International Workshop “Internet, Digital Data, Power and Rivalries in the Post-Soviet Area”

Campus Condorcet, Paris, November 25th 2019

Detailed Programme

9:00 AM : registration and coffee

9:30 AM : Keynote : Kevin Limonier, French Institute of Geopolitics / GEODE

10:00 AM – 12:00 AM : Panel 1 : Between the keyboard and the chair : representations and strategies of the post-soviet Internet actors.

Discussant : Jean-Robert Raviot, Université Paris Ouest la Défense.

The SyTech hack, and what can be drawn from it about Russia in terms of geopolitics

Marie Gabrielle Bertran (French Institute of Geopolitics / GEODE)

Saturday 13th July, the homepage of the internet site of the SyTech company has been defaced (malevolently modified) with a YoBa face. This act of defacement was the signature of a misdeed by a group of crackers (criminal hackers or Black Hats), which had just stolen an enormous bunch of data from the SyTech enterprise: a FSB contractor. By this major hack, the group - called 0v1ru$ - just accomplished the most important breach and data theft in the history of the Russian intelligence services. About 7,5 To of critical data were stolen during the attack. After the hack, they contacted Digital Revolution, another group of crackers which already had attacked a contractor of the FSB in December 2018. This second group used his Twitter account to spread the news of the attack: just like it did in 2018, after the hack of servers belonging to the Kvant research company.

What does that mean in terms of geopolitics? Geopolitical problematics encompass different forms of rivalries and antagonisms involving territorial disputes, or territorial claims, by different type of actors. These claims are always related to the fact that these actors intend to act on, or organize, territories that they perceive as their own. Or as some areas on which their governance or their influence should prevail. The two cases we will touch on here also affect several type of actors: Russian private corporations, the Russian State, and the attackers, who probably are engineers and developers since they were able to deal with the technical part of the cyber attacks. These cases also imply divergences

of perception around several territories: first, the cyberspace, which is employed here as a vehicle to convey cyberattacks. Then, the territory of the Russian Federation, where the Russian government intends to apply its control (policies).

So, we will study the geopolitical aspects which can be drawn from these two leak cases: first, through the analysis of the leak which was performed by Digital Revolution, which is the first known example of a successful attack against servers belonging to a FSB contractor. Then, we will analyse the SyTech hack, and what it reveals about the new Russian policies about cyber and information issues.

Geopolitics of cryptocurrencies mining in Russia. The example of the Irkutsk region, the cryptominers « Siberian Eldorado ».

Hugo Estecahandy (GEODE)

Since 2016, bitcoin mining has been developing in the Russian Federation. The "mining", process of creating this cryptocurrency, requires specific needs in natural or artificial resources in order to operate specific processors. The geographical distribution of cryptocurrencies mining's physical infrastructures finds a spatial logic according to the distribution of its needs across the country. The Irkutsk Oblast, in Siberia, hosts most of this activity because it is the most competitive of the Russian regions for miners. The Oblast offers one of the cheapest electricity in the country and in large quantities: electricity is the most important factor in cryptocurrencies mining. The natural cold that prevails in the region most of the year also makes it possible to save electricity on cooling the processors. Finally, the space is crossed by the Trans Europe-Asia (TEA) optic fiber backbones, providing a fast Internet connection, allowing miners to quickly communicate their results to the rest of the decentralized Bitcoin network. Cryptocurrencies mining in the Irkutsk Oblast involves a wide variety of actors : from large companies with large "mining farms" - equivalent in size and needs to large datacenters - to individuals with processors in their living rooms, and to local entrepreneurs who have seen mining as an interesting business. All this, while no legislation on cryptocurrencies has yet been adopted in the country.

Estonia, a cyber power: how Russia and Russian threat actors shaped Estonian cyber-defense and cyber-security

Léa Ronzaud (Graphika)

This presentation will give an overview on how Estonia has emerged as a powerful cyber country in a context of decades-long tensions with Russia. Over the last fifteen years, Estonia established itself as key player in both cyber-defense and e-governance, fueling the narrative with constant innovation and using its leading position to advocate for increasing resilience capabilities and implementing standardized cyber-norms for international institutions. Far from being an organic process, the development of Estonian cyber defense, cyber security and e-governance is deeply rooted in a geopolitical, ideological and historic context. The heated relationship between Estonia and the Russian Federation laid the foundations of a digitalized state and of a fertile ecosystem for technology to develop. Amid ethnic tensions, the country, after suffering disruptive cyber-attacks attributed to Russia in 2007, invested in both digital governance and cyber-security to the point that it became a pioneer in both fields.

Title TBA

Vincent Lepinay (Médialab, Sciences Po)

Abstract TBA

12:00 AM – 1:30PM : Lunch

1:30 PM – 3:45 PM Panel 2 : The routes of the post-soviet Internet : protocols, measurements and cartography

Discussant : Alberto Dainotti (CAIDA, University of California)

At the edge of the "Ru.net": a topological analysis of Crimean network architecture

Thibaut Alchus (French Institute of Geopolitics)

Since 2014, Crimea has undergone a profound restructuring of its digital ecosystem and connectivity architecture. Interestingly, and alongside with tailored Internet censorship practices developed by Russia to monitor the transition period, the Crimean subnetwork became by itself a target for long-term and peculiar strategies of control.

Thus, a geopolitical analysis of key actors, network measurements and routing data could path the way to a better understanding of topological strategies designed by Russia to project its sovereignty into the peninsula. As the Federation today struggles to implement the forthcoming "isolation" of the Russian segment of the Internet, it seems opportune to discuss how power rivalries shaped the Crimean network landscape since its annexation.

This presentation will therefore focus on the current situation of Crimea as a peripheral grey-zone at the edge of the "Ru.net". Based on a one-year study conducted with Geode and the French Institute of Geopolitics, we will present dedicated methods to map the Crimean cyberspace, quantify autonomous systems' centrality, and analyze macroscopic topological position of the peninsula in its regional environment.

From the lack of oversight to government censorship: the Ukrainian Internet in wartime

Antoine Delaunay (French Institute of Geopolitics)

In an over-competitive setting, several thousands of Internet Service Providers (ISP) have emerged in Ukraine since its independence, preventing any actor from gaining a monopoly over the industry. The State's lack of interest in developing the country's Internet connectivity has left private actors in charge of deploying, often inefficiently, the necessary infrastructures. However, even though many parts of Ukraine are being left behind, this disorganisation led to the construction of a more resilient network. Rivalries between ISP owners, who are often hiding behind offshore companies, result, in some cases,

in illegal practices such abuse of power from people holding public office or even the sabotage of competitors' infrastructures. The unreliability of the judicial system allowed the Ukrainian government to impose Internet censorship without passing any law through the Rada in a bid to regain power over its informational space. Nonetheless, the ambition of a completely free, decentralised and unregulated Internet is still being kept alive by some Ukrainians "pirates".

Engineers Facing the Government: Ruse and Resistance among Internet Service Providers in Russia.

Francesca Musiani (Centre Internet et Société, CNRS)

Starting 2010, a number of laws informed by a "sovereign Internet" vision have profoundly shaped the functioning of the Russian Internet. This increasingly centralized governance operates at two main levels: censorship and surveillance. Most recently, Deep Packet Inspection-type middleboxes were installed throughout the RuNet for these purposes, with substantial additional costs for ISPs to buy, install and maintain them. Faced with a governance that is both blurry and centralized, and with important economic risks, ISPs develop myriad techniques of digital resistance and "ruse", so as to avoid fines or minimize expenses associated with the installation of middleboxes. This paper seeks to analyse this repertoire of ruses, that take place at very different levels: technical bricolages such as "home-made" scripts, allowing to save money vis-à-vis external solutions; legal agencements such as those between the "very small ISPs" and the local agents of the Federal Bureau of Security (FSB); or arrangements between ISPs, in order to share the costs of the solutions necessary to enact the surveillance. Our study (still a work in progress) aims to understand how this mobilization of engineers is particular and if we can analyze it as a form of citizen participation. In a perspective that draws both on pragmatist sociology and Science and technology studies, as well as on the sociology of social movements, participation and digital activism, we analyze this repertoire of ruses at a variety of levels, from technical crafts to legal and economic arrangements. By providing an analytical description of these numerous circumvention practices, we seek to understand how Russian engineers and computer scientists become actors, sometimes in spite of themselves, of RuNet's governance and "counter-governance".

Geopolitics of Routing: Internet connectivity in disputed territories of the post-soviet space

Louis Pétiniaud & Loqman Salamatian (French Institute of Geopolitics / GEODE)

Many territorial entities in the post-soviet area have given rise to different types of conflictual situations: civil war, war by proxy, annexation, frozen conflict, de facto States, borderization etc. Information and communications technologies have played an increasing role in dynamics of territorial rivalries. The dynamics of connectivity in these specific areas allow us to better understand how the Internet is involved in shifts of sovereignty, and manipulated as such. Using data from the Border Gateway Protocol and the RIPE Atlas tool, this presentation aims at showing how various Internet measurement instruments help us identify underlying power rivalries in post-soviet conflicts.

Distance/RTT Ration analysis for some post-Soviet countries

Alex Semenyaka (RIPE NCC, Moscow)

Abstract TBA

4:00 PM – 6:00 PM : Panel 3 : Digital Information and influence

Discussant : Maxime Audinet, Université Paris Ouest / IFRI

"Don't read Telegram channels" : Telegram as the new battleground for information wars in Russia

Dmitri Boschmann (Université Paris Ouest)

"Don't read Telegram channels", Kremlin's spokesman Dmitry Peskov told the journalists who asked him to comment on the arrest of a Russian top-manager in October. What would seem obvious to a Russian needs an explanation to foreign observers.

Telegram has become Russia's new Twitter with its public channels becoming the main platform for expert discussion. The channels, often anonymous, are now a big thing in Russian politics, journalism and corporate PR.

- a Russian cultural exception or the future of digital consumption?
- Telegram farms and deep fake networks,
- loyalists VS opposition channels,
- anonymity on Tegram: a fundamental right or a tool for manipulations?

Russian disinformation in the Baltics and Ukraine

Diyana Dobreva (Cardiff Crime Institute, Cardiff University)

The Russian Federation continues to regard the area of the former-Soviet Union as its sphere of influence and has frequently used various "soft power" and information techniques to try and influence these countries and the political and geostrategic direction they are taking. This presentation will demonstrate two case studies of Kremlin-backed propaganda and disinformation in two post-Soviet regions. Part 1 of the presentation will report the findings of a comparative analysis of Russian disinformation communication tactics and "master narratives" in the Baltic region (Estonia, Lithuania and Latvia) over the last 10 years. Part 2 of the presentation will focus on a recent case study of pro-Kremlin propaganda and disinformation targeting the Ukrainian parliamentary elections, based upon analysis of mainstream media, Reddit and VK data. Both case studies aim to distil some common features of the Kremlin's strategic communications 'playbook' in the near abroad such as using designated regional Kremlin-backed or pro-Kremlin outlets, targeting ethnic Russian minorities in post-Soviet regions, and disseminating similar and established master narratives.

From the local patriotic association to the global company, anatomy of the Internet Research Agency

Colin Gérard (French Institute of Geopolitics / GEODE / INRIA)

In April 2019, the US Department of Justice released the Mueller report, an investigation into Russians efforts to interfere in the 2016 US Presidential campaign to Donald Trump's advantage. Among the

actors indicted by the Special Prosecutor is a shadowy organization based in St. Petersburg: the Internet Research Agency. Better known as the "Troll Factory", the IRA is accused of attempting to influence voters in order to make Donald Trump elected through intense manipulation campaigns on social networks. In this presentation, we will first look back at the origins of the IRA, born in Russia after major demonstrations against Vladimir Putin's reelection in winter 2011/2012. We will then focus on the IRA's internal functioning and on its extremely precise division of tasks, that were uncovered by leaked internal documents. Finally, we will see that despite the significant resources used on popular social networks such as Facebook and Twitter it is still impossible to prove that the IRA's action had a real influence on the election.