Free and open source software in the new digital public policies in Russia

Marie-Gabrielle Bertran

Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Free and open source software in the new digital public policies in Russia

Marie-Gabrielle Bertran

To cite this article: Marie-Gabrielle Bertran (2021) Free and open source software in the new digital public policies in Russia, Journal of Cyber Policy, 6:1, 81-95, DOI: 10.1080/23738871.2021.1942110

To link to this article: https://doi.org/10.1080/23738871.2021.1942110

Published online: 19 Jun 2021.

JOURNAL OF CYBER POLICY
2021, VOL. 6, NO. 1, 81–95
https://doi.org/10.1080/23738871.2021.1942110

Routledge
Taylor & Francis Group

Free and open source software in the new digital public policies in Russia

Marie-Gabrielle Bertran

Lab Geopolitics of the Datasphere (GEODE), Center for Geopolitical Research and Analyses (CRAG – IFGLab), University Paris 8, EA 353, Saint-Denis, France

ABSTRACT

During Dmitrij Medvedev's presidency from 2008 to 2012, the Russian government chose to promote the development of a new digital economy, with the idea that it would become a competitive sector and a tool for the external power of the country on the international market. However, in 2013, Edward Snowden's revelations were used by the Russian government to promote the development of a strong and diversified digital industry on the domestic market, as it presumably became necessary to ensure the digital sovereignty of a country dependent on foreign actors especially American public authorities and digital companies. This new strategy brought the Russian authorities to examine new kinds of development and new standards for the domestic digital market, especially regarding its regulatory framework, in order to ensure the technological independence of the country as soon as possible (before 2020, according to the 'State Program for an information society 2010–2020'; and then, before 2030, after the adoption of the 'State Program for an information society 2017–2030'). In this regard, free and open-source software appeared as a practical solution, since open (i.e. publicly readable) code ensures low exploitation costs and the possibility of controlling its functions.

ARTICLE HISTORY
Received 26 February 2021
Revised 22 March 2021
Accepted 21 April 2021

KEYWORDS
Russia; sovereign technologies; free software; open source software; digital public policies

Introduction

In Russia, as in many countries, the authorities sought to capitalise on the economic interests of digital technology before considering the risks posed by this new technology. Dmitrij Medvedev's presidency (2008–2012) represented a decisive moment for the development of a digital economy in Russia. During his presidency, the interest of the Russian government for the digital sector had translated into new legislations and public policies, which intended to favour Russia's economic influence on the international market (which was still largely dominated by the United States).

Yet, *digital sovereignty* publicly became a major issue for the Russian authorities after Edward Snowden's revelations in 2013, though the Russian security agencies were probably well aware of the possible existence of hidden backdoors in software and hardware components, or of deliberately concealed zero-day exploits in propriety software. They were also probably aware of the fact that the continuity of supply for a digital product

could be threatened or impaired by a company or a state withholding patches and upgrades.

In 2000, the National Security Concept produced by the Russian Ministry of Foreign Affairs already explained that '[t]here [is] an increasing threat to [Russia's] national security in the information sphere', due to the work 'of [certain] countries to dominate the global information space and oust Russia from the external and internal information market[.]' According to the Ministry, this 'serious danger', was further heightened by 'the elaborations […] of a concept of information wars [by a number of states] that envisages [the] creation of means of dangerous influence on the information spheres of other countries […]; disruption of the normal functioning of information and telecommunication systems and of storage reliability for information resources; and gaining of unsanctioned access to them'. See the whole definition of the concept in the official text (Ministry of Foreign Affairs of the Russian Federation 2000).

However, the public disclosure of the massive surveillance conducted by the intelligence agencies of the Five Eyes (United States, United Kingdom, Canada, Australia and New Zealand) over the internet provided the Russian authorities and policymakers with an opportunity to focus on – and to communicate openly about – the strategic aspects of security in digital networks.

Taking advantage of this opportunity, the Russian authorities thus abandoned their quasi laissez-faire approach towards software development in Russia, in order to articulate the digital independence and technical self-reliance of the country. They also wanted to acquire a certain autonomy in the management of the digital data produced by Russian citizens on the internet. In this new policy landscape, free and open source software had a prominent place, which is best illustrated by the measures adopted after 2010 to promote their use by the public institutions in Russia.

Free and *open source* are two modes of software development built on two principles: users' freedom (they must be able to use a computer programme without significant restrictions), and the public accessibility of the source code of computer programmes, which must be available online to any user (hence the name 'open source code' or *open source*). Two movements grew out of these development processes during the late 1970s and early 1980s. They emerged when computing development and programming exceeded the scope of the military and scientific sectors to reach the wider economy (Perens 1999). This evolution led to the commercialisation of the first operating system[1] and of diverse software solutions later on (Logé 1991, 96–97).[2] Originally, the Free and Open Source (FOSS) movements resisted the commercialisation of proprietary and non-accessible computer programmes, and became alternative and dissident schools in the largely for-profit digital development market. They forcefully opposed any form of control by private entities or state institutions. However, after 2010, Russian public and private actors advocated for the sale of free and open source software on the national market, in order to ease the control of their functioning and – by extension – of their very users. This position seemed then to go against the principles which were deemed to preside over their development.

For that reason, we can ask ourselves how free and open source software has come to be included among the prerogatives and interests of the Russian state. Does this recent interest of the Russian government in free and open source solutions correspond to the implementation of an alternative model to the economic and/or geopolitical domination

of multinational digital companies, or of the United States? Or is it merely a means of political and/or economic exploitation of these issues?

First, we will see how and to what ends Russian public policies have favoured the rapid emergence of a software production industry through the use of free and open source software. We will then analyse how, following Edward Snowden's revelations and a convergence of public and private interests, these policies have undergone a security turn and now fall within a self-described strategy of digital sovereignty. Finally, we will question the consequences of this convergence of interests, which has led to an externalisation of public computer capabilities warranted by the need to opt for free and open source solutions developed by private actors. Do these logics really ensure the security of these infrastructures, as the different actors argue? And are they not leading to a misappropriation of free and open source solutions, which could eventually cancel out their technical advantages?

The development of free and open source software in Russia: toward a new Russian digital industry

2010: first phase of the development of free and open source software in Russia

A first state strategy to create a new digital industry in Russia emerged around 2010, during Dmitrij Medvedev's presidency. These efforts were illustrated by the construction of the 'technological city' (technopolis or technology park) of Skolkovo, based on the historical precedents of the science city (*naukograd*) of Akademgorodok, or of the Lomonosov State University (MGU) research campus for high tech. The Skolkovo project was officially launched on 28 September 2010, with the inauguration of the Skolkovo Foundation. As Limonier (2012, 193) explains, it was meant to spearhead the development of a strong IT industry in Russia. Its main objective was to create a new ecosystem of innovative companies and start-ups in the digital field.

However, the project came up against differences of opinion between its proponents, who considered the technological city to be attractive to start-ups and new digital companies, and its detractors, who remained sceptical about the efficiency of a project which had been created from scratch by the state, and had little or no support from the historical players and networks in the field (especially universities and research centres).

Above all, at the beginning of Vladimir Putin's third term as President of the Russian Federation in 2012, the project was slowed down, even shelved. Investments were strongly reduced, as they didn't have the same significance for Putin.[3] The project also suffered from suspicions of corruption against members of its board of directors.[4] But the attempts of the Medvedev presidency to revitalise technological creation in Russia after the stagnation of the 1990s (especially in the digital field) were also marked by the adoption of an executive decree which explicitly endorsed the creation of Russian operating systems for economic reasons in order to stimulate the domestic market and the digital economy in the country.

The implementation of decree 2299-r by the Ministry of Digital Development, Networks and Mass Communications of the Russian Federation (2010), published on 17 October 2010, registered the official launch of a transition plan for the use of free and open source software by federal institutions. The decree thus encouraged the creation and commercialisation of these kinds of solutions in Russia.

The convergence of public and private interests in the development of free and open source software in Russia: for rapid and low-cost production

The decision to opt for free and open source software was not anodyne. The code of operating systems and software applications of this type has the particularity of being freely available online. Some free and open source licences also allow to use this code for free and to modify it, that is, to employ it as a set of ready-to-use bricks to build new applications. This possibility therefore implies a significant reduction in research and development (R&D), design and production time and costs for companies. Moreover, free and open source licences allow companies to benefit from source codes which have already been tested by a community of developers – who often continue to update and correct them – and the usefulness of which has already been established. In practical terms, the use of free and open source software allowed developers to limit considerably the risks for their investments, knowing that the funding invested in unproven projects can be fatal for SMEs[5] and start-ups; especially if the produced software does not find an audience. The focus of the federal government on free and open source software was thus probably meant to support the rapid development of a Russian software industry. Private representatives have thus begun to play a major role in the development of the domestic digital market, which led to a proportional reduction of dependence on software and software licences imported from abroad, which have long been expensive for Russian buyers (for the public institutions in particular).

The prohibitive cost of foreign licenses in Russia has strongly encouraged this policy of empowerment.[6] The falsification of Microsoft Windows licences was a particularly widespread practice in Russia in the 1990s and the 2000s, to the point that it almost led to the rejection of the country's membership to the World Trade Organization (WTO) in the early 2000s.[7] In 2001, Russian schools still mostly used highjacked versions of Windows, which fuelled the reluctance of several members of the WTO to accept the Russian candidacy. Some of them opposed it outright.[8] In order to join the WTO, the Russian authorities decided to launch the development of a new operating system to replace Windows on computers used by public institutions (including schools). To ensure the rapid replacement of existing systems, and to keep the costs down, this operating system was built on an open source code from the Linux family.[9] Following this mission statement eventually led to the creation of the ALT Linux distribution,[10] one of the most widely used open source distributions in Russia today. The successful launch of ALT Linux set a precedent. In 2009, the Russian government decided to launch an open source operating system for the defence sector, ASTRA Linux. The design and maintenance of this distribution was assured by a company specially created for the purpose: RusBITech-ASTRA, a subsidiary of RusBITech, the activities of which are closely linked to strategic areas of the Russian government. In fact, RusBITech offers solutions which are specifically designed for the Russian Ministry of Defence. Since 2011, it has been an official partner of the Linux Foundation (see the partnership announcement by The Linux Foundation [2011]), a status which provides the company with international visibility in the field of open source products.

RusBITech is a perfect example of the convergence between public and private interests in the production of open source software, as it benefited from the opening of a

market for public procurements within the domestic market, but also gained visibility on the international digital market with the creation of the ASTRA software.

So, all in all, the Russian government's legislative and regulatory investment in FOSS software development has been a major policy choice. Not only did it encourage the different Russian IT development actors to invest in the creation of new software, it also opened a new domestic market for the production of software for public institutions.

According to Alexei Smirnov, the managing director of ALT Linux,[11] it also boosted the influence of Russian actors both abroad and on the international stage of open source development. Hence, Smirnov believes that the more Russia invests in open source solutions, the more influential it is in the field.[12]

The replacement of foreign proprietary software by FOSS software in Russia: a Russification of the domestic digital industry

Following the adoption and implementation of the federal decree 2299-r, the Russian authorities discarded altogether the use of software solutions created by US-based companies on public infrastructures. A Russian solution was therefore chosen to replace the Cisco solution used for the video-surveillance management system of the city of Moscow. In the same way, both Microsoft Exchange Server and Outlook e-mail services were removed from the digital infrastructure and the 6,000 computer workstations of the city, and replaced with software produced by the company Rostelecom.

The government intended to eventually apply similar changes to about 600,000 computers and servers across the country. The Russian public services also planned to stop 'buying products made by foreign companies when equivalent solutions developed by Russian companies [were] available'. This was a sign of the direct link between the adoption of laws on the use of free and open source software and the government's desire to promote the use of software developed in Russia. We also learn from the clauses of the decree, that this goal was far from being totally implemented, as 'the authorities [then spent] approximately 300 million dollars for the acquisition of foreign products'.

To better control and monitor the software used in public institutions, the federal law 764677-6 (State Duma 2015) on 'technologies and the protection of information' and on the 'contractual system in the attribution of public markets for goods and services', adopted on 29 June 2015, directed the creation of a register of domestic software (the *Unified Register of Russian Programs for Computers and Databases*, see https://reestr.minsvyaz.ru/reestr/).

Since it came into force on 1 January 2016, companies, the solutions of which belong to this register, are the only vendors allowed to take part in public contracts for the supply of goods or services in the field of IT. The use of foreign software by federal authorities has consequently been banned outright when domestic alternatives exist (the law does, however, allow a public entity to use foreign software when necessary, if it is open source).

This law was actually envisioned by the *MinSvjaz'* (Ministry of Networks and Mass Communications) as a 'program to replace imported products' (*importozameshenie*, 'import substitution') in the digital market, following the publication of a study, the results of which were indisputable. According to this study, imported mobile operating systems (especially Android and iOS) had no Russian-made competitors in the country. Their

penetration in the Russian mobile market was thus almost total, as they accounted for 95 per cent of the operating systems in the sector. The *MinSvjaz'* was prompted by this high rate to design a plan to reduce it to 50 per cent of the market by 2025.

Most importantly, in 2015 the Russian government launched the development of an operating system to be embedded on mobile platforms[13] (smartphones and tablets in particular) based on the open source distribution, Sailfish, developed by the Finnish company Jolla (which has been founded by former Nokia employees). The priority given to the development of Russian operating systems by the government, public institutions and some private actors since 2010 has thus had two objectives. First, at the instigation of Dmitrij Medvedev, the aim was to revitalise the Russian digital economy after the 1990s. Second, the Russian government changed the main objective of this logic to reduce the influence of American multinationals on its territory, in order to ensure, in the long term, the technical self-sufficiency of the country.

With the Snowden affair, the objective of a Russian technical self-sufficiency was reinforced by a (geo)political argument: the need to ensure the digital *sovereignty* of the country, and the security of its computer infrastructures in an increasingly connected world.

After Snowden: the Russian government publicly asserts its will to control software production and the Russian network, to address cyber security issues

Snowden's declarations led to a new debate on computer security in Russia

Although the Russian authorities had officially expressed their concern about the risks associated with the emergence of large-scale computer viruses during the late 1990s (Tchernenko 2013), the topic of computer security (*kiber bezopasnost'*) remained in the background of informational security issues (*informacionnaja bezopasnost'*) during the 2000s, as explained by Morenkova Perrier (2014) in an interesting analysis. It was not until Edward Snowden's revelations – which put the issue of computer security back on the government's agenda – that new federal plans for a secured digital production emerged. These public revelations most certainly put the risks of data leaks in the foreground.[14] Russian authorities were nonetheless aware of the risks pertaining to the development of the internet since the 1990s. They had issued a statement at the United Nations General Assembly (UNGA) for the creation of the first agreement on the 'Developments in the Field of Information and Telecommunications in the Context of International Security' in 1998,[15] that is one year before the largest cyberattack against the United States[16] – Moonlight Maze – was discovered. In fact, the Russian authorities quickly considered the possibility that there were links and collaborations between the GAFAM (Google, Apple, Facebook, Amazon and Microsoft) and the government and intelligence agencies of the United States, especially since these companies, officially domiciled in the United States, could be solicited by the authorities in the context of investigations. In 2014, the existence of this type of collaboration between the public and the private sectors in the United States was confirmed by spokespersons for Google, Facebook, Yahoo and Microsoft, who revealed that the NSA regularly issued warrants, requiring them to disclose data related to some of their users.

More importantly, Snowden's testimony established that the NSA had direct access to the servers of eight companies (Apple, Facebook, Google, Microsoft, Skype, AOL, YouTube and PalTalk), thanks to a surveillance tool named PRISM. According to Snowden, the implementation of direct access to the file hosting platform Dropbox was also in progress.

In 2013, it became obvious that the data given by the citizens of a country to foreign companies was a major geopolitical and strategic issue. The Russian authorities came to the conclusion that foreign software and applications constituted vulnerabilities (or were vectors of vulnerability), since they could allow other countries to conduct computer and informational attacks on Russian soil. The risk was heightened by the fact that the publishers of these software and apps were, as we said before, directly dependent on the laws and authority of the governments of the countries in which they were domiciled.

The development of *domestic* technologies (*otetchestvennye tekhnologii*)[17] thus became a core element of Russian policies, while Snowden's revelations appeared to be a convenient means to justify the strengthening of protectionist logics in the digital field. The temporary asylum granted to Snowden for one year by the authorities on 31 July 2013[18] and the deliverance of a residence card on 1 August 2014 became tools of political and diplomatic communication. The Russian state was able to put forward the need for a third way in the face of the control and surveillance by the United States on the network, and of what it presented as a form of political inaction by the other states, with regard to the protection of their citizens' data. The issues linked to the rights and freedom of internet users were then used to justify the implementation of digital tools to control the network in Russia, under the scrutiny of the international community and Russian users. The foreign and Russian companies which were reluctant to implement the new measures were perceived as being uncooperative in protecting their users' data. It was the case when Facebook, for example, refused to transfer the data of Russian internet users which were stocked in its servers to hosts (or new servers) located in the territory of the Russian Federation in compliance with the 'law on relocation [or "repatriation"] of the personal data of Russian citizens', which came into force on 1 September 2015.

Public policies in the digital field in Russia have thus followed three major phases. First, the Russian digital empowerment driven by the Medvedev presidency permitted the creation of domestic software in Russia for economic reasons. Second, this software was then put forward as a means for technical emancipation from the software produced abroad. Third, with the help of Snowden's revelations, the discourse on Russian economic emancipation and digital self-sufficiency via free and open source solutions led to renewed considerations regarding security. According to the authorities, the use of FOSS solutions – which is mandatory for public institutions in Russia – must ensure the security of the IT infrastructures of the state.

Russian free and open source software to counter the strategic risks of proprietary software developed abroad

The production of FOSS *sovereign software* (and not only of *domestic software*) was thus presented by the authorities as the best solution against digital security issues. Their open source codes offered security guarantees, since they could be directly reviewed and

validated by a community of users capable of attesting the absence of malicious scripts or flaws in their code.

The apparent transparency that open source gives over the functioning of computer processes can be considered as a major advantage in terms of security, whereas the functioning of the code used in commercial tools (which is generally kept secret) is largely unknown to its users. This lack of knowledge makes it possible for these private programmes to perform functions in the background, that their users are unaware of (like hidden tasks). The most common case is the communication of data produced by end devices (computers, cell phones, tablets, connected objects, etc.) concerning their use to the servers of the company which sells them. Although the transmission – and thus, the disclosure – of this data generally intends to improve the software and services offered to users,[19] it constitutes a risk of strategic data leakage, similar to that caused by backdoors installed with malicious intentions, that is, some specific data being exfiltrated without the knowledge of the users of the infected software. According to research carried out in recent years by The Invisible Things Lab,[20] this practice was suspected in the case of the Management Engine embedded microcontrollers produced by the American brand, Intel. These computer components are installed in a particularly large number of machines which are sold worldwide, as the company enjoys a near-monopoly situation thanks to its business contracts with many constructors present on the global PC market. However, according to these researchers, little was known[21] about the inner functioning of this component, managed by proprietary code, the writing and behaviour of which are particularly protected by the company. Nevertheless, some tests and observations indicated that it contained vulnerabilities, although it was difficult to say whether they had been ignored by mistake, by negligence (since the code was not accessible, the company may have deemed it unnecessary to patch it) or by design. In 2017, the researchers from the department of retro-engineering of the Russian company, Positive Technologies demonstrated that it was possible to physically access the ME flash file system of the chip containing the databus of the microcontroller[22] (this system is called a serial peripheral interface [SPI] system). It was thus possible to directly alter the functioning of the Intel Management Engine by rewriting its files.[23] Further research eventually demonstrated that the embedded microcontroller functioned like a real machine within the machine, enjoying full access to the memory of the microprocessors of the computers in which it was inserted (without being detected by the rest of the system). It also had total access to the areas dedicated to the treatment of network connections and data transmission protocols (TCP/IP) – allowing it to send and receive information (network packets) independently of the operating system of its host machine, thus simply bypassing its firewalls. According to these findings, Intel's Management Engine was not only a major point of vulnerability for the millions of computers in which it was embedded, but also the equivalent of a backdoor capable of performing its own tasks and communicating over the network (sending and receiving data) without the awareness of users, as explained by Wallen (2016). Of even more concern, it appeared that the flaws in the proprietary code of Intel's components could have been effectively exploited by hackers (see, for example, Bright [2017]).

These methods of data transmission implemented in proprietary components by some enterprises represent, therefore, a threat to computer security. They can be used to gain information about the nature or the functioning of a piece of equipment to prepare

attacks, to carry out industrial, economic or state intelligence, or even to corrupt or destroy the equipment of a competitor or an enemy, a company or a state. In that sense, any proprietary software based on closed source and private code is not far from being able to constitute a backdoor.

After the Snowden affair, together with discoveries such as those made by Positive Technologies in 2017, the Russian government has apparently decided to accelerate the creation of alternatives to products designed in the United States, in order to reduce the risk of data leaks through backdoors and rootkits (malicious programmes which conceal their activity), by further promoting the development of open source solutions produced in Russia.

Some affairs, like the theft and the public release in 2016 of hacking tools – which had been developed and maintained by the NSA since 2013 – by a group named 'the Shadow Brokers',[24] or the Vault affair in 2017,[25] have probably also influenced the decision to develop open source solutions in Russia. In fact, the materials released in these two affairs showed that both the CIA and the NSA (amongst others) were using zero-day exploits based on vulnerabilities embedded in hardware and software components, which they knew of but did not report.[26] The risks posed by the dependency on other countries for the supply of strategic equipment have also played a major role in this decision. The fear of being cut off from the global internet is one of the facets of these concerns. On 1 May 2019, the Russian presidential administration promulgated a bill (No. 608767-7) to hasten the creation of a 'Sovereign internet'. The text officially launched the creation of an alternative network to bypass the means of control of the Five Eyes, but also – and probably above all – to ensure the resilience of the Russian network in the event of a failure of the global internet, or of its deliberate blocking by the United States.[27] In this regard, both communication equipment (hardware) and software produced in Russia – the functioning of which can be mastered and checked – are perceived as a guarantee for the connectivity of the Russian internet. But the security-oriented use of free and open source software by Russian authorities contradict the principle of users' freedom which animated the FOSS movements at the beginning. That said, this principle was already weakened by the promotion and the massification of the use of this kind of software, with no link to the activities of the Free Software Foundation (FSF) and the Open Source Initiative.[28] Yet, the exploitation of open source codes to ensure the control of software on a large scale constitutes a diversion from the values defended by the Free movement (in particular), which has worked primarily to prevent any form of digital control by states or private entities. The very meaning of these movements disappears in these new discourses around Russian digital sovereignty and security, which serve a convergence of economic and political interests unrelated to the objectives of defending users' freedom and the rights of software creators. State investments in domestic software alternatives go hand in hand with the increasing outsourcing of the digital capabilities of public institutions (especially for the security of their infrastructures), which seems to benefit private actors first and foremost.

We can therefore wonder whether free and open source software allows Russia to reach digital sovereignty, or if it is used to favour the interests of private companies, which would want to benefit from public contracts. If that is the case, the manipulation of the objectives of the FOSS movements by private actors may call into question the very advantages that it presents in terms of security.

Behind the ideas of digital sovereignty and security: a convenient convergence of interests

The externalisation of computer security by the state gives advantage to private actors first

With the problem of computer security now in mind, and the promotion of the idea of digital sovereignty in Russia, various actors, from the private sector in particular, have re-appropriated the new orientations of the state in order to be directly involved – and even to ensure a leading role – in the definition of the new logics to be put in place, especially concerning the management of Russian citizens' data.

The idea of digital sovereignty (*cifrovoj suverenitet*) has become a leading argument in these new logics, notably on the initiative taken by Igor Ashmanov, the main owner of the InfoWatch group which operates in the field of computer and data security. Igor Ashmanov contributed actively to reflect on digital security, especially in the case of state data. In fact, he has presided over the establishment of the concept of sovereignty (*suverenitet*) as an element of national doctrine for the development of a sovereign digital environment (or a Russified digital ecosystem) in Russia; see the explanations he gave on this topic at the St. Petersburg iForum (Ashmanov 2015).

A new informational security (*informacionnaja bezopasnost'*) doctrine, dependent on a certain form of informational sovereignty (*informacionnyj suverenitet*), was adopted by the Russian presidency in December 2016, again with the help and advice of the oligarch (see Presidency of the Russian Federation, 2016).

Within that framework, the public digital infrastructures have become an important domestic market for private actors – as their equipment now has to be secured. Their active participation in the debates over the implementation of new security standards allowed them to make sure that they could effectively respond to the new requirements of the state – which they helped define. The effectiveness of their approach can be seen in the trend towards outsourcing the digital skills of the public institutions at the instigation of the state itself, especially in the area of IT security.

The InfoWatch company is a telling example of a private actor which has benefited from these new logics. It owned 50 per cent of the DLP (*Data Leak(age) Protection*)[29] public market in 2015, which covers the protection of state data, and more broadly the protection of information technology against external threats.[30] The relations between this private actor and the public institutions are generally close, since the managing director of the company, Natalija Kasperskaja, is also one of the main advisors to the government and the Presidency on digital issues. She has actively participated in the implementation of the great project for an 'independent RuNet' (Russian internet) in 2019. She is also the wife of Igor Ashmanov, the oligarch mentioned above.

However, this trend towards outsourcing state IT security skills raises questions, including the very security of state institutions. Two digital security companies contracted by the Russian security services have suffered computer attacks, which led to the largest data leak known in the history of the intelligence services of the country, through the attack on the main server (Active Directory) of the SyTech company on 13 July 2019.

The links between the private sector in IT and the public institutions in Russia are indicative of the new logics of digital defence of the country. They mobilise all players

in the field. But they are also a sign of the decisive influence of private actors, who have taken advantage of the new laws on the use of FOSS software by public institutions, and who have been able to reconcile their needs with those of the authorities, if not those of the authorities with their own.

The new actors of the free and open source movements in Russia: the primacy of economic and technical perspectives on political questions and traditional activism

As a consequence of the incentive policies implemented by the state in Russia, the free and open source movements seem to have lost their political value of contesting the domination of private and governmental entities over the digital world, to the detriment of users' freedom.

Actors interested in the production of free and open source software in Russia are less attached to political questions and to the activism which underpinned the movements. The discursive, legislative and financial support brought by the Russian state to free and open source solutions has ultimately privatized their development and use. FOSS software is now produced, first and foremost, by companies which seek to conclude (and sometimes to take advantage of) state contracts, and employed by users who seek economical, less expensive software and – to a lesser degree – security advantages.

What is more, in accordance with the concept of digital sovereignty in Russia, Russian software is now perceived as more secure for the Russian citizens than foreign software, although this idea remains to be proven. The SyTech leak actually showed that private actors are willing to produce intrusive digital tools for the security services, in order to facilitate the surveillance of internet users in the country.

The largely opportunistic dimension of the public stand taken by Russian companies in the development of free and open source solutions punctually comes into light.

Interestingly, the free software ASTRA Linux used by the Russian armed forces is not really *free* in practice. Though the Linux core and primary functions of this operating system are accessible online, easily downloaded and modifiable by any user,[31] access to the 'Special Edition' distribution employed by the armed forces is limited and based (to a certain extent) on a closed source, since it exists for their exclusive use. The company RusBITech-ASTRA hence benefits from the commercialisation of this version (which cannot be considered as free software in accordance with the requirements of the FSF) mainly to the Ministry of Defense.[32]

Conclusion

Since 2010, there has been an undeniable interest by the Russian state in free and open source software, which has led to an increase in their promotion and use by the public and private sectors. With Edward Snowden's revelations in 2013, the main arguments used to promote them has shifted from the advantages offered by their low cost of purchase and production (which was supposed to help revitalise the Russian digital industry) to the security advantages they are supposed to offer to the Russian state and Russian users, by ensuring the digital sovereignty of the country.

Meanwhile, the Russian state and different entities and administrations under its jurisdiction, have become an important domestic market that Russian companies are seeking

to conquer, especially considering the fact that the scandal caused in the United States by the alleged collusion between Kaspersky Lab (which sells the Kaspersky antivirus) and the Russian intelligence services aroused suspicion abroad.

FOSS development eventually turned into a decisive marketing argument on the internal market. Its intensive promotion tends to modify both the ecosystem of digital development in Russia, and the very meaning of the FOSS movements, since the political and militant aspects of these two modes of production have been gradually evacuated in favour of economic and commercial logics.

Notes

1. Basic software needed to run and use a computer.
2. Hardware was commercialised from the 1950s on the industrial market. For further information, see Logé (1991).
3. He presumably said: '[N]o one will build the sun city in an enclave'. See Nexon and Swarovskaya (2011) on the subject.
4. An official investigation on the possible misappropriation of Skolkovo funds was launched by Vladimir Markin in 2013, with the apparent support of Vladimir Putin. For more information about this case, see Leroyer (2013).
5. Small and medium-sized enterprises.
6. Several companies like Microsoft are now diverting from that model. In 2012, the company launched a subsidiary named Microsoft Open Technologies Inc., with the aim of bridging the gap between proprietary Microsoft technologies and non-Microsoft technologies by engaging with open-source standards. Google also released the code of its Android OS, which became open source. The OS used on its Chromebook computers is also based on UNIX.
7. Illegal Windows copies, and the unregulated sale of its activation keys contributed to the emergence of a parallel economy, which led Microsoft to apply protective measures in the early 2000s.
8. The sitting members of the Trade Policy Review Mechanism of the Services Council, and of the TRIPS [Trade-Related Aspects of Intellectual Property Rights] Council might have been particularly reluctant to the Russian candidacy with regard to this situation.
9. A free operating system. Its development relied on the structure and functioning of the UNIX system, created in 1969. Several families of operating systems have been built on this model, including GNU/Linux, BSD, macOS and iOS.
10. Officially launched in March 2001.
11. The company which created and administers the namesake open source operating system.
12. 'Keep in mind that […] the more Russia will invest in the international Open Source Movement, the more it will influence it'. See the interview by Gingichashvili (2014).
13. 'Selon le ministère russe des Télécommunications, la Russie a son propre système d'exploitation mobile', ['According to the Russian Ministry of Telecommunications, Russia has its own mobile operating system'] *Sputnik*, 19 May 2015.
14. Especially when this data is captured by third parties on networks and platforms. See, for instance, the numerous cases of Russian soldiers who unwillingly disclosed their participation in external operations by posting pictures on social networks: 'Ukraine. Les soldats russes trop bavards sur les réseaux sociaux', [Ukraine. Some Russian Soldiers Are Too Talkative On Social Networks] *Le Figaro*, 4 August 2014.
15. The official text was published on 4 January 1999. See (General Assembly of the United Nations 1999).
16. Until the SolarWind attack last year.
17. It could be literally translated as '*patriotic* technologies' as the adjective *otetchestvennye* takes its root from the word *father* (*otets*).

18. It came into force the day of his official entry on Russian territory, on 1 August 2013.
19. A company can use these data transmission modes (directly provided by, and built into the code of its products) to evaluate the user experience of one of its solutions. To do so, the company implements instructions into the device or software, so that it regularly reports information about, for example, its energy consumption or the total amount of time it is used every day.
20. A research lab on computer security founded and headed by Joanna Rutkowska, a researcher with an MS in Computer Science from the Technological University of Warsaw and founder of the secured distribution Qubes OS.
21. Until 2017, see the following explanations.
22. A physical element (composed of electrical conductors) managed by a programme which transfers data between different hardware and logical blocks. These blocks receive instructions from the databus to start and control their operation. In a computer, the databus is the link between the processor, the main memory and the peripheral controllers (USB controller, network card, graphics card, keyboard, etc.).
23. The functioning of these chips could thus be arbitrarily modified, thanks to the immediate obtainment of the read/write rights on their configuration files, which is a serious vulnerability. For more explanations, see the presentation given by Sklyarov (2017), Head of Reverse Engineering at Positive Technology. Other massive flaws were finally discovered on this microcontroller in 2017, forcing the company to admit defects in its product.
24. Which is thought to have been created by a Russian intelligence agency.
25. The Vault affair consisted in the theft and the publication, by WikiLeaks, of several documents (entitled 'Vault 7' by the organisation) describing some of the techniques and source codes used by the CIA in order to compromise different kinds of endpoint devices (computers, smart televisions or cars).
26. According to current ethical rules, actors are supposed to signal these vulnerabilities to the constructors and developers of hardware and software solutions, so they can patch them and warn their users that these tools may be compromised.
27. This possibility has long been a major concern for the Russian authorities, though it is highly unlikely if one considers the actual functioning of internet governance. On 24 April 2014, during the first 'Forum of Independent Local and Regional Media' in Saint Petersburg, Viktor Levanov (a blogger who is considered to represent a friendly opposition to the Kremlin) declared: 'It is an open secret that the United States control the internet. The Patriot Act gives them all the power they need. Now the former agent Edward Snowden has opened our eyes. This Act, adopted 80 years ago, in 1934, still allows the President of the United States to shut down communications on the entire planet with a single resolution. […]', highlighting that risk. See the whole declaration in the report published by the Presidency of the Russian Federation (2014).
28. In October 1999, IBM announced they wanted to invest in open-source software, as explained in an article published in *The New York Times* on 4 October 1999. The company invested $1 billion dollars in Linux in 2001 CNET (2002), and has reinvested the same amount several times in the project since.
29. Protection against data leaks: *predotvraščenie uteček informacii*.
30. According to the managing director of the company, Natalija Kasperskaja, the former wife of Eugene Kaspersky, who owns the company, Kaspersky Lab (the company was cofounded by the couple in 1997).
31. This 'Common Edition' is thus free.
32. This model (half-free/half-private and commercial), based on a number of closed source modules, is a source of conflict in the FOSS community. The enterprises which use this model argue that the commercialisation of some pieces of software allow them to sustain the development of their free and open source tools, since they can, then, pay on a regular basis or occasionally compensate the developers and coders who contribute to their creation, and maintain them up to date.

Disclosure statement

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

Notes on contributor

Marie-Gabrielle Bertran is a PhD student in geopolitics, University Paris 8, EA 353, Center for Geopolitical Research and Analyses (CRAG – IFGLab), and researcher at the lab Geopolitics of the Datasphere (GEODE). Marie-Gabrielle conducted a research on the RuNet (the Russian internet) during her Master studies at the French Institute of Geopolitics (IFG) in 2017, under the supervision of Kévin Limonier. In 2018, she studied the use of Free and Open Source software (FOSS) in Russia, also under the supervision of Kévin Limonier. She is currently working on a PhD thesis on software development in Russia, under the supervision of Frédérick Douzet and Kévin Limonier at the GEODE research centre.

ORCID

Marie-Gabrielle Bertran http://orcid.org/0000-0003-3225-8324

References

Ashmanov, Igor. 2015. "Informacionnyj Suverenitet – Novaja Realnost'" [Information Sovereignty – The New Reality]. Slides presented at the annual iForum, Saint Petersburg, July 14. https://docplayer.ru/63407402-Informacionnyy-suverenitet-novaya-realnost.html.

Bright, Peter. 2017. "Sneaky Hackers Use Intel Management Tools to Bypass Windows Firewall." *ArsTechnica*. June 9.

CNET. 2002. "IBM to spend $1 billion on Linux in 2001." January 2. https://www.cnet.com/news/ibm-to-spend-1-billion-on-linux-in-2001/.

General Assembly of the United Nations. 1999. "Developments in the Field of Information and Telecommunications in the Context of International Security. Resolution A/RES/53/70." January 4. https://undocs.org/A/RES/53/70.

Gingichashvili, Sarah. 2014. "Russia to Develop a National OS?" *The Internet of Things*, July 9. http://thefutureofthings.com/3893-russia-to-develop-a-national-os/.

Leroyer, Madeleine. 2013. "Poutine Met au Pas le Cabinet Medvedev." [Putin Brings Medvedev's Cabinet to Heel]. *Le Figaro*, May 8. https://www.lefigaro.fr/international/2013/05/08/01003-20130508ARTFIG00354-poutine-met-au-pas-le-cabinet-medvedev.php.

Limonier, Kevin. 2012. "Analyse Géopolitique des Enjeux d'une Politique de Puissance : Le Cas de la Science et de l'Innovation en Russie." [Geopolitical Analysis of Some Issues of Power Politics: The Case of Science and Innovation in Russia]. *Hérodote* 146-147 (3): 193–216.

The Linux Foundation. 2011. "The Linux Foundation Announces New Members from Throughout Europe." October 11. https://linuxfoundation.org/press-release/the-linux-foundation-announces-new-members-from-throughout-europe/.

Logé, Yves. 1991. *L'URSS. Le défi technologique, la révolution inachevée* [*The USSR. The Technological Challenge, the Unfinished Revolution*]. Paris: PUF.

Lohr, Steve. 1999. "I.B.M. Invests in Campaign to Promote its Software." *The New York Times*, October 4. https://www.nytimes.com/1999/10/04/business/ibm-invests-in-campaign-to-promote-its-software.html.

Ministry of Digital Development, Networks and Mass Communications of the Russian Federation. 2010. *Ordinance on the Transition of Federal Executive Bodies and Agencies of the Federal Budget to the Use of Free Software, 2011*–2015. http://minsvyaz.ru/uploaded/files/2299p.pdf.

Ministry of Foreign Affairs of the Russian Federation. 2000. "National Security Concept of the Russian Federation." https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768.

Morenkova Perrier, Elena. 2014. "De la Sécurité Informationnelle à la Cybersécurité: La Redéfinition de la Doctrine Stratégique Russe." [From Information Security to Cyber Security: Redefinition of the Russian Strategic Doctrine]. *Revue défense nationale* 586: 1–7.

Nexon, Marc, and Katia Swarovskaya. 2011. "Medvedev, le Prisonnier de Poutine." [Medvedev, Putin's Prisoner]. *Le Point*, July 7. https://www.lepoint.fr/monde/medvedev-le-prisonnier-de-poutine-07-07-2011-1352727_24.php.

Perens, Bruce. 1999. "The Open Source Definition." In *Open Sources. Voices from the Open Source Revolution*. Sebastopol, CA: O'Reilly & Associates.

Presidency of the Russian Federation. 2014. "Media Forum of Independent Local and Regional Media." April 24. http://en.kremlin.ru/events/president/news/20858.

Presidency of the Russian Federation. 2016. "Doctrine of the Russian Federation on Information Security." http://publication.pravo.gov.ru/Document/View/0001201612060002?index=1&rangeSize=1.

Sklyarov, Dmitry. 2017. "Intel ME: Flash File System Explained." December 6. Black Hat Europe, London, England, Youtube video, 53:14, posted by "Black Hat." June 8, 2020. https://www.youtube.com/watch?v=mYsTBPqbya8.

State Duma. 2015. *Federal Law No.764677-6*. http://pravo.gov.ru/proxy/ips/?docbody=&nd=102374921.

Tchernenko, Elena. 2013. "Cold War 2.0? Cyberspace as the New Arena for Confrontation." *Russia in Global Affairs* 42 (1). https://eng.globalaffairs.ru/number/Cold-War-20-15929.

Wallen, Jack. 2016. "Is the Intel Management Engine a Backdoor?" *TechRepublic*, July 1. https://www.techrepublic.com/article/is-the-intel-management-engine-a-backdoor/.