notion of sovereignty has become central to Russia's identity and foreign policy discourse since the early 2000s (Deyermond, 2016). Sovereignty as communicated by the Kremlin to foreign audiences is meant to convey the strengthening of the Russian state and consolidation of the Russian nation. The ultimate goal of preserving state sovereignty is thus understood as autonomy from real and imagined Western influences

upon Russia's domestic and foreign policymaking. Having consolidated political-economic power at home by the second half of the 2000s, Russia's ruling elite turned more assertively to advocating state sovereignty not only as central to its own Self but as a foundational principle of the world order.

All individual themes of Russia's strategic communication about global internet governance should be understood as ultimately derivable from Russia's self-understanding and self-presentation as a sovereign who is openly challenging what it views as a unipolar world order with the goal to restore state sovereignty as the foundational principle of international relations. For example, a recent annual report by the Ministry of Telecom openly conveys Russia's overarching ambition with regards to the global internet's architecture: "The [2014 Internet Governance Forum] showed potent opportunities for changing the existing world order in the information and communication realm and for strengthening the role of the state" (Russian Ministry of Telecom, 2015, p. 132). Russia argues that it strives for a polycentric ICT world order, the notion at the heart of Russia's foreign policy vision and rhetoric.

A Polycentric World Order:

Opposing Western "Monopoly," Promoting International "Diversity"

The notion of a polycentric world order—as opposed to the notion of a unipolar U.S.-led liberal world order—has been increasingly central to Russia's foreign policy and strategic communication since the late 1990s-early 2000s (Chebankova, 2017; Miskimmon & O'Loughlin, 2017). After the civilizational turn in Russia's political and identity discourse following 2012-2014 (Linde, 2016), the strategic narrative of a polycentric world order has drawn increasingly on illiberal traditionalist elements of the

Russian cultural repertoire in explicit opposition to Western liberalism. For example, Sergey Lavrov, Minister of Foreign Affairs since 2004, said in the annual address to the upper house of the Russian parliament in December 2017:

> We are convinced that the main reason for the current tension is the persistently egocentric and cynical line taken by a number of countries, led by the United States. Having come to believe in its own supremacy and infallibility, and having become accustomed to thinking its opinions should be perceived as the ultimate truth, the so-called "historical West" is trying to obstruct the natural process of the development of a more just and democratic polycentric world order. Those who dissent are subjected to a broad range of reprisals, unilateral coercive measures and direct interference in their internal affairs. (Lavrov, 2017)

The binary that Russia's rhetoric of the polycentric world advances is that of an alleged political-economic monopoly of the U.S.-led West, on the one hand, and the normative ideal of an international sovereignty-based diversity, on the other hand. Russia frames the Western model of liberal-democratic universalism in moralizing terms as egocentric, self-righteous, domineering, and disrespectful to the historical and cultural diversity of the world. At the 2007 Munich Security Conference, for example, Putin decried the unipolar model with "one master [and] one sovereign" as "flawed because at its basis there is and can be no moral foundations for modern civilization" (Putin, 2007a). By contrast, Russia frames its own stance as a just and democratic alternative to the Western unipolar monopoly.

Appeal to democracy and freedom as the highest value by both sides of the internet governance debate illuminates the widely recognized rhetorical value of the democratic ideal across the geopolitical spectrum. At the same time, differing instrumental deployment of the notion of democracy by each side reveals the workings of strategic communication in advancing respective digital visions. Advocates of internet

freedom speak of liberal-democratic norms and institutions in states' *domestic* affairs and criticize those countries that, in their view, do not conform to these standards. Advocates of internet sovereignty focus instead on democracy in *international* affairs, claiming that the U.S.-led unipolar world order is inherently undemocratic.

Russia's foreign policy framing of the world order as a competition between the U.S.-led global monopoly and Russia-led push for polycentric diversity underlies the digital sovereignty narrative. Russia seeks to undermine the supposed U.S. monopoly in all areas of the digital realm, from computer hardware and software to internet governance. These efforts have greatly intensified since the mid-2010s, as a sharp decline in the Russia-West relations fostered a global movement spearheaded by countries like Brazil, China, India, and Russia to reshape the architecture of the global technological governance and market.

For example, speaking in 2016 at the opening of the 8th International IT Forum, which brought together governments of BRICS and Shanghai Cooperation Organization and their national digital champions, Minister of Telecoms Nikolay Nikiforov lamented the fact that the global IT market is "unfortunately, dominated essentially by one country and a few companies" (Nikiforov, 2016). Instead, Nikiforov noted, "in all spheres we should have balance and diversification. Monopoly is bad. Monopoly in the information technologies is a real threat to the digital sovereignty of our countries" (Ibid.).

Global Economic Competitiveness

While challenging U.S. technological dominance, Minister Nikiforov did not question the system of global digital capitalism, as such, but instead called for the leveling of the playing field in order for Russia and its partners to advance more

196

efficiently their competitive identities: "no one county under the conditions of globalization and the so-called flat world can be successful in this sphere if it isn't thinking in global terms, working on the global market, and building mutually beneficial cooperation with colleagues [and] partners who share the same agenda" (Ibid.). Russia and BRICS countries oppose not the neoliberal economic globalization, but their own disadvantaged place in it and the alleged U.S. skewing of the fair competition in its favor.

Russia's foreign policy challenge to the U.S.-led unipolar world order extends both to political and economic domains. There is, however, a long-standing distinction in Moscow's normative approach to *political* and *economic* liberalism of the world order. Unlike Russia's critique of political liberalism in domestic and international affairs, Moscow's critique of current global economic liberalism does not challenge its foundational principles but rather the alleged *violation* of these principles by the United States and their allies. Russia embraces economic globalization and presents itself as a responsible and reliable global capitalist by calling for equitable and fair competition against the alleged U.S. technological-economic hegemony and anti-competitive practices. One manifestation of Russia's aspiration to challenge U.S. geopolitical and geoeconomic IT hegemony can be seen in the creation of the Russian IT Export, RITE, in May 2017, a dedicated governmental agency with a mandate to export Russian IT solutions to friendly governments who wish to decrease their dependence on the U.S.-based solutions.[42]

---

[42] Coverage of the RITE's launch in the state international broadcaster Sputnik News conveys Russia's view of the digital world order and its own mission (Sputnik News, 2017). The article's title, "Freedom for Export: How Russia Sells Digital Sovereignty to the World. Russia has been steadily advocating the idea of the digital sovereignty of states and has now moved to practically sell it, therefore propping up nations' independence and freedom," sets up "sovereignty" and "freedom" not as opposites but as inextricably bound. Within Russia's official discourse of the Self and the world, it is only through attaining genuine sovereignty and independence from the global hegemon that a country can be truly free. This paints Russia,

Internationalization of Internet Governance:

International Law and the United Nations

Russia's normative view of the world order is founded upon the primacy of international law under the auspices of state-based organizations, foremost the United Nations, in conducting international relations. The UN-based order benefits Russia's interests as Russia holds a permanent seat at the UN Security Council and is able to garner mass support for its initiatives at the UN voting. A UN-based international system, in which Russia's vote is equal to that of the United States despite Russia's far inferior economic standing, helps to maintain Russia's geopolitical leverage.

Russia's strategic communication causally links the notion of the UN-based "international law" to the ideals of peace, stability, security, and an overall fair and democratic world order. The notion of the UN-based order thus tends to be decoupled from Russia's immediate interests and instead couched in the language of the common good. For example, Russia's 2016 Concept of Foreign Policy vows to

> [P]romote the efforts to strengthen international peace and ensure global security
> and stability with a view to establishing a fair and democratic international
> system that addresses international issues on the basis of collective decision-
> making, the rule of international law, primarily the provisions of the Charter of
> the United Nations (the UN Charter), as well as equal, partnership relations
> among States, with the central and coordinating role played by the United
> Nations (UN) as the key organization in charge of regulating international
> relations. (Putin, 2016a)

Despite their linguistic similarity, the notions of "the rule of law" promoted by liberal democracies and of "international law" and "the rule of international law"

---

and not the United States, as the global exporter of genuine freedom. Egor Ivanov, RITE CEO featured in the article, echoes Russia's foreign policy discourse in criticizing "the monopoly of one foreign country" over the global IT industry and views RITE's competitive advantage in that it doesn't try to make the customer country dependent on Moscow by offering foreign governments open-source software.

promoted by Russia and its allies are deployed by the two internet governance camps in support of their competing normative positions. The liberal-democratic notion of the rule of law designates a polity governed by law as opposed to the will of an individual ruler or government. Internet freedom rhetoric suggests, first, that borderless communication advances the rule of law and, second, that credibility in the internet governance debate is contingent upon the state's adherence to the principle of the rule of law. Accordingly, advocates of internet freedom persistently frame their policy stance as promoting the rule of law in *domestic* political order and criticize Russia and other illiberal regimes for their alleged disregard for the rule of law. Advocates of internet sovereignty, in turn, use the notion of "the rule of international law" to draw attention to the *international* political order. In line with the overarching trope about supposed Western monopoly over international relations, Russia and its allies aim to discredit their opponents in the debate by alleging their systematic violation of the principles of national sovereignty and international law, such as military and humanitarian interventions that sometimes circumvent the UN Security Council.

Russia's support for international law underlies Moscow's normative narrative of *internationalization* of global internet governance and critiques the alleged monopolization and corporatization of the internet under the auspices of the U.S. government and corporations. Like internet freedom communication, advocates of internet sovereignty often attempt to legitimize their contemporary stance by appealing to the internet's origin myth. For example, Aide to the President Igor Schegolev lamented in 2015 at the VI Safe Internet Forum,

> [D]e facto and de jure the global internet infrastructure and its governance are currently monopolized and are outside of the international law.

… A turning point, however, is approaching. More and more people are starting
to realize that the internet in its current state doesn't reflect the objectives, for
which it was created. It is upon us to return to the forefront the objective of
mankind's humanitarian development. The internet is supposed to provide
unbound access to knowledge and its exchange, and not corporate chase after
personal data of billions of users. (Schegolev, 2015)

As a solution to the alleged monopoly of U.S. governmental and corporate
interests over the global internet, Russia advances an internet governance model founded
upon a binding international legal agreement under the auspices of the United Nations.
This model identifies national governments as primary regulators of the internet within
their territorial borders and in international affairs. For example, at the 2015 World
Internet Conference held in Wuzhen, China, under the auspices of the Chinese
government, then Prime Minister Dmitry Medvedev suggested:

No country alone can claim the role of the sole universal regulator of the world-
wide web. There are no historical privileges or traditions in this sphere.
Russia supports the idea that the international community must play a bigger role
in Internet governance and that a global policy in this sphere be developed. We
believe that this goal should be achieved under the auspices of the leading
international organisations, including the UN, and with reliance on the industry-
specific organization—the International Telecommunication Union (ITU). In the
future, this or any other organisation, were it to be created, could be granted the
authority and powers to develop international legal norms and standards of
Internet governance. (Medvedev, 2015)

Russia's advocacy of multilateral-based global internet governance brings it into
opposition with the multistakeholder model of internet governance advocated by
representatives of the internet freedom camp and discussed further.

State-based Multistakeholder Governance

Multistakeholder governance, or multistakeholderism, in the global internet governance debate means participation in the decision-making process of all relevant stakeholders, such as national governments, private companies, digital advocacy groups, the engineering community, and others. Since the mid-2000s, the concept of multistakeholderism has achieved a hegemonic status within global internet governance discourse, in that it is nearly universally assumed as inherent to global internet governance and is rarely questioned as such. Internet sovereignty and internet freedom narratives, however, assign differing interpretations to this key internet governance concept.

The notion of multistakeholderism espoused by the internet freedom narrative implies *equal* participation by all stakeholders congruent with the participatory democratic ideals of the early internet, even if the practice of multistakeholder governance does not hold up to these ideals. Advocates of the internet freedom narrative equate opposition to this understanding of multistakeholderism with authoritarianism and repression so as to delimit discursively the very possibility of an alternative governance framework. In a characteristic example of such framing, then-President of Estonia Toomas Ilves stated at the annual gathering of the Freedom Online Coalition in 2014:

> A number of authoritarian and repressive regimes want to replace the multi-stakeholder model of Internet governance we have today, led by ICANN, with the innocuously sounding Intergovernmental governance. Do we really want the likes of the authoritarian regimes we see in the world today "governing the Internet"? I don't. (Ilves, 2014b)

Russia, and most other advocates of internet sovereignty, does not rhetorically oppose the principle of multistakeholderism understood as consultative participation of all stakeholders. However, in light of their state-based approach to internet governance,

they advocate the notion of multistakeholderism understood as stakeholder participation *in their respective roles* – an understanding that is reflected in the official definition of "internet governance" by the United Nations. This understanding implies a strict hierarchy of roles in the global political system, in which the state occupies the top position. For example, speaking at the opening of the Netmundial in 2014, Nikolay Nikiforov elaborated Russia's stance on the issue:

> We share the opinion that the model of governing internet infrastructure should be multistakeholder. … However, in our view, we have to unequivocally determine the roles of all interested stakeholders in this process, including the states. It is the states, which are subject to international law, which serve as guarantors of their citizens' rights and freedoms, play the leading role in the economy, security and stability of the internet's informational infrastructure, take measures to preempt, discover and quell illegal activities in the global network. (Nikiforov, 2014)

The central debate between advocates of multilateral and multistakeholder governance models concerns the appropriate role of the Internet Corporation for Assigned Names and Numbers (ICANN) in the governing architecture of the global internet, the subject of the next section.

Internet Corporation for Names and Numbers (ICANN)

In line with its support for state-based global internet governance and opposition to the unipolar world order, Russia opposes the place of a private U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) at the top of the internet's techno-political hierarchy. ICANN occupies this place due to its exclusive authority over the internet's addressing and naming system. For Russia, ICANN is an exemplar of unchecked undemocratic governance that bolsters U.S. hegemony. Despite ICANN's substantial power over national economies through its ultimate control of internet domain

names, influence of governments on the work of ICANN is limited to their voluntary participation in ICANN's Governmental Advisory Committee (GAC), a consultative body with no decision-making powers.[43]

ICANN's historically close relations with the United States and lack of democratic accountability to other governments has been the subject of criticism from many governments, particularly those from the internet sovereignty camp. In the words of Nikolay Nikiforov on the occasion of the termination of the oversight contract over the Internet Assigned Numbers Authority (IANA) between the U.S. government and ICANN, "ICANN initially was founded upon at least two types of unequal rights and powers: first – the power of the United States government in relation to other governments[,] and second – the power of governments in relation to most other stakeholders" (Nikiforov, 2016b).

The first issue raised by Nikiforov was partially alleviated in 2016 when the U.S. government ended its contractual oversight over the IANA, the body within ICANN responsible for the technical coordination of the domains namespace. Whereas many celebrated this as a step toward genuine multistakeholderism, in line with its state-based approach, Russia remained concerned with its second criticism of ICANN: the diminished role of governments vis-à-vis non-governmental stakeholders within ICANN's decision-making process. In 2017, Igor Schegolev, Minister of Telecom and Mass Communications in 2008-2012 and Aide to the President since 2012, critiqued ICANN's new arrangement:

---

[43] In order to communicate its vision, Russia actively partakes in the work of ICANN through attending conferences under its auspices and participating in GAC, while the Ministry of Digital Development has a designated program to liaise with ICANN.

We are told that the fate of the internet will now be decided by a certain

autonomous organization, incorporated in California and living by the laws of the

United States, where decisions are made by directors. They, of course, may well

be gurus, and perhaps are very intelligent people. However, by a "fortunate"

coincidence, these are representatives of the United States, Canada, New

Zealand, and Australia. (Schegolev, 2017)

Schegolev's sarcastic remark about the national backgrounds of leading figures in

ICANN reveal Russia's broader discomfort with and desire to challenge what Vladimir

Putin called in 2013 "the Anglo-Saxon monopoly on the global information streams"

(President of Russia, 2013).

4.5 Conclusion

This chapter presented the second part of a two-chapter examination of Russia's

digital nationalism, the co-constitutive relationship between Russia's national identity

and internet governance. The previous chapter, Re-Making of a Great Power, focused

exclusively on Russia's post-Soviet trajectories of identity-building, domestic media

environment, and strategic communication targeted at foreign audiences. Detailing these

trajectories provided the socio-political context within which Russia's internet

governance at home and abroad should be understood. Building on the previous chapter's

discussion, the exclusive focus of this chapter was Russia's discursive and institutional

construction and communication of internet sovereignty domestically and internationally.

The goal of the chapter was to illuminate how the language and logics of Russian

internet governance relate to its identity discourse. The first half of the chapter addressed

domestic internet governance to illustrate how the internet has become increasingly

integral to Russia's view of the Self as a resurgent great power, as well as how the

changing national identity has contributed to shaping internet governance. The second

half of the chapter focused on Russia's advocacy of internet sovereignty in the domain of global internet governance to illustrate how Russia's construction of international relations and of its place in it has been projected onto the domain of global internet governance.

Russia's internet governance rhetoric is built around the notion of sovereignty, which has ascended to prominence in Russian political discourse since the late 1990s and has served as a proxy that connotes Russia's self-understanding as a resurgent great power that is owed international recognition. Accordingly, Russia has become a leading advocate of the internet sovereignty narrative, which advocates (a) international recognition of Russia's sovereign right to govern its national internet segment and (b) Russia's challenge to the perceived unipolar global digital order and its attempt to internationalize internet governance by bringing its core techno-political institutions under the auspices of the United Nations.

The next and final chapter will apply the analytical framework employed in the Russian case to the study of Estonia's digital nationalism. Estonia's digital nationalism is characterized by the relationship between re-independent Estonia's view of the Self as an ethno-national polity aligned with the Euro-Atlantic community, on the one hand, and its active role in promoting the internet freedom narrative, on the other hand. The chapter will illuminate why and how Estonia's internet governance narrative and policy, despite being couched in the rhetoric of liberal globalism, could be understood as an expression of Estonian nationalism.

Chapter 5: Re-Making of a Western Identity: Estonia's "Return to Europe" as an e-State

5.1 Introduction: "[W]e are actually a European version of the American dream."

This chapter examines Estonia's digital nationalism in the domain of global internet governance. Digital nationalism as a state project refers to the state's discursive and material use of digital technologies to advance the nation's global competitive identity. My claim in this dissertation is that the logics and languages of digital nationalisms reflect respective national identity narratives. The starting point in analytically tracing the working of digital nationalism is to situate state rhetoric and policy pertaining to digital technologies within specific socio-historical circumstances. National digital visions, and global digital politics as their aggregate, can then be related analytically to respective national identities and best understood within national cultural contexts. Whereas Chapters 3-4 illuminated how Russia's identity narrative of a resurgent great power has underlain its advocacy of the internet sovereignty agenda, this chapter illustrates how the same explanatory logic can be applied to the case of Estonia's advocacy of the internet freedom narrative. The internet freedom narrative advanced by Estonia reflects its state identity narrative of an innately European nation returning symbolically and institutionally to the Euro-Atlantic community.

An official visit to the United States in 2016 by then Prime Minister of Estonia Taavi Rõivas, during which he engaged widely with the worlds of American academia, business, and government, provides a revealing snapshot into the logics and language of Estonian digital nationalism.

During Rõivas' appearance as a guest on "The Daily Show with Trevor Noah," the host Trevor Noah lauded Estonia as "one of the most digitally forward countries in the world" and focused almost exclusively on Estonia's internet-related achievements. In turn, Rõivas promoted Estonia as economically "progressive," "a good ally for the U.S.," and noted how getting information from the outside "free world" during the years of Soviet occupation was an important part of Estonia's path to democracy (Noah, 2016).

At Harvard and Duke universities, Rõivas gave talks on the Estonian state's use of technology in governance and economy, "A 21st Century State: Anything is Possible" (Belfer Center, 2016; Moorthy, 2016), while at the George Washington University he addressed the U.S.-Estonia Symposium on Cybersecurity and Defense Cooperation attended by CEOs of major companies in the field (Center for Cyber & Homeland Security, 2016). Like the media, elite academic institutions praised Estonia's digital achievement. Harvard's Belfer Center previewed Rõivas' talk by describing Estonia as

> [O]ne of the great success stories among the nations that reclaimed independence
> after the Cold War. Estonia has built a vibrant democracy and become a model
> for how citizens should interact with their government in the 21st century. …
> Estonia has become one of the most wired countries on Earth, a global leader in
> e-government and high tech start-ups. (Belfer Center, 2016)

In Rõivas' own words conveyed to the audience at Duke, "Even though Estonia is a small country quite far from North Carolina, we actually are a European version of the American dream" (cited in Moorthy, 2016).

The government-to-government part of Rõivas' voyage included a visit to the Fort Stewart military base, whose units are partially stationed in Estonia, and a meeting with Paul Ryan, Speaker of the U.S. House of Representatives (Tõhk, 2016a, 2016b). Rõivas expressed gratitude for the troops' contribution to European and Estonian security and

emphasized the importance of the Euro-Atlantic cooperation. At the Capitol, Ryan, in turn, thanked Rõivas for Estonia's commitment to allocating two percent of the budget to national defense—a normative minimum contribution from all NATO member-states, which only a handful of them achieve.

This recent episode in Estonia's diplomatic history reveals the logics pertaining to the three core pillars of this dissertation's examination of digital nationalism: identity, strategic communication, and digital technologies and their governance.

First, the episode reveals how Estonian official identity and foreign policy narrative is firmly rooted in Estonian self-identification and self-presentation as inherently Western. Estonia portrays the United States as being at once Estonia's ally, defender, and role model. Meanwhile, the Soviet past and contemporary Russian is the Other which Estonia defines itself *against* and from which it seeks protection with the military and intelligence assistance of Western counties and organizations, such as NATO.

The second insight from Rõivas' trip concerns Estonia's approach to strategic communication. In terms of content, in order to communicate Estonia's rootedness in the West, Estonian leadership's rhetoric relies heavily on contemporary Western liberalism's foundational repertoires of freedom, market economy, and democracy, as well as associated cultural tropes of individualism, efficiency, and pragmatism. In terms of communication strategy, Rõivas' visit illustrates how Estonia proactively employs a variety of media, academic, political, and business platforms to convey its message. In turn, Rõivas' enthusiastic reception by his U.S. hosts, often indistinguishable from

Estonia's own narrative, is typical of how Western media and political elites have portrayed Estonia since at least the mid-2000s.

The third point pertains to Estonia's discourse of digital technology and the internet, which was the underlying theme of Rõivas' visit. Estonia's identity discourse has incorporated the rhetoric of the country's technological progress as one of its core pillars: to cultivate Estonia's technological achievements is to validate Estonian identity as a Western, progressive, and developed nation. The notion of Estonia as an e-state is at the center of Estonian strategic communication. This normative linkage between the Western-oriented identity and internet technologies helps to explain why Estonia became one of the leading voices of the internet freedom narrative in the global internet governance debate.

Taking the above premises as an entry point into the discussion of Estonia's internet governance discourse, this chapter investigates why and how Estonia discursively blended its national identity with techno-digital progress and support for the internet freedom agenda. Estonia serves as a particularly apt case study of digital nationalism for its active engagement with all three domains underlying this dissertation: historically informed debates about Estonia's identity and majority-minority identity politics underlie the country's domestic and foreign policy discourse; Estonia is recognized as one of the most active and committed strategic communicators; Estonia is also a leading voice in the internet governance debate as a staunch supporter of the internet freedom narrative. At the same time, Estonia's geopolitical and internet governance discourse is opposed to Russia's. The added analytical purchase of this chapter lays in showing that digital nationalism operates in contexts that discursively

construct themselves as having diametrically opposed values, interests, civilizational identities, and internet governance narratives, such as Estonia and Russia.

Organization of the Chapter

The chapter proceeds in several sections that speak to the logic of digital nationalism and specifically to the three pillars that I deploy in this dissertation to illuminate the workings of digital nationalism: identity, strategic communication, and internet governance. As digital nationalism argues for analytical appreciation of the relationship between identity discourse and digital discourse, the structure of the chapter moves from the discussion of the former to the latter as a way to elaborate this relationship step-by-step.

The first section, e-Estonia: Infrastructures, Institutions, Policies, introduces the materiality of Estonia's ICT sector. As materiality and discourse are mutually constitutive, the purpose of this section is to briefly explain the institutional and infrastructural underpinnings of Estonia's strategic communication about its digital achievements and internet governance.

The second section, Estonian Identity: From National Awakening to Re-Independence, pertains to the identity pillar of this dissertation and explains why and how Estonia's identity narrative came to be entwined with the digital. First, I outline key moments in the development of Estonian nationhood and statehood since the birth of Estonian nationalism in middle of the nineteenth century; then I explain how these historical events, particularly demographic changes during the Soviet occupation, impact present-day identity discourse. I find that Estonia's identity narrative is centrally based around the notion of returning to Europe—symbolic and institutional joining of the Euro-

Atlantic community as a way of finding economic and ontological security from Russia, Estonia's Other. In particular, Estonia relies on ICT developments as a way to communicate to the world its allegedly inherent European and liberal nature.

The next two sections address strategic communication, the second pillar of this dissertation, to explain why and how Estonian leadership communicates its identity and technology to the outside world. The first of these sections, Brand Estonia: Nordic, Environmental, and Digitally Advanced, explains how Estonia's desire to be perceived as a normal Western liberal democracy has shaped the content and strategy of its external communication over the past two decades. The next section, Promoting "Greater Awareness of e-Estonia in the World", focuses on the central narrative of Estonia's strategic communication that portrays Estonia as a digitally advanced country. The narrative portrays Estonia as having successfully transitioned from post-socialism to liberal democracy and market economy through strategic incorporation of ICT into the workings of the state and society. The section draws on the earlier discussion of Estonia's ICT materiality to explain why and how the country's leadership has framed this domestic technological infrastructure to promote an image of Estonia as a global digital leader. Bridging the analysis of Estonia's identity discourse and ICT materiality, on the one hand, with analysis of Estonia's strategic communication content and structure, on the other hand, I show how the strategic narrative of *e-Estonia* has served Estonia's identity goal of joining the West.

The last section of the chapter, An Internet Freedom Champion: Aligning with the West, Othering the East, addresses the third pillar of the dissertation: internet governance. Building on the preceding analysis of Estonia's identity discourse and strategic

communication, this section explicitly illustrates digital nationalism's main claim about how identity narrative informs the logics and language of the state's digital vision. I situate Estonia's strategic narrative of internet freedom within the framework of the country's strategic communication of e-Estonia and analytically juxtapose it against Estonia's identity discourse. I outline key pillars of Estonia's rhetorical and institutional support of internet freedom to argue that their logic is to be found in the country's desire to align itself with the political West while distancing itself from the East.

The majority of speeches used in the chapter belong to Toomas Ilves, Minister of Foreign Affairs from 1996-2002 and President of Estonia from 2006-2016. This is due to several factors. First, his presidency fell during a period when global internet governance arose to geopolitical prominence; second, due to the status of Presidency in Estonian political structure, Ilves served as the voice of Estonia in the international arena; third, Ilves' personal characteristics of a native English-speaker, a long-time computer enthusiast, and an erudite Ivy League-educated intellectual all contributed to his becoming the voice of Estonia's digital discourse in the past decade (Crandall, 2016; Kitman, 2011). At the same time, as the example of Rõivas' visit to the U.S. shows, Ilves' rhetoric is not individual but institutional: it is entirely consistent with Estonia's post-Soviet identity discourse communicated before, after, and concurrently with Ilves' presidential tenure by other representatives of the Estonian political class.

5.2 e-Estonia: Infrastructures, Institutions, Policies

Estonia's leading global advocacy of the internet freedom agenda, which is the primary focus of this chapter, is one element of the country's framework of digital nationalism known as e-Estonia. The concept of e-Estonia as advanced by its

practitioners and proponents refers broadly to the Estonian state's and society's wide-ranging integration of digital technologies into daily life and existential vision of the Estonian nation. Estonia's prioritizing of ICT as a matter of national development over the past two decades turned the country from one of Europe's least into one of the world's most technologically advanced states.[44]

Estonian government has promoted its digital infrastructures with a consistent strategic narrative of "Estonia's emergence as one of the most advanced e-societies in the world – an incredible success story that grew out of a partnership between a forward-thinking government, a pro-active ICT sector and a switched-on, tech-savvy population" (Estonian MFA, 2016). This chapter critically examines this digital strategic narrative to illuminate why and how Estonia has incorporated digital technologies and support for internet freedom in its discourse of the national Self. This section overviews the basic material underpinnings of e-Estonia to familiarize the reader with the logics of Estonia's incorporation of digital technologies into its nation- and state-building.

Estonia was among the first countries in the world to self-consciously construct digital technologies as intrinsic to its national project through policy, legal, and educational initiatives. Estonia's ICT philosophy was first codified in 1998 as Principles of Estonian Information Policy, followed by more comprehensive Principles of the

---

[44] Assessing Estonia's transition to a market economy, a 1993 World Bank report, *Estonia: A Transition to a Market Economy*, wrote: "the telecommunications network is obsolete, provides a low quality of service, requires labor-intensive maintenance, and uses scarce spare parts that can only be purchased in Eastern Europe and ex-Soviet republics for hard currency" (World Bank 1993, p. 153). Less than a decade later, *The Global Information Technology Report 2001-2002* by the World Economic Forum and Harvard University already described Estonia's telecommunications infrastructure as "advanced" and "completely upgraded," ranking the country above all other Central and Eastern European states (World Economic Forum, 2002, pp. 200-201). Recently, the World Bank featured Estonia as an exemplary success story in its 2016 *Digital Dividends* report: "Estonia's use of modern information and communication technologies in public sector and governance has placed the country at the forefront of states that are aiming to modernize their public sector and provide transparent governance" (Vassil, 2015, p. 2).

Estonian Information Policy 2004-2006 in 2004 and Estonian Information Society Strategy 2013 in 2006 (Kalvet, 2007, pp. 10-11). Digital Agenda 2020 for Estonia, the fourth and current iteration, covers Estonia's ICT development in 2013-2020. Like previous iterations, Digital Agenda 2020 frames the use of ICT as an all-permeating solution "to improve the quality of life for people, increase the employment rate, ensure the viability of Estonian cultural space, increase productivity in the economy, and make the public sector more efficient" (Estonian Ministry of Economic Affairs and Communications, 2013, p. 14).

From the beginning, Estonia has posited ICT education and literacy as key to the country's digital development. Information technology was ingrained into school curricula, universities expanded their offerings of ICT-related degrees and courses, and mass short-term digital literacy programs trained rural, elder, and lower income populations in basic computer and internet skills. Tiger Leap (*Tiigrihüpe*) was the first nationwide educational ICT project that computerized and connected schools to the internet in the late 1990s (Runnel et al., 2009).[45] Long after the Tiger Leap program ended, Estonian officials have referred to the Tiger Leap in strategic communication as a metaphor for the country's overall success in transition to digital capitalism. For example, Opening the Tallinn e-Governance Conference 2017, President Kersti Kaljulaid noted that the Tiger Leap "gave the entire Estonian society the momentum to make a digital leap into the future. … Priorities changed for families – instead of a new refrigerator, it was often decided to rather invest into a computer and an Internet connection" (Kaljulaid,

---

[45] The Tiger Leap Foundation was established as a public-private partnership between the Estonian government, the United Nations Development Programme, the Open Estonia Foundation (a national chapter of the Open Society Foundation), the European Union PHARE (an assistance program to pre-accession and new EU members from Central and Eastern Europe), and private enterprises (Farivar, 2011, p. 123).

2017). Building on the successful realization of the Tiger Leap, the government, in cooperation with academic and private stakeholders, established the Information Technology Foundation for Education (HITSA).[46]

Other major domestic initiatives to raise ICT access and literacy in Estonia included Look@World—a public-private partnership that taught 100,000 Estonians computer and internet skills in 2002-2004—and the Village Road program that connected local governments, public libraries, and rural areas to high-speed internet. The framing of Look@World curiously but characteristically of e-Estonia strategic communication combined contemporary neoliberal and traditional nationalist rhetoric. At the closing ceremony for Look@World in 2004, then President of Estonia Arnold Ruutel celebrated the program for helping people to "improve their competitiveness in the labour market" and encouraging small villages to "strive for progress," while simultaneously narrating Look@World as a natural part of Estonia's centuries-long history: "It's just an Estonian tradition that skills and knowledge have always been passed on from generation to generation" (Ruutel, 2004).

The technological crux of e-Estonia is an ever diversifying set of e-government services (see e-Estonia; Ernsdorf & Berbec, 2007; European Commission, 2015, 2016, 2017; Kalvet, 2007; Kitsing, 2011; Kotka et al. 2015, pp. 2-5; Statistics Estonia 2017, pp. 18-21; Vassil, 2015). Two technical solutions underlie the functioning of e-government: electronic ID and X-Road. The X-Road, introduced in 2001, is a data exchange layer that links all public and private e-Estonia services into an interoperable environment. The

---

[46] HITSA manages the IT College, a higher education institutions founded in 2000, and the Tiger University, a program of wide-ranging development of ICT in higher education launched in 2002. Through a special program StudyITin.ee, the state has supported the creation of over a dozen of ICT-related English-language Bachelor's, Master's, and PhD programs aimed at international audiences in an effort to promote Estonia as a prime global destination for ICT education.

Electronic ID (eID)—a credit card sized plastic photo ID with a chip—was introduced in 2002 and serves as a mandatory national identification card that provides access to all e-services.

The public sector has been the primary driving force behind the country's ICT development (Björklund, 2016, pp. 918-920; Siil, 2001, p. 1). Among the first steps, Estonia put in place enabling legal and policy frameworks for the development of the digital environment. Some of the foundational laws that continue to underlie e-Estonia's framework were adopted in the second half of the 1990s and pertain to the operation of public databases, protection of personal data, access to public information, consumer protection, and digital signatures (European Commission, 2015, pp. 23-26).

As with Estonia's political economy writ large, telecommunications policy pursued maximum privatization and liberalization, such as lifting protective measures on foreign trade and restrictions on the movement of international capital, and eliminating nearly all import quotas and license requirements (Siil, 2001, pp. 2-3). This has attracted foreign investment, particularly from Nordic neighbors, and ultimately led to complete liberalization of Estonia's telecommunication market by 2001, when the special monopoly rights of the Estonian Telephone Company ended.

Estonia's overarching digital coordinating body is the Government of Estonia's E-Estonia Council, chaired by the Prime Minister and including several ministers, private sector executives, and leading IT experts (Estonian Government Office, n.d.). Ministry of Economic Affairs and Communications (MEAC) is the division of government most directly involved in the domestic development of e-Estonia. MEAC administers the Information Society program for 2014-2020, worth around 214 million Euros, 85 percent

of which comes from the EU Structural Funds (Estonian MEAC, 2015). The program encompasses all of Estonia's governmental e-activities, including drafting the country's cybersecurity and digital development strategies. MEAC houses the Information System Authority (RIA; Estonian Information Systems Authority, n.d.), an arm responsible chiefly for the technical maintenance and security of the national information system, and is home to the Government Chief Information Officer (e-Governance Academy, n.d.). Ministry of Foreign Affairs (MFA) leads Estonia's foreign policy of the internet, including the institutionalized promotion of internet freedom (Estonian MFA, 2017). The President of Estonia is a ceremonial figure not directly involved in policymaking, whose role is to advance the country's digital vision at high-level international gatherings.

While the government has provided the general impetus and coordination of e-Estonia, the private sector has been critical in its development. For example, the spread of private internet banking in the 1990s was one of the crucial factors in establishing trust and skills among the population toward online services, which laid the groundwork for the ensuing smooth adoption of e-government public services (Kitsing, 2011, pp. 9-10). The key industry partner for the state is the Estonian Association of Information Technology and Telecommunications (ITL), which accounts for over 75 percent of Estonia's ICT turnover, and the head of which sits on the E-Estonia Council (Estonian Association of Information Technology and Telecommunications, n.d.). The government strategically communicates a business-friendly image and advocates its IT sector to foreign audiences (Enterprise Estonia, n.d.-f).[47]

---

[47] Estonian officials often cite the World Economic Forum's ranking of Estonia as Europe's most entrepreneurial-friendly country in 2016 as part of e-Estonia narrative (World Economic Forum, 2016). This entrepreneurial identity was institutionalized as Startup Estonia, a self-described "governmental initiative aimed to supercharge the Estonian startup ecosystem," which works with the country's startup

While Estonia's utilization of digital technologies is among the world's most advanced, certain issues remain. The quality of services is inconsistent, so the government tends to highlight the "islands of excellence," such as the e-tax system, while obscuring the less successful projects, such as the essentially failed attempts at creating online platforms for citizen input and participation in the democratic process (Kitsing, 2011, pp. 10-16). Estonia's own digital doctrine openly acknowledges a number of challenges facing the sector.[48] e-Estonia's shortcomings, many of which are self-disclosed by the Estonian state, arguably do not undermine Estonia's status as one of the leading implementers of digital solutions. Estonia's digital services and accompanying technical, legal, and institutional infrastructures are still superior to the majority of the world's states and populations. For example, while Estonia ranks 25th of 28 countries in the EU in fixed broadband coverage of households with the report labeling Estonia's broadband coverage "low" at 91 percent of fixed broadband penetration (compared to 98 percent EU average), this lagging behind by EU standards is still far ahead of most countries in the world (European Commission, 2017). Moreover, in the provision and uptake of e-government services, Estonia ranks first in the EU.

This section introduced the material underpinnings of Estonia's digital nationalism, such as the key technological solutions, the policy framework, and the political-economic principles. The next section examines Estonia's post-1991 national

---

community by organizing events, developing unified marketing and branding, training entrepreneurs, and eliminating regulative issues and barriers seen as hindering the startup-friendly environment (Startup Estonia, n.d.).

[48] Estonia's Digital Agenda 2020 notes, for example, the shortage of ICT professionals, including due to brain drain; no or limited online access in some locales, particularly in rural areas; inadequate interoperability between the private and public sectors; unequal distribution of benefits from ICT solutions among the population; limited use of higher ICT skills to create jobs with higher added value; insufficient and simplistic use of ICT by Estonian companies, including low competence among owners and managers; and inadequacy of information society statistics (Estonian MEAC, 2013).

identity trajectory to illuminate how digital technologies and internet governance has come to be perceived as the core of its project of symbolically and institutionally joining the Euro-Atlantic community.

5.3 Estonian Identity: From National Awakening to Re-Independence

Estonia frames its digital developments as a way to overcome the Soviet legacy and catch up socio-economically with Western liberal democracies. This section discusses some of the key identity narratives that the modern Estonian state is founded upon in order to contextualize socio-historically the country's digital choices. The discussion is based upon scholarship on Estonian nationalism, history, and politics, as well as primary sources, such as annual addresses by the President on the anniversaries of the 1918 and 1991 independence, as well as national strategic documents that pertain to Estonian culture and identity.

Estonia regained independence from the Soviet Union in August 1991 after five decades of occupation.[49] In re-independent Estonia, negotiation and institutionalization of national identity have played a major role in the socio-political life (Made, 2003; Tamm, 2013; Vetik, 2012; Wulf, 2016). Public discourse in Estonia and neighboring Baltic states is steeped in "debates on the past as much as on the future. … History lives, breathes, provokes and mobilises Baltic publics to an extent almost unimaginable in neighbouring Western European democracies" (Auers, 2015, p. 7). Therefore,

No analysis of the history and politics of the Baltic States is possible without a

---

[49] In Estonia and in the international community, the Soviet rule in Estonia in 1940-1991 is referred to as occupation. Russia never officially recognized the Soviet period as occupation, maintaining the official Soviet position that the Baltic States voluntarily joined the Soviet Union in 1940. This remains one of the key points of contention in post-Soviet Russia-Baltic relations. This dissertation adheres to the internationally recognized terminology and refers to this historic phenomenon as occupation and, accordingly, to Estonia's independence of 1991 as re-independence – as it is used in contemporary official Estonian discourse.

sound understanding of the role and power of identity. … [O]nly by understanding how identity conditions and constrains the actions of elites can we fully comprehend Baltic politics at both the domestic and international levels (Mole, 2012, p. 1).

Given the centrality of history and identity to Estonia's domestic and foreign policy in the post-Soviet era, this section elaborates the historical background to the contemporary official identity discourse and explains how contentious internal identity politics ultimately inform the logics and language of Estonia's digital nationalism.

Re-independent Estonia's official identity discourse is centrally rooted in the notion of Return to Europe and the West (Auers, 2015, p. 228; Kuus, 2012, pp. 177-178; Smith et al. 1998, pp. 108-109). This trope alleges that Estonia historically is an inherently Western nation, but was forcefully separated from its civilizational roots during the period of Soviet occupation. Estonia has thus framed its post-1991 overarching geopolitical goal of symbolically and institutionally joining the Euro-Atlantic community as a return to Estonia's natural and rightful state of being and belonging. The discourse of the Return to Europe has become hegemonic in Estonian mainstream politics soon after independence was won: to question Estonia's Western-centric orientation is to undermine the very foundations of the modern Estonian state. At the same time, about a quarter of Estonia's Russian-speaking people, who constitute about a quarter of the population, have significantly lower levels of support for Estonia's Euro-Atlantic integration.[50] This

---

[50] The survey conducted by the Estonian Ministry of Defense in March 2017 showed, for instance, that "Estonian-speaking and Russian-speaking respondents' trust in the state's political and national defence institutions differs considerably. The greatest difference occurs in the confidence in NATO (78% of Estonian-speaking respondents trusts it completely or rather trusts them, the respective proportion for Russian-speaking respondents is 24%), the Defence League (87% vs 37%), the Defence Forces (92% vs 51%) and the president (77% vs 42%)" (Kivirähk, 2017, p. 4). The survey notes as well: "While Estonian and Russian-speaking respondents assess many global threats similarly, there is a fundamental difference in evaluating the activities of Russia. For Estonians, the threat of Russia shares the fourth and fifth place with the war in Syria (both 48%), whereas Russian-speaking respondents place it last (6%)" (Ibid.).

tension is key to understanding contemporary Estonian politics and is explored below.

The Birth of Estonianhood: From National Culture to National State, 1850s-1940

Estonian nationalism emerged in the 1850s-1860s, a phenomenon known as the National Awakening, when the lands of present-day Estonia were part of the Russian Empire (Kasekamp, 2010, pp. 76-82).[51] As Russian and German empires collapsed in the maelstrom of the First World War in 1917-1918, Estonia proclaimed independence for the first time in its history on 24 February 1918 and attained international recognition by 1921.

Two decades of independence between the World Wars in Estonia and neighboring Latvia and Lithuania were a time of intensive state- and nation-building (Auers, 2015, pp. 17-26; Hope, 1994; Kasekamp, 2010, Ch. 5; Lieven, 1993, Ch. 3). State borders of the Baltic States were for the first time largely congruent with the borders of respective ethnocultural titular majorities. As many countries across Central and Eastern Europe in that period did, Estonia began its independent path as a Western-oriented liberal parliamentary democracy in the 1920s before turning to mild corporatist authoritarian rule after a coup in 1934 (Kasekamp, 2010, pp. 106-112).

Soviet and Nazi Occupations and Ethnic Russification, 1940-1991

During the Second World War, the Baltic states of Estonia, Latvia, and Lithuania were first occupied by the Soviet troops in 1940, then by the Nazi regime in 1941-1944, and then again in 1944 by the advancing Red Army that was driving the German

---

[51] The very term "Estonian people" (*eesti rahvas)—*as opposed to a prior endonym of "country folk" (*maarahvas*)—appeared in 1857 in the address to the readership of the first Estonian-language weekly *Perno Postimees (The Parnu Courier)*. Present-day Estonia was then part of the Russian Empire but was governed by the local German minority. In the meantime, indigenous Balts, who constituted around ninety percent of the population, enjoyed few economic, cultural, and political rights. Estonian national movement at first saw its goals in expanding indigenous cultural-linguistic freedoms. Since the early twentieth century, however, it increasingly strove for full political independence from the imperial metropole.

Wehrmacht westward (Kasekamp 2010, pp. 124-130; Mole 2012, pp. 56-62; Misiunas & Taagepera 1993, pp. 15-44).[52] The second Soviet occupation lasted for half a century until the end of the Soviet Union in 1991 (Kasekamp, 2010, pp. 141-159; Misiunas & Taagepera 1993, Ch. 3-6; Mole, 2012, pp. 62-67). One of the most dramatic and lasting transformations of the Estonian society over the decades of the Soviet rule was demographic. Before the Soviet and Nazi incursions, the ratio of ethnic Estonians to Russians was approximately 9-1 and by the end of the Soviet period it was 2-1 (see Table 2).[53]

Table 2. Ethnic Estonians and Russians as a percentage of Estonia's population.

	1934	1959	1989	2011
Estonians	88,2	74,6	61,5	68,7
Russians	8,2	20,1	30,3	24,8

Sources: Eesti Bank, Estonian Economic Yearbook 1937 (cited in Hope, 1994, p. 52); Results of the All-Union Census of the USSR (cited in Mole, 2012, p. 85); CIA World Factbook (Central Intelligence Agency, 2018).

Estonia regained independence from the Soviet Union in August 1991 (Kasekamp, 2010, pp. 160-171; Misiunas & Taagepera, 1993, Ch. 7; Mole, 2012, pp. 68-80). Ethnic Estonians viewed 1991 as a moment of national liberation and return to the

---

[52] Estonia fell victim of collusion between the Nazi and Soviet regimes. In August 1939, Nazi Germany and Soviet Union signed the infamous Molotov-Ribbentrop Pact of non-aggression (Kirby, 1994). The Pact's secret additional protocols divided Central and Eastern Europe into spheres of influence between Hitler and Stalin; the three Baltic states were to fall under the Soviet rule. Vladimir Putin in the recent years publicly defended the Soviet decision to sign the Pact (Coalson, 2015). In the first year of its rule, the Soviet regime jailed, deported, and executed thousands of real and alleged opponents. In June 1941, Nazi Germany broke the Molotov-Ribbentrop Pact, invaded the Soviet Union, and occupied the Baltic lands that formed the core of the Nazi occupation regime of *Ostland.* Western nations *de jure* never recognized the Soviet occupation of the Baltic countries (see Hiden et al. 2008).

[53] The shift in the majority-minority composition resulted from a number of factors, such as Stalin-era purges and deportations, military and civilian losses of the Second World War, outward migration of German and Swedish minorities and of many ethnic Estonians to the West, and systematic resettlement over decades of hundreds of thousands of Russian-speakers predominantly to the North-Eastern part of Estonia but also Tallinn. Being speakers of the Soviet Union's lingua franca, the majority of Russian-speakers in Estonia did not see the need to become fluent in Estonian or otherwise integrate into the Estonian ethno-cultural space over the several decades of their inhabiting the republic. These changes in Soviet Estonia's demographics would come to profoundly influence post-Soviet Estonia's socio-political life.

ideals of the interwar independence, which by then had been greatly mythologized over the decades of the Soviet rule. Most Russians interpreted the coming of Estonia's independence as their own downfall from the status of a privileged majority within the Soviet empire to an underprivileged minority in a foreign cultural-linguistic environment. Estonians' and Russians' media consumption and cultural, linguistic, and political repertoires in 1991 and to this day differ, making the majority-minority relations one of the most prominent issues of Estonia's socio-political life (Kus-Harbord & Ward, 2015; Steen, 2010; Vihalemm & Kalmus, 2009).

Re-Independent Estonia, 1991-Present: "Our identity is both geographically and spiritually a European one."

Estonia's digital nationalism, the country's development of ICT infrastructure and its communication to the world as a sign of Estonia's progressive European nature, took root several years after re-independence of 1991. This section explains how Estonia arrived at its official liberal pro-Western identity discourse of the past quarter of a century and how it has informed the emergence of its digital nationalism.

In the lead up to independence and its immediate aftermath, when the very foundations of Estonian statehood were being put in place, Estonian conservative nationalists prevailed over the more ethnically accommodating political elites (Lieven, 1993, pp. 274-288; Smith et al., 1998, pp. 94-98). As a result, existential viability of the Estonian culture and language became the single most important *raison d'être* for the Estonian state. The Estonian ethnocultural majority thus established a privileged, and at times exclusive, relationship with state institutions, as the rationale of national protection from the threatening Other—the Russian minority seen as an extension of the Russian

state—trumped the principle of civic equality (Agarin & Regelmann, 2012; Järve, 2005).

Re-independent Estonia adopted the principle of legal continuity from the interwar independence of 1918-1940, thus originally excluding virtually all non-ethnic Estonians from the body politic by making Estonian the sole official language and extending citizenship only to those whose families had lived in Estonia before the Soviet annexation of 1940 (Mole, 2012, pp. 87-92).[54] For instance, there were no ethnically non-Estonian Members of Parliament until 1995. The belief of Estonian elites was that a successful transformation from the "Homo sovieticus toward the rational capitalist actor" would by itself minimize the majority-minority tension through creating appealing economic conditions that would encourage the Russians to voluntarily assimilate (Kennedy, 2002, p. 153-159). In the words of Mart Laar, Prime Minister of Estonia in 1992-1994 and 1999-2002, Estonia needed "a clear cut with the past" in order to turn itself "from the country of the working class to a country of entrepreneurs" (cited in Farivar, 2011, p. 120).[55]

By removing representatives of a competing identity coalition from meaningful participation in national politics, the Western-oriented ethnically Estonian identity coalition was able to instill the notion that Estonia's fate naturally lays in symbolically and institutionally joining the Euro-Atlantic community as the dominant discursive and policy framework of Estonian statehood (Auers, 2015, p. 228; Kuus, 2012, pp. 177-178; Smith et al., 1998, pp. 108-109). For example, in an unequivocally titled speech from

---

[54] Despite Estonia's small population and gradual liberalization of its citizenship policy over the years, Estonia still has the tenth largest stateless population in the world, consisting mostly of Russian Estonians (Human Rights Watch, 2015).

[55] Revealing of Estonia's political-economic orientation at the time, Mart Laar, a historian by training, "has famously claimed that the only book he read on economics prior to taking office was the American economist Milton Friedman's *Free to Choose*, which argues for economically liberal and libertarian policies" (Farivar, 2011, p. 120). In 2006, Laar received the Milton Friedman Prize for Advancing Liberty from the Cato Institute.

1998, "Estonia's Return to Europe," Toomas Ilves stated: "Our ties with the Nordic states of Finland, Sweden, Denmark, and Norway have been strong from our prehistory onward, and our identity is both geographically and spiritually a European one" (Ilves, 1998).[56] Ilves provided a lengthy list of his government's economically liberal measures as supposed evidence that Estonia "made rapid progress in becoming a normal, albeit poor democratic, free-market European country and toward joining European and Euro-Atlantic structures created while [Estonia was] occupied" (Ibid.).

Estonian academic, media, and political establishment narrated Estonia's supposedly obvious belonging to the West in the essentialist language of "banal Huntingtonianism" (Kuus, 2012). Echoing Samuel Huntington's thesis of the Clash of Civilizations, which enjoyed great popularity among Estonian establishment, Estonian elites portrayed their country as the last frontier of Western civilization on the border with Asiatic-Eastern despotism, i.e. Russia, and therefore in need of symbolic and institutional embrace from the Euro-Atlantic community.[57] For example, on the visit to Hamburg in 1994, Lennart Meri, President of Estonia in 1992-2001, insisted that Estonia and other transitional states must be "safely anchored in the West":

> Then it will be possible … to help democracy, free enterprise, private property,
> and not least of all the rule of law, on the road to success. If, however, those
> states, including Estonia, are left to their own devices and exposed to the

---

[56] The use of Estonia's liberal reforms to allege its European identity continued even after Estonia's accession into EU and NATO. In 2010, Marina Kaljurand, then Undersecretary for Economic and Development Affairs and Minister of Foreign Affairs in 2015-2016, wrote in an article "Estonia – Watchdog of free trade": "Estonia's positions regarding trade are more European than those of many European Union member states and the EU as a whole, as well as more liberal than those of the majority of WTO member states" (Kaljurand, 2010).

[57] Estonian translation of Samuel Huntington's *The Clash of Civilizations and the Remaking of the World Order* was published in 1999. Then Minister of Foreign Affairs Toomas Ilves authored the foreword to the book and, alongside Prime Minister Mart Laar and Samuel Huntington himself, spoke at the conference in Tallinn that celebrated the book's publication. Major Estonian-language media interviewed Huntington and extensively covered his work (Kuus, 2012).

potential neo-imperialist appetites of Moscow, the price for it would be too high,

even for all Europe, to pay. (Meri, 1994)

Even as the openly civilizational rhetoric subsided after the 1990s, the logic that

normatively links Estonian identity with Western liberal values has continued to inform

the country's official vision. For example, Integrating Estonia 2014-2020, the current

iteration of the national strategy for integrating minorities into Estonian economic and

social life, defines Estonian national identity as being "based on recognising and valuing

liberal democratic norms, values and procedures" (Estonian Ministry of Culture, 2014, p.

40). The next section examines why and how Estonia's self-proclaimed liberal-

democratic national identity came to incorporate digital technologies as its crux.

From Liberal-Democratic Identity to "High-Tech Identity"

As part of the overarching liberal political-economic restructuring of the country

in pursuit of Euro-Atlantic integration, since the mid-1990s Estonia has incorporated

digital technologies into its state governance and the narrative of the national Self. In the

words of Lennart Meri on his visit to Microsoft in the United States in 1995, the new

national goal lay in "making Estonia the model state of information technology" (cited in

Farivar, 2011, p. 123). Estonia has since completely renovated its ICT infrastructure and

become one of the world leaders of e-governance, while strategically communicating its

identity as epitomizing technological innovation.

Estonia has narrated its national identity as expressive of digital global economy

through bridging the logics and languages of neoliberalism and nationalism (Feldman,

2005). Neoliberal discourse of technology draws a normative causal link between the

adoption of ICT solutions and socio-economic progress (Golumbia, 2009; Mansell, 2012;

Mosco, 2005). Estonia has thus framed the adoption of digital solutions into governance

as a way of overcoming cumbersome and wasteful Soviet *bureaucracy* in favor of minimal, efficient, and market-friendly *public administration*. Illustrative of this rationalist logic, Estonian Information Strategy from 2006 alleges: "It is only natural and reasonable to use information technology for a more rationalized organization of living" (Estonian MEAC, 2006).

Couching its ICT development in the language of neoliberalism, Estonia simultaneously frames this as an expression of ethnocentric nationalism and a matter of cultural survival. For example, Sustainable Estonia 21, the country's national development strategy issued in 2005, posits as one of the key threats to Estonianhood a "certain stagnation of the Estonian language and culture, their failure to adapt to the requirements of the new global civilisation (information society and technological culture), which reduces the functionality of national culture and weakens its motivation for persistence" (Estonian Commission on Sustainable Development, 2005, p. 14).

As early as in 1999, when Estonia was not yet globally known for its ICT innovations, then Minister of Foreign Affairs Toomas Ilves already claimed that Estonians have a "high-tech identity" and that Estonia's being "more interneted [sic] than half the EU" signaled the country's rightful belonging among fellow Northern Europeans: "Clearly the case is to be made that these Protestant, high-tech oriented countries form a Huntingtonian subcivilisation … [with] a similar mindset and a culture geared to the demands of a modern, globalised economy" (Ilves, 1999). The neoliberal nationalist discourse of Estonia's widespread ICT adoption narrates technological savvy as inherent to Estonia's civilizational identity to allege Estonia's inherent belonging among developed Euro-Atlantic states.

This section illuminated why and how digital technologies have become discursively incorporated into Estonia's nationalism. The following discussion examines how this understanding became the centerpiece of Estonia's national strategic communication.

5.4 Brand Estonia: Nordic, Environmental, and Digitally Advanced

Estonia's strategic narrative of e-Estonia and internet freedom is part of the broader strategic communication framework that was established in the early 2000s and has since come to be seen by the Estonian leadership as an essential part of foreign policy. Estonia's Foreign Policy Objectives, the set of official strategic foreign policy principles, name "Estonia's influence and good reputation" as one of its five foundational pillars on par with national security, economic development, protection of Estonians abroad, and promotion of liberal-democratic values (Estonian MFA, 2013). According to Estonia's Foreign Policy Objectives, in pursuit of international influence and good reputation Estonia pledges, inter alia, to take initiative in international organizations, promote reputation of Estonia as an innovative state, share expertise and participate in discussions of global matters, and take international responsibility and commitment. This and the next sections elaborate how these principles came into being and have been put into practice in order to illuminate how the strategic communication of e-Estonia became central to Estonia's digital nationalism.

The logic of Estonia's communication approach conveys at once the government's perception of *cultural* globalization as a threat to the coherence of its domestic identity and *economic* globalization as an opportunity to develop a competitive

identity that stands out and attracts tangible and intangible gains. Sustainable Estonia 21 thus states:

> As a counter-reaction to globalisation, local and regional attempts to diverge from globally spreading trends, to value the local language and culture and to integrate the global and the local are strengthening worldwide. Regions and states that better succeed in cultivating their identity will gain an important competitive advantage. (Estonian Commission on Sustainable Development, 2005, p. 9)

Accordingly, Estonia has actively cultivated and communicated to the West an identity of a normal liberal European nation, so as to escape lingering in the mental geography of Western elites and publics as a backward post-Soviet periphery, which Estonian leadership saw as a direct threat to its "competitive advantage." Thus, since regaining independence in 1991, and in a more concerted and coordinated fashion since the late 1990s-early 2000s, Estonia's political leadership devoted much attention and resources to strategic communication of its identity. In 1999, Toomas Ilves described this strategic communication imperative as attention to "how Estonia is viewed, where it resides subjectively in the perceptions of the West, and then in what sense it would make much more sense to view Estonia in an integrated Europe" (Ilves, 1999).

In the 1990s, however, Estonia possessed scarce financial resources and no external communication infrastructure, so its Westward-oriented messaging was unsystematic and limited in volume. At the same time, the central narrative about Estonia's successful transition to a normal democratic European country remained highly consistent. The main channel of Estonia's outward communication was elite-to-elite, primarily in the form of addresses at high-level international gatherings and publications

in Western media and academic venues by representatives of the Estonian political class.[58]

Despite Estonia's efforts to distance itself from the East, in the 1990s the country's image in the media was overwhelmingly tied to its Soviet past and strained relations with Russia.[59] In order to change Western media and political elites' perceptions of Estonia, the government in the late 1990s-early 2000s was looking to directly communicate a more positive image of Estonia to Western audiences and develop a strategic communication initiative centered around the narrative of the country's digital progress and overall modern outlook (Aronczyk, 2013, pp. 139-144; Jansen, 2012; Jordan, 2014; Mäe, 2017).[60] Many governments of former socialist countries have turned to concerted strategic communication of their identities, particularly in the lead-up to their accession into EU and NATO, in order to convey that they had shed a socialist past and reinvented themselves as normal market democracies (Kaneva, 2012; Saunders,

---

[58] A rare exception to this approach was a paid media campaign in the mid-1990s in the *Newsweek* magazine. With a loan from the World Bank, the government ran a supplement "Estonia: The Little Country that Could" and several follow-up articles that painted Estonia as a place of a successfully going liberal transformation and a stable place for foreign investments (Jordan 2014, p. 33). "The Little Country that Could" has since become an oft-used slogan for advocates of Estonia. Curiously, Mart Laar portrayed this slogan as impartial evidence of Estonia's achievements in an essay "Estonia's Success Story" in the *Journal of Democracy* of the National Endowment for Democracy, itself a characteristic venue of Estonia's self-promotion in the 1990s: "We deserve the moniker that *Newsweek* magazine gave us in one of its headlines: 'The Little Country That Could'" (Laar, 1996, p. 97). In 2002, Laar published a nearly 400-page volume on Estonia's transition titled "Estonia: Little Country That Could" (Laar, 2002).
[59] Occasional media praise for Estonia, even when well-intentioned, often only reinforced the post-Soviet associations Estonia was trying to escape. For example, a *New York Times* author commended the Tallinn Department Store for being "drop-dead riveting, simply because it is normal. There are no guards in camouflage uniforms at the entrances, no dirt, not even a faint whiff of urine" (Erlanger, 1994).
[60] Prime Minister Mart Laar's enthusiasm for nation branding had its critics at home and abroad as a wasteful enterprise with murky prospects. *The Economist* magazine, generally fond of Laar's devout liberalism, dismissively commented: "Mr. Laar has paid a lot of attention to swanky futuristic projects. … [Some] smell of gimmickry, such as finding a new 'national symbol and idea' to 'shape Estonia's identity from the inside and make it more known abroad'. The use of 'e-stonia' to point up the country's voracious use of the Internet is another fancy ploy" (Economist, 2001).

2016). Estonia in particular has shown exceptional diligence, comprehensiveness, and commitment to strategic communication.

The adoption of a nation branding strategy in 2000-2001 signaled a qualitative change in Estonia's strategic communication, as compared to the 1990s. The country gained much greater communicative agency by building an institutionalized external communication infrastructure with continuous, multifaceted, and coordinated messaging. Estonia's strategic communication has grown increasingly voluminous and diverse over the years and now includes several websites (e.g., Estonia.ee, a general introduction to the country, and issue-specific sites on travel, trade, investment, work, and study in Estonia), social media accounts, dozens of brochures, videos, and presentations, and a range of downloadable materials available to anyone wanting to promote Estonia independently. Estonian politicians and diplomats, who directly address global political, business, and media elites, are another medium of strategic communication.

In line with Estonia's official identity discourse, Estonia's strategic communication has for two decades narrated Estonia as a Nordic, environmentally friendly, and digitally advanced nation (Enterprise Estonia, n.d.-e).[61] Enterprise Estonia, the governmental agency responsible for the country's strategic communication, offers the following two-sentence summation of Estonian identity discourse to anyone who wants to promote Estonia: "In Estonia, clean and untouched nature co-exists with the world's most digitally advanced society. It is a place for independent minds where bright ideas meet a can-do spirit" (Enterprise Estonia, n.d.-g).

---

[61] For explication of the logic behind Estonia's branding, see Enterprise Estonia's Brand Estonia site (Enterprise Estonia, n.d.-a).

The trope of Estonia as a digitally advanced society, known as e-Estonia, is particularly central to the country's strategic communication. Estonian elites recognize its digital storytelling as the state's most potent instrument of soft power: "'cyber story' – something that is definitely worth, among other things, to be recorded as a real book – has undoubtedly made Estonia more visible and larger," said then President Toomas Ilves in 2012, while defending the story against critics: "there are some cynics among us, who see our cyber story as a skilfully [sic] yarned myth or national propaganda" (Ilves, 2012a). The next section examines key discursive pillars of the strategic narrative behind e-Estonia.

5.5 Promoting "Greater Awareness of e-Estonia in the World"

Estonia's rise as a leading voice of "internet freedom" needs to be understood as an inherent element of the country's pervasive strategic narrative about itself as a digitally advanced society, e-Estonia. Estonia started to promote its technological advances at the highest level of international diplomacy, such as UN meetings, in the late 1990s, at least several years before global internet governance began its quick ascent as a major geopolitical issue. By 2003-2005, the inaugural years of the global internet governance debate, Estonia had already developed a discursive framework for promoting its digital achievements and established a reputation as a supporter of liberal digital policies. The strategic goal of communicating Estonia as digitally advanced, including its support of internet freedom, is to convey the country's economic and cultural belonging in Western modernity.

This section details Estonia's digital discourse in order to historicize and contextualize the country's internet freedom narrative. The discussion grounds the often

ephemeral rhetoric of an open, borderless, and free (including from geographical constraints) global internet and of Estonia as an e-state in tangible realities of state institutions and policies that emanate from national visions and serve a distinctly national purpose. Such a juxtaposition speaks to the central task of digital nationalism that analytically relates national identity to digital discourse and policy.

At first, I situate efforts to promote the e-Estonia narrative within Estonia's national digital development program in order to emphasize the strategic nature of these efforts. The deep embeddedness of e-Estonia in Estonian foreign policy and strategic communication illustrates the extent to which Estonia has linked these efforts to its very identity. This discussion outlines the key tactics of Estonia's variegated promotion of e-Estonia to illustrate the scope and meticulousness of these efforts. Elaboration of these promotional activities is followed by the analysis of the narrative itself. I examine key tenets of Estonia's digital discourse to explain how they relate to the country's identity discourse.

The discussion of e-Estonia as a narrative is based upon textual analysis of primary documents pertaining to this theme of Estonia's strategic communication: relevant speeches that were located on the websites of the President, the Ministry of Foreign Affairs, and the Ministry of Economic Affairs and Communication (e.g., address by the President of the NATO cybersecurity conference); relevant promotional materials (e.g., the website e-estonia.com); and policy documents (e.g., all iterations of the national digital strategy, the latest of which is Digital Agenda 2020).

e-Estonia: The Structure of Promotional Efforts

President of Estonia Kersti Kaljulaid calls Estonia "the only digital society that has a state" (Kaljulaid, 2017b), while Estonia's official website refers to it as "the world's first country to also function as a digital service" (Enterprise Estonia, n.d.-c). This narrative of Estonia's outstanding digital record punctuates much of the country's official communication, even that which is not directly related to the digital domain, such as Estonia's official tourism portal (Enterprise Estonia, 2017). In addition, there is a multitude of online and offline efforts focused specifically on promoting e-Estonia.[62]

The multifaceted yet rigorously coordinated efforts aimed at advancing the image of Estonia as a global digital maverick are instituted as highest-level national policy. Digital Agenda 2020 notes the ultimate "aspiration for Estonia to become as re-known [sic] for its e-services as Switzerland is in the field of banking" (Estonian MEAC, 2013, n.p.). Digital Agenda 2020 establishes *Greater Awareness of e-Estonia in the World* as one of the country's four strategic goals in the digital domain. These promotional activities are intended to "support the efforts of [Estonia's] businesses in foreign markets, contribute to attracting foreign investments and help Estonia to achieve its general foreign policy goals" (Ibid.). These goals, in turn, serve to solidify Estonia's ties with the Western world.

Proposed steps towards raising Estonia's international profile as a digital champion include, *inter alia*, hosting international information society events in Estonia, participating in relevant international conferences and competitions, promoting Estonia's

---

[62] e-Estonia.com online portal—with a tagline "We have built a digital society and so can you"—offers a wealth of background information on Estonia's e-government, latest news, and practical information on the IT sector (https://e-estonia.com). Enterprise Estonia publishes specialized brochures, catalogs, and investment guides available online and distributed at major professional expos (https://issuu.com/eas-estonia). In Tallinn, a 360 square meter e-Estonia Showroom exhibits the country's digital accomplishments to visiting high-profile delegations of politicians and business people (https://e-estonia.com/showroom). Estonia also regularly hosts major international ICT-related events.

experiences in foreign traditional and social media, conducting and disseminating analyses about the development of Estonia's information society, actively participating in international standardization and policy-making processes in the key areas of information society, and carrying out information society and governance-related trainings in other countries.

Estonian politicians actively promote e-Estonia through diplomatic, media, and academic domains. For example, during Estonia's six-months Presidency of the EU Council in 2017, two of the four declared Priorities directly related to the digital agenda: "An open and innovative European economy" and "A digital Europe and the free movement of data" (Estonian Presidency of the Council of the European Union, n.d.). Here and elsewhere, Estonia relies on foundational rhetorical markers of the liberal digital discourse, such as "open," "innovative," and "free," to assert its liberal-democratic orientation.

Estonian leadership is also attentive to the academic world, as many leading academics through their active involvement in the internet governance debates shape its agenda, discourse, and policies. Besides invited talks by Estonian officials at top-tier global universities,[63] the Estonian Government, for example, co-finances together with the European Social Fund the work of the Cyber Studies Programme at the University of Oxford (University of Oxford, n.d.).

As discussed above, the desire to change Estonia's portrayal and perception in Western media, and therefore among Western elites and publics, inspired Estonia to

---

[63] In addition to talks mentioned in the opening of this chapter, Taavi Rõivas, for example, gave a talk on "Leveraging Technology in Turbulent Times" at Stanford University in 2014 (Rõivas, 2014), while Taavi Kotka, then Estonia's Chief Information Officer and head of the e-Residency program, gave a presentation on "Countries Without Borders, Countries Without Territory, and Digital Citizenship" at Columbia University in 2015 (Kotka, 2015).

begin developing a systematic approach to strategic communication in the late 1990s-early 2000s. Even as Estonia created multiple platforms for outward communication of its identity and digital accomplishments, their reach is understandably far lower than that of established global media, such as the *New York Times* or *Wired*. In order to amplify its message by reaching wider audiences, Estonia has cultivated media relations with foreign outlets as one of key tactics of its digital promotional strategy.

Digital Agenda 2020 lists "Coverage of e-Estonia in international media" as one of the quantitative indicators, by which the government is to assess the success of Estonia's digital development at the end of the program's designated term. To boost the coverage of e-Estonia in international media, top-level Estonian officials make themselves readily available for media commentary and interviews. As a result, much of reporting on e-Estonia features the country's leading figures and essentially reiterates their talking points (e.g., Gaskell, 2017; Hammersley, 2017; Mansel, 2013; Pardes, 2016).

A typical example of such reporting appeared in *The Guardian* under the headline (which is hardly distinguishable from the language of the Estonia state's own strategic narrative) "How tiny Estonia stepped out of the USSR's shadow to become an internet titan. The European country where Skype was born made a conscious decision to embrace the web after shaking off Soviet shackles" (Kingsley, 2012). The article features Toomas Ilves, Estonia's President at the time, and Linnar Viik, a leading e-Estonia evangelist, whose rhetoric the author of the publication readily recites. Thirteen years after Toomas Ilves spoke of Estonians' "high-tech identity" as alleged evidence of their inherently Nordic character, *The Guardian* describes how the internet has become

"tightly entwined with Estonia's identity" as "the country's ethnic Estonian majority feel Nordic, rather than Slavic or eastern European" (Ibid.).

e-Estonia: The Strategic Narrative

The official story of Estonia's post-Soviet trajectory is a typical transitional narrative of a linear progression from socialist planned economy under Soviet occupation to a Western market liberal democracy after regaining independence in 1991 (see Kennedy, 2002). While many countries of Central and Eastern Europe promote real or alleged technological achievements as part of their Western-oriented transitional narrative, Estonia stands out in terms of the centrality of information and communication technologies to its story. Estonia attributes its successful economic transformation to the fact that it decided to overhaul its ICT infrastructure and integrate it into governance. ICT is thus embedded into the very core of Estonia's post-socialist identity narrative.

Representatives of the Estonian state have been advancing this narrative, with slight variations, over almost two decades. For example, President Toomas Ilves shared the story in his characteristically expressive manner with the attendees of the 2011 International Conference on Theory and Practice of eGovernance:

> When Estonia reestablished its sovereignty after a half century of successive thuggish totalitarian foreign occupations …, we knew we wanted to create a democratic country characterized by rule of law and respect for human rights.
> … After the Soviet period we were also poor. Very poor. So in terms of economic reforms, we also knew what needed to be done: restore the market economy.
> … This briefly encapsulates the real problem faced by a small country struggling to climb out of the ruins of totalitarian rule, poverty and general backwardness. Our fundamental existential question was, can a country as small as we make it?
> … [W]e became pioneers in use of ICT in government first because it seemed the best if not only way to leapfrog decades of backwardness caused by awful Soviet

rule; Information technology and its use in the public sector as well as the private became the engine of our rapid development, and enabled us to become a leader offering innovative solutions we gladly share with others. (Ilves, 2011)

This excerpt from Ilves' speech conveys the essence of e-Estonia narrative, key pillars of which have remained constant across time and across institutions and individuals representing the re-independent Estonian state.[64] Below, I deconstruct this characteristic passage as an entry point into the critical analysis of Estonia's digital discourse and its relation to Estonia's identity discourse.

Estonia's digital narrative has a clear temporal arc: from the decades of "thuggish totalitarian foreign occupations" and particularly the "awful Soviet rule" (1940-41, 1944-1991), to the moment of national liberation when "Estonia reestablished its sovereignty" (1991), and to the ensuing transitional years of struggling to "leapfrog" the legacy of totalitarian rule through liberal policies (1991-present). This temporality is rooted in liberal teleology, which views liberal-democratic governance as the only viable governance model and therefore the end goal of political development. After veering off this linear path, which Estonia set out on in the interwar period but was forced off of during the Soviet and Nazi occupations, the task after 1991 was to "restore" liberal economic and political principles. The implication of this rhetorical framing is that Estonia is *returning* to—as opposed to embarking upon anew—its liberal-democratic ways and the European community, and therefore that Estonia naturally is entitled to a place within the Western cultural sphere and political institutions.

---

[64] For example, in July 2017, President Kersti Kaljulaid, Toomas Ilves' immediate successor, recited this narrative in a meeting on cyber and innovation issues with Vice-President of the United States Michael Pence in Tallinn: "A quarter of a century ago when Estonia restored its independent statehood we were a poor country. The crucial question stood in front of us – how to overcome the legacy left to us by the Soviet occupation? Our response was – we need to build up a modern, efficient and democratic state. We carried out radical reforms in all spheres of life. Our principle idea was to harness the innovative potential of ICT" (Kaljulaid, 2017c).

As a supposed sign of Estonia's belonging in technological modernity, the country's leadership continuously emphasizes the conscious strategic nature of its adoption of ICT in national development. Digital Agenda 2020 states: "The development of information society in Estonia is a strategic choice to improve the competitiveness of the state and to increase the overall well-being of people" (Estonian MEAC, 2013, n.p.). This trope is meant to convey the strategic foresight of the Estonian leadership and alleges their natural appreciation of high technologies as "the best if not only way" (Ibid.) to develop the economy. Adoption of ICT, in turn, is narrated as having crucially helped Estonia to "leapfrog" from post-Soviet poverty to "rapid development" (Ibid.). This normative causal framing of the relationship between the spread of ICT and economic growth is in line with the prevailing neoliberal vision of information society (see Mansell, 2012, p. 18).[65] By discursively bridging ICT development and economic development in a causal fashion, Estonia at once signals its strategic vision, economic success, and shared free-market ideals with the liberal West.

Ilves rhetorically distances re-independent Estonia from its Soviet past by referring to it in unequivocal terms as awful, backward, thuggish, ruinous, and totalitarian. Clear rhetorical delineation of the socialist past from the liberal capitalist present is a core pillar of transitional discourse. Immediate post-socialist ruling elites across the region represented the Soviet era as both a temporal and spatial Other—as a threat that emanated from the outside ("foreign occupations") but is now left in the past and beyond the reestablished sovereign borders. In the first post-Soviet years, even

---

[65] Consider, for example, then Secretary of State Hillary Clinton's causal framing of the relationship between connective technologies and economic development in her programmatic "Remarks on Internet Freedom" from 2010: "In many cases, the internet, mobile phones, and other connection technologies can do for economic growth what the Green Revolution did for agriculture. You can now generate significant yields from very modest inputs" (Clinton, 2010).

Moscow, the former Soviet metropole, framed the preceding Soviet rule as foreign to the new Russian polity founded upon liberal-democratic principles and as an unfortunate legacy to be overcome.

The question of the ethnic Estonian nation's existential viability, which Ilves' speech raises, is a prominent theme in Estonia's identity discourse and is also central to the digital discourse in two ways. First, the e-Estonia narrative posits ICT as central in overcoming "poverty and general backwardness," and thus saving the nation by rapidly improving the country's socio-economic conditions.

The second way in which Estonian leaders discursively link ICT with the nation's existential viability is through the direct use of digital technologies in cultural-linguistic preservation. Digital Agenda 2020 thus notes that "the continuity of the Estonian language and culture will be ensured" when developing an information society and that "**[d]igitisation of Estonian cultural heritage**, its **preservation** and **dissemination** in a digitised format (including as open data) will be supported" (Estonian MEAC, 2013, n.p.; original emphasis).

The self-asserted and internationally recognized status of Estonia as a "pioneer" and "leader" of digital innovations allows Estonia to posit itself as a hub of expertise that it is ready to share with the world. This trope follows one of the imperatives of Estonia's Foreign Policy Objectives to promote Estonia's good reputation as a "state that shares its expertise" (Estonian MFA, 2013). Estonian officials thus constantly emphasize the country's status as the world's leading digital hub that enthusiastically shares its knowledge towards the common good of global technological advancement. The tactic contributes to Estonia's image of a mature, productive member of the international

community, as opposed to a dependent aid recipient.

Notably, in the late 1990s-early 2000s Estonia began to promote its status of a technological expert very early into the existence of e-Estonia as a concerted effort. For example, in 2000, then Minister of Foreign Affairs Toomas Ilves was already praising Estonia's technological progress, including Tiger Leap, and willingness to assist others. Although Tiger Leap was carried out with substantial assistance from international donors, Estonia's strategic communication discursively employed the program as an example of the country's indigenous technological ingenuity in the face of limited resources:

> Estonia has the honour of finding itself among the 20 most computerized nations in the world. More importantly, we have done this not as a rich country, but as a nation with rather modest means. … We have seen this in my country firsthand through our Tiger Leap programme whereby every school in Estonia has, for some time now, been connected to the Internet. … This is why Estonia wholeheartedly endorses, and will actively participate in, the United Nations plans to assist all Members in making the information technology dream a reality. (Ilves, 2000)

Estonia's status of a pioneer of digital technologies at home conferred credibility upon it in the eyes of international audiences to become a leading voice in global digital affairs, including internet governance. For example, in a complimentary article from 2017, "Estonia's rise into a digital nation," a British online portal for IT professionals writes that "Estonia, which currently holds the European Presidency, attracted EU leaders to Tallinn in September to encourage Europe to be more digital. It's in a position to do this because of its advanced digital society" (Marzouk, 2017).

Whereas in most areas of international relations Estonia's geopolitical influence is limited due to objective demographic and economic constraints, in global politics of the

internet, Estonia's clout far exceeds its nominal weight. The next section investigates

Estonia's official narrative in the debates surrounding global internet governance.

5.6 An Internet Freedom Champion: Aligning with the West, Othering the East

Global Internet Governance as a Site of Digital Nationalism

Policy debates about who should govern the internet and how it should be

governed have become one of the key sites of digital nationalism. In this novel domain of

global governance, states promote digital policies, informed by local identities, that

advance their sovereign interests. The two poles of the internet governance debate are

those of internet freedom and internet sovereignty. I view both positions as strategic

narratives that advance national identities in the domain of internet regulation.

Internet freedom rhetoric, spearheaded by the United States, builds upon the

concept of free flow of information. Free flow of information posits that national states

should not impose undue restrictions on the global data flows, such as restricting access

to social media platforms and the news content they carry. Internet sovereignty rhetoric,

advanced chiefly by Russia and China, argues that it is the concept of national

sovereignty and the ensuing right of governments to restrict data flows in accordance

with local cultural and legal norms that should serve as the guiding principle of internet-

related policymaking. This approach manifests itself, for example, in data localization

laws that require Western media companies, such as Facebook and LinkedIn, to maintain

servers within geographical borders of the state.

The very vocabularies of the two approaches differ. Internet freedom deploys the

tropes of an open, global, borderless, and free internet governed by a multistakeholder

model: participation in internet governance of all relevant state and non-state stakeholders. Internet freedom links this vision to socio-political tropes of democracy, freedom (of expression and otherwise), human rights, and rule of law. Internet sovereignty privileges the language of protecting local cultures within national geographical borders, primacy of national legislation and governments over global non-state structures, and reliance on international law and multilateral state-based organizations, such as the United Nations, in governing the internet.

Digital nationalism critically approaches both narratives with an understanding of their strategic nature and the fact that the workings of the internet incorporate strains of both globality and national sovereignty. The primary goal of digital nationalism as an analytical approach is not to expose internet governance rhetoric of any one actor as untrue or show that one narrative is preferable to the other. Instead, digital nationalism examines the *logic* behind the state's internet governance discourse to explain why and illustrate how it emerged by examining respective national socio-historical contexts.

This section highlights key pillars of Estonia's internet freedom narrative to illustrate the main argument of digital nationalism that identity discourse informs the logics and language of digital discourse. In the case of Estonia, identity discourse stems from the notion of Return to Europe, symbolic and institutional aligning with the Euro-Atlantic community. Accordingly, Estonia's internet freedom rhetoric relates to Western liberal discourse.

The section is based on the analysis of Estonia's internet governance discourse located through the websites of President of Estonia and the Ministry of Foreign Affairs as the two most pertinent governmental institutions to Estonia's external strategic

communication (see above). The entirety of speeches of Estonian Presidency were searched to locate those addressing internet governance, while the MFA documents were located through searches of the website for the keywords "internet," "cyber," and "digital."

Estonia's Internet Freedom Narrative: "We need our Locke, Jefferson and Voltaire for the digital age."

Estonia is arguably second only to the United States in championing the internet freedom agenda at the international level. The logic of Estonia's rhetorical and institutional involvement in promoting internet freedom should be understood within the longer and broader effort by Estonia to communicate an image of an exemplary digital society, e-Estonia. Like the e-Estonia narrative generally, Estonia's internet freedom narrative rhetorically aligns the country's discourse of the internet and its governance with that of the United States and Western European states. By echoing some of the core pillars of Western liberalism (e.g., democracy, human rights, rule of law, freedom of expression) in its discussion of internet governance, Estonia discursively contributes to its foundational identity narrative of the Return to Europe.

Discussions of internet governance, an area of global politics where Estonia is viewed on par with some of the world's great powers, draws attention to the country that otherwise infrequently finds itself in the international spotlight. Western media and political establishments have widely praised Estonia for its role in internet governance. For example, in the words of John Kerry, U.S. Secretary of State in 2013-2017, "Estonia has set the gold standard, really, the global gold standard in cyber security, in e-governance, and in technological innovation. In many ways, Estonia is defining the future

for advances in management of the internet" (Kerry, 2014). Maintaining cyber-related issues high on the international agenda thus serves Estonia's goal of continuing integration into the Euro-Atlantic community.

Estonia's promotion of internet freedom is institutionalized as part of national development. Digital Agenda 2020 devotes significant attention to the task of enhancing the country's global reputation as digitally advanced through internet freedom rhetoric:

> A reputation of Estonia as a hub for innovation and development on information society will be promoted. This will be done by sharing our experience in e-governance and to promote [sic] the underpinning concepts of information society, such as internet freedom, protection of privacy, etc.
> … Estonia will advocate for **free and open internet (including social media channels) as well as related human rights**, and contribute to relevant international cooperation. (Estonian MEAC, 2013, n.p.; original emphasis)

In implementing this strategic communication plan, Estonia has been actively involved in internet governance fora. Estonia is a founding member of the Freedom Online Coalition, an intergovernmental organization of thirty member-states that support internet freedom. Estonia regularly hosts internet-related international conferences and trains foreign civil servants and NGOs on e-government and cybersecurity. As a matter of usual practice, Estonia addresses the issues of internet governance at non-specialized high-profile meetings on the floors of the United Nations, European Union, OSCE, and other major international organizations. For example, nearly all of Estonian representatives' remarks at the annual UN General Assembly touched upon cyber-issues and, specifically, Estonia's technological achievements. These initiatives all ensure that target audiences of foreign political, business, and media elites, as well as the general public that has increasing access to the news coverage of internet governance, are exposed to Estonia's digital expertise and strategic messaging.

Digital nationalism argues that the meaning assigned to material technology varies by context, yet the tropes employed to talk about technology need not be unique; they can be shared across strategic narratives of multiple governments. Digital nationalism is seen in the *logic* behind adopting a certain understanding and vocabulary pertaining to technology, even if the language almost fully mimics that of another context. Such is the case of Estonia, whose internet governance discourse aligns closely with that of the U.S.-led discourse of a free, open, borderless internet and the liberal-democratic tropes associated with it. For example, according to Toomas Ilves, "the very purpose of the Internet is to dismantle obstacles to free exchange" (Ilves, 2009). Although Estonia shares this understanding of the internet with other countries of the internet freedom agenda, Estonia's championing of this rhetoric advances its sovereign goal of reasserting Estonian national identity and borders through economic and security benefits that membership in the Euro-Atlantic institutions brings.

Estonia persistently reaffirms the internet freedom/sovereignty binary as defining the field of internet governance in order to emphasize its own commitment to and belonging in the internet freedom grouping with developed Western liberal democracies. For example, in opening remarks at the Freedom Online Coalition annual gathering held in Tallinn in 2014, Ilves described countries of the internet freedom as forming "the world wide web of democracies … connected by optical cables and computers, but most importantly, by the faith in the sanctity of the individual human spirit and freedom" (Ilves, 2014b).

Estonia uncompromisingly presents the choice between internet freedom and internet sovereignty not as a legitimate choice between two policy orientations, but as a

choice between allegedly the very nature of the internet, on the one hand, and corrupting its true nature, on the other hand: "either we can change the nature of the internet by placing a Westphalian regulatory structure on internet governance, or we can change the world" (Ilves, 2012b). This framing instrumentally puts forth a false binary by alleging the internet to have a certain natural unchanging state, whereas the internet's nature has been ever changing and diversifying.

Estonia frames the debate over internet governance in existential terms as the battle over the very future of the world order, such as in Ilves' address to the International Conference of Cyber Conflict in 2012:

> [W]e have now entered a new period of struggle between competing systems of government and economic organization. This time, there is no Iron Curtain, no statement of hostilities, no declared conflict of ideologies. What is at stake in this struggle is the liberal-democratic model of an open society and market economies that are transparent and rule bound. This time, the struggle will play itself out in cyberspace. (Ibid.)

Ilves here equates support for internet freedom with support for liberal democracy, open society, market economy, transparency, and rule of law to emphasize Estonia's commitment to these markers of belonging in the Euro-Atlantic community. Additionally, Ilves rhetorically elevates the status of internet governance in the hierarchy of geopolitical issues: internet governance, he claims, is not solely about the internet but the very persistence of the liberal political-economic order. Since Estonia is one of key actors in the global internet governance debate, this rhetorical maneuver by extension elevates the country's role in global politics writ large.

Another lens that Ilves regularly employs to frame the internet governance as a binary is that of political philosophies of Thomas Hobbes and John Locke. In his

Leviathan treatise, Hobbes argues for a rule by an absolute sovereign to maintain social order. According to Ilves, this is an approach that countries of the internet sovereignty persuasion have applied to the internet, turning it into a dangerous chaotic space akin to a war of all against all depicted in *Leviathan*. Estonia and countries of the internet freedom persuasion, on the other hand, are alleged to base their internet policy on a different philosophical approach: "in democracies we rely on John Locke's solution positing a contract between government and the citizenry, which underpins all modern democracies. … We need our Locke, Jefferson and Voltaire for the digital age" Ilves noted in the Opening address at the Munich Security Conference in 2014 (Ilves, 2014a). By rhetorically linking Estonia's internet governance orientation to some of the founding fathers of Western liberal thought, Ilves gives a mythical temporal depth to Estonia's claims of belonging to the centuries-old Western liberal tradition.

In addition to painting the internet governance debate as a clash of political philosophical ideologies, Ilves frames the debate as a clash of civilizational identities. As in the 1990s when Estonian officials extensively deployed Samuel Huntington's Clash of Civilizations framework to contrast their nation to Russia and promote Estonia's identity as inherently European, Ilves again draws on Huntington to emphasize the incompatibility of the two internet visions:

> Today we see a sort of Huntingtonian clash of civilisations between those
> countries, mainly authoritarian, that want to censor and restrict the internet and a
> coalition of democratic nations that stand up for the universal norms of freedom
> of speech and unhindered spread of ideas. Between those that want an internet
> ruled by states and one with all relevant stakeholders. This fight will be one of
> the major international political clashes of the digital age. (Ibid.)

The role of the internet in spreading democracy is one of the central discords

between the camps of internet freedom and internet sovereignty. The Arab Spring, a wave of popular uprisings across the Middle East in 2011-2012, often surfaces as an example in these debates. In mainstream Western political discourse, the Arab Spring bears positive connotations as a liberation movement against oppressive authoritarian regimes. Addressing the inaugural Freedom Online Coalition forum in 2011, Estonian MFA Urmas Paet framed social media as "irreplaceable tools for the promotion of democracy. This Spring's events in the Arab world are a good example of the role that the Internet and modern information and communications technology can play in promoting participation in politics" (Paet, 2011).

To the contrary, in official political discourse in Russia and other non-liberal regimes, the very term "democracy promotion" bears staunchly negative connotations as synonymous with the U.S.-led regime change diplomacy. Russian officials often use the Arab Spring as a cautionary tale of chaos and violence that erupts when a legitimate government is toppled under the guise of democratization, while the internet and social media are framed as subversive instruments that foster such events. Ilves decries this logic professed by countries of the Shanghai Cooperation Organization (SCO) and the Commonwealth of Independent States (CIS), two regional intergovernmental organizations where Russia plays a leading role:

> Authoritarian kleptocracies … fear the West is attempting to orchestrate an Arab Spring or an Orange Revolution. This helps explain why illiberal states want to develop new regulations for the internet, to put another brick in the wall (or is it another wall in the BRICs?), expanding their Westphalian space to cyber. This would be sovereignty on their terms, disabling the freedom and sovereignty of our citizens and businesses. (Ilves, 2012b)

In the lead-up to the World Conference on International Telecommunications (WCIT-12), an intergovernmental conference under the auspices of the UN International Telecommunication Union held in 2012 to review and update existing telecommunications regulations, Toomas Ilves again drew a sharp divide between the two internet governance camps at the NATO International Conference on Cyber Conflict:

> The outcome of this conference, and related processes, will help determine the topography of the web for the next two decades. … The CIS and SCO will again present proposals that would undermine the current multi-stakeholder model of the internet, replacing it with a scheme that would allow them to expand their control of their own populations and economies extending it to undermine the freedom and openness we value today. They will claim that sovereignty in cyberspace is necessary to rein in cybercrime and cyber-terrorism. (Ilves, 2012b)

The passage is characteristic of the ways Estonia's internet governance discourse strives to legitimize the internet freedom agenda and delegitimize the opposing internet sovereignty narrative. First, the very labels Ilves uses to describe the two internet governance approaches—a laudatory "model" for multistakeholder governance and a derogatory "scheme" for state-based governance—paint the former approach as a proper governance instrument and the latter as a criminal-like ploy. Second, Ilves rhetorically associates internet freedom with conventionally positive notions of "freedom" and "openness" while linking internet governance to the notion of "control" with decidedly negative connotations. Third, by characterizing the multistakeholder governance model as a "current" governance structure that would be "replac[ed]" with another one, Ilves draws on the common internet freedom trope that portrays multistakeholderism as a self-evident, natural way of governing the internet. This is done so as to make any proposals by the internet sovereignty camp seem contradictory to the very nature of the internet and thus merely a cover to advance authoritarian rule. Finally, the preemptive alleging ("will

present," "will claim") of what the internet sovereignty camp is about to do intones a warning about a looming criminal activity by the Other that was uncovered in advance and requires vigilance on the part of those concerned with maintaining the existing order. Talking about those proposals before they are officially presented allows Estonia to strategically assign to them a particular meaning that favors its own interpretation.

Continuity in Estonia's Internet Governance Rhetoric

The global internet governance ascended to geopolitical prominence during Toomas Ilves' two presidential terms, lasting from 2006 to 2016, but Estonia's narrative of internet freedom reflects institutionalized identity discourse that is not bound by any one political leader. Continuity in Estonia's internet governance discourse is evident, for example, in the speeches of President Kersti Kaljulaid, who succeeded Ilves as President in 2016. Like her predecessor, Kaljulaid discursively delineates internet governance debate into two distinct positions: one is explicitly positive while the other is negative.

At the opening of the EuroDIG 2017, Europe's main annual forum on internet governance held in Tallinn that year, Kaljulaid called on the audience: "We must make sure we maintain cyber space for the white powers and not abandon it to the dark forces" (Kaljulaid, 2017b). Kaljulaid elaborated the difference between white and dark sides of the debate:

> While there are some authoritarian regimes out there who would like to replace the multi-stakeholder model of Internet governance we have today into something different, "a governance of Internet", I firmly believe that security cannot be used as an excuse to limit freedom of expression. Cyber security, while important, cannot lie in highly restrictive legislation that plays into the hands of those who have a fundamentally different value system and no regard for human dignity and freedom of speech. Or who want to quash or limit free expression in the name of "domestic security". Those we should not trust to regulate our

Internet. (Ibid.)

Like Ilves, Kaljulaid differentiates the two camps with the very labels she assigns to them: the internet freedom camp is said to strive for a "multi-stakeholder model," while supporters of internet sovereignty stand are said to be proposing something allegedly so absurd that it is placed in quotation marks, "'a governance of the Internet.'" The framing of the two approaches to internet governance as normal/absurd is meant to rhetorically naturalize the multistakeholder model and discredit the state-based model. The internet sovereignty stance is further delegitimized through its unequivocal equation with authoritarian rule that has no regard for human dignity and freedom of expression. Finally, Kaljulaid's reference to the internet as "our Internet" is meant to further naturalize the connection between the internet freedom camp and the internet as such. This framing paints the internet as having an inherent natural state of being, which countries of the internet freedom coalition defend.

As digital nationalism suggests, Estonia uses global internet governance as a site to advance its sovereign interests, namely symbolic and institutional strengthening of ties with the Euro-Atlantic community. Estonia's discourse of internet governance is rooted in the logic and language of its identity discourse, which narrates the country as an inherently Western liberal democracy and in contrast to its Eastern Other, imperial/Soviet/post-Soviet Russia. Estonia's rhetoric of internet freedom thus shares key tropes with its identity discourse writ large: those of Estonia's commitment to liberal democracy, market economy, human rights, rule of law, transparency, and others. In line with Estonia's strategic communication of its identity, Estonia's internet governance communication is ultimately about drawing a clear boundary between the internet freedom and internet sovereignty camp and firmly placing Estonia in the former.

Estonian leaders thus narrate the us/them divide using numerous categories and metaphors: white powers versus dark forces, democracies versus autocracies, multilateral institutions (CIS, SCO, UN WCIT) versus multistakeholder groups, followers of Hobbes versus Locke, and others.

5.7 Conclusion

The previous two chapters illustrated the workings of digital nationalism in Russia. Russia's identity narrative challenges the U.S.-led liberal world order, while its digital discourse champions internet sovereignty to challenge the U.S.-led internet freedom narrative in the global internet governance debate. This chapter investigated the case of digital nationalism in another socio-historical context of re-independent Estonia from the early 1990s and until the present. Estonia's digital nationalism manifests itself in the country's strategic communication of widespread adoption of digital solutions by the state and society and support for the internet freedom agenda. This is done so as to signal Estonia's rightful belonging among economically and technologically developed Western liberal democracies.

Both Estonia and Russia articulate their identities in relation to the liberal West. However, where Russia has increasingly defined itself in opposition to the West over the past two decades, Estonia strives to align itself with the West in opposition to Russia. The analytical purchase of this chapter lays in illustrating how digital nationalism is applicable as an analytical framework to socio-historical contexts on both sides of the geopolitical and internet governance debate.

Estonia's digital discourse is couched in the normative rhetoric of Western globalism with its traditional markers of liberal democracy and the rule of law, borderless

flows of capital and information, and market economy. The ideological roots of this discourse, however, are to be found in Estonia's nationalism and the country's national identity re-building during the so-called post-Soviet transition. Estonia's self-fashioning as a global champion of techno-digital progress and internet freedom alongside powerful liberal democracies—and in contrast to Russia, its oppositional Other—serves to discursively solidify the country's national borders and national identity. Ultimately, Estonia's digital discourse conveys to the world that Estonia, an independent, territorialized, and sovereign nation-state, is an inherent part of the Euro-Atlantic community.

Through analysis of Estonia's digital nationalism, the chapter advances several interrelated theoretical propositions underlying this dissertation.

In examining the language and logic of Estonia's nation- and state-building after 1991, I illustrate identity discourse as a site of a power struggle between cultural repertoires represented by competing identity coalitions. In Estonia's case, the two main repertoires are advanced by the ethno-cultural Estonian majority and Russian minority. As the ethnic Estonian majority established privileged relations with the state institutions, its vision of Estonia as returning to Europe after the Soviet occupation was established as the country's official discourse and has informed its political-economic trajectory since regaining independence.

Estonia's identity discourse underlies its external communication discourse and strategy—the second pillar of the dissertation—which aims to portray Estonia as inherently European and thus advance its goal of symbolic and institutional joining of the Euro-Atlantic community. This discussion illustrates the rise of international reputation

and national strategies of reputation management as a growing factor in statecraft and, by extension, global politics.

My approach to Estonia's strategic communication is three-tiered. At the broadest level, I outline the structure and discourse of Estonia's strategic communication and situate it within the country's foreign policy. Estonia promotes itself as Nordic, environmental, and digital. Narrowing the focus, the second tier examines specifically the most pervasive of the three narratives, which is also most relevant to this dissertation – that of Estonia as a digitally advanced society. This discussion explains how the narrative of e-Estonia fits into Estonia's strategic communication and reflects the country's identity.

The third tier further narrows the analytical lens to examine the specific narrative of e-Estonia: Estonia's support of internet freedom in the global internet governance debate—the third pillar of the dissertation. This three-tiered structure demonstrates "internet freedom" to be a discursive formation informed by the national identity discourse and anchored in specific state visions, policies, and goals. At the theoretical level, this discussion of internet freedom proposes a discursive understanding of the field of global internet governance and advances a critical cultural approach to the study of digital technologies.

Read as an analytical whole, discussions of Estonia's identity discourse, strategic communication, and internet freedom discourse support digital nationalism's main argument that the national continues to inform the logics and language of the digital, and therefore this relationship must to be carefully studied with attention to specific socio-historical circumstances.

Conclusion

This dissertation examined the co-constitutive relationship between nationalism and digital technologies that I conceptualized as *digital nationalism*. Of the many levels and manifestations of this intertwined relationship, my focus was limited to examining how the state discursively utilizes digital technologies in constructing and communicating the national identity, interest, and image. The central argument of the dissertation was that national identity narratives underlie national digital visions and, by extension, also infuse the dynamics of digital globalization. I investigated this proposition by examining how official identity narratives in Russia and Estonia inform these countries' championing of, respectively, internet sovereignty and internet freedom agendas.

The dissertation contributed novel evidence to the continued relevance of nationalism as a category of practice and analysis in the modern world that is characterized by digital globalization. By relating national identity narratives to state rhetoric and policy of internet governance, I demonstrated that global digital communication technologies are not antithetical to national logics but are increasingly contributing to the imagining and constructing of the national Self and its significant Others.

The dissertation consisted of three parts. Part I, Digital Nationalism, outlined the theoretical and analytical foundations of the digital nationalism framework and then applied it to the case of global internet governance in order to illustrate how identity narrative relates to internet governance. Part II, The Narrative of Internet Sovereignty, and Part III, The Narrative of Internet Freedom, illustrated the workings of digital

nationalism by examining empirically the logics and language of internet governance in Russia and Estonia. Russia served as the primary country case study and Estonia was a secondary illustrative case for limited comparison.

Chapter 1, *Digital Nationalism: A Framework*, elaborated the concept of digital nationalism as an analytical orientation and a social phenomenon. The chapter first situated digital nationalism within existing literature on the relationship between technologies, and the internet in particular, on the one hand, and the administrative state and the cultural nation, on the other hand. The second part of the chapter elaborated digital nationalism as an analytical lens and a social phenomenon. The analytical lens of digital nationalism refers to self-conscious analytical understanding of the nation's sociocultural identity narratives as underlying the state's digital discourse and policy. The discussion of digital nationalism as a social phenomenon applied Craig Calhoun's three-part framework of nationalism as discourse, project, and evaluation to the relationship between nationalism and digital technologies to elaborate a three-pronged understanding of digital nationalism, accordingly, as discourse, project, and evaluation. Digital nationalism as discourse refers to how nationalism as a hegemonic discourse of modernity shapes the imagination behind some material digital artifacts and practices while these practices, in turn, reproduce the discursive framework of nationalism. Digital nationalism as project refers to concerted state efforts at engaging with digital technologies domestically and internationally in the name of the nation's interest, identity, and image. Digital nationalism as evaluation refers to the global competition among national digital projects, whereby states advance their national digital identities and attempt to shape the global digital order in their favor.

Chapter 2, *Global Internet Governance*, applied the framework of digital

nationalism to the case of global internet governance—an international policymaking

process pertaining to the legal and technological architectures of the global internet. The

chapter first discussed how global internet governance is an analytic borderland that lays

at once in national and global spaces by depicting briefly its rise from an experimental

scientific project under the auspices of a national military to geopolitical prominence.

Illustrating the dissertation's key proposition about the co-constitutive relationship

between nationalism and digital technologies, the second part of the chapter then focused

on how identity narratives underlie the logics and languages of national internet

governance visions of the global internet.

Part II, The Myth of Internet Sovereignty, consisted of Chapters 3 and 4 and

illustrated how Russia's narrative of internet sovereignty is underlain with its national

identity narratives. Chapter 3, *Re-Making of a Great Power Identity: Russia's Identity*

and Strategic Communication, focused on how Russia's gradually changing official

identity narratives from a Western liberal democracy, to a normal power, to a great power

have shaped its domestic media policy and external strategic communication. This

discussion illuminated the several interconnections foundational to my understanding of

digital nationalism: those between national cultural repertoires and state identity, between

domestic identity and foreign policy, and between identity narratives and the logic and

language of external strategic communication. Chapter 4, *A Digital Sovereign: Russia's*

Internet Governance at Home and Abroad, drew on Chapter 3 to examine Russia's digital

nationalism as application of its identity logics to its domestic and foreign policy of the

internet. The chapter showed how Russia's increasingly assertive identity narrative of a

self-professed global counter-hegemonic great power, and the specific cultural repertoires that underlie this narrative, form the meaningful context for understanding the logics and language of the Russian state's engagement with digital technologies. Thus, Russian sovereigntist identity narrative was shown to infuse its identity and associated rhetoric and policy of internet sovereignty.

Part III, The Myth of Internet Freedom, consisted of Chapter 5, *Re-Making of a Western Identity: Estonia's "Return to Europe" as an e-State*. The case study of Estonia's digital nationalism project self-branded as *e-Estonia: The Digital Society*, which includes vocal support of the internet freedom agenda, illustrated how these efforts are underlain with the identity narrative of Estonia's cultural and institutional returning to the Euro-Atlantic community after the Soviet occupation.

While Estonia and Russia propagate opposing visions of the global internet's governing architecture, this dissertation found that they nevertheless share many approaches. Estonia and Russia treat cultural and economic globalization in similar ways: while both states perceive cultural globalization as threatening their traditional identity and heritage, they embrace economic globalization as an opportunity to advance their economic interests. Moreover, they view economic globalization as a means to partially ameliorate the negative effects of cultural globalization by articulating and communicating a competitive national identity and offering it for the consumption of global audiences of tourists, students, consumers, skilled workers, and media audiences.

At the same time as Estonia and Russia frame global digital communication technologies as potentially threatening to their traditional identities, they embrace their affordances in protecting these very identities in two ways. First, both countries directly

employ digital technologies to preserve national cultures, such as, for example, Estonia's strategy of digitization of its national heritage and Russia's securing of the Cyrillic online domain extension. Second, as this dissertation argued, both countries' participation in the geopolitical debate over global internet governance is ultimately in pursuit of their existential identity visions: recognition as a full and equal member of the Euro-Atlantic community in the Estonian case and recognition as a full and equal great power in the Russian case.

Although Estonian and Russian identity narratives and ruling political regimes currently draw upon opposing liberal-democratic and illiberal discourses respectively, since gaining independence in 1991, both states have been unwavering supporters of the neoliberal economic globalization and participants in its key institutions and initiatives, such as the World Trade Organization, the World Economic Forum, and others. This fact signals the extent to which the neoliberal market-based economic imaginary has become hegemonic in the early twenty-first century, irrespective of the political nature of the regimes.

Estonian and Russian cases illustrate as well that strategic communication—narration by the government of its identity in pursuit of reputational and material gains—has become intrinsic to statecraft. Since the late 1990s-early 2000s, Estonian and Russian ruling elites have proclaimed strategic communication of their national interests and identities to global audiences as a matter of highest-level national priority meant to enhance the country's political status, economic competitiveness, and security. Both countries have since allocated great resources to building strategic communication capabilities that encompass diverse instruments of persuasion, including television and

radio channels, news websites, social media accounts, hosting of political and entertainment events, humanitarian aid, political rhetoric, and others. Strategic narratives of national digital identity and the global digital order emerged as increasingly central elements within these nations' strategic communication. Global internet governance has become one major discursive site of competition among national strategic narratives vying to institutionalize their normative visions.

Future Research

This dissertation laid out a broad framework for examining the co-constitutive relationship between national culture and digital discourse and policy. The focus of this study was limited to how national identity narratives rooted in respective cultural repertoires contribute to shaping state rhetoric and policy pertaining to digital communication technologies and, specifically, internet governance. It is hoped that this dissertation opens new avenues for further studies on the relationship between nationalism and digital communication technologies.

Research could focus in greater detail on other actors beyond the state. Whereas this work focused on the private sector and the civil society only to the extent that they interacted with or were instrumentally utilized by the state, future research could place these sectors at the center of its analysis to ask if and how national identity narratives and national cultural repertoires shape the actions of digital companies and civil society actors in various national contexts, as well as their relationship with the state and with each other. The users could be another category of actors fruitfully incorporated into the study of digital nationalism to investigate empirically the degree to which state-led strategic narratives of national identity and internet policy reflect popular beliefs and are accepted

by the populace. For example, to what extent do Estonians feel like their individual identity is predisposed toward the adoption of digital technologies? Whether and how this feeling varies depending on the ethno-cultural identity of the Estonian citizens (e.g., ethnic Estonians and ethnic Russians)?

This dissertation employed interpretive textual analysis of political discourse as its primary research method. This method allows to uncover the cultural repertoires that make up the institutionalized national identity as articulated by the state and its representatives. Future research could employ other methods in the study of digital nationalism in order to illuminate additional aspects of digital nationalism. Ethnographic methods, such as long-term observation and interviews, could add more nuance to understanding how various actors—officials, private companies, non-profits, the citizens—internalize and enact (or not) state-led digital nationalism and how their individual views and actions, in turn, inform such state-led efforts. A close analysis of institutional dynamics of the state could be fruitful in illuminating how particular institutional arrangements in various national contexts influence respective digital visions and their implementations. Political-economic analysis combined with the proposed identity-based lens could explore in greater detail the link between the materiality of the internet and socio-cultural context in which these material developments take place.

List of References

Abbate, J. (1999). *Inventing the Internet*. Cambridge, MA: MIT Press.

Abbate, J. (2017). What and where is the Internet? (Re)defining Internet histories. *Internet Histories*, *1*(1–2), 8–14.

Ackerman, E. (2012, December 14). The U.N. fought the Internet -- And the Internet won; WCIT Summit in Dubai ends. Retrieved September 5, 2018, from https://www.forbes.com/sites/eliseackerman/2012/12/14/the-u-n-fought-the-internet-and-the-internet-won-wcit-summit-in-dubai-ends/#65adc1c37cc8

Agarin, T., & Regelmann, A. (2012). Which is the only game in town? Minority rights issues in Estonia and Slovakia during and after EU accession. *Perspectives on European politics and society*, *13*(4), 443–461.

Alasuutari, P. (2015). *The synchronization of national policies: Ethnography of the global tribe of moderns*. London: Routledge.

Alexanyan, K., Barash, V., Etling, B., Faris, R., Gasser, U., Kelly, J., … Roberts, H. (2012). *Exploring Russian cyberspace: Digitally-mediated collective action and the networked public sphere* (No. ID 2014998). Cambridge, MA: Berkman Klein Center for Internet and Society at Harvard University. Retrieved from https://papers.ssrn.com/abstract=2014998.

Allan, B. B. (2016). Recovering discourses of national identity. In T. Hopf & B. B. Allan (Eds.), *Making identity count: Building a national identity database*. Oxford, UK: Oxford University Press.

Allsalu, V. (2005). Estonia. A cool country with a warm heart. In *Estonia. A cool country with a warm heart* (p. 3). Tallinn, Estonia: Enterprise Estonia. Retrieved

September 11, 2018, from http://arhiiv.pixel.ee/eas/eesti-brand/2002-2008/2005-print-a-cool-country-with-a-warm-heart.pdf

Anderson, B. (2006). *Imagined communities: Reflections on the origin and spread of nationalism* (Revised Edition). London: Verso.

Ang, P. H., & Pang, N. (2012). Globalization of the Internet, sovereignty or democracy: The trilemma of the Internet Governance Forum. *Revue Française d'études Américaines*, (134), 114–127.

Appadurai, A. (1996). *Modernity at large: Cultural dimensions of globalization*. Minneapolis, MN: University of Minnesota Press.

Aronczyk, M. (2013). *Branding the nation: The global business of national identity*. Oxford; New York: Oxford University Press.

Aronczyk, M. (2017). Narratives of legitimacy: Making nationalism banal. In M. Skey & M. Antonsich (Eds.), *Everyday nationhood: Theorising culture, identity and belonging after banal nationalism*. London: Palgrave Macmillan.

Aronczyk, M., & Budnitsky, S. (2017). Nation branding and Internet governance: Framing debates over freedom and sovereignty. In U. Kohl (Ed.), *The net and the nation-state: Multidisciplinary perspectives on Internet governance* (pp. 48–66). Cambridge, UK: Cambridge University Press.

Asmolov, G., & Kolozaridi, P. (2017). The imaginaries of RuNet. *Russian Politics*, *2*(1), 54–79.

Auers, D. (2015). *Comparative politics and government of the Baltic States: Estonia, Latvia and Lithuania in the 21st century*. Basingstoke, UK: Palgrave Macmillan.

Backes, O. (2014, January 22). Rossiya Segodnya: The national champion of news. Retrieved September 9, 2018, from https://www.csis.org/blogs/post-soviet-post/rossiya-segodnya-national-champion-news

Balleste, R. (2015). *Internet governance: Origins, current issues, and future possibilities*. Lanham, MD: Rowman & Littlefield Publishers.

Bandelj, N., & Wherry, F. (Eds.). (2011). *The cultural wealth of nations*. Stanford, CA: Stanford University Press.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4-5), 1–12.

Bay, M. (2017). What is "internet"? The case for the proper noun and why it is important. *Internet Histories*, *1*(3), 203–218.

BBC News. (2012, May 25). Yandex oboshel Perviy kanal po populyarnosti [Yandex surpassed Channel One in popularity]. *BBC News Russian Service*. Retrieved August 24, 2018, from https://www.bbc.co.uk/russian/russia/2012/05/120525_yandex_audience_tv_channell

Beck, U. (2006). *Power in the global age: A new global political economy*. Cambridge, UK and Malden, MA: Polity.

Becker, J. (2004). Lessons from Russia: A neo-authoritarian media system. *European Journal of Communication*, *19*(2), 139–163.

Belfer Center for Science and International Affairs, Harvard Kennedy School. (2016, March 21). Taavi Rõivas: A 21st Century State - Anything is Possible. Retrieved

August 28, 2018, from https://www.belfercenter.org/event/taavi-roivas-21st-century-state-anything-possible

Belin, L. (2002). The Russian media in the 1990s. *Journal of Communist Studies and Transition Politics*, *18*(1), 139–160.

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

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven, CT: Yale University Press.

Berger, P. L., & Luckmann, T. (1966). *The social construction of reality: A Treatise in the sociology of knowledge*. New York: Anchor.

Beumers, B., Hutchings, S., & Rulyova, N. (Eds.). (2011). *The post-Soviet Russian media: Conflicting signals*. London: Routledge.

Bijker, W. E., Hughes, T. P., & Pinch, T. (Eds.). (2012). *The social construction of technological systems: New directions in the sociology and history of technology* (Anniversary Edition). Cambridge, MA: The MIT Press.

Billig, M. (1995). *Banal nationalism*. Thousand Oaks, CA: SAGE Publications.

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

Black, J. L. (2015). *The Russian Presidency of Dmitry Medvedev, 2008-2012: The next step forward or merely a time out?* Abingdon, Oxon; New York: Routledge.

Blakkisrud, H. (2016). Blurring the boundary between civic and ethnic: The Kremlin's new approach to national identity under Putin's third term. In P. Kolstø & H.

Blakkisrud (Eds.), *The new Russian nationalism: Imperialism, ethnicity and authoritarianism 2000-2015*. Edinburgh: Edinburgh University Press.

Blau, J. (2012, December 26). Is this the start of an Internet Cold War? Retrieved March 4, 2018, from https://spectrum.ieee.org/telecom/internet/is-this-the-start-of-an-internet-cold-war

Bowcott, O. (2017, August 23). Dispute along cold war lines led to collapse of UN cyberwarfare talks. *The Guardian*. Retrieved August 24, 2018, from https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges

Bradshaw, S., DeNardis, L., Hampson, F. O., Jardine, E., & Raymond, M. (2015). The emergence of contention in global Internet governance. *Centre for International Governance Innovation*. Retrieved September 10, 2018, from https://www.cigionline.org/publications/emergence-contention-global-internet-governance

Breuilly, J. (1994). *Nationalism and the state*. Chicago: University of Chicago Press.

BRICS. (2015). Communique of BRICS ICT Ministers on results of the meeting "Expanding of collaboration in spheres of telcom and infocommunications." Russian Ministry of Digital Development, Communications and Mass Media. Retrieved August 22, 2018, from http://minsvyaz.ru/en/events/34194

Brooks, J. (2012, December 6). Hands off the Internet! *The New York Times*. Retrieved September 4, 2018, from https://www.nytimes.com/2012/12/07/opinion/hands-off-the-internet.html

Brousseau, E., Marzouki, M., & Méadel, C. (Eds.). (2012). *Governance, regulation and powers on the Internet*. Cambridge, UK: Cambridge University Press.

Brown, D. (2013, March 29). Debunking the myth of a Digital Cold War, before it's too late. Retrieved September 4, 2018, from https://www.aljazeera.com/indepth/opinion/2013/03/201332914172838453.html

Browning, C. S., & Oliveira, A. F. de. (2017). Introduction: nation branding and competitive identity in world politics. *Geopolitics*, *22*(3), 481–501.

Brüggemann, K., & Kasekamp, A. (2008). The politics of history and the "War of Monuments" in Estonia. *Nationalities Papers*, *36*(3).

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

Bulashova, N., Burkov, D., Platonov, A., & Soldatov, A. (2013). An Internet history of Russia in 1990s. In K. Chon (Ed.), *An Asia Internet history: First decade (1980-1990)*. Seoul, Republic of Korea: Seoul National University Press. Retrieved September 10, 2018, from https://sites.google.com/site/internethistoryasia/book1/an-internet-history-of-russia-in-1990s

Buttarelli, G. (2014). Europe's role in shaping the future of Internet governance. European Data Protection Supervisor. Retrieved August 22, 2018, from https://edps.europa.eu/sites/edp/files/publication/14-06-23_internet_governance_en.pdf

Bygrave, L. A., & Bing, J. (Eds.). (2009). *Internet governance: Infrastructure and institutions*. New York: Oxford University Press.

Cadier, D., & Light, M. (Eds.). (2015). *Russia's foreign policy: Ideas, domestic politics and external relations*. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.

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

Carman, D. (2002). Translation and analysis of the Doctrine of Information Security of the Russian Federation: Mass media and the politics of identity. *Pacific Rim Law & Policy Journal*, *11*(2), 339–369.

Carpentier, N. (2011). Policy's hubris: Power, fantasy, and the limits of (global) media policy interventions. In R. Mansell & M. Raboy (Eds.), *The handbook of global media and communication policy*. Malden, MA: Wiley-Blackwell.

Carpentier, N. (2017). *The discursive-material knot: Cyprus in conflict and community media participation*. New York: Peter Lang Inc., International Academic Publishers.

Carr, M. (2015). Power plays in global Internet governance. *Millennium*, *43*(2), 640–659.

Carr, M. (2016). *US power and the Internet in international relations*. London: Palgrave Macmillan.

Castells, M. (2009). *The power of identity* (2nd Edition). Malden, MA: Wiley-Blackwell.

Center for Cyber & Homeland Security, Elliott School of International Affairs, George Washington University. (2016, March 22). U.S.-Estonia Symposium on

Cybersecurity and Defense Cooperation. Retrieved August 28, 2018, from

https://cchs.gwu.edu/us-estonia-symposium-cybersecurity-and-defense-cooperation

Central Intelligence Agency. (2018). Estonia. In *The world factbook*. Central Intelligence

Agency. Retrieved August 29, 2018, from

https://www.cia.gov/library/publications/the-world-factbook/geos/en.html

Cerf, V. G. (2014). The Internet governance ecosystem. *Communications of the ACM*,

57(4), 7.

Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, *64*, 676–739.

Charland, M. (1986). Technological nationalism. *Canadian Journal of Political and

Social Theory*, *10*(1–2), 196–220.

Chebankova, E. (2017). Russia's idea of the multipolar world order: origins and main

dimensions. *Post-Soviet Affairs*, *33*(3), 217–234.

Checkel, J. T., & Katzenstein, P. J. (Eds.). (2009). *European identity*. Cambridge, UK:

Cambridge University Press.

Chen, C. (2016). *The return of ideology: The search for regime identities in

postcommunist Russia and China*. Ann Arbor: University of Michigan Press.

Chenou, J.-M. (2014). From cyber-libertarianism to neoliberalism: Internet

exceptionalism, multi-stakeholderism, and the institutionalisation of Internet

governance in the 1990s. *Globalizations*, *11*(2), 205–223.

Chernilo, D. (2011). The critique of methodological nationalism: Theory and history.

Thesis Eleven, *106*(1), 98–117.

Chernykh, A., & Polous, M. (2015, August 5). Chinovniki vynosyat' Sorosa iz izby-chitalni [Officials are removing Soros from the reading room]. *Kommersant*. Retrieved September 7, 2018, from https://www.kommersant.ru/doc/2782240

Chinese State Council. (2010). The Internet in China. Information Office of the State Council of the People's Republic of China. Retrieved August 23, 2018, from http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_7.htm

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, MA: The MIT Press.

Christou, G., & Simpson, S. (2011). The European Union, multilateralism and the global governance of the Internet. *Journal of European Public Policy*, *18*(2), 241–257.

Clinton, H. (2010, January). *Remarks on Internet freedom*. Presented at the Newseum, Washington, D.C. Retrieved September 10, 2018, from https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Clinton, W., & Gore, A. (1997, July 1). A framework for global electronic commerce. The White House. Retrieved September 4, 2018, from https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html

Clunan, A. L. (2009). *The social construction of Russia's resurgence: Aspirations, identity, and security interests*. Baltimore: Johns Hopkins University Press.

Coalson, R. (2015, May 15). Turning back time: Putting Putin's Molotov-Ribbentrop defense into context. Retrieved September 10, 2018, from https://www.rferl.org/a/putin-russia-molotov-ribbentrop-pact/27017723.html

Comaroff, J. L., & Comaroff, J. (2009). *Ethnicity, Inc.* Chicago: University of Chicago Press.

Conneally, P. (2012, November 23). The Google campaign – An ITU view. Retrieved September 5, 2018, from https://news.itu.int/google-campaign-itu-view

Connolly, R., & Hanson, P. (2016). *Import substitution and economic sovereignty in Russia*. London, UK: Chatham House.

Corse, S. M. (1997). *Nationalism and literature: The politics of culture in Canada and the United States*. Cambridge, UK; New York: Cambridge University Press.

Costigan, S. S., & Perry, J. (Eds.). (2012). *Cyberspaces and global affairs*. Farnham, Surrey; Burlington, VT: Ashgate.

Cottiero, C., Kucharski, K., Olimpieva, E., & Orttung, R. W. (2015). War of words: the impact of Russian state television on the Russian Internet. *Nationalities Papers*, *43*(4), 533–555.

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

Crandall, M. (2016, October 11). Matthew Crandall: President Ilves' global impact. *ERR*. Retrieved August 28, 2018, from https://news.err.ee/119347/matthew-crandall-president-ilves-global-impact

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

Cull, N. J. (2012). *The decline and fall of the United States Information Agency: American public diplomacy, 1989–2001*. New York: Palgrave Macmillan.

Curran, J., Fenton, N., & Freedman, D. (2016). *Misunderstanding the Internet* (2nd Edition). London; New York: Routledge.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2008). *Access denied: The practice and policy of global Internet filtering*. Cambridge, MA: The MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: The MIT Press.

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770.

DeNardis, Laura. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press.

DeNardis, Laura, & Musiani, F. (2016). Governance by infrastructure. In F. Musiani, D. L. Cogburn, L. DeNardis, & N. S. Levinson (Eds.), *The turn to infrastructure in Internet governance*. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.

Deyermond, R. (2016). The uses of sovereignty in twenty-first century Russian foreign policy. *Europe-Asia Studies*, *68*(6), 957–984.

Diamond, L. (2010). Liberation technology. *Journal of Democracy*, *21*(3).

DLA Piper Rus Limited, Thomson Reuters Foundation, Robert Bosch Stiftung, & Fritt Ord Foundation. (2016). *Media regulation in Russia - A landscape analysis of laws and trends*. Thomson Reuters Foundation. Retrieved September 11, 2018, from http://www.trust.org/contentAsset/raw-data/4798c68a-eed1-4660-b7c9-fc16a0032cc9/file

Domanski, R. J. (2015). *Who governs the Internet?: A political architecture*. Lanham, MD: Lexington Books.

Dow Jones. (2014). *Dow Jones VentureSource. Europe -- 1Q 2014*. Dow Jones.
Retrieved August 23, 2018, from http://images.dowjones.com/company/wp-
content/uploads/sites/15/2014/04/Dow-Jones-VentureSource-1Q14-EMEA.pdf

Drake, W. J. (2004). Reframing Internet governance discourse: Fifteen baseline
propositions. Social Science Research Council's Research Network on IT and
Governance. Retrieved September 11, 2018, from
https://www.unngls.org/orf/drake.pdf

Drake, W. J., Cerf, V. G., & Kleinwächter, W. (2016). *Internet fragmentation: An
Overview* (Future of the Internet Initiative). Geneva, Switzerland: World Economic
Forum.

Drake, W. J., & Wilson, E. J. (2008). *Governing global electronic networks:
International perspectives on policy and power*. Cambridge, MA: The MIT Press.

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in.
Political Science Quarterly, *119*(3), 477–498.

Drezner, D. W. (2007). *All politics is global: Explaining international regulatory
regimes*. Princeton, NJ: Princeton University Press.

Dumitrica, D. (n.d.). Imagining the Canadian Internet: A case of discursive
nationalization of technology. *Studies in Ethnicity and Nationalism*, *15*(3), 448–
473.

Ebert, H., & Maurer, T. (2013). Contested cyberspace and rising powers. *Third World
Quarterly*, *34*(6), 1054–1074.

Economist, The. (2001, February 22). Mart Laar, Estonia's punchy prime minister. *The Economist*. Retrieved September 11, 2018, from

http://www.economist.com/node/512067

Economist, The. (2012, December 14). A digital Cold War? Retrieved September 4, 2018, from https://www.economist.com/blogs/babbage/2012/12/internet-regulation

Edensor, T. (2002). *National identity, popular culture and everyday life*. Oxford: Berg Publishers.

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

Eeten, M. J. van, & Mueller, M. (2013). Where is the governance in Internet governance? *New Media & Society*, *15*(5), 720–736.

e-Governance Academy. (n.d.). Siim Sikkut. Retrieved August 29, 2018, from https://www.ega.ee/people/siim-sikkut

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

Eko, L. (2001). Many spiders, one Worldwide Web: Towards a typology of internet regulation. *Communication Law and Policy*, *6*(3), 445–484.

Eko, L. S. (2012). *New media, old regimes: Case studies in comparative communication law and policy*. Lanham, MD: Lexington Books.

Eko, L. S. (2013). *American exceptionalism, the French exception, and digital media law*. Lanham, MD: Lexington Books.

Ellis, F. (1998). *From glasnost to the Internet: Russia's new infosphere*. Basingstoke, UK: Palgrave Macmillan.

Engel, C., & Keller, K. H. (Eds.). (2000). *Governance of global networks in the light of differing local values*. Baden-Baden, Germany: Nomos Verlagsgesellschaft.

Enterprise Estonia. (2017, June 2). Estonia is a digital society. Retrieved August 29, 2018, from https://www.visitestonia.com/en/why-estonia/estonia-is-a-digital-society

Enterprise Estonia. (n.d.-a). Brand Estonia. Retrieved August 29, 2018, from https://brand.estonia.ee

Enterprise Estonia. (n.d.-b). Character — Brand Estonia. Retrieved August 30, 2018, from https://brand.estonia.ee/principles/character

Enterprise Estonia. (n.d.-c). e-estonia — Estonia. Retrieved August 29, 2018, from https://estonia.ee/enter

Enterprise Estonia. (n.d.-d). Enterprise Estonia. Retrieved August 22, 2018, from https://www.eas.ee/eas/?lang=en

Enterprise Estonia. (n.d.-e). Estonia (Official website). Retrieved August 29, 2018, from https://estonia.ee

Enterprise Estonia. (n.d.-f). IT sector. Retrieved August 29, 2018, from https://e-estonia.com/it-sector

Enterprise Estonia. (n.d.-g). Story — Brand Estonia. Retrieved August 29, 2018, from https://brand.estonia.ee/principles/story

Epstein, C. (2008). *The power of words in international relations: Birth of an anti-whaling discourse*. Cambridge, MA: The MIT Press.

Epstein, D. (2013). The making of institutions of information governance: the case of the Internet Governance Forum. *Journal of Information Technology*, *28*(2), 137–149.

Erlanger, S. (1994, June 13). Estonia savors economic success, but the reformers may be in trouble. *The New York Times*. Retrieved September 11, 2018, from http://www.nytimes.com/1994/06/13/world/estonia-savors-economic-success-but-the-reformers-may-be-in-trouble.html

Ernsdorff, M., & Berbec, A. (2007). Estonia, the short road to e-government and e-democracy. In P. G. Nixon & V. N. Koutrakou (Eds.), *E-government in Europe: Re-booting the state*. New York: Routledge.

ERR. (2017, January 13). A new brand for Estonia. Retrieved August 10, 2017, from http://news.err.ee/120339/a-new-brand-for-estonia

Estonian Association of Information Technology and Telecommunications. (n.d.). ITL. Retrieved August 29, 2018, from https://www.itl.ee/Eng

Estonian Commission on Sustainable Development. (2005). Estonian national strategy on sustainable development "Sustainable Estonia 21." Estonian Government. Retrieved August 29, 2018, from https://riigikantselei.ee/sites/default/files/content-editors/Failid/estonia_sds_2005.pdf

Estonian Government Office. (n.d.). E-Estonia Council. Retrieved August 29, 2018, from https://riigikantselei.ee/en/supporting-government/e-estonia-council

Estonian Information System Authority. (n.d.). Retrieved August 29, 2018, from https://www.ria.ee/en

Estonian Ministry of Culture. (2014). The strategy of integration and social cohesion in Estonia "Integrating Estonia 2020." Republic of Estonia Ministry of Culture.

Retrieved August 29, 2018, from

http://www.kul.ee/sites/kulminn/files/integrating_estonia_2020.pdf

Estonian Ministry of Economic Affairs and Communications. (2006). Estonian

information society strategy 2013. Estonian Ministry of Economic Affairs and

Communications. Retrieved August 29, 2018, from

http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan033997.pdf

Estonian Ministry of Economic Affairs and Communications. (2013). Digital agenda

2020 for Estonia. Estonian Ministry of Economic Affairs and Communications.

Retrieved August 29, 2018, from

https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf

Estonian Ministry of Economic Affairs and Communications. (2015, March 26).

Information society. Retrieved August 29, 2018, from

https://www.mkm.ee/en/objectives-activities/information-society

Estonian Ministry of Foreign Affairs. (2013, May 21). Estonia's foreign policy

objectives. Retrieved August 29, 2018, from https://vm.ee/en/estonias-foreign-

policy-objectives

Estonian Ministry of Foreign Affairs. (2016, June 16). e-Estonia. Retrieved August 29,

2018, from https://vm.ee/en/e-estonia

Estonian Ministry of Foreign Affairs. (2017, January 9). Internet freedom. Retrieved

August 29, 2018, from https://vm.ee/en/internet-freedom

Estonian Presidency of the Council of the European Union. (2017, May 17). Priorities of

the Estonian presidency. Retrieved August 29, 2018, from

https://www.eu2017.ee/priorities-estonian-presidency

European Commission. (2015). *eGovernment in Estonia* (No. 17). European

 Commission. Retrieved August 28, 2018, from

 https://joinup.ec.europa.eu/sites/default/files/document/2015-03/egov_in_estonia_-

 _january_2015_-_v_17_final.pdf

European Commission. (2016). *eGovernment in Estonia*. European Commission.

 Retrieved August 29, 2018, from

 https://joinup.ec.europa.eu/sites/default/files/ckeditor_files/files/eGovernment%20i

 n%20Estonia%20-%20February%202016%20-%2018_00_v4_00.pdf

European Commission. (2017). *Europe's digital progress country reports: Estonia*

 (Europe's digital progress report 2017). Retrieved August 29, 2018, from

 http://ec.europa.eu/newsroom/document.cfm?doc_id=44300

European Parliament. (2012, November 22). European Parliament resolution of 22

 November 2012 on the forthcoming World Conference on International

 Telecommunications (WCIT-12) of the International Telecommunication Union,

 and the possible expansion of the scope of international telecommunication

 regulations. European Parliament. Retrieved September 11, 2018, from

 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-

 //EP//NONSGML+TA+P7-TA-2012-0451+0+DOC+PDF+V0//EN

Farivar, M. C. (2011). *The Internet of elsewhere: The emergent effects of a wired world*.

 New Brunswick, NJ: Rutgers University Press.

Feenberg, A. (2010). *Between reason and experience: Essays in technology and*

 modernity. Cambridge, MA: The MIT Press.

Feklyunina, V. (2008). Battle for perceptions: Projecting Russia in the West. *Europe-Asia Studies*, *60*(4), 605–629.

Feklyunina, V. (2016). Soft power and identity: Russia, Ukraine and the 'Russian world(s).' *European Journal of International Relations*, *22*(4), 773–796.

Feldman, G. (2005). Neo-liberal nationalism: Ethnic integration and Estonia's accession to the European Union. In J. Stacul, C. Moutsou, & H. Kopnina (Eds.), *Crossing European boundaries: Beyond conventional geographical* (pp. 41–63).

Flichy, P. (2007). *The Internet imaginaire*. Cambridge, MA: The MIT Press.

Forbes. (2018). The world's largest public companies. Retrieved September 4, 2018, from https://www.forbes.com/global2000/list

Force Hill, J. (2012). *Internet fragmentation: Highlighting the major technical, governance and diplomatic Challenges for U.S. Policy Makers*. Belfer Center for Science and International Affairs. Retrieved September 11, 2018, from https://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf

Fossato, F., Lloyed, J., & Verkhovsky, A. (2008). *The web that failed: How opposition politics and independent initiatives are failing on the Internet in Russia*. Oxford: Reuters Institute for the Study of Journalism.

Fox, J. E., & Miller-Idriss, C. (2008). Everyday nationhood. *Ethnicities*, *8*(4), 536–563.

France 24. (2017, May 30). Video: Macron slams RT, Sputnik news as "lying propaganda" at Putin press conference. *France 24*. Retrieved August 24, 2018, from https://www.france24.com/en/20170530-macron-rt-sputnik-lying-propaganda-putin-versailles-russia-france-election

Franke, U., & Pallin, C. V. (2012). *Russian politics and the Internet in 2012*. Stockholm, Sweden: Swedish Ministry of Defence. Retrieved September 7, 2018, from https://www.foi.se/report-search/pdf?fileName=D%3A%5CReportSearch%5CFiles%5Cebb043f5-26fc-41be-982b-da589398eeb7.pdf

Freedom Online Coalition. (2017). Document Pack. Freedom Online Coalition. Retrieved August 22, 2018, from https://freedomonlinecoalition.com/wp-content/uploads/2018/04/FOC-Document-Pack-Final-040717.pdf

French Government. (2016). The digital republic bill - Overview. French Government. Retrieved August 21, 2018, from https://www.republique-numerique.fr/pages/in-english

French Ministry of Foreign Affairs. (2017). France's international digital strategy [France Diplomatie]. Retrieved August 20, 2018, from https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy

French Ministry of Foreign Affairs. (2018). Digital and soft diplomacy [France Diplomatie]. Retrieved August 20, 2018, from https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-s-international-digital-strategy

Friedman, T. (2005). *Electric dreams: Computers in American culture*. New York: NYU Press.

Froomkin, A. M. (2003). Habermas@discourse.net: Toward a critical theory of cyberspace. *Harvard Law Review*, *116*(3), 749–873.

G7. (2017). G7 ICT and industry ministers' declaration. Making the next productive

    revolution inclusive, open and secure. G7. Retrieved August 22, 2018, from

    http://www.g7italy.it/sites/default/files/documents/G7_ICT_and_Industruy_Ministe

    rs%27_Declaration_2017.pdf

Gabowitsch, M. (2017). *Protest in Putin's Russia*. Cambridge, UK: Polity.

Galloway, A. R. (2004). *Protocol: How control exists after decentralization*. Cambridge,

    MA: The MIT Press.

Gaskell, A. (2017, June 23). How Estonia became the digital leader of Europe. *Forbes*.

    Retrieved September 11, 2018, from

    http://www.forbes.com/sites/adigaskell/2017/06/23/how-estonia-became-the-

    digital-leaders-of-europe

Geertz, C. (1973). *The interpretation of cultures*. New York: Basic Books.

Gehlbach, S. (2010). Reflections on Putin and the media. *Post-Soviet Affairs*, *26*(1), 77–

    87.

Gellner, E. (2009). *Nations and nationalism* (2nd Edition). Ithaca, NY: Cornell

    University Press.

Gel'man, V. (2015). *Authoritarian Russia: Analyzing post-Soviet regime changes*.

    Pittsburgh, PA: University of Pittsburgh Press.

Gerovitch, S. (2002). *From newspeak to cyberspeak: A History of Soviet cybernetics*.

    Cambridge, MA: The MIT Press.

Gerovitch, S. (2008). InterNyet: why the Soviet Union did not build a nationwide

    computer network. *History and Technology*, *24*(4), 335–350.

Gerring, J. (2006). *Case study research: Principles and practices*. New York: Cambridge University Press.

GfK. (2018, January). Proniknovenie internet v Rossii: Itogi 2017 goda [Internet penetration in Russia: 2017 Summary]. GfK. Retrieved September 11, 2018, from https://www.gfk.com/fileadmin/user_upload/dyna_content/RU/Documents/Reports/2018/GfK_Rus_Internet_Penetration_in_Russia_2017-2018.pdf

Giacomello, G. (2005). *National governments and control of the Internet: A digital challenge*. New York, NY: Routledge.

Gill, G. (2015). *Building an authoritarian polity: Russia in post-Soviet times*. Cambridge, UK: Cambridge University Press.

Glen, C. M. (2017). *Controlling cyberspace: The politics of Internet governance and regulation*. Santa Barbara, CA: Praeger.

Goggin, G., & McLelland, M. (Eds.). (2008). *Internationalizing Internet studies: Beyond Anglophone paradigms*. New York: Routledge.

Goldsmith, J. (1998a). Regulation of the Internet: Three persistent fallacies. *Chicago-Kent Law Review*, *73*(4), 1119.

Goldsmith, J. (1998b). The Internet and the abiding significance of territorial sovereignty. *5 Indiana Journal of Global Legal Studies 475 (1998)*, *5*(2).

Goldsmith, J. (1998c). Against cyberanarchy. *University of Chicago Law Review*, *65*(4).

Goldsmith, J., & Wu, T. (2006). *Who controls the Internet?: Illusions of a borderless world*. New York: Oxford University Press.

Goldstein, G. (2012, December 16). The fight to keep a state-free internet. *Financial Times*. Retrieved September 4, 2018, from https://www.ft.com/content/22b57874-4607-11e2-b780-00144feabdc0

Golumbia, D. (2009). *The cultural logic of computation*. Cambridge, MA: Harvard University Press.

Google. (2012). *Take action: Add your voice to keep the Internet #freeandopen*. Retrieved September 5, 2018, from https://www.youtube.com/watch?v=z-lwA9GJ1e0

Google. (n.d.). Take Action. Retrieved September 5, 2018, from https://www.google.com/intl/en/takeaction/whats-at-stake

Gorbunova, Y. (2017). *Online and on all fronts: Russia's assault on freedom of expression*. Human Rights Watch. Retrieved August 23, 2018, from https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression

Gore, A. (1994, March). *Inauguration of the first World Telecommunication Development Conference (WTDC-94)*. Presented at the World Telecommunication Development Conference, Buenos Aires, Argentina. Retrieved August 22, 2018, from http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.144.57.en.104.pdf

Gorham, M., Lunde, I., & Paulsen, M. (Eds.). (2014). *Digital Russia: The language, culture and politics of new media communication*. London; New York: Routledge.

Greene, S. (2014). *Moscow in movement: Power and opposition in Putin's Russia*.

    Stanford, CA: Stanford University Press.

Greenfeld, L. (2011). The globalization of nationalism and the future of the nation-state.

    International Journal of Politics, Culture, and Society, *24*(1/2), 5–9.

Greenstein, S. (2010). The emergence of the Internet: Collective invention and wild

    ducks. *Industrial and Corporate Change*, *19*(5), 1521–1562.

Haigh, T., Russell, A. L., & Dutton, W. H. (2015). Histories of the Internet: Introducing

    a special issue of information & culture. *Information & Culture*, *50*(2), 143–159.

Hammersley, B. (2017, March 27). Concerned about Brexit? Why not become an e-

    resident of Estonia. *Wired UK*. Retrieved August 29, 2018, from

    https://www.wired.co.uk/article/estonia-e-resident

Harvey, D. (1989). *The condition of postmodernity: An enquiry into the origins of

    cultural change*. Oxford, UK; Cambridge, MA: Wiley-Blackwell.

Hay, C., & Marsh, D. (Eds.). (2000). *Demystifying globalization*. Houndmills,

    Basingstoke, Hampshire: Palgrave Macmillan.

Hayden, C. (2011). *The rhetoric of soft power: Public Diplomacy in global contexts*.

    Lanham, MD: Lexington Books.

Hearn, J. (2006). *Rethinking nationalism: A critical introduction*. Houndmills,

    Basingstoke, Hampshire, England: Palgrave Macmillan.

Herman, A. (2012, November 29). Will thugs rule the web? Retrieved September 5,

    2018, from https://nypost.com/2012/11/29/will-thugs-rule-the-web

Hiden, J., Made, V., & Smith, D. J. (Eds.). (2008). *The Baltic question during the Cold

    War*. London: Routledge.

Hill, R. (2014). *The new International Telecommunication Regulations and the Internet: A commentary and legislative History*. Berlin: Springer.

Hobsbawm, E. J. (2012). *Nations and nationalism since 1780: Programme, myth, reality* (2nd Edition). Cambridge, UK: Cambridge University Press.

Hobsbawm, E., & Ranger, T. (Eds.). (2012). *The invention of tradition* (Reissue edition). Cambridge, UK: Cambridge University Press.

Hofmann, J. (2016). Multi-stakeholderism in Internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, *1*(1), 29–49.

Hofmann, J., Katzenbach, C., & Gollatz, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society*.

Hope, N. (1994). Interwar statehood: Symbol and reality. In G. Smith (Ed.), *The Baltic states: The national self-determination of Estonia, Latvia and Lithuania*. New York: St. Martin's Press.

Hopf, T. (2002). *Social construction of foreign policy: Identities and foreign policies, Moscow, 1955 and 1999*. Ithaca, NY: Cornell University Press.

Hopf, T. (2007). The limits of interpreting evidence. In R. N. Lebow & M. I. Lichbach (Eds.), *Theory and evidence in comparative politics and international relations* (pp. 55–84). New York: Palgrave Macmillan.

Hopf, T., & Allan, B. B. (Eds.). (2016). *Making identity count: Building a national identity database*. New York: Oxford University Press.

Hough, K., Crum, J., Bascara, V., Liu, W., Chu, S.-Y., Kosnik, A. D., … Park, C. (2015). *Techno-Orientalism: Imagining Asia in speculative fiction, history, and*

media. (D. S. Roh, B. Huang, & G. A. Niu, Eds.). New Brunswick, NJ: Rutgers
University Press.

Howard, P. N. (2010). *The digital origins of dictatorship and democracy: Information
technology and political Islam*. Oxford; New York: Oxford University Press.

Human Rights Watch. (2015). *Human Rights Watch UPR submission to OHCHR:
Estonia*. Human Rights Watch. Retrieved from
https://www.hrw.org/news/2015/07/07/human-rights-watch-upr-submission-ohchr-
estonia

Hutchinson, J., & Smith, A. (Eds.). (1995). *Nationalism*. Oxford: Oxford University
Press.

Ikenberry, G. J. (2018). The end of liberal international order? *International Affairs*,
94(1), 7–23.

Ilves, T. (1998, January). *Estonia's Return to Europe*. Lecture presented by Toomas
Hendrik Ilves, Cyprus. Retrieved from https://vm.ee/en/news/estonias-return-europe

Ilves, T. (1999, December). *Estonia as a Nordic Country*. Speech presented at the
Swedish Institute for International Affairs, Stockholm, Sweden. Retrieved from
https://vm.ee/et/node/42622

Ilves, T. (2000, September). *Statement by Minister Ilves at the 55th session of the UN
General Assembly*. Presented at the 55th Session of the UN General Assembly,
New York. Retrieved August 30, 2018, from https://vm.ee/en/news/statement-
minister-ilves-55th-session-un-general-assembly

Ilves, T. (2009, September). *President Ilves at the International Cyber Conflict Legal
and Policy Conference in Tallinn*. Presented at the International Cyber Conflict

Legal and Policy Conference, Tallinn, Estonia. Retrieved from https://vp2006-2016.president.ee/en/official-duties/speeches/2685-president-ilves-at-the-international-cyber-conflict-legal-and-policy-conference-in-tallinn

Ilves, T. (2011, September). *President Toomas Hendrik Ilves at ICEGOV conference (International Conference on Theory and Practice of Electronic Governance)*. Presented at the International Conference on Theory and Practice of Electronic Governance, Tallinn, Estonia. Retrieved August 30, 2018, from https://vp2006-2016.president.ee/en/official-duties/speeches/6512-president-toomas-hendrik-ilves-at-icegov-conference-international-conference-on-theory-and-practice-of-electronic-governance-september-26-2011-viru-conference-center/index.html

Ilves, T. (2012a, March). *President of the Republic at the "E-governance or E-Dependence?" conference in Swissôtel, Tallinn, 14 March 2012*. Presented at the "E-governance or E-Dependence?" conference, Tallinn, Estonia. Retrieved August 30, 2018, 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

Ilves, T. (2012b, June). *The President of Estonia at the International Conference of Cyber Conflict*. Presented at the International Conference of Cyber Conflict, Tallinn, Estonia. Retrieved August 30, 2018, from https://vp2006-2016.president.ee/en/official-duties/speeches/7589-the-president-of-estonia-at-the-international-conference-of-cyber-conflict-8-june-2012/index.html

Ilves, T. (2014a, January). *Rebooting Trust? Freedom vs Security in Cyberspace*. Presented at the Munich Security Conference Cyber, Munich, Germany. Retrieved

August 30, 2018, from https://vp2006-2016.president.ee/en/official-duties/speeches/9796-qrebooting-trust-freedom-vs-security-in-cyberspaceq

Ilves, T. (2014b, April). *Remarks by the President of Estonia, Toomas Hendrik Ilves at the Freedom Online Coalition Conference in Swissotel, April 28, 2014*. Presented at the Freedom Online Coalition Conference, Tallinn, Estonia. Retrieved August 30, 2018, from https://vp2006-2016.president.ee/en/official-duties/speeches/10101-remarks-by-the-president-of-estonia-toomas-hendrik-ilves-at-the-freedom-online-coalition-conference-in-swissotel-april-28-2014/index.html

International Telecommunication Union. (2005, December). WSIS Outcome Documents. International Telecommunication Union. Retrieved September 4, 2018, from https://www.itu.int/net/wsis/outcome/booklet.pdf

International Telecommunication Union. (2012a). Final Acts of the World Conference on International Telecommunications (Dubai, 2012). Retrieved September 5, 2018, from https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

International Telecommunication Union. (2012b). Signatories of the Final Acts: 89. Retrieved September 5, 2018, from https://www.itu.int/osg/wcit-12/highlights/signatories.html

International Telecommunication Union. (2012c). WCIT-12 myth busting presentation. Retrieved September 5, 2018, from https://www.itu.int/en/wcit-12/Documents/wcit-myth-buster-en.pptx

International Telecommunication Union. (2012d, June 21). WCIT-12 Frequently Asked Questions. Retrieved September 5, 2018, from https://www.itu.int/en/wcit-12/Documents/WCIT-background-brief-FAQ.pdf

International Telecommunication Union. (2015). Percentage of individuals using the internet, 2000-2015. ITU. Retrieved August 23, 2018, from https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2016/Individuals_Internet_2000-2015.xls

Internet Assigned Numbers Authority. (n.d.). IANA — Root Servers. Retrieved September 4, 2018, from https://www.iana.org/domains/root/servers

Internet Engineering Task Force. (n.d.). Number of attendees per country across meetings. Retrieved September 4, 2018, from https://datatracker.ietf.org/stats/meeting/country/

Internet Freedom Project. (n.d.). Internet Freedom Project: Online, engaged, and on guard. Retrieved August 22, 2018, from http://internetfreedom.io

Internet World Stats. (2018, August 28). Internet Growth Statistics 1995 to 2018 - the Global Village Online. Retrieved September 4, 2018, from https://www.internetworldstats.com/emarketing.htm

Jackson, C. (2016). Legislation as an indicator of free press in Russia. *Problems of Post-Communism*, *63*(5–6), 354–366.

Jackson, J. (2015, September 21). RT sanctioned by Ofcom over series of misleading and biased articles. *The Guardian*. Retrieved August 24, 2018, from https://www.theguardian.com/media/2015/sep/21/rt-sanctioned-over-series-of-misleading-articles-by-media-watchdog

Jansen, S. C. (2012). Redesigning a nation: Welcome to E-stonia, 2001-2018. In N. Kaneva (Ed.), *Branding post-communist nations: Marketizing national identities in the "new" Europe*. New York: Routledge.

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

Jiang, Y. (2012). *Cyber-nationalism in China*. Adelaide, Australia: University of Adelaide Press.

Johnson, D. R., & Post, D. (1996). Law and borders - The rise of law in cyberspace. *Stanford Law Review*, *48*(5).

Jordan, P. (2014). *The modern fairy tale: Nation branding, national identity and the Eurovision song contest in Estonia*. Tartu, Estonia: University of Tartu Press.

Jowett, G. S., & O'Donnell, V. J. (2014). *Propaganda & Persuasion* (6th Edition). Thousand Oaks, CA: SAGE Publications.

Kahin, B., & Nesson, C. (Eds.). (1997). *Borders in cyberspace: Information policy and the global information infrastructure*. Cambridge, MA: The MIT Press.

Kaljulaid, K. (2017a, May). *President of the Republic at the Tallinn e-Governance Conference 2017*. Presented at the 2017 Tallinn e-Governance Conference, Tallinn, Estonia. Retrieved August 29, 2018, from https://president.ee/en/official-duties/speeches/13319-president-of-the-republic-at-the-tallinn-e-governance-conference-2017-30-may-2017/index.html

Kaljulaid, K. (2017b, June). *President of the Republic at the Opening of EuroDIG*. Presented at the EuroDIG (European Dialogue on Internet Governance), Tallinn, Estonia. Retrieved August 29, 2018, from https://president.ee/en/official-duties/speeches/13336-president-of-the-republic-at-the-opening-of-eurodig/index.html

Kaljulaid, K. (2017c, July). *President Kaljulaid at the Cyber & Innovation listening session*. Presented at the Cyber & Innovation listening session, Tallinn, Estonia. Retrieved August 30, 2018, from https://president.ee/en/official-duties/speeches/13488-president-kaljulaid-at-the-cyber-a-innovation-listening-session/index.html

Kaljurand, M. (2010). Estonia – Watchdog of free trade. *Estonian Ministry of Foreign Affairs Yearbook*. Retrieved August 29, 2018, from https://vm.ee/sites/default/files/content-editors/Marina_Kaljurand_0.pdf

Kalvet, T. (2007). *The Estonian information society developments since the 1990s* (Working Paper No 29). Tallinn, Estonia: Praxis. Retrieved September 11, 2018, from http://praxis.ee/wp-content/uploads/2014/03/2007-Estonian-information-society-developments.pdf

Kaneva, N. (Ed.). (2011). *Branding post-communist nations: Marketizing national identities in the "new" Europe*. New York: Routledge.

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

Keating, V. C., & Kaczmarska, K. (2017). Conservative soft power: liberal soft power bias and the 'hidden' attraction of Russia. *Journal of International Relations and Development*, 1–27.

Kerry, J. (2014, April). *Remarks to the Freedom Online Coalition Conference*. Presented at the Freedom Online Coalition, Via Teleconference. Retrieved August 30, 2018, from https://2009-2017.state.gov/secretary/remarks/2014/04/225290.htm

Kiggins, R. (2012). U.S. Identity, Security, and Governance of the Internet. In S. S. Costigan & J. Perry (Eds.), *Cyberspaces and global affairs*. Farnham, UK; Burlington, VT: Ashgate.

Kingsley, P. (2012, April 15). How tiny Estonia stepped out of USSR's shadow to become an internet titan. *The Guardian*. Retrieved September 11, 2018, from https://www.theguardian.com/technology/2012/apr/15/estonia-ussr-shadow-internet-titan

Kirby, D. (1994). Incorporation: The Molotov-Ribbentrop Pact. In G. Smith (Ed.), *The Baltic states: The national self-determination of Estonia, Latvia and Lithuania*. New York: St. Martin's Press.

Kiseleva, Y. (2015). Russia's soft power discourse: Identity, status and the attraction of power. *Politics*, *35*(3–4), 316–329.

Kitman, J. (2011, November 3). President Ilves: The man who made E-stonia. *The Guardian*. Retrieved August 28, 2018, from https://www.theguardian.com/world/2011/nov/03/president-ilves-made-estonia

Kitsing, M. (2011). Success Without Strategy: E-Government Development in Estonia. *Policy & Internet*, *3*(1), 1–21.

Kivirähk, J. (2017). *Public opinion and national defense* (Survey). Tallinn, Estonia: Estonian Ministry of Defence. Retrieved August 29, 2018, from http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/public_opinion_and_national_defence_2017_march.pdf

Kleinwächter, W. (2012, December 17). WCIT and Internet governance: Harmless resolution or Trojan Horse? Retrieved September 5, 2018, from

http://www.circleid.com/posts/20121217_wcit_and_internet_governance_harmless _resolution_or_trojan_horse/

Klyueva, A. (2016). Taming online political engagement in Russia: Disempowered publics, empowered state and challenges of the fully functioning society. *International Journal of Communication*, *10*, 4661-4680.

Klyueva, A., & Mikhaylova, A. (2017). Building the Russian World: Cultural Diplomacy of the Russian Language and Cultural Identity. *JOMEC Journal*, *11*, 127–143.

Kolstø, P., & Blakkisrud, H. (Eds.). (2016). *The new Russian nationalism: Imperialism, ethnicity and authoritarianism 2000-2015*. Edinburgh: Edinburgh University Press.

Koltsova, O. (2006). *News media and power in Russia*. London and New York: Routledge.

Kondratyev, A. (1996, December 24). Internet i FAPSI [Internet and the Federal Agency of Government Communications and Information]. *Kommersant*. Retrieved August 24, 2018, from https://www.kommersant.ru/doc/245444

Konradova, N., & Schmidt, H. (2014). From the utopia of autonomy to a political battlefield: towards a history of the "Russian internet." In M. Gorham, I. Lunde, & M. Paulsen (Eds.), *Digital Russia: The language, culture and politics of new media communication*. London: Routledge.

Kotka, T. (2015, November). *Countries without borders, countries without territory, and digital citizenships (e-Residency)*. Talk, Columbia University, New York. Retrieved August 29, 2018, from http://harriman.columbia.edu/event/countries-without-borders-countries-without-territory-and-digital-citizenships-e-residency

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 August 29, 2018, from

    https://www.politics.ox.ac.uk/publications/estonian-e-residency-redefining-the-

    nation-state-in-the-digital-era.html

Kraidy, M. M. (2005). *Hybridity: The cultural logic of globalization*. Philadelphia:

    Temple University Press.

Kramer, T. (2012, December 9). ITU interview @ WCIT - 12: H.E Terry Kramer,

    Ambassador, Department of State, USA [Video]. Retrieved September 5, 2018,

    from https://www.youtube.com/watch?v=HXWvlSbGRE4

Krigman, E. (2012, November 30). The plot against the Internet. Retrieved September 5,

    2018, from http://www.politico.com/story/2012/12/the-plot-against-the-internet-

    84468.html

Kurbalija, J. (2016). *An introduction to Internet governance* (7th edition). Geneva:

    DiploFoundation.

Kus-Harbord, L., & Ward, C. (2015). Ethnic Russians in post-Soviet Estonia: Perceived

    devaluation, acculturation, well-being, and ethnic attitudes. *International*

    Perspectives in Psychology: Research, Practice, Consultation, *4*, 66–81.

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. Cambridge, UK: Cambridge University Press.

La French Tech. (n.d.). La French Tech. Retrieved August 20, 2018, from

    https://meetlafrenchtech.com

Laar, M. (1996). Estonia's success story. *Journal of Democracy*, *7*(1), 96–101.

Laar, M. (2002). *Estonia: Little country that could*. London: Centre for Research into Post-Communist Economies.

Laikam, K. (2017). *Informatsionnoe obschestvo v Rossiiskoi Federatsii: Statisticheskii sbornik [Information society in the Russian Federation: A statistical collection]*. Russian Ministry of Telecom and Mass Communications, Russian Federal State Statistical Service, National Research University - Higher School of Economics. Retrieved September 7, 2018, from http://www.gks.ru/free_doc/doc_2017/info-ob.pdf

Lamont, M., & Thévenot, L. (Eds.). (2000). *Rethinking comparative cultural sociology: Repertoires of evaluation in France and the United States*. Cambridge, UK: Cambridge University Press.

Lane, D. (2008). From chaotic to state-led capitalism. *New Political Economy*, *13*(2), 177–184.

Larson, D. W., & Shevchenko, A. (2010). Status seekers: Chinese and Russian responses to U.S. primacy. *International Security*, *34*(4), 63–95.

Larson, D. W., & Shevchenko, A. (2014). Russia says no: Power, status, and emotions in foreign policy. *Communist and Post-Communist Studies*, *47*(3), 269–279.

Laruelle, M. (2010). *In the name of the nation: Nationalism and politics in contemporary Russia*. New York: Palgrave Macmillan.

Laruelle, Marlene (Ed.). (2009). *Russian nationalism and the national reassertion of Russia*. London and New York: Routledge.

Laruelle, Marlene. (2015). *The "Russian World:" Russia's soft power and geopolitical imagination*. Washington, DC: Center on Global Interests. Retrieved September 12, 2018, from http://globalinterests.org/wp-content/uploads/2015/05/FINAL-CGI_Russian-World_Marlene-Laruelle.pdf

Lavrov, S. (2017, December). *Foreign Minister Sergey Lavrov's remarks and replies to media questions during the Government Hour in the Federation Council of the Federal Assembly of the Russian Federation, Moscow, December 15, 2017*. Presented at the the Government Hour in the Federation Council of the Federal Assembly of the Russian Federation, Moscow, Russia. Retrieved August 28, 2018, from http://www.mid.ru/en/press_service/video/-/asset_publisher/i6t41cq3VWP6/content/id/2992396

Lebow, R. N. (2009). *A cultural theory of international relations*. Cambridge, UK: Cambridge University Press.

Ledeneva, A. V. (2013). *Can Russia modernise?: Sistema, power Networks and informal governance*. Cambridge and New York: Cambridge University Press.

Lee, D. (2014, June 23). France sparks .wine address row. *BBC News*. Retrieved August 23, 2018, from https://www.bbc.co.uk/news/technology-27974293

Legvold, R. (Ed.). (2007). *Russian foreign policy in the twenty-first century and the shadow of the past*. New York: Columbia University Press.

Legvold, R. (2016). *Return to Cold War*. Cambridge, UK and Malden, MA: Polity.

Lessig, L. (2006). *Code: And other laws of cyberspace, version 2.0* (2nd Revised Edition). New York: Basic Books.

Levitsky, S., & Way, L. A. (2010). *Competitive authoritarianism: Hybrid regimes after the Cold War*. New York: Cambridge University Press.

Levy, C. J. (2008, August 21). Russia prevailed on the ground, but not in the media. *The New York Times*. Retrieved August 24, 2018, from

https://www.nytimes.com/2008/08/22/world/europe/22moscow.html

Levy, C. J. (2009, December 21). Russians Wary of Cyrillic Web Domains. *The New York Times*. Retrieved August 24, 2018, from

https://www.nytimes.com/2009/12/22/world/europe/22cyrillic.html

Li, B., Churkin, V., Aslov, S., & Askarov, M. (2011). International code of conduct for information security. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved August 23, 2018, from

https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

Lieven, A. (1994). *The Baltic revolution: Estonia, Latvia, Lithuania and the path to independence*. New Haven, CT: Yale University Press.

Lipman, M. (2015). The media. In S. Wegren (Ed.), *Putin's Russia: Past imperfect, future uncertain*. Lanham, MD: Rowman & Littlefield.

Liu, J., Abdrakhmanov, K., Kydyrov, T., Churkin, V., Mahmadaminov, M., & Madrakhimov, M. (2015, January 13). International code of conduct for information security. United Nations DAG Repository. Retrieved August 28, 2018, from

http://repository.un.org/bitstream/handle/11176/158448/A_69_723-EN.pdf?sequence=3&isAllowed=y

Lucas, E. (2014). *The new Cold War: Putin's Russia and the threat to the West* (3rd revised edition). New York, NY: St. Martin's Griffin.

Lungescu, O. (2004, April 7). Tiny Estonia leads internet revolution. *BBC News*.

    Retrieved September 12, 2018, from http://news.bbc.co.uk/2/hi/europe/3603943.stm

MacKenzie, D., & Wajcman, J. (Eds.). (1999). *The social shaping of technology* (2nd

    Edition). Buckingham, UK and Philadelphia: McGraw Hill Education / Open

    University.

Made, V. (2003). Estonia and Europe: A Common identity or an identity Crisis? In M.

    Lehti & D. Smith (Eds.), *Post-Cold War identity politics - Northern and Baltic*

    experiences. London, UK: Frank Cass Publishers.

Mäe, R. (2017). The story of e-Estonia: A discourse-theoretical approach. *Baltic Worlds*,

    10(1–2), 32–44.

Mailland, J., & Driscoll, K. (2017). *Minitel: Welcome to the Internet*. Cambridge, MA:

    The MIT Press.

Makarychev, A., & Mommen, A. (Eds.). (2013). *Russia's changing economic and*

    political regimes: The Putin years and afterwards. New York: Routledge.

Malcolm, J. (2008). *Multi-stakeholder governance and the Internet Governance Forum*.

    Perth, Australia: Terminus Press.

Mansel, T. (2013, May 16). How Estonia became E-stonia. *BBC News*. Retrieved

    September 12, 2018, from http://www.bbc.com/news/business-22317297

Mansell, R. (2012). *Imagining the Internet: Communication, innovation, and*

    governance. Oxford: Oxford University Press.

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of Information:

    Understanding Russian internet policy. *Media and Communication*, *5*(1), 29–41.

Marvin, C. (1988). *When old technologies were new: Thinking about electric communication in the late nineteenth century*. New York: Oxford University Press.

Marzouk, Z. (2017, November 6). Estonia's rise into a digital nation. *IT PRO*. Retrieved August 30, 2018, from http://itpro.co.uk/go/29868

Mattelart, A. (2000). *Networking the World, 1794-2000*. Minneapolis, MN: University of Minnesota Press.

Maurer, T., & Morgus, R. (2014, February 19). Stop calling decentralization of the Internet "Balkanization." Retrieved September 4, 2018, from http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html

McCarthy, D. (2015). *Power, information technology, and international relations theory: The power and politics of US Foreign policy and the Internet*. New York: Palgrave Macmillan.

McDowell, R. M. Statement of Commissioner Robert M. McDowell, Federal Communications Commission: Fighting for Internet freedom: Dubai and beyond, § U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Communications and Technology, and Committee on Foreign Affairs, Subcommittee on Terrorism, Nonproliferation, and Trade, and Committee on Foreign Affairs, Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations (2013). Washington, D.C.: U.S. House of Representatives. Retrieved September 5, 2018, from https://docs.house.gov/meetings/IF/IF16/20130205/100221/HHRG-113-IF16-Wstate-McDowellR-20130205.pdf

McKinsey Global Institute. (2016). *Digital globalization: The new era of global flows*.

Retrieved August 22, 2018, from

https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey

%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20

of%20global%20flows/MGI-Digital-globalization-Full-report.ashx

McNair, B. (2000). Power, profit, corruption, and lies: The Russian media in the 1990s.

In J. Curran & M.-J. Park (Eds.), *De-Westernizing media studies*. London:

Routledge.

Medina, E. (2011). *Cybernetic revolutionaries: Technology and politics in Allende's

Chile*. Cambridge, MA: The MIT Press.

Medvedev, D. (2008). The foreign policy concept of the Russian Federation. President of

Russia. Retrieved August 23, 2018, from http://en.kremlin.ru/supplement/4116

Medvedev, D. (2009a). Dmitry Medvedev's article, Go Russia! President of Russia.

Retrieved August 23, 2018, from http://en.kremlin.ru/events/president/news/5413

Medvedev, D. (2009b, April 22). A new recording on Dmitry Medvedev's blog: On

Internet development in Russia. Retrieved August 24, 2018, from

http://en.kremlin.ru/events/president/transcripts/25186

Medvedev, D. (2015, December). *Address at the 2nd World Internet Conference*.

Presented at the 2nd World Internet Conference, Wuzhen, China. Retrieved August

28, 2018, from http://government.ru/en/news/21075

Melville, A., & Shakleina, T. (2005). *Russian foreign policy in transition: Concepts and

realities*. Budapest: Central European University Press.

Mendelson, S. The Medvedev thaw: Is it real? Will it last?, Pub. L. No. CSCE 111-1-4, § Commission on Security and Cooperation in Europe (2012). Washington, D.C.: U.S. Government Printing Office. Retrieved August 23, 2018, from https://www.csce.gov/sites/helsinkicommission.house.gov/files/The%20Medvedev%20Thaw%20-%20Is%20it%20Real,%20Will%20it%20Last_Compiled.PDF

Meri, L. (1994, February). *Address by H.E. Lennart Meri, President of the Republic of Estonia, at a Matthiae-Supper in Hamburg on February 25, 1994*. Presented at the Matthiae-Supper, Hamburg, Germany. Retrieved August 29, 2018, from https://vp1992-2001.president.ee/eng/k6ned/K6ne.asp?ID=9401

Meyer, J. W., Boli, J., Thomas, G. M., & Ramirez, F. O. (1997). World society and the nation-state. *American Journal of Sociology*, *103*(1), 144–181.

Miller, D., & Slater, D. (2000). *The Internet: An ethnographic approach*. Oxford and New York: Berg Publishers.

Milliken, J. (1999). The study of discourse in international relations: A critique of research and methods. *European Journal of International Relations*, *5*(2), 225–254.

Misiunas, R., & Taagepera, R. (1993). *The Baltic states: Years of dependence, 1940-1990*. Berkeley: University of California Press.

Miskimmon, A., & O'Loughlin, B. (2017). Russia's narratives of global order: Great power legacies in a polycentric world. *Politics and Governance*, *5*(3), 111–120.

Miskimmon, A., O'Loughlin, B., & Roselle, L. (2013). *Strategic narratives: Communication power and the new world order*. New York and London: Routledge.

Mole, R. (2012). *The Baltic states from the Soviet Union to the European Union: Identity, discourse and power in the Post-Communist transition of Estonia, Latvia and Lithuania.* New York: Routledge.

Montresor, S. (2001). Techno-globalism, techno-nationalism and technological systems: Organizing the evidence. *Technovation*, *21*, 399–412.

Moorthy, N. (2016, March 24). Estonian Prime Minister Taavi Rõivas: Technology sparked country's economic growth, government efficiency. *The Chronicle*. Retrieved August 28, 2018, from

http://www.dukechronicle.com/article/2016/03/estonian-prime-minister-taavi-rivas-technology-sparked-countrys-economic-growth-government-efficiency

Morozov, V. (2008). Sovereignty and democracy in contemporary Russia: A modern subject faces the post-modern world. *Journal of International Relations and Development*, *11*(2), 152–180.

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

Mueller, M. (2004). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: The MIT Press.

Mueller, M. (2007). *The Politics and Issues of Internet Governance*. Institute for Research and Debate on Governance. Retrieved September 12, 2018, from http://www.institut-gouvernance.org/en/analyse/fiche-analyse-265.html

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: The MIT Press.

Mueller, M. (2012, December 18). ITU phobia: Why WCIT was derailed. Retrieved

    September 5, 2018, from https://www.internetgovernance.org/2012/12/18/itu-

    phobia-why-wcit-was-derailed

Mueller, M. (2013, July 19). Are we in a digital Cold War? Retrieved March 4, 2018,

    from https://www.internetgovernance.org/2013/07/19/are-we-in-a-digital-cold-war

Mueller, M. (2017). *Will the Internet fragment?: Sovereignty, globalization and*

    cyberspace. Cambridge, UK and Malden, MA: Polity.

Mueller, M. L. (2011). China and global Internet governance: A Tiger by the tail. In R.

    Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access contested: Security,*

    identity, and resistance in Asian cyberspace. Cambridge, MA: The MIT Press.

Müller, M. (2011). Market meets nationalism: Making entrepreneurial state subjects in

    post-Soviet Russia. *Nationalities Papers*, *39*(3), 393–408.

Musiani, F., & Pohle, J. (2014). NETmundial: Only a landmark event if "Digital Cold

    War" rhetoric abandoned. *Internet Policy Review*, *3*(1).

Nakayama, S. (2012). Techno-nationalism versus techno-globalism. *East Asian Science,*

    Technology and Society, *6*(1), 9–15.

National Cybersecurity Agency of France. (2015). French national digital security

    strategy. National Cybersecurity Agency of France. Retrieved August 23, 2018,

    from

    https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_e

    n.pdf

Naughton, J. (2012, November 25). Would you trust Vladimir Putin with the keys to the

    web? *The Guardian*. Retrieved September 4, 2018, from

https://www.theguardian.com/technology/2012/nov/25/vladimir-putin-plot-internet-freedom

Naughton, J. (2016). The evolution of the Internet: From military experiment to general purpose technology. *Journal of Cyber Policy*, *1*(1), 5–28.

Negro, G. (2014). Chinese Internet governance—Some domestic and foreign issues. In R. Radu, J.-M. Chenou, & R. H. Weber (Eds.), *The evolution of global Internet governance: Principles and policies in the making*. Heidelberg, Germany: Springer.

Neskromny, V. (1997, January 6). Duma o rossiiskom Internete [Duma on the Russian internet]. *Computerra*, *1*(178). Retrieved August 24, 2018, from http://old.computerra.ru/1997/178/193182

Neumann, I. B. (2016a). *Russia and the idea of Europe: A study in identity and international relations* (2nd edition). Milton Park, Abingdon, Oxon and New York, NY: Routledge.

Neumann, I. B. (2016b). Russia's Europe, 1991–2016: Inferiority to superiority. *International Affairs*, *92*(6), 1381–1399.

Nikiforov, N. (2014, April). *Address at the Netmundial*. Presented at the Netmundial, Sao Pulo, Brazil. Retrieved August 28, 2018, from http://minsvyaz.ru/ru/events/30031

Nikiforov, N. (2016a, June). *Address at the 8th International IT Forum with BRICS and SCO Participation*. Presented at the 8th International IT Forum with BRICS and SCO Participation, Khanty-Mansiysk, Russia. Retrieved August 28, 2018, from http://minsvyaz.ru/ru/events/35261

Nikiforov, N. (2016b, October 1). Official statement by Minister of Telecom Nikolay

    Nikiforov on the occasion of the statement by U.S. Deputy Secretary of Commerce

    Lawrence Strickling about the termination of state control by the United States over

    the Internet Assigned Numbers Authority (IANA), previously carried out by the

    Internet Corporation for Assigned Names and Numbers (ICANN). Russian Ministry

    of Digital Development, Communications and Mass Media. Retrieved August 28,

    2018, from http://minsvyaz.ru/ru/events/35815

Noah, T. (2016, March 22). Exclusive - Taavi Roivas Extended Inerview Pt. 1

    [Interview]. *The Daily Show with Trevor Noah*. New York: Comedy Central.

    Retrieved September 12, 2018, from http://www.cc.com/video-clips/bz2f5k/the-

    daily-show-with-trevor-noah-exclusive---taavi-roivas-extended-interview-pt--1

Noam, E. (2013). Towards the federated Internet. *InterMEDIA*, *41*(4), 10–13.

Nocetti, J. (2011). *"Digital Kremlin": Power and the Internet in Russia*. Paris: Institut

    Francais des Relations Internationales. Retrieved September 12, 2018, from

    https://www.ifri.org/sites/default/files/atoms/files/ifrinocettirussianwebengmars201

    1.pdf

Nocetti, J. (2015a). Contest and conquest: Russia and global internet governance.

    International Affairs, *91*(1), 111–130.

Nocetti, J. (2015b). Russia's "Dictatorship of the law" approach to internet policy.

    Internet Policy Review, *4*(4).

Nordenstreng, K. (2011). Free flow doctrine in global media policy. In R. Mansell & M.

    Raboy (Eds.), *The handbook of global media and communication policy*. Malden,

    MA: Wiley-Blackwell.

Oates, S. (2006). *Television, democracy and elections in Russia*. Abingdon, Oxon, England and New York: Routledge.

Oates, S. (2007). The neo-Soviet model of the media. *Europe-Asia Studies*, *59*(8), 1279–1297.

Oates, S. (2013). *Revolution stalled: The political limits of the Internet in the post-Soviet sphere*. Oxford and New York: Oxford University Press.

Oates, S. (2016). Russian media in the digital age: Propaganda rewired. *Russian Politics*, *1*(4), 398–417.

Obama, B., & Medvedev, D. (2009, April 1). Joint statement by President Dmitriy Medvedev of the Russian Federation and President Barack Obama of the United States of America. The White House. Retrieved August 23, 2018, from https://obamawhitehouse.archives.gov/the-press-office/joint-statement-president-dmitriy-medvedev-russian-federation-and-president-barack-

Open Technology Fund. (n.d.). About the program. Retrieved August 22, 2018, from https://www.opentech.fund/about/program

Østbø, J. (2017). Securitizing "spiritual-moral values" in Russia. *Post-Soviet Affairs*, *33*(3), 200–216.

Ostry, S., & Nelson, R. R. (1995). *Techno-nationalism and techno-globalism: Conflict and cooperation*. Washington, D.C.: Brookings Institution Press.

Oushakine, S. (2000). In the state of post-Soviet aphasia: Symbolic development in contemporary Russia. *Europe-Asia Studies*, *52*(6), 991–1016.

Owen, T. (2015). *Disruptive power: The crisis of the state in the digital age*. Oxford and New York: Oxford University Press.

Oxford Dictionaries. (n.d.). Alternative. *Oxford Dictionaries*. Retrieved August 21,

    2018, from https://en.oxforddictionaries.com/definition/alternative

Ozkirimli, U. (2017). *Theories of nationalism: A critical introduction* (3rd edition).

    London: Palgrave.

Pacer, V. (2016). *Russian foreign policy under Dmitry Medvedev, 2008-2012*. London:

    Routledge.

Paet, U. (2011, December). *Address by Foreign Minister Urmas Paet at the Internet

    Freedom Conference in The Hague*. Presented at the Internet Freedom Conference,

    The Hague, the Netherlands. Retrieved August 30, 2018, from

    https://vm.ee/en/news/address-foreign-minister-urmas-paet-internet-freedom-

    conference-hague

Pallin, C. V. (2017). Internet control through ownership: The case of Russia. *Post-Soviet

    Affairs*, *33*(1), 16–33.

Pardes, A. (2016, May 5). Estonia's e-Residency program is the future of immigration.

    Retrieved August 29, 2018, from

    https://www.vice.com/en_us/article/avyx5a/estonias-e-residency-program-is-the-

    future-of-immigration

Paré, D. J. (2002). *Internet governance in transition: Who is the master of this domain?*

    Lanham, MD: Rowman & Littlefield Publishers.

Paul, T. V., Larson, D. W., & Wohlforth, W. C. (Eds.). (2014). *Status in world politics*.

    New York: Cambridge University Press.

Pavan, E. (2012). *Frames and connections in the governance of global communications: A network study of the Internet Governance Forum*. Lanham, MD: Lexington Books.

Perritt, H. (1998). The Internet as a threat to sovereignty? Thoughts on the Internet's role in strengthening national and global governance. *Indiana Journal of Global Legal Studies*, *5*(2), 423–442.

Peskov, D. (2011, June 10). Doing business in Russia. *The New York Times*. Retrieved August 24, 2018, from https://www.nytimes.com/2011/06/11/opinion/l11nocera.html

Peters, B. (2016). *How not to network a nation: The uneasy history of the Soviet Internet*. Cambridge, MA: The MIT Press.

Peterson, D. J. (2005). *Russia and the information revolution*. Santa Monica, CA: Rand Corporation.

Petrov, N. (2005). From managed democracy to sovereign democracy: Putin's regime evolution in 2005. *PONARS Eurasia - Policy Memos*. Retrieved September 12, 2018, from http://www.ponarseurasia.org/sites/default/files/policy-memos-pdf/pm_0396.pdf

Petrov, N., & Lipman, M. (Eds.). (2015). *The State of Russia: What Comes Next?* Houndmills, Basingstoke, Hampshire and New York: Palgrave McMillan.

Poe, M. T. (2006). *The Russian moment in world history*. Princeton, NJ: Princeton University Press.

Pohle, J. (2016). Multistakeholder governance processes as production sites: Enhanced cooperation "in the making." *Internet Policy Review*, *5*(3).

Pohle, J., Hösl, M., & Kniep, R. (2016). Analysing internet policy as a field of struggle. *Internet Policy Review*, *5*(3).

Post, D. G. (1995). Anarchy, state, and the Internet - An essay on law-making in cyberspace. *Journal of Online Law*, *Article 3*. Retrieved September 12, 2018, from https://papers.ssrn.com/abstract=943456

Post, D. G. (2009). *In Search of Jefferson's Moose: Notes on the State of Cyberspace by David G. Post*. Oxford: Oxford University Press.

Pouzin, L. (1973). Presentation and major design aspects of the Cyclades computer network. In R. L. Pickholtz, T. Pyke, P. E. Jackson, & R. Filipowski (Eds.), *DATACOMM '73 Proceedings of the third ACM symposium on Data communications and Data networks: Analysis and design* (pp. 80–87). New York: Association for Computing Machinery. Retrieved September 4, 2018, from http://delivery.acm.org/10.1145/820000/811034/p80-pouzin.pdf?ip=165.123.234.123&id=811034&acc=PUBLIC&key=A792924B58C015C1%2E18947888DF2D0EEA%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1536095940_be47dd93f1597aca7daf95b15b304000

Powers, M., & Vera-Zambrano, S. (2018). The universal and the contextual of media systems: Research design, epistemology, and the production of comparative knowledge. *The International Journal of Press/Politics*, *23*(2), 143–160.

Powers, S. M., & Jablonski, M. (2015). *The real cyber war: The political economy of Internet Freedom*. Champaign, IL: University of Illinois Press.

President of Russia. (2013, June 11). Visit to Russia Today television channel. Retrieved August 24, 2018, from http://en.kremlin.ru/events/president/news/18319

Price, M. E. (2002). *Media and sovereignty: The global information revolution and its challenge to state power*. Cambridge, MA: The MIT Press.

Price, M. E. (2014). *Free expression, globalism, and the new strategic communication*. New York: Cambridge University Press.

Price, M. E. (2017). The global politics of Internet governance: A case study in closure and technological design. In D. R. McCarthy (Ed.), *Technology and world politics*. Abingdon, Oxon and New York: Routledge.

Price, M. E., Richter, A., & Yu, P. K. (Eds.). (2002). *Russian media law and policy in Yeltsin decade: Essays and documents*. The Hague: Kluwer Law International.

Putin, V. (2000a). Information security doctrine of the Russian Federation. International Telecommunication Union. Retrieved August 24, 2018, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf

Putin, V. (2000b, July). *Annual address to the Federal Assembly of the Russian Federation*. Moscow, Russia. Retrieved August 24, 2018, from http://en.kremlin.ru/events/president/transcripts/21480

Putin, V. (2005a). Foreign policy conception of the Russian Federation (2000). In A. Melville & T. Shakleina (Eds.), *Russian foreign policy in transition: Concepts and realities*. Budapest: Central European University Press.

Putin, V. (2005b). Russia at the turn of the millennium. In A. Melville & T. Shakleina (Eds.), *Russian foreign policy in transition: Concepts and realities*. Budapest: Central European University Press.

Putin, V. (2005c, November). *Press statement and answers to questions on the results of Russian-Dutch talks*. Presented at the Russian-Dutch talks, The Hague, the Netherlands. Retrieved August 24, 2018, from

http://en.kremlin.ru/events/president/transcripts/23246

Putin, V. (2007a, February). *Speech and the Following Discussion at the Munich Conference on Security Policy*. Presented at the Munich Security Conference, Munich, Germany. Retrieved August 23, 2018, from

http://en.kremlin.ru/events/president/transcripts/24034

Putin, V. (2007b, September). *Meeting with Members of the Valdai International Discussion Club*. Presented at the Valdai International Discussion Club, Sochi, Russia. Retrieved August 23, 2018, from

http://en.kremlin.ru/events/president/transcripts/24537

Putin, V. (2008). Strategiya razvitiya informatsionnogo obschestva v Rossiiskoi Federatsii [Strategy of information society development in the Russian Federation]. Russian Ministry of Digital Development, Communications and Mass Media. Retrieved August 24, 2018, from

http://minsvyaz.ru/uploaded/files/strategiya_razvitiya_inf_obschestva_1.pdf

Putin, V. (2012a, January 23). Vladimir Putin. Rossiya: Natsional'nyi vorpos [Vladimir Putin. Russia: The national question]. *Nezavisimaya Gazeta*. Retrieved September 9, 2018, from http://www.ng.ru/politics/2012-01-23/1_national.html

Putin, V. (2012b, December 19). Strategiya gosudarstvennoi natsional'noi politiki Rossiiskoi Federatsii na period do 2025 goda [Nationalities policy strategy of the

Russian Federation until 2025]. President of Russia. Retrieved September 9, 2018,

    from http://static.kremlin.ru/media/acts/files/0001201212190001.pdf

Putin, V. (2013a, February 12). Concept of the foreign policy of the Russian Federation.

    Russian Ministry of Foreign Affairs. Retrieved August 24, 2018, from

    http://www.mid.ru/foreign_policy/official_documents/-

    /asset_publisher/CptICkB6BZ29/content/id/122186

Putin, V. (2013b, September). *Meeting of the Valdai International Discussion Club*.

    Presented at the Valdai International Discussion Club, Novgorod Region, Russia.

    Retrieved August 23, 2018, from http://en.kremlin.ru/events/president/news/19243

Putin, V. (2013c, December). *News conference of Vladimir Putin*. News conference of

    Vladimir Putin, Moscow, Russia. Retrieved August 23, 2018, from

    http://en.kremlin.ru/events/president/news/19859

Putin, V. (2014). *Internet entrepreneurship in Russia forum*. Presented at the Internet

    entrepreneurship in Russia forum, Moscow, Russia. Retrieved August 23, 2018,

    from http://en.kremlin.ru/events/president/news/45886

Putin, V. (2015, December 31). Strategiya natsional'noi bezopasnosti Rossiiskoi

    Federatskii [National security strategy of the Russian Federation]. President of

    Russia. Retrieved August 24, 2018, from

    http://static.kremlin.ru/media/acts/files/0001201512310038.pdf

Putin, V. (2016a, November 30). Foreign policy concept of the Russian Federation.

    Russian Ministry of Foreign Affairs. Retrieved August 24, 2018, from

    http://www.mid.ru/foreign_policy/official_documents/-

    /asset_publisher/CptICkB6BZ29/content/id/2542248

Putin, V. (2016b, December 5). Doctrine of information security of the Russian

    Federation. Russian Ministry of Foreign Affairs. Retrieved August 24, 2018, from

    http://www.mid.ru/foreign_policy/official_documents/-

    /asset_publisher/CptICkB6BZ29/content/id/2563163

Putin, V. (2017, May 9). Strategiya razvitiya infortsionnogo obschestva v Rossiiskoi

    Federatsii na 2017-2030 [Information society development strategy of the Russian

    Federation for 2017-2030]. President of Russia. Retrieved August 24, 2018, from

    http://static.kremlin.ru/media/acts/files/0001201705100002.pdf

Rabinow, P., & Sullivan, W. M. (Eds.). (1988). *Interpretive social science: A Second

    Look* (2nd edition). Berkeley: University of California Press.

Raboy, M., Landry, N., & Shtern, J. (2010). *Digital solidarities, communication policy

    and multi-stakeholder global governance: The legacy of the World Summit on the

    Information Society*. New York: Peter Lang Inc., International Academic

    Publishers.

Radu, R., Chenou, J.-M., & Weber, R. H. (Eds.). (2014). *The evolution of global Internet

    governance*. Berlin: Springer.

Rantanen, T. (2004). *The media and globalization*. London and Thousand Oaks, CA:

    SAGE Publications Ltd.

Rawnsley, G. D. (2015). To know us is to love us: Public diplomacy and international

    broadcasting in contemporary Russia and China. *Politics*, *35*(3–4), 273–286.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate

    global institution. *International Theory*, *7*(3), 572–616.

Reed, C. (2012). *Making laws for cyberspace*. Oxford: Oxford University Press.

Reich, R. (1987). The rise of techno-nationalism. *Atlantic Monthly*, *259*(5).

Reidenberg, J. (1997). Lex Informatica: The formulation of information policy rules

through technology. *Texas Law Review*, *76*(3), 553–593.

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory*

Law Journal, *45*, 911-930.

Reidenberg, J. R. (2005). Technology and Internet jurisdiction. *University of*

Pennsylvania Law Review, *153*(6), 1951–1974.

Reiman, L. (2005, November). *Vystuplenie L. Reimana, Ministra Rossiiskoi Federatsii*

po svyazi i informatsii, glavy delegatsii Rossiiskoi Federatsii [Address by Leonid

Reiman, the Minister of Communication and Information of the Russian Federation,

the head of the Russian delegation]. Presented at the World Summit on the

Information Society, Second Phase, Tunis, Tunis. Retrieved August 28, 2018, from

https://www.ifap.ru/library/book193.pdf

Renshon, J. (2017). *Fighting for status: Hierarchy and conflict in world politics*.

Princeton, NJ: Princeton University Press.

Reynolds, P. (2008, August 15). Russians losing propaganda war. *BBC News*. Retrieved

August 24, 2018, from http://news.bbc.co.uk/2/hi/europe/7562611.stm

Richter, A. (2011). The post-Soviet media and communication policy landscape: The

case of Russia. In R. Mansell & M. Raboy (Eds.), *The handbook of global media*

and communication policy. Hoboken, NJ: Wiley-Blackwell.

Ringmar, E. (1996). *Identity, interest and action: A cultural explanation of Sweden's*

intervention in the Thirty Years War. Cambridge, UK, and New York: Cambridge

University Press.

Rohozinski, R. (1999). *Mapping Russian cyberspace: Perspectives on democracy and the net* (UNRISD Discussion Paper No. 115). Geneva, Switzerland: United Nations Research Institute for Social Development. Retrieved September 12, 2018, from http://www.unrisd.org/80256B3C005C2802/(ViewPDF)?OpenAgent&parentunid= 879B8965BF0AE0ED80256B67005B738A&parentdb=80256B3C005BCCF9&par entdoctype=paper&netitpath=80256B3C005BCCF9/(httpAuxPages)/879B8965BF0 AE0ED80256B67005B738A/$file/dp115.pdf

Rõivas, T. (2014, December). *Leveraging technology in turbulent times: How to ensure security and economic growth in an unpredictable global environment*. Stanford, CA. Retrieved September 12, 2018, from https://www.youtube.com/watch?v=XOg0o3nmCYQ

Rosenzweig, R. (1998). Wizards, bureaucrats, warriors, and hackers: Writing the history of the Internet. *The American Historical Review*, *103*(5), 1530–1552.

Rossotrudnichestvo. Federal agency for the Commonwealth of Independent States Affairs, Compatriots Living Abroad, and International Humanitarian Cooperation. (n.d.). Retrieved August 24, 2018, from http://rs.gov.ru/en

Roudakova, N. (2017). *Losing Pravda: Ethics and the press in post-truth Russia*. Cambridge: Cambridge University Press.

Royce, E. R. (2018). Cyber Diplomacy Act of 2017. U.S. Congress. Retrieved August 22, 2018, from https://www.congress.gov/115/bills/hr3776/BILLS-115hr3776rs.pdf

Rozman, G. (2014). *The Sino-Russian challenge to the world order: National identities, bilateral relations, and East versus West in the 2010s*. Stanford, CA: Stanford University Press.

Rubio, M. (2012, December 5). A concurrent resolution expressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived. U.S. Congress. Retrieved September 5, 2018, from https://www.congress.gov/112/bills/sconres50/BILLS-112sconres50enr.pdf

Rudenko, G. (2004, March 31). "Kto on takoy, my znaem. On - maroder!" ["Who he is, we know. He is a marauder!"]. *Kommersant*. Retrieved September 7, 2018, from https://www.kommersant.ru/doc/462332

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.

Russell, A. L. (2014). *Open standards and the digital age: History, ideology, and networks*. New York: Cambridge University Press.

Russian Association of Electronic Communication. (n.d.). Ekonomika Runeta [Runet Economics]. Retrieved September 7, 2018, from http://экономикарунета.рф

Russian Federal State Statistics Service. (n.d.-a). BRICS joint statistical publications. Retrieved September 7, 2018, from http://www.gks.ru/free_doc/new_site/m-sotrudn/eng_site/brics.html

Russian Federal State Statistics Service. (n.d.-b). Informatsionnoe obschestvo [Information society]. Retrieved September 7, 2018, from http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innovations/it_technology/

Russian Federation Council. (n.d.). Vremennaya komissiya Soveta Federatsii po zaschite

    gosudarstvennogo suvereniteta i predotvrasheniyu vmeshatel'stva vo vnutrennie

    dela Rossiiskoi Federatsii [Temporary Committee to Protect State Sovereignty and

    Prevent Interference in Russia's Internal Affairs]. Retrieved August 23, 2018, from

    http://council.gov.ru/structure/commissions/iccf_def/

Russian Government. (2014a). Elektronnaya Rossiya, 2002-2010 [Federal Program

    Electronic Russia, 2002-2010]. Russian Ministry of Digital Development,

    Communications and Mass Media. Retrieved from

    http://minsvyaz.ru/ru/activity/programs/6/

Russian Government. (2014b). Gosudarstvennaya programma "Sozdanie v Rossiiskoi

    Federatskii tekhnoparkov v sphere vysokikh tekhnologii" (State program

    Development in the Russian Federation of High Technology Parks). Russian

    Ministry of Digital Development, Communications and Mass Media. Retrieved

    from http://minsvyaz.ru/ru/activity/programs/2/

Russian Government. (n.d.). Pravitel'stvennya komissiya po importozamescheniyu

    [State Commission on Import Substitution]. Retrieved August 23, 2018, from

    http://government.ru/department/314/about

Russian Ministry of Digital Development, Communications and Mass Media. (2014).

    Nikolay Nikiforov vystupil pered uchastnikami mezhdunarodnogo molodezhnogo

    foruma "Tavruda-2014" [Nikolay Nikiforov gave a speech before the international

    youth forum Taurida-2014]. Retrieved August 23, 2018, from

    http://minsvyaz.ru/ru/events/31483

Russian Ministry of Digital Development, Communications and Mass Media. (2015a). Plan importozamesheniya programmnogo obespecheniya [Plan of Software Import Substitution]. Russian Ministry of Digital Development, Communications and Mass Media. Retrieved from minsvyaz.ru/uploaded/files/plan-importozamescheniyaprikaz-96.xls

Russian Ministry of Digital Development, Communications and Mass Media. (2015b, October 22). The First Ever Meeting of BRICS ICT Minister Was Launched [Russian Ministry of Digital Development, Communications and Mass Media]. Retrieved August 28, 2018, from http://minsvyaz.ru/en/events/34185

Russian Ministry of Digital Development, Communications and Mass Media. (2018, June 29). Statistika otrasli [Statistics of the Sector]. Retrieved September 7, 2018, from http://minsvyaz.ru/ru/pages/statistika-otrasli/#section-490

Russian Ministry of Digital Development, Communications and Mass Media, & Russian Federal State Statistics Service. (n.d.). Edinaya mezhvedomstvennaya informatsionnon-statisticheskaya sistema [Integrated Interdepartmental Informational-Statistical System]. Retrieved September 7, 2018, from https://fedstat.ru

Russian Ministry of Foreign Affairs. (2008, March). "Vneshnepoliticheskaya i diplomaticheskaya deyatel'nost' Rossiiskoi Federatsii v 2007 godu." Obzor MID Rossii [Foreign Policy and Diplomatic Activities of the Russian Federation in 2007. A Review by the MFA of Russia]." Retrieved August 28, 2018, from http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/345430

Russian Ministry of Foreign Affairs. (2017, April 14). Kontseptsiya konventsii OON (ili kontseptsiya bezopasnogo funktsionirovaniya i razvitiya seti Internet) [Concept of a UN Convention (or the Concept of secure functioning and development of the Internet]. Russian Ministry of Foreign Affairs. Retrieved August 28, 2018, from http://minsvyaz.ru/uploaded/files/prilozheniekontseptsiikonventsiioon.docx

Russian Ministry of Telecommunications and Mass Media. (2010, May 13). Igor Schegolev: kirrilicheskii domen - shag na puti sokrascheniya tsifrovogo razryva [Igor Schegolev: Cyrillic domain is a step toward narrowing the digital divide]. Retrieved August 24, 2018, from http://minsvyaz.ru/ru/events/25261

Russian Ministry of Telecommunications and Mass Media. (2012). Minkomsvyaz.rf. Itogi 2008-2012 [Ministry of Telecommunications and Mass Media. Overview, 2008-2012]. Retrieved August 24, 2018, from http://minsvyaz.ru/uploaded/files/God_Otch_2012.pdf

Russian Ministry of Telecommunications and Mass Media. (2015, April). Kniga uchastnika Godovoi rasshirennoi kollegii Ministerstva svyazi i massovykh kommunikatsii RF [The Book of a Participant of the Annual Extended Board Meeting of the Ministry of Telecom and Mass Communications of the Russian Federation]. Russian Ministry of Telecom and Mass Communications. Retrieved August 28, 2018, from http://minsvyaz.ru/uploaded/files/mskbooklet2015print1-2.pdf

Russian Prosecutor General's Office. (2015, November 30). General'naya prokuratura Rossiiskoi Federatsii prinyala reshenie o priznanii nezhelatel'noi na territorii Rossiiskoii Federatsii deyatel'nosti dvukh inostrannykh nepravitel'stvennykh

organizatsii [The Prosecutor General's Office of the Russian Federation deems two foreign non-governmental organizations as undesirable in the Russian Federation]. Retrieved September 7, 2018, from http://genproc.gov.ru/smi/news/genproc/news-978768

Rutland, P. (2013). Neoliberalism and the Russian transition. *Review of International Political Economy*, *20*(2), 332–362.

Ruutel, A. (2004, April). *The President of the Republic at the closing ceremony of the training project Look @World*. Presented at the Closing ceremony of the training project Look @World, Tallinn, Estonia. Retrieved August 29, 2018, from https://vp2001-2006.president.ee/en/duties/speeches.php?gid=47702

Ruutu, K. (2017). The concepts of state and society in defining Russia's domestic political unity: A research note. *Europe-Asia Studies*, *69*(8), 1153–1162.

Sakwa, R. (2014). *Putin redux: Power and contradiction in contemporary Russia*. Abingdon, Oxon and New York: Routledge.

Sassen, S. (2000). Digital networks and the state: Some governance questions. *Theory, Culture & Society*, *17*(4), 19–33.

Sassen, S. (2006). *Territory, authority, rights: From Medieval to global assemblages*. Princeton, NJ: Princeton University Press.

Saunders, R. (2016). *Popular geopolitics and nation branding in the post-Soviet realm*. New York: Routledge.

Schegolev, I. (2015, May). *Plenarnoe zasedanie. Tema: Formirovanie bezopasnogo informtsionnogo prostranstva dlya buduschikh pokolenii [Address at the Plenary "Forming secure informational space for future generations"]*. Presented at the VI

Safe Internet Forum, Moscow, Russia. Retrieved from

https://www.youtube.com/watch?v=dxfxWaHdE-A

Schegolev, I. (2017, March 27). Pomoschnik prezidenta - RBK: "Nash internet uyazvim

vneshnemu vozdeistviyu" [Presidential aide to RBC: "Our internet is vulnerable to

the outside influence"]. *RBC*. Retrieved September 13, 2018, from

http://www.rbc.ru/interview/technology_and_media/27/03/2017/58d3bc559a79471

ca8c1fbbd

Schewick, B. van. (2010). *Internet architecture and innovation*. Cambridge, MA: The

MIT Press.

Schmidt, V. (2008). Discursive institutionalism: The explanatory power of ideas and

discourse. *Annual Review of Political Science*, *11*(1), 303–326.

Schmitt, M., & Vihul, L. (2017, June 30). International cyber law politicized: The UN

GGE's failure to advance cyber norms. Retrieved August 24, 2018, from

https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-

failure-advance-cyber-norms

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

Scholte, J. A. (2005). *Globalization: A critical introduction* (2nd Edition). Basingstoke,

Hampshire: Palgrave Macmillan.

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

York: NYU Press.

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive research design: Concepts and

processes*. New York: Routledge.

Sergunin, A., & Karabeshkin, L. (2015). Understanding Russia's soft power strategy. *Politics*, *35*(3–4), 347–363.

Shanghai Cooperation Organization. (2009). Agreement between the governments of the member states of the Shanghai Cooperation Organization on cooperation in the field of international information security. NATO Cooperative Cyber Defence Centre of Excellence. Retrieved August 23, 3028, from https://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

Sharafutdinova, G. (2014). The Pussy Riot affair and Putin's démarche from sovereign democracy to sovereign morality. *Nationalities Papers*, *42*(4), 615–621.

Shen, H. (2016). China and global Internet governance: Toward an alternative analytical framework. *Chinese Journal of Communication*, *9*(3), 304–324.

Shim, Y., & Shin, D.-H. (2016). Neo-techno nationalism: The case of China's handset industry. *Telecommunications Policy*, *40*(2), 197–209.

Siil, I. (2001). *Estonia: Preparing for the Information Age* (ICA Information No. 74: General Issue No. 74). International Council for Information Technology in Government Administration. Retrieved September 13, 2018, from https://slideblast.com/estonia-preparing-for-the-information-age_5950a06f1723dd426aa28cc8.html

Simons, G. (2014). Russian public diplomacy in the 21st century: Structure, means and message. *Public Relations Review*, *40*.

Skey, M. (2011). *National belonging and everyday life: The significance of nationhood in an uncertain world*. Houndmills, Basingstoke, Hampshire: Palgrave Macmillan.

Skey, M., & Antonsich, M. (Eds.). (2017). *Everyday nationhood: Theorising culture, identity and belonging after banal nationalism*. London: Palgrave Macmillan.

Sklair, L. (1999). Competing Conceptions of Globalization. *Journal of World-Systems Research*, *5*(2), 142–163.

Sklair, L. (2002). *Globalization: Capitalism and its alternatives* (3rd edition). Oxford and New York: Oxford University Press.

Smith, G., Vivien, L., Wilson, A., Bohr, A., & Allworth, E. (1998). Nation re-building and political discourses of identity politics in the Baltic states. In *Nation-building in the post-Soviet borderlands: The politics of national identities*. Cambridge, UK: Cambridge University Press.

Soldatov, A. (2015). The taming of the Internet. *Russian Politics & Law*, *53*(5–6), 63–83.

Soldatov, A., & Borogan, I. (2015). *The red web: The struggle between Russia's digital dictators and the new online revolutionaries*. New York: PublicAffairs.

Solum, L., & Chung, M. (2004). The layers principle: Internet architecture and the law. *Notre Dame Law Review*, *79*(3), 815-948.

Soyfer, V. (2015, July 28). Ne nado plevat' v ruku dayuschego [Don't spit into the hand that feeds you]. Retrieved September 7, 2018, from https://trv-science.ru/2015/07/28/ne-nado-plevat-v-ruku-dayushchego

Sputnik News. (2017, May 26). Freedom for export: How Russia sells digital sovereignty to the world. *Sputnik News*. Retrieved August 28, 2018, from https://sputniknews.com/science/201705261054001026-russia-digital-sovereignty-sell

Standage, T. (1998). *Victorian Internet*. New York: Bloomsbury Publishing.

Startup Estonia. (n.d.). Retrieved August 29, 2018, from http://www.startupestonia.ee/en

Statistics Estonia. (2017). Minifacts about Estonia 2017. Statistics Estonia. Retrieved
    August 29, 2018, from https://www.stat.ee/603927

Steen, A. (2010). National elites and the Russian minority issue. Does EU–NATO
    integration matter? *Journal of European Integration*, *32*(2), 193–212.

Steger, M. B. (2009). *The rise of the global imaginary: Political ideologies from the
    French Revolution to the Global War on Terror*. Oxford and New York: Oxford
    University Press.

Steinmetz, G. (Ed.). (1999). *State/Culture: State-formation after the cultural turn*. Ithaca,
    NY: Cornell University Press.

Stent, A. E. (2015). *The limits of partnership: U.S.-Russian relations in the twenty-first
    century*. Princeton, NJ: Princeton University Press.

Stepanova, E. (2015). 'The spiritual and moral foundation of civilization in every nation
    for thousands of years': The traditional values discourse in Russia. *Politics,
    Religion & Ideology*, *16*(2–3), 119–136.

Streeter, T. (2010). *The net effect: Romanticism, capitalism, and the Internet*. New York:
    NYU Press.

Strickling, L. E., Genachowski, J., & Verveer, P. L. (2012, November 30). The necessity
    of an inclusive, transparent and participatory Internet. U.S. Department of
    Commerce, National Telecommunications and Information Administration.
    Retrieved September 5, 2018, from https://www.ntia.doc.gov/blog/2012/necessity-
    inclusive-transparent-and-participatory-internet

Suny, R. G. (Ed.). (2006). *The Cambridge history of Russia: Volume 3, the twentieth century*. Cambridge: Cambridge University Press.

Suttmeier, R., & Yao, X. (2004). *China's post-WTO technology policy: Standards, software, and the changing nature of techno-nationalism*. Seattle, WA: The National Bureau of Asian Research.

Swidler, A. (1986). Culture in action: Symbols and strategies. *American Sociological Review*, *51*(2), 273–286.

Szulc, L. (2017). Banal nationalism in the Internet age: Rethinking the relationship between nations, nationalisms and the media. In M. Skey & M. Antonsich (Eds.), *Everyday nationhood: theorising culture, identity and belonging after banal nationalism*. London: Palgrave Macmillan.

Tamm, M. (2013). In search of lost time: Memory politics in Estonia, 1991–2011. *Nationalities Papers*, *41*(4), 651–674.

Taneja, H., & Webster, J. (2016). How do global audiences take shape? The role of institutions and culture in patterns of web use. *Journal of Communication*, *66*(1), 161–182.

Taras, R. (Ed.). (2014). *Russia's identity in international relations: Images, perceptions, misperceptions*. London: Routledge.

Taylor, B. D. (2011). *State building in Putin's Russia: Policing and coercion after communism*. Cambridge and New York: Cambridge University Press.

Taylor, C. (2004). *Modern social imaginaries*. Durham, NC: Duke University Press.

Taylor, H. (2016, April 28). If social networks were countries, which would they be? Retrieved September 4, 2018, from

https://www.weforum.org/agenda/2016/04/facebook-is-bigger-than-the-worlds-largest-country

Taylor, P. M. (2003). *Munitions of the mind: A history of propaganda* (3rd Edition). Manchester, UK: Manchester University Press.

Thussu, D. K. (2015). Digital BRICS: Building a NWICO 2.0? In K. Nordenstreng & D. K. Thussu (Eds.), *Mapping BRICS media* (pp. 242–263). Abingdon, Oxon and New York: Routledge.

Tõhk, T. (2016a, March 22). Prime Minister Rõivas met with the Speaker of the U.S. House of Representatives. Retrieved August 28, 2018, from https://www.valitsus.ee/en/news/prime-minister-roivas-met-speaker-us-house-representatives

Tõhk, T. (2016b, March 25). Prime Minister Rõivas in the U.S. military base: You are strengthening Estonia's security. Retrieved August 28, 2018, from https://www.valitsus.ee/en/news/prime-minister-roivas-us-military-base-you-are-strengthening-estonias-security

Tolz, V. (2001). *Russia (Inventing the nation)*. London: Bloomsbury Academic.

Trading Economics. (n.d.). Russia GDP, 1989-2018. Retrieved August 23, 2018, from https://tradingeconomics.com/russia/gdp

Trump, D. (2017). National security strategy of the United States of America: The White House. Retrieved August 22, 2018, from https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Tsang, R., & Woods, E. T. (Eds.). (2013). *The cultural politics of nationalism and nation-building: Ritual and performance in the forging of nations*. London and New York: Routledge.

Tsygankov, A. P. (2014). *The strong state in Russia: Development and crisis*. Oxford and New York: Oxford University Press.

Tsygankov, A. P. (2016). *Russia's foreign policy: Change and continuity in national identity* (4th Edition). Lanham, MD: Rowman & Littlefield.

Turner, F. (2006). *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. Chicago: University of Chicago Press.

Turner, F. (2017). Can we write a cultural history of the Internet? If so, how? *Internet Histories*, *1*(1–2), 39–46.

Tusikov, N. (2016). *Chokepoints: Global private regulation on the Internet*. Oakland, CA: University of California Press.

Twomey, P. (2007). *ICANN and Russia*. Presented at the International Economic Forum, St Petersburg, Russia. Retrieved August 24, 2018, from https://www.icann.org/en/system/files/files/d3-ief-russia-10jun07-en.pdf

UNESCO. (2009). *National information society policy: A template* (Information for All Programme). Paris: UNESCO. Retrieved August 21, 2018, from http://unesdoc.unesco.org/images/0018/001871/187135e.pdf

UNESCO, & UN University. (2016). *Knowledge societies policy handbook*. Guimarães, Portugal: UNESCO. Retrieved August 21, 2018, from https://en.unesco.org/sites/default/files/knowledge_socities_policy_handbook.pdf

United Nations General Assembly. (1999, January 4). Developments in the field of

    information and telecommunications in the context of international security. United

    Nations Office for Disarmament Affairs. Retrieved August 28, 2018, from

    http://undocs.org/A/RES/53/70

United Nations General Assembly. (2017). Developments in the field of information and

    telecommunications in the context of international security. United Nations Office

    for Disarmament Affairs. Retrieved August 28, 2018, from

    http://undocs.org/A/72/315

United Nations Office for Disarmament Affairs. (n.d.). Developments in the field of

    information and telecommunications in the context of international security.

    Retrieved August 28, 2018, from

    https://www.un.org/disarmament/topics/informationsecurity

University of Oxford, Department of Politics & International Relations. (n.d.). Cyber

    Studies Programme - About Us. Retrieved August 29, 2018, from

    https://www.politics.ox.ac.uk/cyber-studies-programme/cyber-studies-programme-

    mission.html?cenid=380

Urry, J. (1995). *Consuming places*. London and New York: Routledge.

Urry, J. (2000). *Sociology beyond societies: Mobilities for the twenty-first century*.

    London and New York: Routledge.

U.S. Agency for Global Media. (n.d.). Office of Internet Freedom. Retrieved August 22,

    2018, from https://www.usagm.gov/worldwide-operations/office-internet-freedom

U.S. Department of Commerce, National Telecommunications and Information

    Administration. (1998a, February 20). Improvement of Technical Management of

Internet Names and Addresses; Proposed Rule. U.S. Department of Commerce,

National Telecommunications and Information Administration. Retrieved

September 4, 2018, from https://www.ntia.doc.gov/federal-register-

notice/1998/improvement-technical-management-internet-names-and-addresses-

proposed-

U.S. Department of Commerce, National Telecommunications and Information

Administration. (1998b, June 5). Management of Internet Names and Addresses.

U.S. Department of Commerce, National Telecommunications and Information

Administration. Retrieved September 4, 2018, from

https://www.ntia.doc.gov/federal-register-notice/1998/statement-policy-

management-internet-names-and-addresses

U.S. Department of State. (2018). United States and France strengthen relationship on

cyber policy. Retrieved August 23, 2018, from

http://www.state.gov/r/pa/prs/ps/2018/02/278181.htm

U.S. Department of State. (n.d.). Internet Freedom. Retrieved August 22, 2018, from

https://www.state.gov/j/drl/internetfreedom/index.htm

U.S. Embassy & Consulates in France. (2016, September 15). Cyber Bilateral Meeting in

Paris, France on September 8-9, 2016. Retrieved August 23, 2018, from

https://fr.usembassy.gov/governments-united-states-france-held-cyber-bilateral-

meeting-paris-france-september-8-9-2016

Van Gelder, S. (2012, December 14). Is WCIT failure the start of a digital Cold War?

Retrieved September 4, 2018, from

http://www.circleid.com/posts/20121214_is_wcit_failure_the_start_of_a_digital_co ld_war/

Vartanova, E. (2012). The Russian media model in the context of post-Soviet dynamics. In D. Hallin & P. Mancini (Eds.), *Comparing media systems beyond the Western world*. New York: Cambridge University Press.

Vartanova, E. (2016). Russia. In E. Noam (Ed.), *Who owns the world's media?: Media concentration and ownership around the world*. New York: Oxford University Press.

Vassil, K. (2015). *Estonian e-Government ecosystem: Foundation, applications, outcomes* (Background paper). Washington, D.C.: World Bank. Retrieved August 29, 2018, from http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf

Vetik, R. (Ed.). (2012). *Nation-building in the context of post-communist transformation and globalization: The case of Estonia*. Frankfurt am Main: Peter Lang.

Vey, J.-B., & Kelly, J. (2017, June 16). Macron says France must be country that 'thinks and moves like a startup.' *Reuters*. Retrieved August 22, 2018, from https://www.reuters.com/article/us-france-tech-macron/macron-says-france-must-be-country-that-thinks-and-moves-like-a-startup-idUSKBN1962L3

Vihalemm, T., & Kalmus, V. (2009). Cultural differentiation of the Russian minority. *Journal of Baltic Studies*, *40*(1), 95–119.

Volcic, Z., & Andrejevic, M. (Eds.). (2016). *Commercial nationalism: Selling the nation and nationalizing the sell*. London: Palgrave Macmillan.

Volkmer, I. (1997). Universalism and particularism: The problem of cultural sovereignty and global information flow. In B. Kahin & C. Nesson (Eds.), *Borders in cyberspace: Information policy and the global information infrastructure*. Cambridge, MA: The MIT Press.

Weedon, C. (1987). *Feminist practice and poststructuralist theory*. Oxford, UK: Blackwell Publishers.

Wegren, S. K. (Ed.). (2015). *Putin's Russia: Past imperfect, future uncertain* (6th edition). Lanham, MD: Rowman & Littlefield Publishers.

Weinstein, L. (2012, December 14). Beware a sleeping Godzilla: The UN's Internet treaty fiasco. *Wired*. Retrieved September 4, 2018, from https://www.wired.com/2012/12/godzilla-itu

Weldes, J. (1999). *Constructing national interests: The United States and the Cuban missile crisis*. Minneapolis, MN: University of Minnesota Press.

Wendt, A. (1999). *Social theory of international politics*. Cambridge, UK: Cambridge University Press.

Wenzlhuemer, D. R. (2013). *Connecting the nineteenth-century world: The telegraph and globalization*. Cambridge and New York: Cambridge University Press.

Wilson, A. (2009). Computer gap: The Soviet Union's missed revolution and its implications for Russian technology policy. *Problems of Post-Communism*, *56*(4), 41–51.

Wilson, E. J. (2005). What is Internet governance and where does it come from? *Journal of Public Policy*, *25*(1), 29–50.

Wilson, J. L. (2015). Soft power: A comparison of discourse and practice in Russia and China. *Europe-Asia Studies*, *67*(8), 1171–1202.

Wilson, K. (2015). Modernization or more of the same in Russia: Was there a "Thaw" under Medvedev? *Problems of Post-Communism*, *62*(3), 145–158.

Wilson, M. R. (2017, September 12). Russian network RT must register as foreign agent in US. *The Hill*. Retrieved August, 24, 2018, from http://thehill.com/business-a-lobbying/business-a-lobbying/350226-russian-network-rt-must-register-as-foreign-agent-in

Wimmer, A., & Glick Schiller, N. (2002). Methodological nationalism and beyond: Nation–state building, migration and the social sciences. *Global Networks*, *2*(4), 301–334.

Winseck, D. (2012, June 19). The ITU and the real threats to the Internet, Part IV: the Triumph of state security and proposed changes to the ITRs. Retrieved September 5, 2018, from https://dwmw.wordpress.com/2012/06/19/the-itu-and-the-real-threats-to-the-internet-part-iv-the-triumph-of-state-security-and-proposed-changes-to-the-itrs

Winseck, D. (2017). The geopolitical economy of the global Internet infrastructure. *Journal of Information Policy*, *7*, 228–267.

Winseck, D. R., & Pike, R. M. (2007). *Communication and empire: Media, markets, and globalization, 1860–1930*. Durham, NC: Duke University Press.

World Bank. (1993). *Estonia: The transition to a market economy* (A World Bank Country Study). Washington, D.C. Retrieved August 29, 2018, from

http://documents.worldbank.org/curated/en/715701468771070270/pdf/multi0page.p
df

World Economic Forum. (2002). *The global information technology report 2001-2002:
Readiness for the networked world*. New York: Oxford University Press. Retrieved
August 29, 2018, from

http://unpan1.un.org/intradoc/groups/public/documents/un/report.pdf

World Economic Forum. (2016). *Europe's hidden entrepreneurs: Entrepreneurial
employee activity and competitiveness in Europe*. Geneva, Switzerland: World
Economic Forum. Retrieved August 29, 2018, from

http://www3.weforum.org/docs/WEF_Entrepreneurship_in_Europe.pdf

Wu, T. S. (1997). Cyberspace sovereignty? – The Internet and the international system.
Harvard Journal of Law & Technology, *10*(3), 647-666.

Wu, X. (2007). *Chinese cyber nationalism: Evolution, characteristics, and implications*.
Lanham, MD: Lexington Books.

Wulf, M. (2016). *Shadowlands: Memory and history in post-Soviet Estonia.* Oxford:
Berghahn Books.

Xi, J. (2015, December). *Remarks by H.E. Xi Jinping President of the People's Republic
of China at the Opening Ceremony of the Second World Internet Conference*.
Presented at the Second World Internet Conference, Wuzhen, China. Retrieved
August 23, 2018, from

http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

Yablokov, I. (2015). Conspiracy theories as a Russian public diplomacy tool: The case
of Russia Today (RT). *Politics*, *35*(3–4), 301–315.

Yang, G. (2014). The return of ideology and the future of Chinese Internet policy. *Critical Studies in Media Communication*, *31*(2), 109–113.

Yeltsin, B. (1996). Kontseptsiya natsional'noi politiki [Concept of the state nationalities policy]. President of Russia. Retrieved August, 23, 2018, from http://kremlin.ru/acts/bank/9571

Yeltsin, B. (2005). Foreign policy conception of the Russian Federation (1993). In A. Melville & T. Shakleina (Eds.), *Russian foreign policy in transition: Concepts and realities*. Budapest: Central European University Press.

Zeng, J. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "Internet sovereignty." *Politics & Policy*, *45*(3), 432–464.

Zevelev, I. (2016). *Russian national identity and foreign policy*. Washington, DC: Center for Strategic & International Studies. Retrieved September 13, 2018, from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/161208_Zevelev_RussianNationalIdentity_Web.pdf

Zhegulev, I. (2015, December 25). Prodazha aktyvnykh [Selling of the active ones]. *Meduza*. Retrieved August 23, 2018, from https://meduza.io/feature/2015/12/25/prodazha-aktivnyh

Ziegler, C. E. (2012). Conceptualizing sovereignty in Russian foreign policy: Realist and constructivist perspectives. *International Politics*, *49*(4), 400–417.

Ziewitz, M., & Pentzold, C. (2014). In search of internet governance: Performing order in digitally networked environments. *New Media & Society*, *16*(2), 306–322.

Zimmerman, W. (2014). *Ruling Russia: Authoritarianism from the Revolution to Putin*. Princeton, NJ: Princeton University Press.

Zubrzycki, G. (Ed.). (2017). *National matters: Materiality, culture, and nationalism*.

    Stanford, CA: Stanford University Press.

Zuckerman, E. (2014). *Digital cosmopolitans: Why we think the Internet connects us,*

    why it doesn't, and how to rewire it. New York: W. W. Norton & Company.