f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine

by Kevin Limonier, Frédérick Douzet, Louis Pétiniaud, Loqman Salamatian, and Kavé Salamatian

Abstract

In this paper, we argue that data routing is of geopolitical significance. We propose new methodologies to understand and represent the new forms of power rivalries and imbalances that occur within the lower layers of cyberspace, through the analysis of Eastern Ukraine. The Internet is a network of networks where each network is an Autonomous System (ASes). ASes are independent administrative entities controlled by a variety of actors such as governments, companies, and universities. Their administrators have to agree and communicate on paths followed by packets travelling across the Internet, which is made possible by the Border Gateway Protocol (BGP). Agreements between ASes are often confidential but BGP requires neighbouring ASes to interact with each other in order to coordinate routing through the constant release of connectivity update messages. These messages announce the availability (or withdrawal) of a sequence of ASes that can be followed to reach an IP address prefix. We select Eastern Ukraine as a case study as in 2020, six years after the beginning of the war in Donbass, data is available to analyze and map changes to data routing. In our study, we conducted a longitudinal analysis of Ukraine's connectivity through the capture and analysis of these BGP announcements. Our results show how Donbass ASes progressively migrated from Ukraine's cyberspace towards Russia, while still sharing connections with Ukrainian ASes. Donbass cyberspace therefore sits at the interface of Ukraine and Russia but has been relegated to the periphery of both networks; it is marginalized from the Ukrainian network but not fully integrated into the Russian network. These evolutions both reflect and affect ongoing geopolitical power rivalries in the physical world and demonstrate their strategic significance. Our methodology can be used to conduct studies in other regions subject to geopolitical open conflicts and to infer the strategies developed by states in anticipation of potential threats.

Contents

Introduction

On 2 August 2018, the segment of the Internet network located in the separatist areas of Eastern Ukraine was reorganized. On that day, the connections for local Internet access changed, and the available data paths entering or leaving the separatist regions of Donetsk and Luhansk were suddenly only transiting through Russia and not through

Ukraine anymore, as was the case prior to this date. The changes of routing in the separatist area had started well before, but the summer of 2018 brought about the completion of a split-up process of Eastern Ukraine's networks.

This routing modification probably did not have any visible effect on the average Internet user in the separatist zone. Aside from specific economic activities requiring optimal traffic speed (online video providers, cloud storage, financial activities ...), modifications in the routing of digital data don't really impact everyday uses of the network. Furthermore, users wouldn't have found out that their data suddenly transited through Russia instead of Ukraine unless they had a specific interest in the paths data take when accessing servers on the other side of the planet — and they would still need some technical knowledge to look into them.

But this transformation is strategically significant for two reasons. First, this rerouting underscores a new step toward the greater integration of the Donbass region in the Russian sphere of influence, at the expense of Ukraine. Following the rerouting of commercial exchanges and of part of the economic trade, digital streams have in turn been rerouted eastward.

Second, it potentially reveals the strategy of local actors as this integration highlights the existing political networks at least as much as the technological networks. The entity behind the rerouting was a company registered at the time in Rostov-on-Don that used the same postal address as several other digital companies managing strategic resources in the separatist territories [1]. In other words, we can lay out the hypothesis that the rerouting was deliberately orchestrated by actors somewhat connected to the sovereign structures of the separatist entities. Of course, this cannot be formally proven and remains a conjecture. But even without any intentional character, the routing change would be significant, because it happened in the wider context of the normative and technical construction of a "sovereign" Russian Internet (Limonier, 2018; Akimenko and Giles, 2020; Zorina, 2017; Artamonov, 2017; Kučerjavyj, 2014), as well as in the frame of the ongoing integration process of Donbass and Crimea into Russia.

In this paper, we argue that data routing is of geopolitical significance, and can be instrumentalized for strategic motives. We propose new methodologies to understand and represent these new forms of power rivalries and imbalances that occur within the lower layers of cyberspace, through the analysis of Eastern Ukraine.

The lower layers of cyberspace, a new battlefield

Cyberspace has become a full-blown "geopolitical object" (Lacoste, 1993) and a new field of strategic studies. The concept of cyberspace encompasses both the Internet itself and the space of information, communication and interactions between users its global expansion has generated (Douzet, 2014; Adams, 1997; Dunn Cavelty, 2013; Lambach, 2020).

The Internet is a network of networks interconnected through a series of physical contact points and routing protocols that altogether aim at transporting packets of digital data which, put together, form a message (text, video, image, etc.). The Internet was built in a decentralized manner without any tutelar authority and grew exponentially at the global level, leading to an extreme complexity and diversity that can be hard to fathom.

To simplify, scholars usually represent cyberspace as an organized system of overlapping and interdependent layers where the upper layer represents the space of information and interactions between users and the lower layers the infrastructures and protocols that allow packets of data to be sent, received, decrypted and understood within a few milliseconds (Zave and Rexford, 2019). These layers are vertically structured: the "upper layers" could not be functioning without the "lower layers."

The lowest layer is the physical network made of infrastructures such as submarine cables, optical fiber backbones and satellites that carry data across the world and can be geolocated, therefore easily mapped. It also includes the computers, smartphones, pads and connected devices that provide users with access to data. On top is the protocol layer made of the programs and protocols that direct packets of data to their destinations unhindered. Data circulation is indeed normed with a number of protocols such as the TCP/IP, a protocol suite used to transmit data on the Internet and allow computers to communicate, the Border Gateway Protocol (BGP) that allows the many subnetworks of the Internet to communicate between each other, and the DNS protocol (Domain Name System) that matches IP addresses with domain names (*i.e.*, Web site addresses) to allow users to easily navigate the Web (Leguay, *et al.*, 2007). These two layers constitute the "lower layers" of cyberspace and have been manipulated in the past for geopolitical reasons through, for example, the physical destruction of infrastructure (the cutting of submarine cables, a cyberattack to sabotage computers) or traffic hijack (Dainotti, 2014).

In this paper, we choose to focus on the lower layers of cyberspace, and most specifically on the protocols of data routing, for several reasons. First, it is theoretically possible to reroute data through servers or infrastructure and a number of recent incidents could be interpreted as deliberate handling of data routing, even though it is difficult to formally prove (Levin, *et al.*, 2015). In addition, a number of actors have stated an interest in gaining control over the lower layers of cyberspace (Voelsen, 2019). Russia's project of a sovereign Internet [2] is widely based on a nationwide reorganization of Internet routes, a rationalisation of its border gateways, and the creation of an alternate, sovereign DNS table. China and Iran are two countries where political authorities have a strong control of their local Internet architecture (Segal, 2020; Creemers, 2020; Tian, *et al.*, 2012). Mapping the structure of connectivity can help in understanding the geopolitics underpinning the routes that data travel through and the strategies of control implemented by state and non-state actors. It can provide an overview of how geopolitical rivalries contribute to shaping cyberspace as technical structures are often the result of political power balances and struggles (Hecht, 1998).

Second, the cartography of the lower layers can help understand how the shape of cyberspace can in turn influence power relationships in the context of territorial rivalries. Control over the lower layers can indeed give the power to monitor or block data traffic, disconnect specific territories or users, or even hide cyberattacks (Pétiniaud and Salamatian, 2019). Thus, it raises the question of the relationships between physical space, political space (territory) and technical space. The concept of territory has long been defined as a claim over a share of space by some individuals or groups (Bergues, 1981). While cyberspace cannot be considered a territory according to a classical geographic definition, it has been the subject of a process of territorialization over the past decades (Lambach, 2020), leading to the division of space into formally or informally bounded entities. Territorial strategies are used to achieve specific goals and the control of geographic space — digital space in this case — can be used to assert or maintain power (Lacoste, 2014).

However, the appropriation and control of a non-physical space generated by a digital network requires the development of new technical means, tools, and strategies that need to be uncovered by interdisciplinary research (Douzet, *et al.*, 2020). This process is embedded in the social and political relations that exist between a set of actors (Ermoshina and Musiani, 2017) in specific territories and it can be studied through graph theories (Boullier, *et al.*, 2016) which provide tools to graphically represent complex digital networks (Beaude, 2015) but also link key actors to territorial strategies. As a result, this study also participates in the literature about "topological powers" (Allen, 2016).

Eastern Ukraine, a disputed territory at the heart of the strategic competition between great powers

We selected the disputed areas of Eastern Ukraine [3] as a case study to demonstrate the geopolitical significance of Internet topologies and we developed methodologies to map them. The Russian and Ukrainian segments of the Internet are among the most complex in the world, and they do share a 30-year-long common history, going back to the Soviet Union. This complexity has historical roots. During the Soviet period, the network was highly centralized and rather isolated from the global Internet with very few points of connection to the rest of the world. The lack of bandwidth resulting from this architecture encouraged the proliferation of small autonomous systems to better redistribute connectivity at a local level. This trend accelerated during the post-Soviet period when the Internet developed fast with very little supervision, leading to an exceptionally high number of autonomous systems, making the network unusually complex.

The ongoing Ukrainian crisis which started with the Maidan revolution and the annexation of Crimea in 2014, has progressively and dramatically changed the regional structure of connectivity, alongside an open territorial conflict that has extended to the digital space. Indeed, before "going cyber", the Ukrainian conflict is above all the most remarkable illustration of Russia's "post imperial symptom" (Radvanyi and Laruelle, 2016), as well as the geopolitical expression of "competing memories" (Kappeler, 2014) around the definition of Ukraine's and Russia's national identities. The territorial effects of such post imperial conflicts in Ukraine and in other former Soviet republics are well documented (Arel, 2018).

Being a reticular topic *par excellence*, the Internet remains less investigated in that perspective — putting aside studies about information manipulations. Yet, Ukraine and Russia both seek to shape the way data circulate on their national networks, using "national security" or "digital sovereignty" as justifications for a greater digital control. For example, the existence of major Russian intermediation platforms that are widely used throughout the post-Soviet region has been not only a tool of influence for Moscow, but also a lever to promote a wider conception of Russia's "sovereign Internet". It also represents a tremendous economic opportunity for national companies to secure contracts with the government to deploy their digital equipment and technologies. Such policies are now meant to be implemented at the routing level, according to the 2019 law dubbed "on sovereign Runet". On the Ukrainian side, the war in Donbass has, for example, led the government to implement several legislations to limit the influence of Russian digital platforms (Shumilo, *et al.*, 2019).

Even if some valuable work has been made on the actors and the strategies that they implement to bypass the limitations induced by such policies (Ermoshina, 2019), the territorial effects of the "post imperial symptom" regarding the digital space are still a blind spot of the strategic literature. Some first results based on our measurements and data have been published (Douzet, *et al.*, 2020), but we so far have not engaged in a methodological paper that addresses both the (post-Soviet) area studies and Internet studies communities. Moreover, most of the published research — including ours — has so far mainly focused on the case of routing changes in Crimea, mainly because the simplicity of the local Internet topology made it an ideal initial case study (Ermoshina, 2019). The situation of Donetsk and Luhansk Peoples' Republics is different. First, its geographical situation differs from the easily circumscribed Crimean Peninsula: the Ukrainian and Russian mainland infrastructures are numerous and hard to easily map. Second, the geopolitical status of Donbass is much more hybrid than Crimea's. Donbass and Luhansk have been able, with help from Russia, to declare themselves *de facto* States. Our ability to understand the situation there is limited by their instability but also by their control of the information delivered to the international community. Third, the network situation of Donbass at the routing level is much more complex and denser than in the Crimean case. A substantial number of networks operate there, and its observation deserves a finer grained analysis.

In that perspective, this paper has two ambitions. First, it aims to demonstrate the geopolitical significance of Internet topology and routing changes in an open conflict area. Six years after the beginning of the war in Donbass, data is available to analyze and map these changes, which can be replaced in the wider context of the "post imperial symptom". Our main hypothesis is that these evolutions are strategically significant and both reflect and impact ongoing geopolitical power rivalries in the physical world. Such analysis can be conducted in other regions subject to geopolitical open conflicts. They can also be used to infer the strategies developed by states in anticipation of potential threats. Previous work demonstrated how Iran adapted the structure of its connectivity to be able to isolate its domestic cyberspace from the global Internet (Douzet, *et al.*, 2020). Pakistan unsuccessfully tried to manipulate data routing in 2010 (Singel, 2008) and is investing in a cross-border cable with China in order to by-pass India for Pakistani Internet traffic [4]. Second, building on previous work (Douze, *et al.*, 2020), it aims at consolidating our methodological approach by providing an in-depth analysis of the case of Donbass. Our main hypothesis here is that the complexity of the geopolitical situation in Donbass is reflected in its Internet topology. In addition, we provide a detailed explanation of data routing through the example of traceroute in order to provide pedagogical background for our BGP analysis.

The first section of this paper focuses on the general structure of the Internet at the routing level and its entanglement with geography. This section has mostly an illustrative purpose, by following the journey of several data packets on the worldwide network of cables, routers and protocols. The goal here is to give to the reader the key elements to understand how data routes actually work and how it can (or cannot) be represented from a topographical point of view. Eventually, these journeys give us a first insight into the geopolitical value of data routes, especially in conflictual spaces such as the disputed territories of Eastern Ukraine: data paths avoid the military frontline, sketching a new topological polarization of the network at the regional level, between Kiev and Moscow.

The second section seeks to systematize the empirical illustration depicted in the first section, by presenting a methodology for mapping the routes of the Internet using graph theory. Here, the method is used to analyse the general structure of the Ukrainian Internet, and to show how the polarization we sketched in Eastern Ukraine in the first section can actually be mapped and graphically represented. This cartography is eventually put into a wider perspective, as the technical structure of the network and its polarization correspond to some political and economic power dynamics — suggesting that a geopolitical cartography of data routes is possible.

1. Tracking data movements between Ukraine and Russia to understand the structure of Internet routing

When dealing with the geopolitics of cyberspace, one of the least studied — and yet most significant — protocols is BGP. Created in 1989, it regulates data transit between the different subnetworks of the Internet, the Autonomous Systems (ASes). BGP is the successor of several previous protocols which allowed early digital networks to transmit data from one computer to another. In the early days of the Internet, when the network was still working on the original ARPANET model, gateway protocols had a seemingly decentralized structure (Mathew, 2016). Every machine was a possible gateway, but a hierarchy between paths quickly emerged when some of them became important transit points for economic reasons (investments made on specific actors or infrastructures due to the massification of the Internet), but also political reasons (countries like Iran or China maintain a small number of international gateway so they can be easily controlled; Salamatian, *et al.*, 2019) or even geographical reasons (several remote regions or islands are still connected to the rest of the world via a limited number of gateways).

The contemporary Internet is a combination of ASes of unequal size, i.e. subnetworks with their own particular internal routing policies (hence this idea of autonomy carried in the name). Typically, an AS can be an Internet Service Provider, the network of a large university or a ministry, or the administrator of an optic fiber backbone. In a way, ASes are the elementary bricks that, connected together by BGP agreements [5], constitute the framework of the contemporary Internet. In November 2020, the Internet was made of about 70,000 active ASes [6].

Each AS possesses BGP agreements with several — but never all — other ASes on the Internet. BGP agreements are contractual relationships between AS administrators: as such they are the product of commercial, and sometimes political, negotiations. These autonomous entities are bounded by geographical limits: a cable is needed to connect two ASes, which is possible only when they share a common infrastructure. In other words, the agreements between autonomous systems are developed by human operators after taking into consideration the existing contingencies. Once the agreement is settled, it is included in the routing tables of the AS and daily uses are managed by automatic systems (routing algorithms) that are tasked with choosing the "best route" [7] to transport a data packet from point A to point B on the Internet. Consequently, to transit from point A to point B, a data packet will go through intermediary ASes, depending on the agreements negotiated by the actors involved.

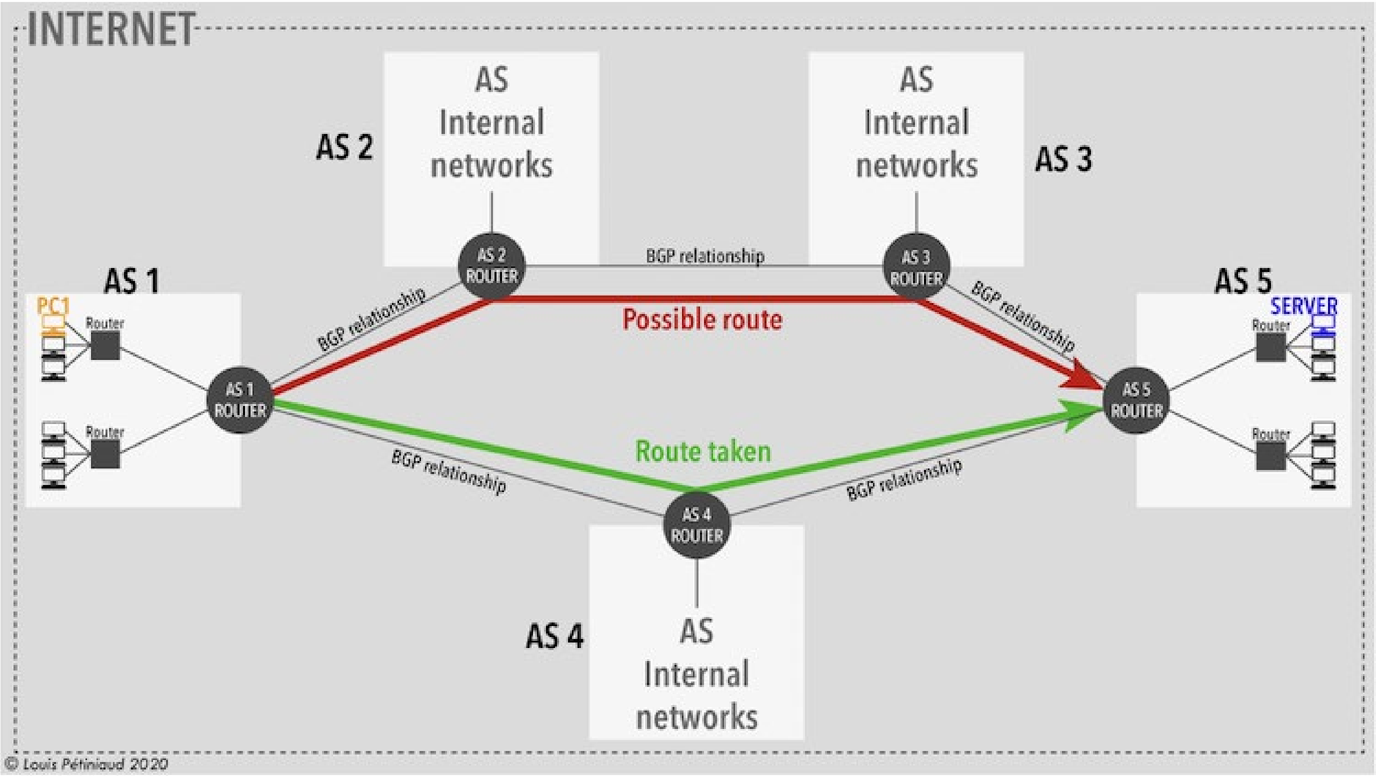


Figure 1: Simplified architecture of interconnections between Autonomous Systems.

In concrete terms, it means that a data packet sent by an Internet user from Dnipro (formerly Dnipropetrovsk) to Moscow will follow a route determined by BGP agreements, from one AS to another, until it reaches its final destination. Although these agreements are commercial and often confidential, these routes can be inferred and mapped.

To follow such a data packet, we use a traceroute command. This command was originally designed by the administrators of complex networks to monitor the performance of their networks. But it can be diverted for research purpose. Indeed, every time a packet transits through a router — called a "hop" — it signals to the sender that it has crossed this router. The signal sent by the data packet gives an IP address — *i.e.*, the unique string of numbers that identifies each computer on the Internet — that can be linked to a specific AS (despite difficulties and with a level of uncertainty as explained below). The infrastructures of this AS can in turn be located in a specific territory and registered under a specific jurisdiction. Altogether these methodologies allow us to track the technical routes the data take within the computer network and to match them with the geographical locations of the infrastructures in order to visualize the routes.

Limitations inherent to the methodology

There are limitations to the methodology because the geolocalization of IP addresses remains difficult for two main reasons. The first is political and organizational: the attribution of IP addresses to autonomous systems is regulated by the Internet Corporation for Assigned Names and Numbers (ICANN) and its regional registrars, as they act as the "guardians" of the tables of the global Internet. But, there is currently a shortage of IPV4 addresses (the last IVP4 address for the Eurasian zone, administered by RIPE, was assigned in November 2019 [8]), their market value increases and their circulation between systems is increasingly rapid: it has become impossible to keep registrars up to date in real time. For example, Russian IPs can be sold to an Asian operator that needs them but they are still registered as Russian in the registrars. In fact, it has fueled different traffics; hence, one of the pioneers of the Russian Internet, Alexei Soldatov, was arrested in December 2019 because he was accused of illegally transferring the ownership of 460,000 IPV4 addresses from a Russian research institution to his own firm [9].

The second explanation is technical: traceroutes infer the path taken by a packet after extracting the IP address of the router. But in practice, the administrators of the network have little interest in publicly identifying their internal architecture. For that reason, many IP addresses are programmed not to answer traceroute requests, or worse, to provide fake data. Furthermore, some ISPs delegate some of their IP addresses to their clients in order to let them administer the interconnection. It makes it more difficult to transform the observed path of IPs observed by the traceroute into an AS path [10].

Last but not least, a traceroute is an instant snapshot of the path taken by a packet. Given the fact that routers automatically choose what they identify as the "best" route (usually the fastest), it is possible that if we had made the same traceroute a few seconds earlier or later, it would have identified a slightly different path. Some tools allow to make multiple traceroutes [11] in order to compare results and to identify several major paths (Limonier, 2016), but they were not used for this paper as we value the following cases as methodological and pedagogical examples for introducing network-territory imbrications.

Example of a traceroute

The traceroute described below is an illustration of how the transportation of digital data works in practice [12].

Table 1: Data resulting from a traceroute command made in November 2019 from Dnipro to Moscow.

IP address	Name of router	Presumed AS number	Round trip time (milliseconds)
192.168.1.1 (**signal origin**)			1.875 ms
178.151.198.254	254.198.151.178.triolan.net	AS 13188	
10.65.200.65			2.369 ms
10.81.100.81			5.553 ms
87.245.239.217	xe120.RT.ATR.ZPR.UA.retn.net	AS 9002	3.607 ms
87.245.232.234	ae3-4.RT.IRX.FKT.DE.retn.net	AS 9002	50.15 ms
213.254.225.245	et-0-0-13.cr10-fra2.ip4.gtt.net	AS 3257	49.523 ms
213.200.122.182	ae3.cr1-stk3.ip4.gtt.net	AS 3257	78.315 ms

77.67.90.97	rostel-gw.ip4.gtt.net	AS 3257	61.991 ms
213.59.212.117 (**signal destination**)		AS 12389	64.183 ms

Table 1 lists the routers crossed by a data packet sent from Dnipro (Ukraine) to Moscow based on the information given by a traceroute request. Overall, our packet had to cross 10 routers (10 hops) to reach its destination, in about 78 milliseconds. During this trip, our packet crossed four different autonomous systems starting with AS13188, owned by Triolan, the Internet service provider that allowed us to send our request in Dnipro. This provider forwarded our packet during four hops before it was taken on by AS9002, administered by the firm RETN. This company is a transit provider, a data carrier dealing with long-distance data transits; it owns several terrestrial optic fiber backbones and specializes in carrying data from eastern to western Europe.

RETN then transmitted our packet to AS3257, property of GTT Network, a transit provider specialized in U.S.-Europe-Russia connections with several transatlantic cables of its own. After three hops, GTT Network transmitted the data to AS12389, property of Rostelecom and veritable “doorway” to the Russian network.

Routing and physical cartography

It is thus theoretically possible to map the route followed by packets, taking into account methodological limitations explained earlier: several elements disclosed by the traceroute command allow us to infer the path taken by the data packet, with a limited margin of uncertainty.

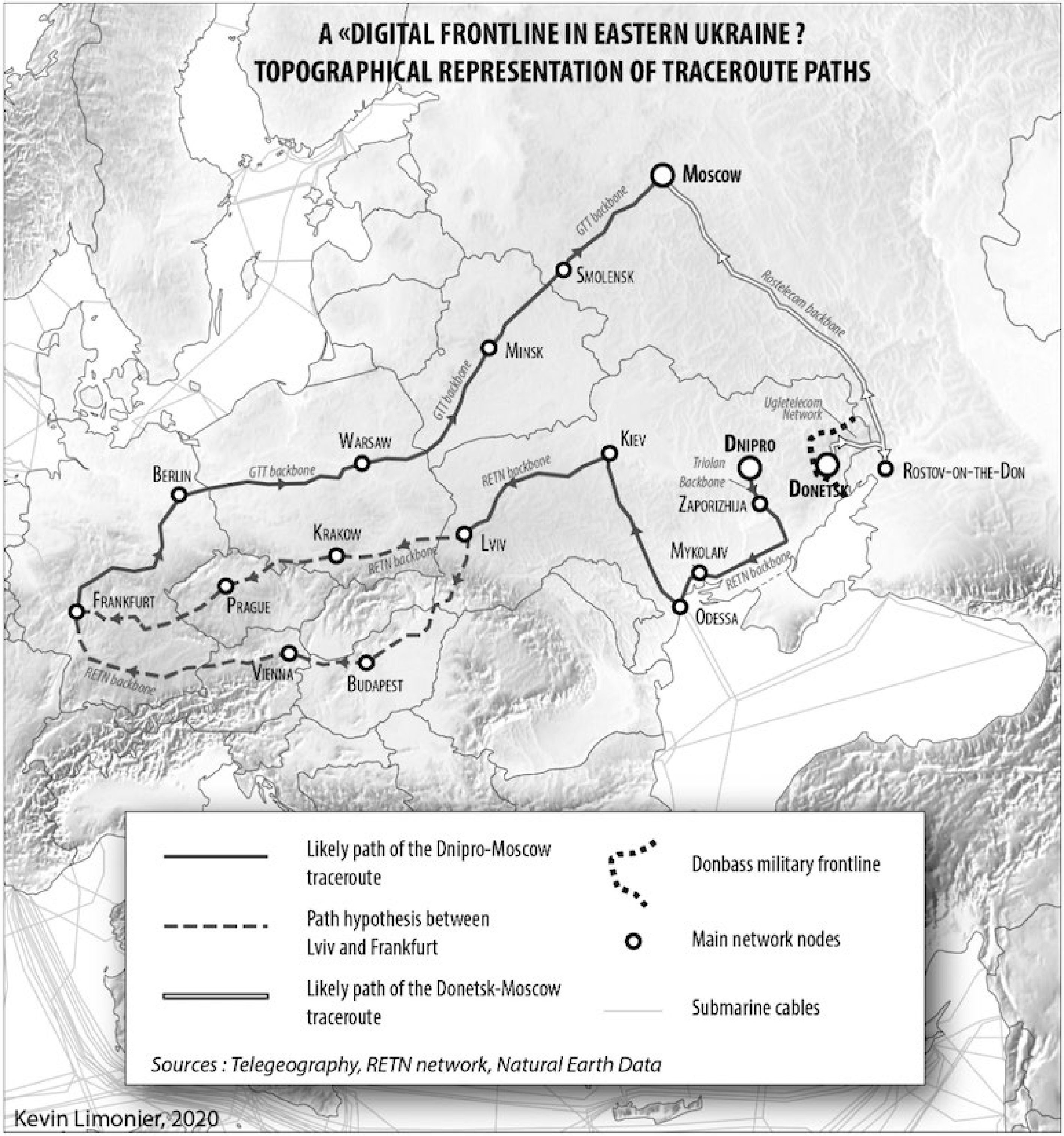


Figure 2: Topographical representation of traceroutes.

Concretely, a BGP agreement leads to the materialization of a physical connection between the routers of two ASes. These connections are usually established through dedicated facilities where routers of various ASes are connected to each other. There are several thousands of these facilities in the world today which constitute highly strategic points of the Internet. Some of them have a global reach and it would probably isolate several autonomous systems if they were to be disconnected.

These facilities are connected to each other through a network of terrestrial and submarine cables through which transit 99 percent of the data exchanged daily throughout the world (the remainder is transported via satellite) [13]. This network represents the “backbone” of the Internet: if a cable were to be cut, traffic would be severely disrupted and, if no alternative route exists, even completely interrupted.

In our example of Dnipro-Moscow traceroute, and as shown on Figure 2, we can stipulate with a high degree of certainty [14] that our packet was transported by Triolan from Dnipro to an exchange point situated several dozen kilometers south of the city, in Zaporizhia. In this town down the Dnieper, Triolan owns a physical connection with the RETN network, the second operator having taken over the packet to carry it on to Frankfurt. Between Zaporizhia and Frankfurt, we couldn’t precisely determine the paths taken by the data packet from the data we had: the routing was internal to RETN’s AS and we only have the information tracing external routings (between ASes). However, we were able to identify the two possible paths the data packet could have taken through a cartographic analysis of the infrastructures available on RETN’s Web site. These two pathways follow the same trail up to Lviv as RETN only owns one cable linking Zaporizhia to the eastern capital of Ukraine, via Mykolaiv, Odessa, and then north through Kiev. From Lviv, our packet may have followed the backbone to Frankfurt crossing Warsaw, Krakow, and Prague or it could have taken a more meridional path through the Carpathians (Uzhgorod), Budapest, Vienna, Salzburg, Munich, Stuttgart, and finally Frankfurt, the city being a veritable European “hub” for data exchange.

Indeed, the city hosts DE-IX, the largest public facility (also called IXP) in the world in terms of the volume of data exchanged [15]. Most of the data transiting between the United States, Europe, and the post-Soviet space go through the routers based in Frankfurt, a city that extends its central transportation nodality to cyberspace. Some of the largest Russian operators connect their own networks to some transit providers based in Frankfurt that administer submarine and terrestrial cables. As such, our packet was picked up by Rostelecom (the historical operator of Russian telecommunications) there, via the intermediary routers of the transit provider GTT Communication. Then, Rostelecom transported our data packet to Moscow through the Fastline cable that links the Russian capital to Frankfurt, following more or less the large road and train corridors that link Warsaw, Minsk and Smolensk together (Highway M1).

A digital frontline in Eastern Ukraine?

The packet we analyzed here made an important detour to reach its final destination: it carefully avoided the Russian-Ukrainian border and was delivered to Moscow through prominent international Network Service Providers (NSPs) and their infrastructures based in Frankfurt. Therefore, our data packet did not take a direct route between Ukrainian and Russian operators, which does not mean that none exists. On the contrary, several backbones link directly the two countries, but the available paths directly exchanged between them have sharply decreased after 2014 (F. Douzet, *et al.*, 2020). Although it remains difficult to assert that there is a direct correlation between the deterioration of the Ukrainian-Russian relation in the wake of the 2014 crisis and the diminishing number of paths between Ukraine and Russia, we can hypothesize that, in the midst of the ongoing conflict East of Ukraine, power rivalries and national security concerns have played a key role in drastic changes in data routes.

To test our observation from the other side of this hypothetical frontline of transit, we reproduced the same traceroute command, but with a starting point of the packet sent to Moscow within the territory of the separatist-controlled Donetsk People’s Republic (DNR, *Doneckaja Narodnaja Respublika*, Донецкая Народная Республика). From a connected terminal situated in the city of Donetsk (the capital of the self-proclaimed namesake republic), the path to Moscow was faster and simpler. When 11 hops were necessary to rally Dnipro to Moscow, via Western Europe, only three were needed to rally Donetsk to Moscow — hence seriously reducing the duration of the trip, from 78 to 13 milliseconds.

In Donetsk, our packet was taken by a local operator controlled by the separatists, Ugltelecom. The company, registered within the separatist authorities in Donetsk, owns an autonomous system registered in Rostov-on-Don (Russia), at an address used by other important ASes from the DNR network. Our packet — like most data sent from the region — was directly transported from Donetsk to Rostov, probably through the Russian border city of Kamensk-Shakhtinsky. From Rostov, the packet was immediately picked up by Rostelecom’s network, which quickly carried it to Moscow following the Voronezh-Lipetsk-Tula axis, according to maps published by the operator.

Following these two packets thanks to traceroute allowed us to have a first overview of what the situation might look like in Eastern Ukraine regarding route modifications in the frame of the war in Donbass. Of course, these two snapshots are not sufficient to conclude that there is a durable routing modification because of the war. For that, it would have been necessary to conduct at least thousands of traceroutes during a given range of time. But this allowed us to have a first insight on the technical and territorial logics we're dealing with, thus making it possible to develop a more systematic approach.

2. A topological analysis of post-Soviet territorial conflicts: The Donbass

This first insight can indeed be pushed further to understand the global restructuring of the Ukrainian network in the context of the ongoing crisis. Undertaking a traceroute study could be compared to following the trajectory of a car on superhighways. Similarly, the routing analysis that follows could be compared to the cartography of the network of highways and its evolution overtime. It therefore offers a global picture of all the possible routes a data packet can take as opposed to the actual route taken by the specific data packet we tracked. These routes are predetermined by BGP agreements linking ASes to each other. This information is not made public but can be inferred and mapped by our methodologies.

Representing the structure of Internet routes with a graph

This graph represents all existing ASes and BGP agreements connecting them. Put another way, it is a graphic representation of the entire set of paths that can be taken by a data packet to link together any of the represented points on the graph.

Each node on this graph is an autonomous system, and each link is a BGP agreement. In other words, this graph represents a vast proportion of all the available paths a data packet could take to go from one AS to another. The size of the nodes corresponds to the number of BGP agreements the AS maintains with the rest of the Internet. The colour of the nodes refers to the nationality the autonomous system announces in its Whois metadata.

Data collection methodology and limitations

This graph contains approximately 60,000 nodes and 220,000 links obtained by processing up to 30 BGP flows — announcing possible paths through a series of ASes — coming from different routers across the network. As a complete data collection methodology has been recently published (Douzet, *et al.*, 2020), we will only emphasize several limitations that need to be kept in mind when conducting a BGP graph analysis.

First, the BGP view is well-known to be incomplete (Gao, 2001; Ager, *et al.*, 2012). But even this incompleteness provides valuable geopolitical insights as many links reflect real economic strains and are therefore better indicators of the power relationships that shape the topology of the network.

Another shortcoming of a BGP analysis is usually caused by the incompleteness of the available information on AS owners stored in the Whois registry, as well as by the unreliability of IP geolocation databases at the regional and local levels, as we already mentioned earlier.

In addition, our graph is based on the routes available for data traffic and not on the quantification of the actual volume of traffic that circulates through these routes, as we cannot access this level of granularity in BGP data. Although these routes do not precisely indicate the amount of traffic, they allow us to understand how central a link is for the overall routing.

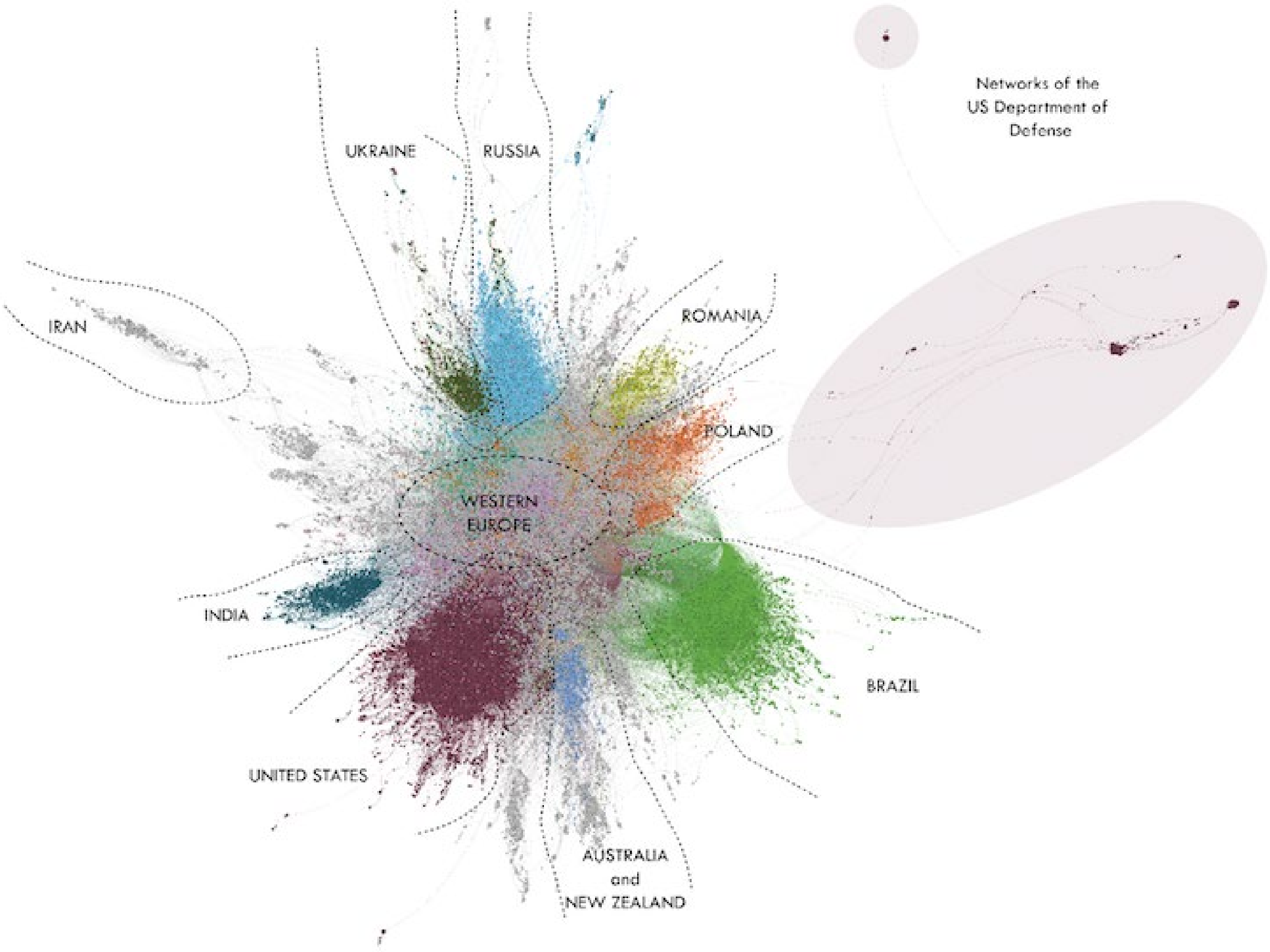


Figure 3: Worldwide graph representing all existing autonomous systems and the BGP agreements linking them.

Graph interpretation for geopolitical purposes

The precise arrangement of nodes (ASes [16]) has been determined by Force Atlas 2 [17], a spatialization algorithm often used in social sciences. Concretely, the closer to the center, the more relations the node possesses with the rest of the network. Hence, ASes with a central position in the graph are also central to the Internet in general: data packets transit more often through these central systems as they represent genuine switches for the Internet. This is also the case for the large NSPs — such as Level3, GTT, or Zayo — that link together geographically distant systems. Therefore, unlike with other types of cartographies, the centrality of some of the countries in this graph is not a deliberate choice of visual representation but the result of an algorithm that places at the center of the graph the nodes the most connected to the other nodes of the graph.

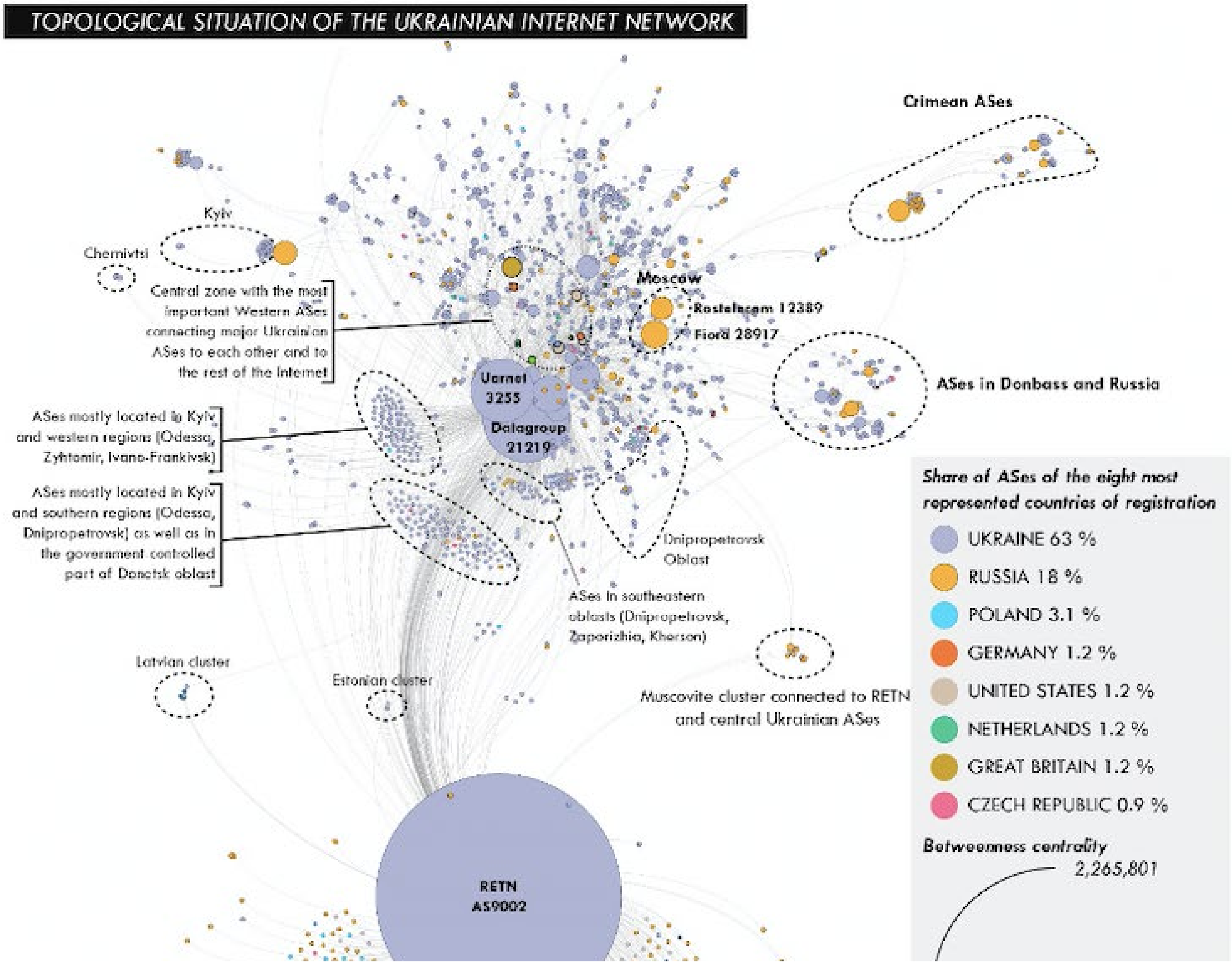
Conversely, the more peripheral the node, the more isolated it is from the rest of the network. This explains the presence of outgrowths such as the one situated in the upper right corner of the graph, the one representing the network of the U.S. Department of Defense. This military network is connected to the larger Internet through a few autonomous systems, for security reasons probably: the fewer doorways in and out of a network, the easier it is to control it.

Aside from centrality, proximity is another important notion on the graph: the closer the nodes, the greater the number of connections between them. For that reason, the autonomous systems of some countries are grouped together on this graph (they form clusters): at the center, western Europe holds an indisputable position, along with the United States. At the periphery, we can note several countries that are less connected to the rest of the network. Here, American actors are strikingly preeminent.

We can see that Russia and Ukraine are two “heavyweights” of the global Internet. Together, they account for almost 9,000 autonomous systems — 10 percent of the world’s total. Correlated to their population of Internet users, it means that, in Russia and Ukraine, there is one autonomous system for every 17,000 Internet users, compared to one for 40,000 in the rest of the world (and one for 31,000 in France) [18].

There is an historical explanation for this imbalance: like in the Western world (but unlike China or Cuba), the post-Soviet Internet emerged without any strong government regulations during the 1990s and 2000s, with a lot of ASes created by private persons or small companies. But on the contrary to what happened back then in Europe or in the U.S., the immensity of the Russian territory, along with the lack of investments in large Internet infrastructure projects did not lead to any kind of “simplification” of the AS network. Local ISPs providing Internet to small cities or villages did not disappear under the pressure of big nationwide actors, on the contrary to what happened in many other countries. Small ISPs in Russia or Ukraine were able to build their own local physical networks without facing serious competitors, thus gaining sometimes monopolistic positions at their level [19]. This situation of a persistent complexity still prevails today: according to the Russian accounting chamber, there were at least 15,433 ISPs in Russia in 2015 [20].

Analyzing the structure of the Ukrainian Internet


TOPOLOGICAL SITUATION OF THE UKRAINIAN INTERNET NETWORK
Crimean ASes
Kyiv
Chernivtsi
Central zone with the most important Western ASes connecting major Ukrainian ASes to each other and to the rest of the Internet
Moscow
Rostelecom 12389
Fiord 28917
ASes in Donbass and Russia
Uarnet 3255
Datagroup 21219
ASes mostly located in Kyiv and western regions (Odessa, Zyhtomir, Ivano-Frankivsk)
ASes mostly located in Kyiv and southern regions (Odessa, Dnipropetrovsk) as well as in the government controlled part of Donetsk oblast
Dnipropetrovsk Oblast
ASes in southeastern oblasts (Dnipropetrovsk, Zaporizhia, Kherson)
Latvian cluster
Estonian cluster
Muscovite cluster connected to RETN and central Ukrainian ASes
RETN AS9002
Share of ASes of the eight most represented countries of registration
● UKRAINE 63 %
● RUSSIA 18 %
● POLAND 3.1 %
● GERMANY 1.2 %
● UNITED STATES 1.2 %
● NETHERLANDS 1.2 %
● GREAT BRITAIN 1.2 %
● CZECH REPUBLIC 0.9 %
Betweenness centrality
2,265,801

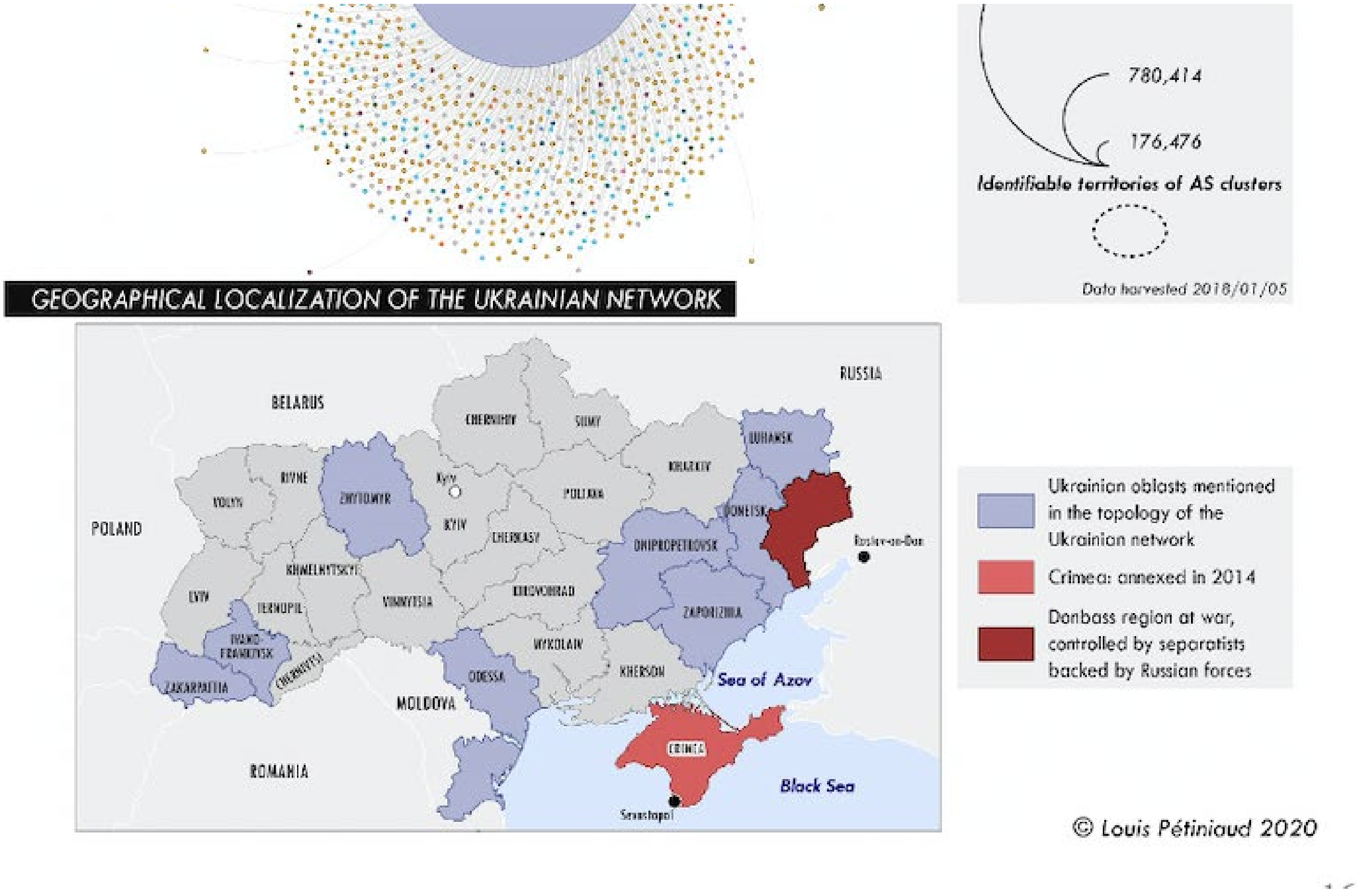


Figure 4: Connectivity architecture and territorialization of the Ukrainian network of Autonomous Systems, January 2018.

In order to observe the Ukrainian network, we used a selection of ASes. Figure 4 represents the set of ASes registered in Ukraine, and their immediate neighbors, that is to say the ASes with which Ukrainian ASes have signed BGP agreements, as of 5 January 2018. The color of a node reflects the country where it was registered, and the size of the node corresponds to its betweenness centrality. The betweenness centrality is a measure, for any given node, of the number of times the shortest paths between two other nodes of the graph cross it. It measures the probability for a given AS that a data packet traveling between any two nodes will transit through it.

First, we notice in Figure 4 the high number of ASes described above. This abundant ecosystem is highly polarized around major foreign actors.

Russia plays a predominant role in the connectivity of Ukraine. Russian ASes make up 18 percent of ASes in the “extended Ukrainian network” (Ukrainian ASes and their direct neighbors). A number of Russian ASes are intermediaries toward the global network, such as AS 12389 (Rostelecom [21]) and 28917 (Fiord [22]), two Eurasian transit operators. Russian ASes as a whole make up for about 35 percent of foreign ASes neighbouring the Ukrainian network. This figure has slightly decreased since 2013: at that time, 40 percent of neighbouring ASes of Ukraine were Russian.

In addition, a group of relatively large and central foreign ASes is noticeable at the heart of the national network, here with thick black outlines. They connect the biggest Ukrainian ASes with many other Ukrainian and foreign ASes of medium centrality. The United Kingdom, Germany, the United States, the Netherlands, and a few other states are the main gateways to the global Internet. This observation is confirmed by the analysis of the Ukrainian network conducted by Stas Yurasov in 2016 and published under the title *The eastern threat; or, How the Ukrainian network works* [23]. The author reminded his readers that if Russia played an important role in the Ukrainian network, “there [were] many more American and pro-American actors (large multinational companies)” there.

The case of AS 9002 (RETN) requires specific attention since it played an important role, at the time the data was collected, as a major intermediary between the Ukrainian network and many foreign ASes, including many distant ones not central to the Ukrainian network but important at the global level: operators based in South Korea, India, Turkey, or in the United States among others. Some of these ASes are indeed important for global connectivity.

We also notice on the graph several clusters corresponding to more or less circumscribed political territories. We can see the Latvian and Estonian states for example, and some Ukrainian cities are perfectly identified, such as Dnipro, the industrial capital East of the country. Kiev, the economic heart of the region, is well connected to the rest of the country through many small ASes identifiable throughout the graph.

Finally, some clusters in the graph are particularly remote from the heart of the system and can be noticed at the periphery of the graph. Most particularly, Donbass and Crimea appear in 2018 as clearly distinct from the Ukrainian network. To understand the significance and the importance of this pattern, we increased the granularity of the analysis and focused specifically on these ASes.

Territorial conflicts and topology: Reading geopolitical rivalries on Internet graphs

Our main hypothesis is that these patterns are strategically significant and reflect ongoing geopolitical power rivalries in the physical world. In Ukraine, the territories of Donbass and Crimea have followed very distinct territorial dynamics since the start of the crisis. In Donbass, the frontiers of the people’s republics of Donetsk and Luhansk are still evolving. They often changed at the start of the conflict between Kiev and the separatists, keeping pace with the fighting; but then, the movement slowed and frontier have stabilized almost completely since July 2016 [24]. In Crimea, however, the new frontier had fast been implemented, keeping with the border of the former Ukrainian Autonomous Republic of Crimea. Yet, some incidents have occurred now and then along a frontier [25] that has remained somewhat porous. The physical separation — an “high-tech frontier” [26] — was only achieved at the end of 2018.

We zoomed in Figure 5 to study the structure of connectivity in these territories. The observation shows the materialization, through BGP agreements, of new topological “frontiers” within the Ukrainian network in these two different territories.

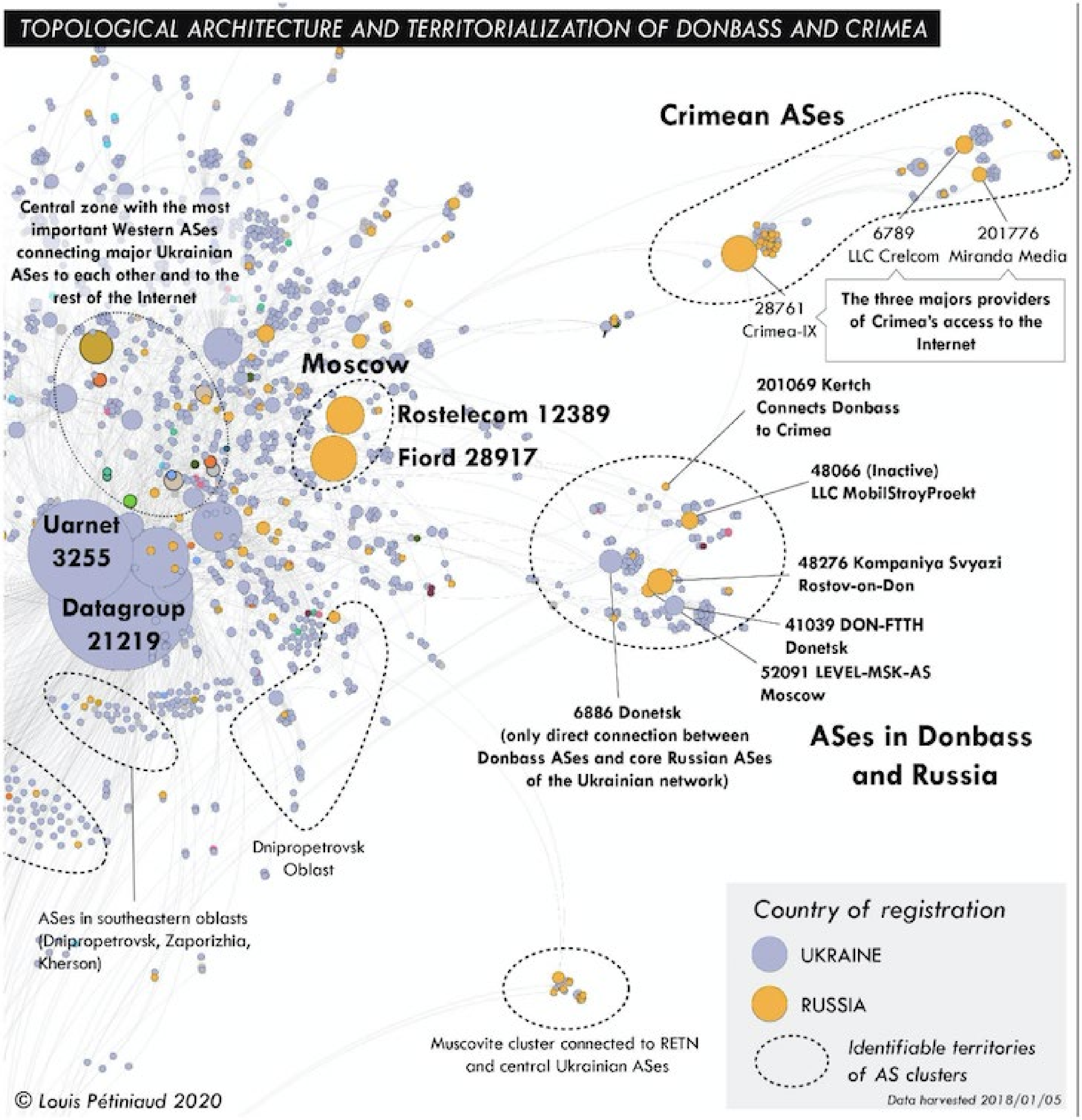

TOPOLOGICAL ARCHITECTURE AND TERRITORIALIZATION OF DONBASS AND CRIMEA
Crimean ASes
6789
LLC Crelcom
201776
Miranda Media
28761
Crimea-IX
The three majors providers of Crimea's access to the Internet
Central zone with the most important Western ASes connecting major Ukrainian ASes to each other and to the rest of the Internet
Moscow
Rostelecom 12389
Fiord 28917
201069 Kertch
Connects Donbass to Crimea
48066 (Inactive)
LLC MobilStroyProekt
Uarnet
3255
Datagroup
21219
48276 Kompaniya Svyazi
Rostov-on-Don
41039 DON-FTTH
Donetsk
52091 LEVEL-MSK-AS
Moscow
6886 Donetsk
(only direct connection between Donbass ASes and core Russian ASes of the Ukrainian network)
ASes in Donbass and Russia
Dnipropetrovsk Oblast
ASes in southeastern oblasts (Dnipropetrovsk, Zaporizhia, Kherson)
Country of registration
UKRAINE
RUSSIA
Identifiable territories of AS clusters
Data harvested 2018/01/05
Muscovite cluster connected to RETN and central Ukrainian ASes
© Louis Pétiniaud 2020

Figure 5: Connectivity architecture and the territorialization of the Autonomous Systems network in Donbass and Crimea (2018).

Figure 5 reveals the archipelagic structure of the subnetworks of Donbass and Crimea, with clusters relatively well separated from the rest of the network. From left to right, we can delineate loose agglomerations of ASes representing several regions of south and southeast Ukraine, and the large oblast of Dnipropetrovsk. On the right, we see three real clusters: Moscow, Donbass, and Crimea.

All of the ASes from Donbass and Crimea are grouped in two distinct archipelagos and form two clear spatial ensembles, reflecting the geopolitical separation between these territories. This harmony between topological ensembles (networks in clusters) and classical geopolitical ensembles (disputed territories partially isolated from Ukraine) appears very strong, although it is difficult to represent them on the same map. We can postulate that these two spatial ensembles are not simply superposed but actively interacting. This interaction is evident in the case of Crimea: the peninsula was integrated into Russia progressively after 2014. Through its infrastructures and the gradual closing of the northern frontier of the peninsula, Crimea was almost totally incorporated in the Federation after 2018, including at the level of its telecommunication infrastructures (Ermoshina, 2018). This is reflected in the structure of its connectivity, as we will see. In Donbass, however, the territory is still at war, and hasn't been *de facto* integrated into the Russian Federation. Its connectivity also moves progressively toward a greater closeness to the Russian network. But, compared to Crimea, the evolution of Donbass is slower and more erratic.

We can observe a number of differences between the 2018 situation and the regional connectivity before the start of the Ukrainian crisis. Figure 6 shows the interconnections of Ukrainian ASes and their neighbors in September 2013, three months before the first protestations in Kiev. We have highlighted significant ASes for the networks of Ukraine, Eastern Ukraine, and the Donbass region.

In order to analyze the situation of 2013, there is a methodological caveat which has to be mentioned. The AS numbers are allocated by Regional Internet Registries, and can go from one administrator to the other. In the case of the 2013 graph, we use geographic data (country and city of location) from 2018, for the reason that it is difficult to gather metadata from before the collection of BGP data. We can however postulate that intermediary ASes (such as small and medium-sized ISPs) rarely change their AS number or their city. This information is difficult to check, in part because of the lack of trustworthiness of available databases. Yet we are able to assess that in the graph below, few of the highlighted ASes' organizations have changed between 2013 and 2018. Luganet (AS39728) was, for an unknown amount of time, dubbed "malfik", at least between 2018 and 2019. CrimeaCom South LLC (AS28761) was in 2018 called "Crimea-IX". In 2013, it was however registered to a different organization, "Scientific-Industrial Enterprise Myst". The only AS today to bear this organization name (AS43802) is nowadays inactive [27]. The other ASes' organizations have remained the same between 2013 and 2018.

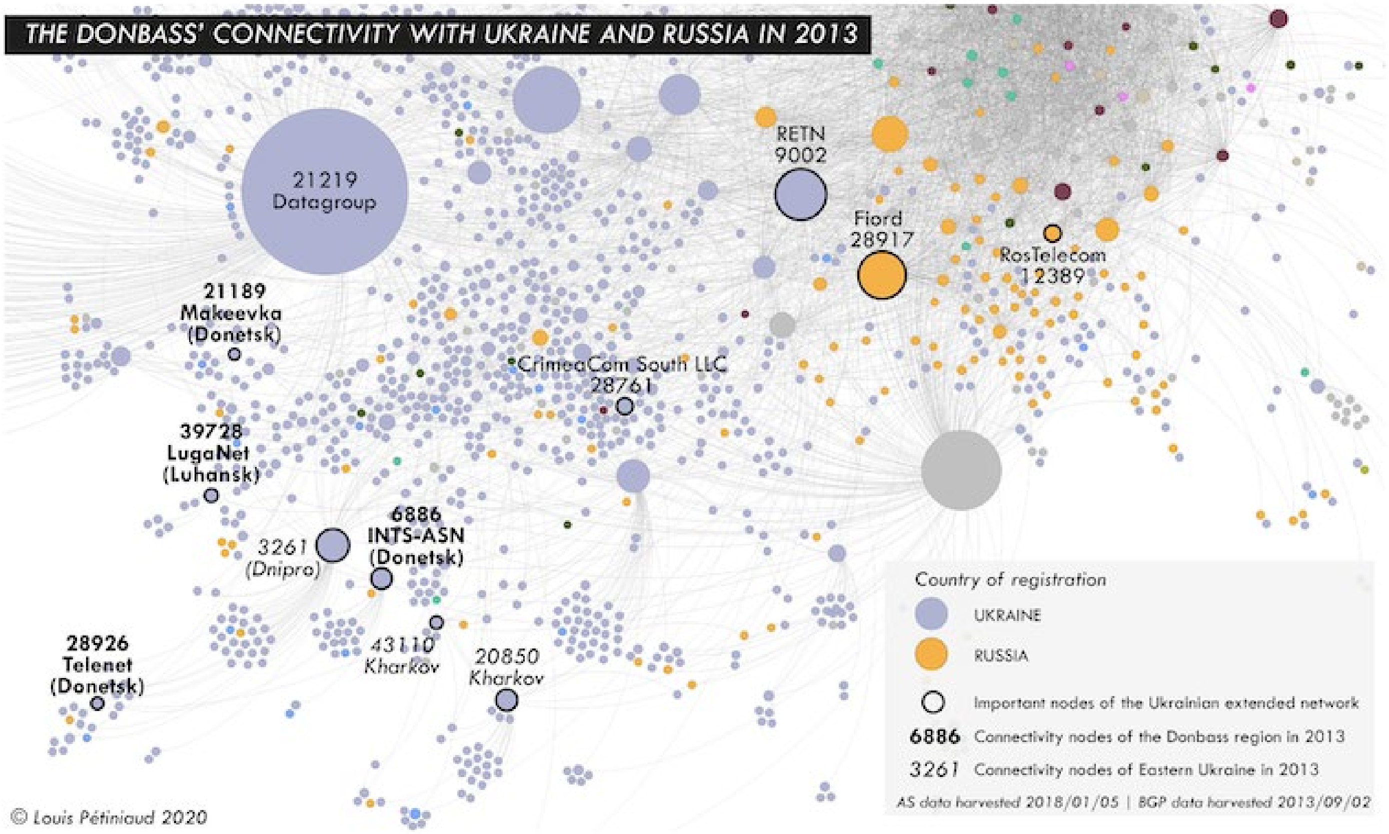

THE DONBASS' CONNECTIVITY WITH UKRAINE AND RUSSIA IN 2013
21219
Datagroup
RETN
9002
Fiord
28917
RosTelecom
12389
21189
Makeevka
(Donetsk)
CrimeaCom South LLC
28761
39728
LugaNet
(Luhansk)
6886
INTS-ASN
(Donetsk)
3261
(Dnipro)
43110
Kharkov
20850
Kharkov
28926
Telenet
(Donetsk)
Country of registration
UKRAINE
RUSSIA
Important nodes of the Ukrainian extended network
6886 Connectivity nodes of the Donbass region in 2013
3261 Connectivity nodes of Eastern Ukraine in 2013
AS data harvested 2018/01/05 | BGP data harvested 2013/09/02
© Louis Pétiniaud 2020

Figure 6: The Donbass' connectivity with Ukraine and Russia in 2013.

On this 2013 graph, we observe a sizable proportion of the extended Ukrainian network (ASes registered in Ukraine and their neighbors). We label on the graph both some of the major nodes of the Ukrainian networks (both Russian and Ukrainian ones), and the connectivity gateways of Eastern Ukraine. We differentiate between connectivity nodes of the Donbass region (in bold) and of the eastern part of the country as a whole (in italic). We notice two relevant results from this observation. First, the Donbass network is far more scattered in 2013 than in 2018, and it does not reveal any specific coherence, contrary to its situation in 2018. The connectivity nodes of Donbass (in bold, *e.g.*, AS6886 in Donetsk) are spread among the rest of Eastern Ukraines networks (in italic, *e.g.*, AS3261 in Dnipro). Second, the Eastern networks are located at the edge of Ukraines network (bottom left). In 2013, the Donbass was not as remote from Ukraine as in 2018, but it was already far from most of the Ukrainian ASes. However, they are located at the opposite side from the important Russian ASes for Ukrainian networks (top right). In 2013, Eastern Ukrainian ASes are obviously better integrated into the rest of the Ukrainian networks, but also much more separated from the Russian ones. We can find in 2013 no important connectivity node for the Donbass region that would be under any kind of dependency from Russian networks. Furthermore, most of them only have remote connections with the Russian stakeholders of the Ukrainian connectivity.

At the start of the war, important networks such as bank services in separatist territories were cut off by Kiev [28]. The self-proclaimed authorities in Donbass only became truly interested in the structure of their Internet networks in 2017. In fact, on 23 January 2017, armed men took control of the local branch of the operator Vega Telecom [29]. Vega Telecom is a Ukrainian operator owned by Ukrtelecom, property of the Ukrainian businessman Rinat Akhmetov, the most prominent oligarch of the Donbass region (Matuszak, 2012). As a consequence, a few weeks later, Ukrtelecom completely suspended its services in the occupied territories [30]. Early March as well, the Ukrainian operator LifeCell in turn lost control of its network in Donbass to the self-proclaimed authorities [31]. In 2017, the two republics even created their own ISPs: Feniks [32] for the Donetsk People's Republic, and Lugacom [33] in Luhansk. The separatist authorities' stranglehold on the regional network increased early 2018, probably after the rupture of an optic fiber backbone in the buffer zone keeping apart separatist troops from Ukrainian forces [34]. As a result, the graph of January 2018 highlights the clear separation of the Donbass networks from Ukraine, and their relative dependency on two ASes: AS 6886 and AS 48276. The first one is an operator connecting Donbass ASes to Russian providers from the core of Ukraine's networks, and the second one is Kompaniya Svyazi, an important network of Rostov-on-Don.

In addition, between 2018 and 2020, Donbass's dependency on Russia was reinforced. In August 2018, Telematika became one of the main service providers for the Donbass network. In June 2019, Telematika (AS 43201), registered in Rostov-on-Don, still remained the main gateway for the Donbass separatist republics (Douzet, *et al.*, 2020).

This topological analysis therefore reveals the impact of the Ukrainian conflict on the shape of cyberspace. The trends reflect the geopolitical situation. Between 2013 and 2018, the autonomous systems (ASes) of the separatist region of Donbass progressively broke away from the Ukrainian network and migrated toward the Russian network, increasing the dependency of Donbass over Russia for its connectivity. Yet Donbass ASes retained many links to Ukraine. As a result, Donbass now sits at the interface of Ukraine and Russia. In addition, our graphs show that Donbass has been relegated to the periphery of both networks, as it has been marginalized from the Ukrainian network but not fully integrated into the Russian network. These trends clearly reflect the geopolitical situation of Donbass, caught in between two stools, both in cyberspace and in the physical world. In return, this new shape of cyberspace creates new dependencies that have strategic implications as they affect the performance and security of Donbass's network for both public and private actors.

Conclusion

Observing connectivity graphs reveals many aspects of the connectivity structure of a country. Although the methodologies we developed present a number of limitations, they can provide very interesting insights on the strategies potentially developed by diverse actors to increase or maintain their power in the digital space, in a context of geopolitical power rivalries. These strategies have implications for the private sector as they can impact the performance and security of data routing and create potential threats to the integrity, availability and confidentiality of the circulating data.

Concretely, we noticed the dependence of an entire population to a limited number of specific actors. In Donbass, this dependency may not be total [35], but local inhabitants must now mainly rely on Russian operators for their connection to the Internet. This dependency is not a problem in itself. But some indispensable nodes connecting the region to the global Internet can effectively be subjected to Russian laws, rules or injunctions at the very moment when the Russian government is bringing the paths to, and within, the Internet under heightened control.

If the consequences of this rerouting are evident, the intentions behind it aren't clear. Indeed, it is now impossible to determine whether this rerouting was the result of a political, strategic, or military decision that aimed at reorganizing the separatist networks to limit, for example, the risk of being spied on, or of being disconnected, by the adverse side. It would require proving that a Russian and/or separatist strategy was devised to reorganize the network, based on a cartography of the network precise enough to make any change fully efficient. It would also involve a high level of cooperation between the government and the multiplicity of public and private actors that own and run different parts of the network's infrastructure. None of those hypotheses can be confirmed or disproved at this moment as it would require multiple interviews and fieldworks that are out of the scope of this study but could be an interesting continuation of it. However, it is evident that Russia has grown very proactive on these topics lately, with the law on a sovereign Internet coming into force — a text that promotes greater controls over the pathways inside and outside of the RuNet (Musiani, *et al.*, 2019; Limonier and Bertran, 2019).

Besides, the situation described in Donbass is not specific to this large region at war. It also applies to Crimea, pulled more severely away from the Ukrainian network after 2018, only to become closer to Russian networks. Today, the Crimean network is almost completely integrated in the Russian network (Douze, *et al.*, 2020) which is on par with its administrative, economic, and infrastructural integration within the Russian Federation. Further case studies are needed to understand whether this type of territorial appropriation in cyberspace has occurred in the midst of other open geopolitical conflicts or whether it is limited to this specific region.

At the very least, these topological transformations reinforce the current power rivalries in Ukraine and they might even be completely imbricated in them. With the installation of an architecture of dependency, services and transit providers are becoming crucial links for the availability of an Internet connection in strategic territories. Hence, these companies offer an important form of topological power to the political actors overseeing them. Thus, the topological reconfiguration of these territorial entities is one element of self-sustained dynamics. In those enclaved and disputed territories, a connectivity dependency risk is becoming even more significant as the Internet grows more strategic, *i.e.*, as its use becomes critical to the stability and prosperity of societies.

Finally, the methodology we developed in this paper questions the links between Internet and territorial control and suggests a way to map it and could be deployed on other cases outside of the Ukraine or even of the former Soviet Union. Comparison with other regions would allow to validate the systematic character of the protocols we developed, as we started to do with the case of Iran (Salamatian, *et al.*, 2019). In the same perspective, interesting developments could also be found in trans-disciplinary approaches, and especially with sociology. As geographers, we questioned the link between the network structure and its spatial and territorial significance. But it would definitely be of interest to also question its "social significance", as the role and the intentions of many actors participating in the network structure remains to be explored.

About the authors

Kevin Limonier is an associate professor in slavic studies and geography at the French Institute of Geopolitics (University of Paris-8). He is the vice-director of the GEODE research center (www.geode.science).
E-mail: klimonier02 [at] univ-paris8 [dot] fr

Frédérick Douzet is a professor in geopolitics at the French Institute of Geopolitics (University of Paris-8). He is the director of the GEODE research center.
E-mail: fdouzet [at] gmail [dot] com

Louis Pétiniaud is a Ph.D. candidate in geography at the French Institute of Geopolitics (University of Paris-8) and at the GEODE research center.
E-mail: l [dot] petiniaud [at] gmail [dot] com

Loqman Salamatian is a Ph.D. candidate in computer science at Columbia University and an associate researcher at the GEODE research center.
E-mail: ls3748 [at] Columbia [dot] edu

Kave Salamatian is a professor in computer science at the University of Savoie-Mont-Blanc and an associate researcher at the GEODE research center.
E-mail: Kave [dot] salamatian [at] univ-smb [dot] fr

Notes

[1] The entity behind the rerouting, named Telematika, is registered to the same address as the firm IPSvyaz, an operator hosting some official Internet Web sites of the Donetsk People's Republic, such as the Ministry of Finance of the DPR (www.minfindr.ru). Another company, named Future Communication LLC, is also registered at the same address and hosted, at the time of the changes, several other Web sites such as the main mobile phone operator in the Luhansk People's Republic, but also mail servers for several ministries.

[2] Federal law № 90-F3 from 5 January 2019 — http://publication.pravo.gov.ru/Document/View/0001201905010025?index=0&rangeSize=1, accessed 19 March 2021.

[3] Territories under DNR (Donetsk People's Republic) and LNR (Lugansk People's Republic) control, as well as the anti-terrorist operation zone established by the Ukrainian government in the region.

[4] See "China builds 'Digital Silk Road' to bypass India for Pakistani internet traffic," *Tribune* (6 February 2021), at https://tribune.com.pk/story/2282931/china-builds-digital-silk-road-to-bypass-india-for-pakistani-internet-traffic, accessed 14 February 2021.

[5] Two types of agreements exist: peering and customer links. A peering link is set up when two ASes agree to share

roughly the same equivalent of traffic for free. Customer-top-provider (c2p) links are set up in the case of one AS paying another AS for access.

[6] https://www.potaroo.net/tools/asn32/, accessed 19 March 2021.

[7] Technical experts often refer to the "shortest" route because, in a network, the best route is often the one that transits through the least number of ASes. But, from the perspective of network operators, the best route is not always the shortest one. Many criteria exist to define a "best path", including its financial cost, its speed, the number of nodes on the route, its kilometric distance, its safety and so on. See, for example, https://labs.ripe.net/Members/gih/bgp-more-specifics-routing-vandalism-or-useful, accessed 19 March 2021.

[8] On 25 November 2019 at 3:35 PM UTC+1, RIPE NCC (Réseaux IP Européens — Network Coordination Centre), the European Regional Internet registry made its last IPV4 allocation due to shortage of such addresses. The IPV4 protocol was first described in 1980 and progressively became one of the core protocols of the Internet. IPV4 addresses (such as 192.168.0.1) use 32-bit space, which theoretically provide 4,294,967,296 unique addresses. When the protocol was first described in 1980, it was supposed to last a very long time, as the number of allocated addresses was very low. The massification of the Internet in the 1990s and the 2000s, as well as the development of the "Internet of things" (IoT) consumed IPV4 addresses much faster than expected, as every connected device such as a router or a server corresponds to an IPV4 address. Today, RIPE and other registries are progressively implementing IPV6, which is meant to replace IPV4.

[9] See https://www.bbc.com/russian/news-50912682, accessed 19 March 2021.

[10] See https://dl.acm.org/doi/pdf/10.1145/863955.863996, accessed 19 March 2021.

[11] It is the case of Nmap, an open-source network scanner.

[12] The traceroute commands haven't been designed to follow the routing precisely. They simply indicate an IP address and the name of the router it crossed.

[13] https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.20-2019-PDF-E.pdf, accessed 19 March 2021.

[14] The conversion of our traceroutes into georeferenced data has here been made via a qualitative analysis. To do so, we identified all the infrastructures that are administered by companies who own different ASes that our data went through. Usually, such information is available on Web sites of these companies, as they most of the time are either ISPs, either tier-1 or tier-2 networks — that is to say services that provide connections between distant ISPs. This information is purely declarative and for commercial purposes, and does not allow us to geo-reference a path with complete certainty.

[15] On 28 April 2020, according to the data gathered by Packet Clearing House: https://www.pch.net/ixp/dir#!mt-sort=traf%2Cdesc!mt-pivot=traf, accessed 28 April 2020.

[16] ASes can be of different types: governmental, private, universities, etc.

[17] Force Atlas 2 is a visualization algorithm that creates a graphic representation of a network. Underlying it is the possibility to simulate a mechanical system to spatialize the graph. Two nodes repel each other while an edge brings them closer. These forces entice movements in the system until it reaches an equilibrium; this representation is interesting to understand the diverse interactions between the actors of a network.

[18] Estimations based on data provided by ipinfo.io and the World Bank.

[19] For a case study about small local Russian ISPs, see Kevin Limonier, 2014. "Russia in cyberspace: Issues and representations," *Hérodote*, volume 152–153, number 1, pp. 140–160.

[20] *Bulletin of the Accounts Chamber of the Russian Federation* № 7 (211), 2015, p. 18, https://old.ach.gov.ru/upload/uf/031/03161d2a9f99123823f5cea5341d7977.pdf, accessed 19 March 2021.

[21] https://www.company.rt.ru, accessed 19 March 2021.

[22] http://www.fiord.ru/, accessed 19 March 2021.

[23] Stas Yurasov, 2016. “Ugroza s vostoka.” See https://project.liga.net/projects/eastern_threat/, accessed 2 January 2020.

[24] The Web site https://liveuamap.com/ charted precisely this evolution since the start of the conflict. See also, the series by the *New York Times* (“Ukraine crisis in maps”) that has been regularly updated since 2014: https://www.nytimes.com/interactive/2014/02/27/world/europe/ukraine-divisions-crimea.html, accessed 1 January 2019.

[25] https://www.theguardian.com/world/2016/aug/10/russia-accuses-ukraine-of-armed-crimea-incursion, accessed 10 January 2019.

[26] “The fence, [...] is topped with barbed wire and has hundreds of sensors. [...] Most of its sensors pick up vibrations from any potential intruders, the FSB said, but some are also radio-location devices,” in “Ukraine conflict: Russia completes Crimea security fence,” https://www.bbc.com/news/world-europe-46699807, accessed 2 January 2020.

[27] https://ipinfo.io/AS43802, accessed 12 November 2020.

[28] https://www.theguardian.com/world/2014/nov/26/ukraine-banks-suspend-services-pro-russia-donetsk, accessed 4 January 2020.

[29] https://www.telegeography.com/products/commsupdate/articles/2017/01/27/vegas-donetsk-branch-occupied-by-gunmen/, accessed 4 January 2020.

[30] http://en.mediasat.info/2017/03/02/ukrtelecom-cuts-off-communication-in-the-occupied-donetsk-region-because-of-following-its-offices-seizure/, accessed 4 January 2020.

[31] https://www.telegeography.com/products/commsupdate/articles/2017/03/03/ukrtelecom-lifecell-lose-control-of-donetsk-networks-to-rebels, accessed 4 January 2020.

[32] http://dnr-phoenix.ru, accessed 4 January 2020.

[33] https://lugacom.com, accessed 4 January 2020.

[34] https://www.telegeography.com/products/commsupdate/articles/2018/01/16/separatists-threaten-takeover-of-vodafone-ukraine-network-in-donetsk-luhansk-after-five-day-shutdown/, accessed 4 January 2020.

[35] It is impossible to assert full control of it. The inherent incompleteness of the data collected by RIPE or Routeviews does not allow us to cover exhaustively the entire network.

References

Paul C. Adams, 1997. “Cyberspace and virtual places,” *Geographical Review*, volume 87, number 2, pp. 155–171.
doi: https://doi.org/10.1111/j.1931-0846.1997.tb00069.x, accessed 18 April 2021.

Bernhard Ager, Nikolaos Chatzis, Anja Feldmann, Nadi Sarrar, Steve Uhlig, and Walter Willinger, 2012. “Anatomy of a large European IXP,” *SIGCOMM ’12: Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, pp. 163–174.
doi: https://doi.org/10.1145/2342356.2342393, accessed 18 April 2021.

Valeriy Akimenko and Keir Giles, 2020. “Russia’s cyber and information warfare,” *Asia Policy*, volume 15, number 2, pp. 67–75.
doi: https://doi.org/10.1353/asp.2020.0014, accessed 18 April 2021.

John Allen, 2016. *Topologies of power: Beyond territory and networks*. London: Routledge.
doi: https://doi.org/10.4324/9780203101926, accessed 18 April 2021.

Dominique Arel, 2018. “How Ukraine has become more Ukrainian,” *Post-Soviet Affairs*, volume 34, numbers 2–3, pp. 186–189.

doi: https://doi.org/10.1080/1060586X.2018.1445460, accessed 18 April 2021.

D.S. Artamonov, 2017. “Souveraineté informationnelle, aspect théorique,” In: D.V. Belenkov, P.A. Gjulazjan, and D.È. Mazlumjan, 2018. *Souveraineté informationnelle de la Russie et de l’Union européenne, politique de l’information et guerre informationnelle: essence et contenu. Bulletin international des sciences pour les étudiants, Université d’État de Saint Pétersbourg*, number 5, pp. 12. [in Russian]

Boris Beaude, 2015. “Spatialités algorithmiques,” In: Alberto Romele and Marta Severo (editors). *Traces numériques et territoires*. Paris: Presses des Mines, pp. 135–162.

Hélène Bergues, 1981. “Raffestin Claude — *Pour une gographie du pouvoir*,” *Population*, volume 36, number 6, p. 1,201.

Dominique Boullier, Maxime Crépel, and Mathieu Jacomy, 2016. “Zoomer n’est pas explorer. Spatialiser les graphes, catégoriser et (dé)construire les réseaux,” *Réseaux*, volume 1, number 195, pp. 131–161.
doi: https://doi.org/10.3917/res.195.0131, accessed 18 April 2021.

Rogier Creemers, 2020. “China’s conception of cyber sovereignty,” In: Dennis Broeders and Bibi van den Berg (editors). *Governing cyberspace: Behavior, power and diplomacy*. Lanham, Md.: Rowman & Littlefield, pp. 107–142.

Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapé, 2014. “Analysis of country-wide Internet outages caused by censorship,” *IEEE/ACM Transactions on Networking*, volume 22, number 6, pp. 1,964–1,977.
doi: https://doi.org/10.1109/TNET.2013.2291244, accessed 18 April 2021.

Frédérick Douzet, 2014. “La géopolitique pour comprendre le cyberespace,” *Hérodote*, volumes 1–2, numbers 152–153, pp. 3–21.
doi: https://doi.org/10.3917/her.152.0003, accessed 18 April 2021.

Frédérick Douzet, Louis Pétiniaud, Loqman Salamatian, Kevin Limonier, Kavé Salamatian, and Thibaut Alchus. 2020. “Measuring the fragmentation of the Internet: The case of the Border Gateway Protocol (BGP) during the Ukrainian crisis,” *2020 12th International Conference on Cyber Conflict (CyCon)*, pp. 157–182.
doi: https://doi.org/10.23919/CyCon49761.2020.9131726, accessed 18 April 2021.

Myriam Dunn Cavelty, 2013. “From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse,” *International Studies Review*, volume 15, number 1, pp. 105–122.
doi: https://doi.org/10.1111/misr.12023, accessed 18 April 2021.

Ksenia Ermoshina, 2019. “For code and country: Civic hackers in contemporary Russia,” In: Mario Biagioli and Vincent Antonin Lépinay (editors). From *Russia with code: Programming migrations in post-Soviet times*. Durham, N.C.: Duke University Press, pp. 87–112.
doi: https://doi.org/10.1215/9781478003342-004, accessed 18 April 2021.

Ksenia Ermoshina, 2018. “yber annexation: Information control and digital security in Crimea,” *Personal Democracy Forum*, at https://www.youtube.com/watch?v=rDeM9kC7tko, accessed 18 April 2021.

Ksenia Ermoshina and Francesca Musiani, 2017. “Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era,” *Media and Communication*, volume 5, number 1, pp. 42–53.
doi: http://dx.doi.org/10.17645/mac.v5i1.816, accessed 18 April 2021.

Lixin Gao, 2001. “On Inferring autonomous system relationships in the Internet,” *IEEE/ACM Transactions on Networking*, volume 9, number 6, pp. 733–745.
doi: https://doi.org/10.1109/90.974527, accessed 18 April 2021.

Gabrielle Hecht, 1998. *The radiance of France: Nuclear power and national identity after World War II*. Cambridge, Mass.: MIT Press.
doi: https://doi.org/10.7551/mitpress/7822.001.0001, accessed 18 April 2021.

Andreas Kappeler, 2014. “Ukraine and Russia: Legacies of the imperial past and competing memories,” *Journal of Eurasian Studies*, volume 5, number 2, pp. 107–115.

doi: https://doi.org/10.1016/j.euras.2014.05.005, accessed 18 April 2021.

Polina Kolozaridi and Dmitry Muravyov, 2020. "The narratives we inherit: The local and global in Tomsk's Internet history," *Internet Histories*, volume 4, number 1, pp. 49–65.
doi: https://doi.org/10.1080/24701475.2020.1723980, accessed 18 April 2021.

Mihajl Mihajlovitch Kučerjavyj, 2014. "Politique d'État pour la souveraineté informationnelle de la Russie dans un monde moderne mondialisé," *Conseil en gestion*, number 9, pp. 7–14. [in Russian]

Yves Lacoste, 2014. *La géographie, ça sert, d'abord, à faire la guerre*. Paris: La Découverte.

Yves Lacoste (editor), 1993. *Dictionnaire de géopolitique*. Paris: Flammarion.

Daniel Lambach, 2020. "The territorialization of cyberspace," *International Studies Review*, volume 22, number 3, pp. 482–506.
doi: https://doi.org/10.1093/isr/viz022, accessed 18 April 2021.

Jérémie Leguay, Matthieu Latapy, Timur Friedman, and Kav Salamatian, 2007. "Describing and simulating Internet routes," *Computer Networks*, volume 51, number 8, pp. 2,067–2,085.
doi: https://doi.org/10.1016/j.comnet.2006.10.008, accessed 18 April 2021.

Dave Levin, Lee Youndo, Luke Valenta, Zhihao Li, Victoria Lai, Cristian Lumezanu, Neil Spring, and Bobby Bhattacharjee, 2015. "Alibi routing," *SIGCOMM '15: Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, pp. 611–624.
doi: https://doi.org/10.1145/2785956.2787509, accessed 18 April 2021.

Kevin Limonier, 2018. *Ru.net: Géopolitique du cyberespace russophone*. Paris: Les eéditions L'Inventaire.

Kevin Limonier, 2016. "Cartographier les routes de l'Internet grce à La commande Traceroute: L'exemple du Caucase du sud," *Poussière d'empire*, at https://villesfermees.hypotheses.org/410, accessed 18 April 2021.

Kevin Limonier and Marie-Gabrielle Bertran, 2019. "Russie: Vers un Internet souverain?" *Diplomatie*, number 101, pp. 33–37.

Ashwin J. Mathew, 2016. "The myth of the decentralised Internet," *Internet Policy Review*, volume 5, number 3.
doi: https://doi.org/10.14763/2016.3.425, accessed 18 April 2021.

Sławomir Matuszak, 2012. "The oligarchic democracy. The influence of business groups on Ukrainian politics," *OSW Studies*, number 42, at https://www.osw.waw.pl/en/publikacje/osw-studies/2012-10-16/oligarchic-democracy-influence-business-groups-ukrainian-politics, accessed 18 April 2021.

Francesca Musiani, Benjamin Loveluck, Françoise Daucé, and Ksenia Ermoshina, 2019. "Souveraineté numérique: l'Internet russe peut-il se couper du reste du monde?" *The Conversation* (18 March), at https://theconversation.com/souverainete-numerique-linternet-russe-peut-il-se-couper-du-reste-du-monde-113516, accessed 18 April 2021.

Louis Pétiniaud and Loqman Salamatian, 2019. "Geopolitics of routing," RIPE Labs, at https://labs.ripe.net/author/louis_petiniaud/geopolitics-of-routing/, accessed 18 April 2021.

Jean Radvanyi and Marlène Laruelle (editors), 2016. *La Russie, entre peurs et défis*. Paris: Armand Colin.

Loqman Salamatian, Frederick Douzet, Kevin Limonier, and Kav Salamatian, 2019. "The geopolitics behind the routes data travels: A case study of Iran," arXiv:1911.07723 (19 November), at https://arxiv.org/abs/1911.07723, accessed 18 April 2021.

Adam Segal, 2020. "China's vision for cyber sovereignty and the global governance of cyberspace," *National Bureau of Asian Research, special report*, number 87, at https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/, accessed 18 April 2021.

Olga Shumilo, Tanel Kerikme, and Archil Chochia, 2019. "Restrictions of Russian Internet resources in Ukraine:

National security, censorship or both?" *Baltic Journal of European Studies*, volume 9, number 3, pp. 82–95.
doi: https://doi.org/10.1515/bjes-2019-0023, accessed 18 April 2021.

Ryan Singel, 2008. "Pakistan's accidental YouTube re-routing exposes trust flaw in net," *Wired* (25 February), at https://www.wired.com/2008/02/pakistans-accid/, accessed 18 April 2021.

Ye Tian, Ratan Dey, Yong Liu, and Keith W. Ross, 2012. "China's Internet: Topology mapping and geolocating," *2012 Proceedings IEEE INFOCOM*, pp: 2,531–2,535.
doi: https://doi.org/10.1109/INFCOM.2012.6195646, accessed 18 April 2021.

Daniel Voelsen, 2019. "Cracks in the Internet's foundation. The future of the Internets infrastructure and global Internet governance," *Stiftung Wissenschaft und Politik, Research Paper*, number 14.
doi: https://doi.org/10.18449/2019RP14, accessed 18 April 2021.

Pamela Zave and Jennifer Rexford, 2019. "The compositional architecture of the Internet," *Communications of the ACM*, volume 62, number 3.
doi: https://doi.org/10.1145/3226588, accessed 18 April 2021.

E.G. Zorina, 2017. "Souveraineté informationnelle de l'État moderne et principaux instruments permettant de l'assurer," *Izv. Saratov Université, (N.S.) Sociologie. Sciences politiques*, volume 17, number 3, pp. 345–348. [in Russian]

Editorial history

Received 2 April 2021; accepted 7 April 2021.

Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine
by Kevin Limonier, Frédérick Douzet, Louis Pétiniaud, Loqman Salamatian, and Kavé Salamatian.
First Monday, volume 26, number 5 (May 2021).
doi: https://dx.doi.org/10.5210/fm.v26i5.11700