What Open Source Investigations (OSINT) Can Bring to Russian Studies

Limonier, Kevin

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Limonier, K. (2023). What Open Source Investigations (OSINT) Can Bring to Russian Studies. *Russian Analytical Digest*, 293, 4-5. https://doi.org/10.3929/ethz-b-000600973

ANALYSIS

What Open Source Investigations (OSINT) Can Bring to Russian Studies

Kevin Limonier (University of Paris 8)

DOI: 10.3929/ethz-b-000600973

Abstract

For many years, Open Source Intelligence (OSINT) has been the domain of hackers, journalists, and activists. However, it also has the potential to aid researchers focusing on the political or strategic dimensions of contemporary Russia. The integration of these methods is urgently needed, as the war in Ukraine—by making *in situ* fieldwork almost impossible—may create a "phenomenological vacuum" that OSINT can help to fill.

The invasion of Ukraine has deprived many Western researchers of the ability to access Russia for the purpose of conducting fieldwork. This is particularly true for those working on policy or security issues. For them, the impossibility of conducting on-the-ground investigations, along with the disappearance of independent journalism within the country, has created a "phenomenological vacuum" that will be very difficult to fill. In the medium term, they could find themselves in a situation comparable to what their predecessors experienced during the Soviet era, when they could hardly travel to the USSR or had access only to falsified data.

Unless a major political shift occurs, the situation is likely to persist and gradually impoverish our empirical knowledge of contemporary Russia. This is precisely why we need to think of circumvention strategies, even if these will never replace anthropological or sociological research *in situ*. In its day, Sovietology conceived many strategies, both good and bad, for overcoming the extreme difficulty of conducting fieldwork in the USSR. Among these, observation "from the margins" of the country (politically and geographically) was popular and may soon be revived, although this is not relevant to every research topic. Similarly, the use of online sources circumvents part of the problem but creates others: digital censorship makes Runet, the Russian-speaking segment of the Internet, a source of information to be handled carefully.

However, and this is the paradox of the Russian Internet today, it remains a strong vector of emancipation, particularly through the conduct of "digital counter-investigations."[1] These investigations, which are based on digital footprints collected online, use gaps in the network to identify abuses of power, cases of corruption or political assassination attempts. From the Bellingcat investigation that proved Russian culpability in the destruction of MH17 over Ukraine in 2014 to the poisoning of Alexei Navalny in 2020, many big Russian stories have been uncovered through the use of advanced digital investigation methods known as OSINT (Open Source Intelligence). Broadly speaking, OSINT refers to a set of methods that make it possible to uncover previously unknown information through the collection and aggregation of data freely available on the Internet. Since the beginning of the war in February 2022, OSINT has become a widespread practice: countless social media accounts have flourished that cover the war live, sharing digital traces generated by combat or other maneuvers. Elsewhere, the activity of the PMC Wagner in Africa is being scrutinized, making it possible for journalists and future investigators working on human rights violations to document Moscow's "return" to the continent.

Overall, open source digital investigation has become a genre in itself, practiced by journalists, activists, and even magistrates to document political, criminal or strategic phenomena. Researchers, meanwhile, have not yet taken up these techniques, probably for various ethical or methodological reasons. However, there is a real need to think about the use of digital investigation as a strategy for circumventing the dangers and impossibilities of conducting physical fieldwork in Russia.

This is true, first and foremost, because OSINT shares with fieldwork a desire to decipher polity and power relations. Every day, we use a large number of connected machines (smartphones, computers, connected objects) that capture a growing share of our interactions and activities. These omnipresent "sensors" thus record and digitize an infinite number of flows through which the *mots d'ordre* (Deleuze) that constitute the very essence of power, in Foucault's sense, are spread. There is therefore a need to think of methods for extracting and deciphering the relevant flows and metadata to analyze a given (geo)political phenomenon.

Second, and despite extensive digital censorship, contemporary Russia is probably the largest source of

1 The French journal *Multitudes* has dedicated an entire issue to the emergence of such digital "counter-investigations": https://www.multitudes.net/category/l-edition-papier-en-ligne/89-multitudes-89-hiver-2022/.

OSINT data one can dream of today. This is evidenced by the fact that even the FSB has not been immune to investigations, which exposed its attempts to poison Navalny. The Russian authorities encourage digital control (and thus the production of all kinds of databases), while being deeply corrupt. This results in a profusion of freely accessible leaked data, which are then processed by journalists or experts, as has been the case with the Navalny poisoning and many others.

Finally, many activities within the vast clientelist system that underpins the Russian leadership generate metadata, which can then be collected and studied. For instance, in a paper published in *Post-Soviet Affairs* in 2020, we illuminated the economic and political development pattern of the "Prigozhin galaxy" on the African continent thanks to a meticulous OSINT investigation. Furthermore, Runet's intermediation platforms allow for the collection of more metadata overall than their Western counterparts, making it possible to conduct large-scale extraction campaigns on VK, Telegram or other networks for the purposes of speech or text analysis.

There is therefore enormous potential to study contemporary Russian power by analyzing the digital traces it generates. However, such "digital fieldwork" cannot become mainstream without the development of appropriate toolkits for data collection and analysis, as well as related methodological frameworks. It is therefore necessary to consider the development of a comprehensive toolkit that would allow researchers to crawl, scrape, collect, and analyze data from Runet, as well as from the technical bases generally used in OSINT.

This poses a major challenge, as it would require significant technical resources, not to mention the danger posed by the so-called "sovereign Runet" law (FZ90), which gives the Russian authorities the legal means to control all Internet traffic entering and leaving the country. While this vast project of integral network censorship is as yet largely a fiction, it could eventually make it impossible to access certain Russian digital resources from abroad (which would, in turn, necessitate new complex circumvention maneuvers).

Finally, the manipulation of digital traces collected on the Runet for academic research purposes raises numerous ethical questions that remain as yet unanswered. For example, what about the countless data leaks from the Russian state apparatus? Although most of them are the product of data theft perpetrated by hackers, they provide invaluable glimpses of the inner mechanisms of power.

About the Author

Kevin Limonier is an Associate Professor of Geography and Slavic Studies at the French Institute of Geopolitics (University of Paris 8). He is also deputy director of the GEODE Research Center and the scientific director of the Russian-speaking infosphere observatory (French Ministry of the Armed Forces). He was for several years a lecturer in geography/geopolitics at the Russian State University of Humanities (RGGU, Moscow). His research focuses on the development of new methods of cyberspace mapping and digital investigation (OSINT) in the post-Soviet context. His academic blog (in French) is available at https://villesfermees.hypotheses.org/.