Book Review

Review of Biagioli, Mario, and Vincent Antonin Lépinay (eds.). 2019. *From Russia with Code: Programming Migrations in Post-Soviet Times*. Durham, NC: Duke University Press.
384 pp. US\$ 28.95. Paper. ISBN: 9781478002994.

Alexandra V. Orlova

Ryerson University, Canada
aorlova@ryerson.ca

The recent focus on Russian cybercriminality and hacking, especially in light of the alleged 2016 meddling by the Russian state in the US elections, has highlighted the need for a deeper understanding of the Russian information technology (IT) sector. Currently, many Western nations discuss the “Russian hacker threat” as a challenge to their democratic process and institutions, and ultimately to their sovereignty. *From Russia with Code: Programming Migrations in Post-Soviet Times*, edited by Mario Biagioli and Vincent Antonin Lépinay, is both timely and unique as it provides an insight into the activities, identities, and migration experiences of Russian IT specialists both in Russia and abroad. This collection of essays examines factors that shape Russian IT specialists as professionals and how they in turn shape the world around them. Biagioli and Lépinay’s volume is an exceptional collaborative effort by a team of Russian, American, French, and Dutch academics who conducted over 300 in-depth interviews from 2013 to 2015 with Russian IT specialists both in Russia and abroad (Biagioli and Lépinay 2019: 6) to provide the reader with detailed insight into their “daily practices.”

The volume looks at the heterogeneous population of Russian IT specialists both in Russia and abroad. It deals with their experiences as well as fundamental questions of identity and how their identities have been shaped by their education, their political, historical, economic, and social circumstances, and their migration decisions. Biagioli and Lépinay note that they “were confronted with the heterogeneity and fluidity of [their] subjects prior to their diasporas” (4). *From Russia with Code* does not constitute a study of a diasporic population and its relationship with the home country. While various chapters do indeed examine the movement of Russian IT specialists, the focus is rather on the technological uniqueness of this population and how their coding skills and practices frame “both migration options” and the IT specialists’ sense of “being Russian,” which at times conflicts with their professional identity (8). In truth, the volume’s central concern is identity and its relationship with the concept of sovereignty. Biagioli and Lépinay state that “the remarkable mobility of IT specialists, especially highly skilled individuals such as those who have traditionally been produced by the Soviet and then Russian pedagogical system, is a particularly thorny issue for [Russia] because it turns pedagogical strength into an economic and possibly even political threat” (5).

While the identity of Russian IT specialists has been shaped and continues to be reshaped by a multitude of factors, the identities of others outside of Russia have also been altered by the so-called “Russian IT threat.” Estonia’s digital identity emerged in large part due to a series of cyberattacks that the Estonian

government attributed to Russia (214). For Estonia to set itself apart from Russia and overcome its communist past, the creation of a new digital identity was paramount (221). Biagioli and Lépinay's volume focuses not only on physical migration but also examines the migration and transformation of ideas, both within and outside Russia, due to the creation of transnational IT communities. Code itself can become an instrument of diplomacy and has the potential to challenge dominant geopolitical and power relations (92). Hence, code and coder become key players in relation to state sovereignty and surveillance. Code serves to create groups and communal identities; for example, the chapter examining the case of Russia's most successful search engine, Yandex, notes that "routine engagement with code serves to transform a diversified body of newcomers with different educational backgrounds into a coherent body of IT professionals while simultaneously creating a unified community" (60).

It was a hope of the Russian state that the focus on innovation and the growth of the IT sector would gradually limit Russia's dependence on oil and gas. The chapter dealing with Skolkovo technopark notes that while Silicon Valley in the United States emerged due to many local factors as well as collaboration between private and public initiatives, the Russian supposed equivalent was entirely designed by the state (180) and hence possesses many top-down features that result in a fundamental disconnect between its administration and residents (188). The Skolkovo project, as well as IT infrastructure investments outside of Russia's capital, such as in Kazan (162) or Vladivostok (138), demonstrate that the Russian state had its own particular vision of IT development. It was aiming not simply to imitate the West, but rather to "Russianize" innovation in order to keep it within state control, especially as levels of internet penetration grew increasingly high (237). The state was also aiming to control the peripheral regions of the country through regional IT projects (162). In the process of asserting central control over the periphery, authoritarian policy decisions tend to disregard the regional context and "end up disrupting the local IT ecology" (138). However, Russian IT specialists do not necessarily trust the state to control innovation and frequently reference their unique position and developed collaborative relations as something that is absent from top-down state-controlled projects (21, 23, 25). Ultimately, IT specialists, whether in Russia or abroad, can be perceived by the state as a threat to state sovereignty, although many IT specialists do not critique politics but focus instead on economics (353). When the state fails to respond to political, social, and economic challenges, the online community often steps in (97), challenging state sovereignty in the process and creating new forms of citizen political participation. The chapter on civic hackers in contemporary Russia describes the creation of civic apps to respond in a bottom-up way to political, social, and economic challenges "with the help of volunteer coders and crowdsourcing technologies" (87). While civic hackers operate within the law, they demand absolute transparency. They refuse to engage in traditional forms of political participation, such as demonstrations and protests, instead choosing to do politics differently and with different tools. By using "assemblages of programming code and law [they] have the potential to fight political apathy and improve the everyday lives of Russian citizens" without the help of top-down governmental institutions (88). Each individual civic app can be conceptualized as adding to the political action toolkit, which in the long run "helps in creating a sustained sense of social justice, where regular acts of state violence are slowly being transformed into well-articulated political demands that resonate across divergent constituencies" (Orlova 2018: 188). Coding becomes a way to participate on a local scale in processes of social and political change (Biagioli and Lépinay 2019: 95). However, the processes of multiplication and reiteration transform individual problems in a more global context, resulting in the emergence of multiple collaborative relationships (103). In the process, the very notion of local and global gets redefined. This type of "apptivism" (105) contributes to the transformation of the concept of sovereignty. The 2014 Russian annexation of Crimea and the war in Eastern Ukraine, as well as the allegations of Russian computer hacking and meddling in the 2016 US presidential race, have highlighted and heightened normative differences between Russia and the West (Lipman 2015). Hence, Russian legislative and judicial bodies increasingly discuss the idea of "local norms," "traditional values," and "local constitutional identities" as a way of reasserting domestic sovereignty (Orlova 2018b: 442). Not only has the Russian state continued to cling to the idea of state sovereignty as the "cornerstone of the international system" (Laughland 2007: 6), it also expanded the concept of sovereignty to include such things as morality and information. As with the traditional concept of state sovereignty, which grants the state the ultimate right and power to regulate its internal affairs without foreign interference, concepts of

“moral sovereignty” and “information sovereignty” are used to describe the supposed right claimed by the Russian state to make decisions, without foreign interference, about matters that concern morality and information within Russia (Orlova 2018b: 443). Hence, sovereignty is no longer just about physical space, but can be viewed as an expanding social contract between the state, its citizens, and the international community, with IT professionals potentially playing key roles in either maintaining or disrupting this social contract. The Russian government’s efforts to deliberately establish and maintain “information sovereignty” by purging dissenting viewpoints from the mainstream is considered a major security challenge (Skillen 2016: 326, 333). Loss of “information sovereignty” is perceived to be dangerous; hence governmental control over most information channels is presented as socially useful for Russian society (Rossoshanskii 2018: 23). Thus, controlling information flows is perceived as key to ensuring security and political sovereignty (24). IT specialists’ ability to challenge government monopoly on information is viewed as especially threatening due to their potential mobility and independence from physical location within Russia as well as their connections with various local and global communities (Biagioli and Lépinay 2019: 24).

Biagioli and Lépinay make it clear that Russian IT identity is in a state of flux. While the drive to innovate is strong among Russian IT professionals and their high levels of education make them highly skilled, their lack of business and marketing skills (203) challenges their migration success (340). Migration decisions are frequently justified in retrospect by referencing values and lifestyles. For example, Russian IT specialists working in Finland (351) or Russian Jewish IT professionals in Boston (361) cite the importance of a balanced work environment and control over their time as key factors to justify their migration decisions.

Overall, Biagioli and Lépinay’s volume offers the reader a glimmer of hope for IT professionals’ ability to change Russian domestic politics, especially as Russian IT professionals abroad experience a “re-identification through professional motives”; that is a proactive renewal of a sense of national belonging and reconnection to the home country through participation in professional networks” (273). Biagioli and Lépinay’s volume demonstrates that IT professionals both in Russia and abroad have the potential to disrupt the Russian state’s current conception of sovereignty, including information sovereignty, and to redefine the relationship between the state, its citizens, and the international community. Biagioli and Lépinay state that Russian IT professionals are “the vectors of information in the Russian Federation not only because they work on information technologies but because they are the sector of the population that is most exposed to the information disseminated by those technologies, much of it coming from outside the Russian Federation” (15). Hence, Russian IT professionals could become vectors of change and transformation.

References

- Biagioli, Mari, and Vincent Antonin Lépinay, eds. 2019. *From Russia with Code: Programming Migrations in Post-Soviet Times*. Durham, NC: Duke University Press.
- Laughland, John. 2007. The Crooked Timber of Reality: Sovereignty, Jurisdiction, and the Confusion of Human Rights. *The Monist* 90 (1): 3–25.
- Lipman, Maria. 2015. How Russia has Come to Loathe the West. *European Council on Foreign Relations*, March 13. https://www.ecfr.eu/article/commentary_how_russia_has_come_to_loathe_the_west311346 [accessed August 7, 2019].
- Orlova, Alexandra V. 2018a. Challenging Everyday Violence of the State: Developing Sustained Opposition Movements through Anti-Corruption Protests. *Research in Social Movements, Conflicts and Change* 42: 173–196.
- Orlova, Alexandra V. 2018b. Sovereignty, Dissent, and the Shaping of International Consensus around Human Rights: An Examination of Russian “Disengagement” from the European Court of Human Rights. *Arizona Journal of International and Comparative Law* 35 (3): 435–468.
- Rossoshanskii, A.V. 2012. Infortatsionnyi Suverenitet I Svoboda Slova v Kontekste Politicheskoi Modernizatsii v Sovremennoi Rossii. *Izvestiya Irkutskogo Gosudarstvennogo Universiteta* 1 (8): 19–26 [in Russian].
- Skillen, Daphne. 2016. *Freedom of Speech in Russia: Politics and Media from Gorbachev to Putin*. London: Routledge.