weasa { WARSAW EURO-ATLANTIC SUMMER ACADEMY

Grasping the virtual:

(geo)politics, economics and privacy in a digital era

Copyright: College of Europe Natolin Campus
Warsaw 2018

Polish-American Freedom Foundation

Fundacja Liderzy Przemian

College of Europe
Collège d'Europe
Brugge
Natolin

G|M|F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Table of contents

{ Leapfrogging to the Digital Future

Wojciech Przybylski

When reflecting on the digital revolution's impact on democratic institutions and processes, most of the attention focuses on established democracies rather than countries of post-soviet heritage.

The European Commission's European Innovation Scoreboard 2017 (EIS) seems to support this bias, since the ranking of countries with the highest score is somehow correlated with a high level of democracy standards (compare, for example, the EIS with the Democracy Index 2016 by The Economist Intelligence Unit) or significant prosperity (as shown, for example, by the Legatum Institute Prosperity Index 2017). Yet, it would be a hasty generalisation to see it as an obvious dependency that traps underdeveloped countries. Low democratic standards or economic underperformance do not need to hamper digital development and vice versa – digital development may very well become a tool for upgrading social and economic systems.

There is at least one documented example that shows how the linking up of the digital revolution with the upgrade of democratic standards may speed up a country's transition towards the EU average and beyond. Estonia is one of the early adopters of digital tools, which it linked with a process of societal and political transformation. In the very beginnings of its transition to democracy from the Soviet regime, it identified innovation as the driver of the desired changes (Ilves 2015).

Even though Estonia currently has 79.8 points in the EIS index (compared to an EU average of 102), it ranks far above other post-communist countries and just after the Czech Republic and Slovenia. Also, its prosperity and democracy rankings put it even at a greater distance from other post-Soviet countries in the region.

The story of Estonia's digitalisation is matched with its story of democratic transition. There are many reasons to believe that the two are, in fact, so closely intertwined that one sped up the other. One of rationales to introduce the massive digitalisation to Estonia was a lack of skilled workers in both the public and private sectors which, at the time, were overburdened with slow and inefficient Soviet-era work culture. Since then, the digital culture became a big part of the now-renowned national brand that Estonia built up both for international as well as for internal audiences.

However, the e-success of Estonia did not come without a price. The nation became exposed to cyber security threats. It became possibly the first nation to ever suffer from hybrid digital attacks in April 2007, when most of its institutions (including government, banks, and the press) were digitally incapacitated by hackers linked to Russia. Still, since then Estonia has improved its digital resilience and continues on the digital transformation path.

Although other Eastern Partnership countries, except for Ukraine, are not listed on the EIS, it is safe to assume that their ranking would not score even close to Estonia. Ukraine currently ranks the lowest so far, with 28.9 points, just after Romania (33.8) and Macedonia (FYROM; 44.2). In fact, if we assume that internet penetration rate correlates with a rank on the EIP, then the other Eastern Partnership countries may rank a bit higher since all of them enjoy higher internet penetration than Ukraine.

In fact, 78% of Azerbaijan's population had access to internet, followed by 70% of Armenians, 71% of Belarusians, 60.7% of Georgians and only 52.5% of Ukrainians. In the Western Balkans, 80.4% of Kosovars had internet access, as did 72.2% of Macedonians, 69.9% of Montenegrins, 69.3% of citizens of Bosnian Herzegovinians, 67.1% of Serbians, and 66.4% of Albanians (Internet World Stats, June 2017). As global internet penetration will sooner or later reach nearly 100%, as in the case of Iceland, the potential of digital technology will be similar everywhere.

This presents Eastern Partnership and Western Balkan countries with a unique opportunity to make use of the digital revolution a part of their democratic transition process, one that will shift them into an unknown but hopefully prosperous and a more democratic future. If the opportunity is well used, then countries might benefit from a phenomenon known as leapfrogging, which could significantly boost their position in both digital and democratic performance rankings.
The concept of digital leapfrogging in developing countries describes a situation in which a development of a particular industry is non-linear. It is, for example, not necessary to lay down a network of cables for landlines in order to develop mobile telecommunications, allowing the new technology to develop at a far faster speed than its older counterparts. Democratic performance - for instance regarding transparency or levels of public participation - could also leapfrog with the aid of digital technologies.

This non-linear development of public policy requires the next generations of elites in those countries to research and reflect on the potential of the digital revolution, along with the threats it can bring to personal freedoms and national security.

On the following pages we demonstrate what such elites must keep in mind if they wish to prepare their countries for a digital leapfrog. Such a jump would force them to think deeply about topics such as the digital administration of a country, the role of digital currency within it, the security threats that hybrid and information warfare could bring about, as well as the role of a nation state in protecting human rights in the digital age.

This publication is part of the 2017 edition of the Warsaw Euro-Atlantic Summer Academy 2017, whose participants studies the digital culture and policies influencing the Eastern Partnership and Western Balkans.

It comprises of six very interesting essays written by some of the many fantastic participants of the Academy. They deal with three main themes: the digital potential for growth and democratic potential, cyber-security and resilience to digital threats, and a reflection on the cultural changes brought about by the proliferation of digital technology.

Although many of those texts seem country-specific at first glance, they are a great representation of global trends and potential. The digital world, after all, is the fastest advancing front of globalisation.

The authors did a great job researching topics of their choice that would be related to their policy interests. Therefore, it is safe to assume that the very same authors and their extended circles will be at the forefront of new reforms and policy implementations that will lead their countries and the region further.

On a personal note, I wish to thank organisers for entrusting this volume to me and especially to Lukasz Krol and Kateryna Pryshchepa who tirelessly worked on this very ambitious project. I was involved in the program over the summer first as one of lecturers and a consultant of the program because of my experience as the leader of the New Europe 100 network of innovators. NE100 is a program by the Res Publica Foundation that promotes and connects digital communities in this part of the world, run in cooperation with Google, Financial Times and the Visegrad Fund.

Having been offered to edit this volume, I gladly agreed. I hope the readers will appreciate this publication that was possible thanks to the organisers of WEASA, the excellent lecturers who came from both sides of the Atlantic and to discussions between authors and WEASA participants. The latter consisted of an extraordinary group of up-and-coming policy analysts, experts, advisers, civil servants, private sector/NGO professionals and journalists from the Eastern Partnership and the Western Balkans. We owe thanks to all of them for sharing their experiences, knowledge and reflections with the authors in this volume.

Information resilience in Eastern Partnership countries – evaluation of prevention mechanisms in Georgia, Moldova and Ukraine

Danu Marin

Information warfare is a major challenge for Georgia, Moldova and Ukraine because of the way in which information has been instrumentalised to support armed interventions, harm political and economic infrastructure, undermine social cohesion and erode confidence in democratic institutions. To tackle this challenge, policy and decision-makers need a comprehensive approach to build information resilience. Similarly to dealing with a natural disaster, information warfare can be treated through the prism of disaster management, which consists of four elements: prevention, preparedness, response, and recovery. The article analyses the prevention aspect of information resilience. It describes a series of preventive measures from awareness raising activities to alert relevant stakeholders about the dangers of disinformation, to long-term educational programmes designed to improve societal vigilance towards propaganda and reduce its impact on public discourse.

Due to technological advancements and the changing nature of international conflicts, information has become an integral part of the interstate competition. In operational terms, information is seen as an extension of military actions, thus rephrasing Clausewitz's famous quote, "*information is the continuation of war by other means.*" This approach is exemplified in the Russian Federation's "Gerasimov Doctrine" (Giles, 2016), the Chinese concept of "*Three Warfares*" (Lee 2014) or the concept of "*Strategic Communication*" (Tatham and Le Page, 2014) promoted by the Euro-Atlantic community, which gave birth to the now-infamous concept of information warfare.

The issue of information warfare has become a major concern for the Eastern European states bordering the Russian Federation, in particular for Georgia, Moldova and Ukraine – the three frontrunners of European integration. After Russia's unsuccessful transformation and return to a centralised governance system, it started building up its information clout in the neighbouring countries. Even though this process alerted some observers and policy-makers, it was largely ignored due to a *normalcy bias*[1] both at the political and societal level. The illegal annexation of Crimea and the proxied armed conflict in the Donbass region highlighted how Russia instrumentalised information to serve politico-military purposes. These events were a game-changer for local decision makers and the international community. They needed to acknowledge the existence of a broader security problem where information warfare is used to support armed interventions, harm political and economic infrastructure, undermine social cohesion and erode confidence in democratic institutions (Toucas, 2017).

The realisation that information reliance on foreign actors results in a national security vulnerability requires a new approach to policy-making. Taking into consideration the fact that information-related threats are unpredictable and have a wide range of negative consequences, an effective way to tackle them is through the prism of emergency management mechanism, which consists of four elements: prevention, preparedness, response, and recovery. This methodological framework can allow us to formulate a more comprehensive and systemic solution to the existing problem by allowing for a better allocation of resources and distribution of responsibilities among different stakeholders.

[1] Normalcy bias – is a belief that causes people to underestimate the possibility of a catastrophe and its negative effect, because of the persisting assumption that things will function the way they normally function.

Information resilience – prevention, preparedness, response and recovery

For the information warfare, **prevention** relates to the actions taken in advance to minimize its negative effect. The first component of preventive measures is the awareness raising campaigns to alert the public, decision-makers and international partners about the dangers of disinformation and harmful narratives. The second component is a long-term investment in educational programmes to improve media literacy and critical thinking that would raise societal vigilance towards propaganda and reduce its impact on public discourse.

Preparedness against information warfare is an early warning system that encompasses media awareness and monitoring mechanisms. It should focus on three layers of analysis:

1. Detecting "*fakes*" which requires both human-based and tech-based monitoring instruments to track the disinformation footprint in traditional and social media and to prevent misleading information from going viral and swaying public opinion.
2. Recognising media spin, which proved to be highly disruptive and polarising for modern societies. This situation greatly benefits disinformation and propaganda efforts, which thrive in an environment of media uncertainty.
3. Identifying foreign narratives – unlike the media spin, narratives are a much more complex construction embedded in culture and history. They are the building blocks of propaganda designed to influence society's behaviour and erode the system of values.

Response relates to the particular countermeasures designed to address the challenges of information warfare. Depending on the goals and the implementing actors, the response measures may fall into three categories:

1. Legislative/Regulatory – includes activities aimed at enforcing stronger regulation on the media content and dissemination channel.
2. Communication/Information – entails improving the Government's public communication to raise transparency and accountability and boost support for

the national policies.

3. Investigative/Analytical – includes the maintenance of fact-checking and debunking platforms to expose and counteract false, exaggerated, or pretentious claims.

Finally, the element of **recovery** denotes the assessment and evaluation phase. It should include a series of quantitative indicators, such as enacting relevant regulatory legislation, improving institutional communication and public relations. Its progress can also be measured through qualitative indicators associated with healthy democratic governance, such as trust in democratic institutions, improved media freedom, and better citizen participation.

Prevention aspect: awareness raising activities and their impact

Prevention consists of two main components: awareness-raising in the short term and educational programmes designed to improve media literacy and critical thinking in the long term Awareness of foreign information influence in Eastern Partnership countries had been present even before the game-changing events in Ukraine (Media Landscape, 2009), but it was not enough to encourage active policy-making. The more recent awareness raising efforts in Georgia, Moldova and Ukraine were primarily bottom-up initiatives led by volunteers and civil society to inform relevant stakeholders about the dangers of targeted disinformation and toxic foreign narratives.

Ukraine

In Ukraine, notable awareness raising initiatives include the StopFake platform launched by Mohyla School of Journalism in March 2014, the MediaSapiens initiative by the Detektor Media platform and media projects promoted by Internews Ukraine. These efforts were further complemented by other small-scale activities such as roundtables, discussion clubs and regional conferences. Altogether these activities have a broad scope and include socio-political, cultural, economic and international aspects. At a governmental level, the awareness raising activity is part of the larger concept or strategic communication implemented by Ukrainian authorities. Due to the ongoing conflict in Donbass region, which is a source of daily information confrontation with the Kremlin, the government efforts are primarily framed in the context of the Anti-Terrorist Operation (ATO) and thus narrowed down to a politico-military scope.

In terms of its effectiveness, awareness raising activities can be evaluated on three target groups. The first target group are domestic policy and decision-makers. In Ukraine, the political establishment and public authorities are largely aware of the danger of foreign propaganda and disinformation and are themselves agents of awareness raising on the national and international stage. Moreover, in the context of active information war with the Russian Federation, a more hawkish information and security policy is encouraged. Such policy enjoys notable public support, with 56% of people agreeing with the practice of promoting own propaganda messages through mass media, while only 22% stand opposed (Media Sapiens, 2015). The second target group are the development partners, in particular the Euro-Atlantic community. Awareness raising for this target group can be largely considered a success: they have exponentially increased funding and support at regional and national level for projects associated with strategic communication and resilience building. As a result, Ukraine benefits from a series of assistance programs from NATO, the European Union, the United States and other development partners, as well as tailored grant schemes from donor organisations aimed (directly or indirectly) at improving information resilience. The third target group is the general public, whose support is paramount in counteracting the negative effect of propaganda and disinformation. Surveys show an improvement in understanding of the propaganda and disinformation as the majority of citizens (58%) share the opinion that there is a threat of Russian propaganda (Stopfake.org 2017). Opinion polls indicate that the news preferences and viewers' consumption patterns have shifted to primarily national channels (Media Sapiens, 2017) and that citizens' attitude towards Russian media has worsened considerably with 60% having a negative attitude (Media Sapiens, 2015). This stands in contrast to the pre-Maidan period, when Russian media was trusted by 45% of the people (Razumkov Center, n.d.). A radically different perception is shown by the people in the separatist regions of DNR/LNR, where 62% distrust Ukrainian media and 53% trust Russian media (Sasse 2017) pointing to the existence of strong information bubble.

Georgia

Georgia has demonstrated a proactive approach to awareness raising. In 2015 a consortium of 17 organisations launched an information campaign called *Support Georgia to Defend Liberty*, which aimed to warn about the advancing Kremlin propaganda. Another awareness raising project is "*Myth Detector*" implemented by Media Development Foundation to inform about disinformation. At the government level, Georgian authorities approach awareness raising in the context of strategic communication.

The effectiveness of the awareness raising in Georgia had positive results on all three target groups. The political establishment and public authorities, despite the existing political differences, have a consolidated position on the issue of external information influence, particularly the one coming from the Russian Federation. Decision-makers and security experts are not only aware of the dangers of propaganda and disinformation, but demonstrate an activist approach to tackling this problem. When it comes to the development partners, their awareness of Kremlin information influence in region has considerably improved, even though their reaction during the Russo-Georgian war in 2008, which was the first indicator of Kremlin revisionist foreign policy backed by information warfare capabilities, was rather inadequate.

At the moment, Georgia has wide support from development partners to improve information resilience as it benefits from Euro-Atlantic expertise in areas such as strategic communication, media capacity building and tailored grants for civil society. The Georgian public awareness concerning the foreign propaganda and disinformation activities is difficult to assess directly since there is little primary data on this issue, therefore the author relies on secondary indicators. A profound change in viewership and news consumption took place in the context of the 2008 Russo-Georgian War. A 2009 Media survey shows that 70% of respondents never got information from Russian TV, Radio or newspaper and only 7-9% trusted Russian mass media (Caucasus Research Resource Center, 2009), similar results were reproduced in the 2011 Media survey (Caucasus Research Resource Center, 2011). The more recent studies display a slight decline in awareness as 23% of Georgians get their news from foreign channels of which the top three sources are Russian channels

(Media development Foundation, 2015; 2017). Nonetheless, the population still displays high alertness as 47% of respondents believe that Russia deploys propaganda activities in Georgia, ranking it 4th biggest security challenge (National Democratic Institute 2017). Expectedly, South Ossetia and Abkhazia share a completely different view on the issue, the majority of their population having complete trust in Russian media (O'Loughlin and Toal 2013); (O'Loughlin and Kolossov, 2011) and sharing the narratives it promotes.

Moldova

In Moldova the first major awareness campaign, entitled *Stop Fals*, was launched in 2015 by a consortium of three media NGOs[2] . Another notable organisation to raise awareness is the Information and Documentation Centre on NATO, which organised a series of public events dedicated to information warfare. At Government-level, the Moldovan authorities showed more restrain about the problem of information warfare both in words and actions. When it comes to the Moldovan political establishment, it does not have a consolidated position on the issue. This attitude is largely dictated by lack of national cohesion and strong socio-political polarization within the society, which encourages divisive politics that exploit geopolitical cleavages.

The awareness raising activities of the development partners have proven more successful. Similarly to their counterparts in Georgia and Ukraine, they have extended support to build information resilience. However, because Moldovan authorities lack political will, the development partners' resources are streamlined to the NGO sector and far less to state-led efforts to tackle the problem at national level. Unlike Georgia and Ukraine, the Moldovan public shows more uncertainty on the impact of information warfare, particularly concerning Russia influence activities. The study results on public perception of false media information highlight that over 50% of people can identify media manipulations (Independent Journalism Center 2016) however, far fewer are able to recognize external information influence, as Russian media is the second most watched and trusted source of information (Puiu et.al., 2016). Even more dramatic is the state of affairs in the autonomous

[2] Independent Press Association, Independent Journalist Center and Association of Moldovan Independent Journalists.

regions of Gagauzia[3] and Taraclia[4] . A 2016 study in the region reveals a strong cultural and informational affinity to Russian Federation, where an overwhelming majority (over 95%) prefer Russian media to the local channels (Nantoi et.al. 2016).

Prevention aspect: educational programs for media literacy and their impact

The second component of prevention is a long-term investment in educational programmes to improve media literacy and critical thinking to raise societal vigilance towards propaganda and reduce its impact on public discourse. When it comes to media literacy programmes, there needs to be a differentiation between government-led efforts and community-led efforts with the assistance of development partners.

At governmental level, Georgia, Moldova and Ukraine have made some progress in introducing media literacy in the educational process. The Georgian National Curriculum 2011-2016 introduced a series of courses on media literacy and digital competences for primary and secondary education. It is difficult to estimate whether the pupils and teachers could properly embrace this knowledge because the courses were optional and there was no tailored allocation of resources. Furthermore, no evaluation of programme implementation has been done so it is difficult to review its effectiveness. The tertiary education in Georgia provides a larger array of opportunities to improve media literacy. Georgian universities with a humanities-based profile offer bachelor, master and doctoral programmes in journalism, media studies and communication, however, they are concentrated in big urban centres, and have a reduced impact on the population with lower media and digital skills.

Moldova also introduced media literacy courses in the formal education programme. The Ministry of Education of Moldova launched an optional course for media literacy for the primary cycle. Similarly to the Georgian case, it is difficult to estimate the impact of the course due to lack of assessment studies on this issue, but generally speaking there was

[3] Gagauzia (Gagauz Yeri) is an autonomous region Moldova inhabited by Turkic minority named Gagauz.

[4] Taraclia is a district in Moldova (not autonomous) inhabited by ethnic Bulgarians.

little investment in these initiatives and owing to the overload of the mandatory school program, pupils rarely choose optional courses. In the tertiary education, there are fewer Moldovan universities that offer specialized programmes in media literacy. Furthermore, they are concentrated primarily in the capital, which limits the learning options for the students from the regions.

Ukraine has advanced considerably more in introducing media literacy to the formal education system. The Ministry of Education in partnership with Ukrainian Academy of Press and National Academy of Social and Political Psychology has been implementing a pilot project for media literacy in secondary education. The project was launched in 2011 covering 10 oblasts of Ukraine. According to the 2015 report (Internews, 2015), the successful implementation of pilot project contributed to its proliferation in other schools, however, it also highlighted a substantial disjunction between theoretical and practical aspects of the programme. In the tertiary education, Ukrainian Universities offer an array of subjects to promote media literacy, but similarly to Moldova and Georgia they are predominantly concentrated in larger cities, therefore people in rural areas have less access to media literacy opportunities.

The grassroots and development partners were more proactive in improving media literacy. A notable example is the IREX program for Georgia, Moldova and Ukraine sponsored by USAID. The nation-wide project to renovate public libraries[5] and transform them into learning centres has produced impressive results for local communities with lower levels of access to information and educational opportunities. Under IREX, Georgia and Ukraine also benefit from Media Partnership Programs aimed at improving the quality of journalism and citizen engagement. Other large-scale education and media-related projects were launched by European Union through the neighbourhood instrument. Among them the most notable are the "*Open Media Hub*" project designed to provide training and support to media professionals across the EU Neighbourhood area, and the "*Creative Europe*" programme aimed at supporting the cultural and creative sectors in particular by improving access to the digital age opportunities. These efforts were further complemented by other donor foundations through tailored grants to support

[5] In Georgia – Beyond Access Project; in Moldova – Novoteca Project; in Ukraine – Bibliomist Project.

independent journalism, media research and analysis. As a result, civil society in Georgia, Moldova and Ukraine has seen a boom in training initiatives such as media workshops, summer schools and training camps addressing the issue of media literacy.

It is still early to evaluate the effectiveness of these efforts since these are long-term investment but the available data already shows upward trends. First of all, there is diversification of information consumption: while TV still remains the most viewed and trusted sources of information in all three countries, the Internet and Social Media are gaining ground as the second most important channel[6] . They allow broader access to information and alternative sources. This, however, does not indicate a better understanding of the media environment and manipulation techniques. According to the opinion poll, 90% of respondents watch and 80% trust Georgian media sources, in contrast with only 7% who watch and 1% who trust Russian media. On the other hand, as social media share as a news source grows, people are less capable identifying the ownership and interests behind news distribution. (International Republican Institute, 2017). The IREX report on its project shows that media literacy has improved but the public still needs to develop a series of skills and abilities to better interact with mass media (IREX Georgia 2014). A report in Moldova reveals that the public has a critical attitude towards mass media – 56% of respondents are dissatisfied with media responsibility and accountability. People have the least confidence in national media outlets (68%) followed by Russian ones (57%) and other (EU/USA) foreign outlets (44%). In terms of their ability to discern media manipulation, 51% of the respondents believed to be well equipped for this task, however, the majority displayed hesitation in recognizing signs of manipulation and propaganda (Independent Journalism Center 2016). In Ukraine satisfaction with the media is around 50% for TV and 60% for the Internet (Internews 2016). The respondents show better viewership standards looking for more balanced and objective coverage from the media. This, however, is more of an intuitive rather than trained process.

[6] Data compiled from Public Opinion Polls by National Democratic Institute (NDI) https://www.ndi.org/eurasia and Public Opinion Polls by International Republican Institute (IRI) http://www.iri.org/country/eurasia/details

Conclusion

Prevention, as a combination of awareness raising activities in the short term and educational programmes in the long term, requires the effort of multiple stakeholders: government, civil society, the private sector, and development partners. Georgia, Moldova and Ukraine have developed preventive measures against information warfare, but their effectiveness varies from country to country.

The least equipped at the moment is Moldova, which, despite having an awareness raising campaign to warn about propaganda and disinformation, has not been able to persuade the political establishment to take action nor consolidate a common civic stance. Furthermore, studies indicate low levels of public alertness for foreign propaganda and disinformation and strong socio-political polarization. Georgia and Ukraine show far better results with high support from both the public and national authorities. Surveys indicate that the people have at least basic levels of awareness about propaganda and disinformation and encourage a more active approach to tackling the problem. The downside of the actions taken by all three countries is the disproportionate distribution of awareness raising efforts between the centre and periphery, which indicates a considerable gap in understanding between different target groups. Furthermore, there are strong *information bubbles* in the unrecognised regions on the territory of Georgia, Moldova and Ukraine – a problem which needs to be tackled if the countries truly aspire to reintegrate these regions.

As for long-term educational programmes, the work is still at the earlystage. Judging by the government-led efforts to improve media and digital literacy in schools it is clear that this issue is not a priority. Media literacy courses are poorly integrated into the school curriculum and very little resources are allocated for this type of programme. The civil society and development partners are far more proactive in this regard. They support a wide range of curricular and extracurricular activities, ranging from small-scale projects such as media camps and training sessions to nation-wide projects to renovate libraries and transform them into local learning centres. However, without government support, media literacy initiatives have only a marginal effect.

Bibliography

Caucasus Research Resource Center. 2009. Media survey in Georgia. http://caucasusbarometer.org/en/me2009ge/codebook/

Caucasus Research Resource Center. 2011. Media survey in Georgia. http://caucasusbarometer.org/en/me2011ge/codebook/

Giles. 2016. *Russia's 'New' Tools for Confronting the West Continuity and Innovation in Moscow's Exercise of Power.* Chatham House, Russia and Eurasia Programme.

Independent Journalism Center. 2016. "*Population perception of false and distorted information covered by mass media. Survey published in the framework of Stop Fals campaign*". http://media-azi.md/en/public-perception-false-and-distorted-information-covered-media-january-2016

International Republic Institute . 2017. "*Survey of Public Opinion in Georgia February 22– March 8*", 2017.

Internews. 2015. "*Implementation of media education and media literacy courses in secondary schools of Ukraine.*" Report on the results of complex study commissioned by U-Media Program.

Internews. 2016. "*Media Consumption Survey Ukraine 2016.*" U-Media Project. https://www.internews.org/sites/default/files/resources/Media_Consumption_Survey_2016-09_Eng_Internews.pdf

IREX Georgia. 2014. *Georgian Media Enhance Democracy, Informed citizenry and Accountability. Final Performance Report.*

Lee. 2014. "*China's 'Three Warfares': Origins, Applications, and Organizations. Journal of Strategic Studies*". Vol. 37 , Iss. 2.
http://dx.doi.org/10.1080/01402390.2013.870071

Media development Foundation. 2015. "*Anti-Western propaganda. Media monitoring report 2014-2015.*" http://mdfgeorgia.ge/uploads/Antidasavluri-ENG-web.pdf

Media development Foundation. 2017. "*Anti-Western propaganda. Media monitoring report 2016.*" http://mdfgeorgia.ge/uploads/library/65/file/eng/Antidasavluri-ENG-web_(2).pdf

Media Landscapes: Georgia, Moldova and Ukraine. 2009. European Journalist Centre.

Media Sapiens. 2015. "*Ставлення населення до ЗМІ, пропаганди та медіареформ в період конфлікту.*" http://osvita.mediasapiens.ua/mediaprosvita/research/ukrainski_zmi_vtrachayut_doviru_ale_stavlennya_do_rosiyskikh_zmi_kritichno_pogirshilos_navit_na_skhodi_sotsopituvannya/

Media Sapiens. 2017. "Survey of Russian Propaganda Influence on Public Opinion in Ukraine Findings." http://osvita.mediasapiens.ua/detector_media_en/reports_eng/survey_of_russian_propaganda_influence_on_public_opinion_in_ukraine_findings/

Nantoi O., Cantarji V., Boțan I., Gremalschi A., Sirkeli M. 2016. "*Moldova Between East and West: Views from Gagauzia and Taraclia.*" Institute for Public Policy.

National Democratic Institute. 2017. "*Public attitudes in Georgia. Results April, 2017. Survey carried out for NDI by CRRC Georgia.*"
https://www.ndi.org/sites/default/files/NDI%20poll_April%202017_Foreign%20Affairs_ENG_vf.pdf

O'Loughlin J. and Kolossov V. 2011. "*Inside Abkhazia: A Survey of Attitudes in a De Facto State.*" Post-Soviet Affairs Vol. 27 , Iss. 1.
https://www.colorado.edu/ibs/intdev/johno/pub/InsideAbkhazia.pdf

O'Loughlin J. and Toal G. 2013. "*Inside South Ossetia: A Survey of Attitudes in a De Facto State*". Post-Soviet Affairs Vol. 29 , Iss. 2.
https://www.colorado.edu/ibs/intdev/johno/pub/PSA2013.pdf

Puiu T., Gotișan V., Marin C., Țurcanu V., Gonța A., State V., Ciorici D., Dumitru Lazur D., Prodan S. 2016. "*Information security from Media perspective*". National Study. Soros Foundation Moldova. Chisinau. [Romanian]

Razumkov Center. "*Trust in Russian mass media 2000-2013.*"
http://old.razumkov.org.ua/eng/poll.php?poll_id=86

Sasse. 2017. "*The Donbas– Two parts, or still one? The experience of war through the eyes of the regional population.*" Centre for East European and International Studies (ZOiS)
http://www.zois-berlin.de/fileadmin/media/Dateien/ZOiS_Reports/ZOiS_Report_2_2017.pdf

StopFake.org. 2017. "*Awareness and Attitude toward the Problem of Disinformation and Propaganda in Mass Media.*" StopFake.org Ukraine.
https://www.stopfake.org/en/awareness-and-attitude-toward-the-problem-of-disinformation-and-propaganda-in-mass-media/

Tatham S. and Le Page R. 2014. *NATO Strategic Communication: More to be Done?* National Defence Academy of Latvia, Center for Security and Strategic Research.

Toucas. 2017. *Exploring the Information-Laundering Ecosystem: The Russian Case.* The Center for Strategic and International Studies.

{ Blockchain and cryptocurrencies and their impact in the new economic order

Erda Cani

Abstract

While blockchain seems to be an extremely attractive breakthrough technology, the development of cryptocurrencies and ICO (Initial Coin Offering) is changing the traditional role of national governments and central banks in influencing the economies via the supply of national currencies. Digital currency will improve the payment system and facilitate exchange but if central banks decide to issue cryptocurrencies, their impact will be visible not only in the way they conduct monetary policy but also in the economic performance of the countries. The world's biggest banks are preparing themselves for the cryptocurrency era by implementing a number of projects and assessing the possibility of implementing digital currencies in traditional business models. Although is still uncertain if this technology is secure enough or whether its infrastructure will make it possible to process large volumes of transactions currently performed by banks, some countries are already using blockchain in financial instruments or preparing for issuing national digital currencies. Cryptocurrencies may cause important structural changes, which need to be accompanied by precise policies from the regulatory bodies in order to mitigate risks and protect investors in a highly interconnected financial world. Moreover, cryptocurrencies

guarantee a high level of anonymity that may be subject of misuse for illegal activity and anti-money laundering.

Methodology: The research is based on in-depth analysis of the technology, functions, level of usage and structural changes caused by blockchain and cryptocurrencies in the financial world. Considering the complexity of the process, the analysis will be based on qualitative and quantitative approaches, which will include a literature review, economic and financial structural analysis, statistical data analysis as well as an impact assessment.

Introduction and problem description

Although money is so important in fulfilling our needs and facilitating our lives, defining money has always been a challenge. The most common form of defining money between people is to treat it only as a medium of payment. More elaborated and academic based definitions analyse the function that money fulfils in a certain society or economy[1]. (Mishkin, 2004). In general, scholars emphasise three main functions of money: money as a medium of exchange, a store of value, and as a unit of account. Throughout the centuries, money has changed more than anything else or, to be more precise, has been undergoing continuous transformation (in its physical appearance, weight, type of material, given nationality, and the like) and recently money has even become invisible in the everyday life of many consumers. The use of cash is diminishing and there are several countries that are heading towards the creation of cashless societies, with Sweden being one nation that has made some of the biggest progress on this path. Between 2007 and 2017, cash in circulation decreased by 15%, and 95% of Swedes have access to debit and credit cards. Other countries like Singapore, the Netherlands and France are following in their footsteps. (World Economic Forum). The forces behind the transformation of money have been both supply and demand driven. In order to better fulfil its main functions, money needed to be lighter, easier to transfer, and widely accepted; all of these have an impact on its liquidity.

[1] Economists define *money* (also referred to as the *money supply*) as anything that is generally accepted in payment for goods or services or in the repayment of debts...., F.S. Mishkin, *The economics of money and Banking and Financial Markets*, Columbia University.

In 1983 David Chaum, working at the University of California, developed a system based on cryptocurrency cash. (Narayanan, 2016). Although the cryptographer marketed and patented his invention, the technology failed to attract investors. Twenty-five years later, a white paper was published signed by Satoshi Nakamato (*The name is a pseudonym and the real identity of Nakamoto is not known*) explaining the creation of a new system based on cryptocurrencies. (Nakamato, 2008). This genius invention, which established the first decentralized digital payment system, was based on two main pillars. The first one is the creation of bitcoins that practically serve as virtual cash, and the second pillar is the use of blockchain technology. Blockchain enables the creation of digital ledger where all the transactions are recorded, linked and secured using cryptography, ensuring a very high level of anonymity. (Narayanan, 2016).

The Initial Coin Offering of cryptocurrencies has introduced two main features that raise many questions and may impact the payment and monetary system. The first aspect is the total decentralization of the issuing of the currency; a central institution such as a central bank is not backing these currencies. In addition to this, this process entirely eliminates the role of financial intermediaries. The new innovative solution may diminish the role of central banks as they lose control over the supply of money and mechanisms to conduct the monetary policy and at the same time cause structural changes, with the "elimination" of secondary banks.

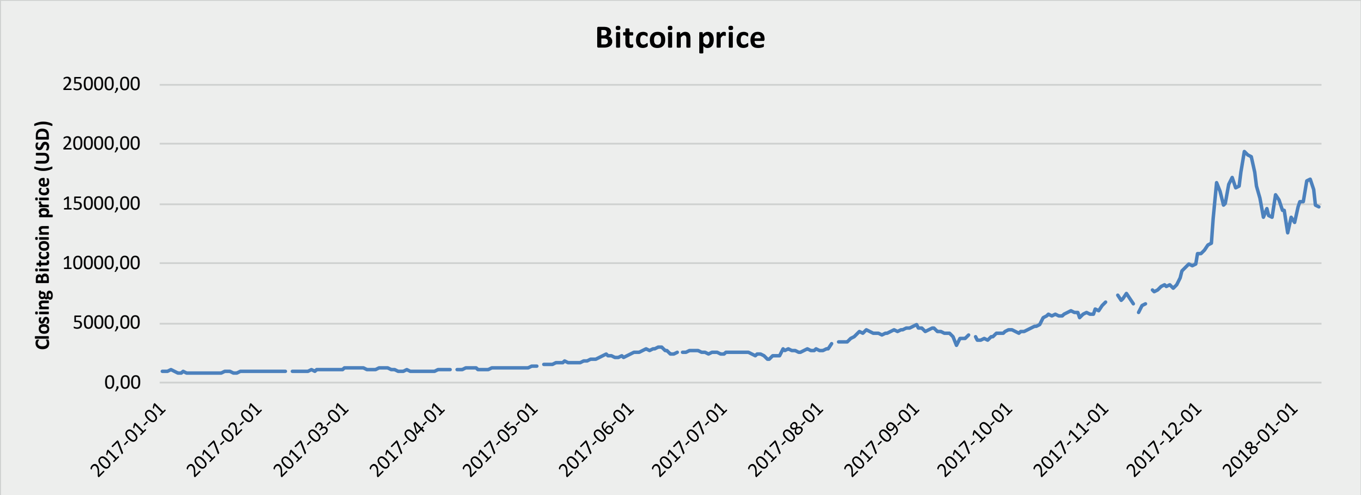
The second important aspect is related to anonymity. While evolution has permitted money to become more comfortable and user friendly, this transformation led to a loss of the anonymity previously associated with money. Cash still remains the most anonymous way of transaction, but a cryptocurrency payment system has also been demonstrated to ensure a very high level of anonymity. Although anonymity is a key factor in the development of currencies, it opens the doors to additional risks related to laundering and other criminal activities.

Technological innovation and main features of cryptocurrencies

A bitcoin is produced/ issued by a computer that produces numerical solutions to complicated mathematical operations and then verifies them. These computers are running programmes called mining scripts, which are based on US-NSA's Secure Hash Algorithms (SHA256 algorithm). (Narayanan, 2016). The verification of the answer is called a Proof-of-Work. Bitcoins generation is not endless and the difficulty of algorithms is automatically adjusted on a predictable schedule so that the number of solutions found globally for a given unit of time is constant: the global system aims for 6 per hour (Narayanan, 2016), resembling the mining of natural resources, which are not infinite. However, unlike other digital currencies, the inventor has already set the maximum amount of Bitcoin cryptocurrency that could ever be generated to 21 Million. Since the beginning of November 2017, 16 700 000 Bitcoins have already been mined. (https://blockchain.info, 2017)

To keep up the mining work, a function called halving has been introduced. The bitcoin generation gets halved every four years. The last block halving occurred on July 2016 and the next one will take place in 2020. Currently, new bitcoins are generated roughly every 10 minutes in batches of 12.5 coins. Miners are required to maintain the list of validated transactions known as the blockchain, which is the most crucial part of this cryptocurrency technology. (Narayanan, 2016). For ordinary users or investors, Bitcoins are easily purchasable through several bitcoin wallets or exchange platforms.

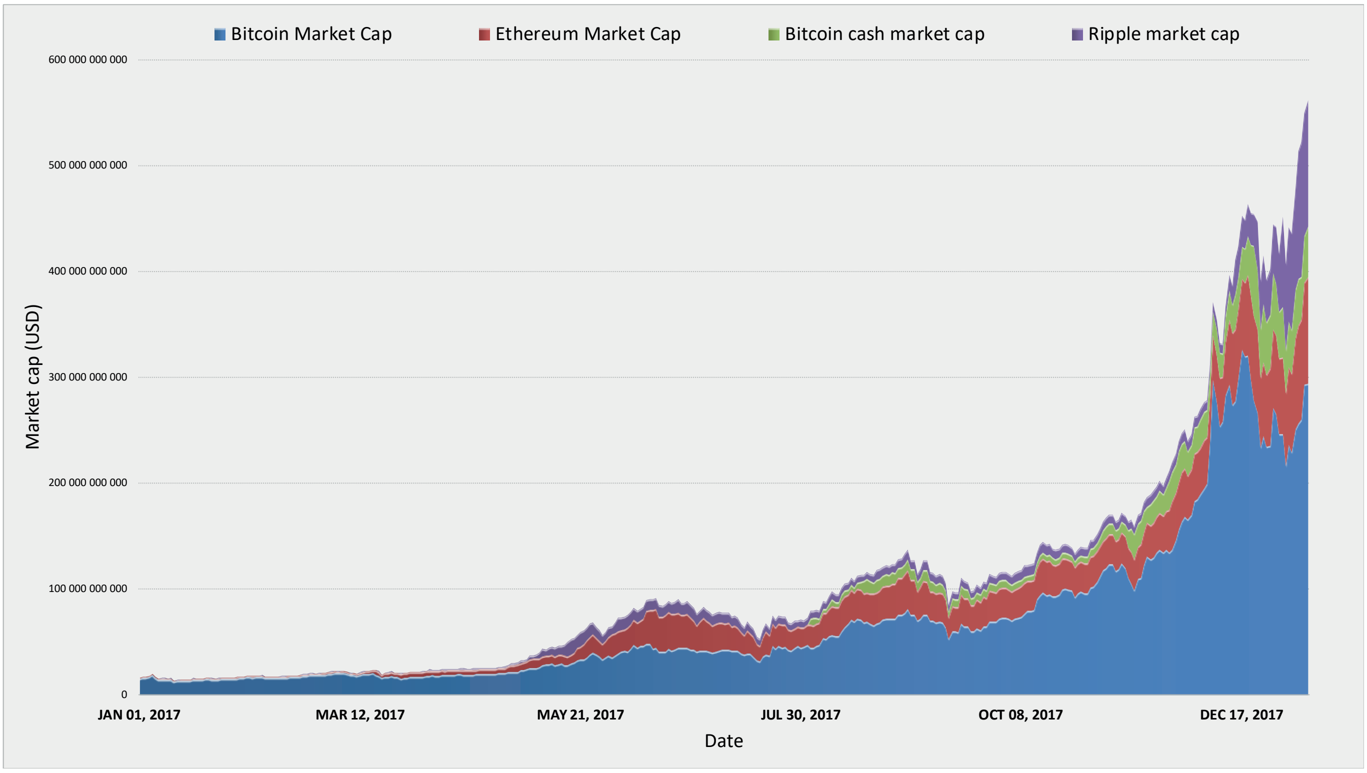
Graph No.1: Evolution of price of Bitcoin in bitcoin/usd



Source: https://www.coindesk.com/price/

While performing a transaction, Bitcoins are sent to the payee in the form of a code called a hash that is digitally signed by the payer. When the payment is confirmed and signed the transaction is locked in the hash in what is called a block. This block is recorded in the blockchain and it becomes public to everyone. Generally, clients prefer the longest chain of blocks since these tend to also represent the most difficult combinations. (Biryukov, Khovratovich, 2016)

Graph. No 2. The market value of cryptocurrencies



Source: Produced based on data derived from CoinMarketCap

From the consumer point of view the increasing use of cryptocurrencies is due to the following factors:

Transactions in bitcoins are automatically published in the public domain and participants can see the amount of the sum that was engaged in the transaction. No one can doubt the legitimacy of the transaction, ensuring a high level of *transparency*.

In the cryptocurrency world, transactions are performed in a peer–to–peer manner, and intermediaries or third parties are eliminated. In the traditional system, banks are the most prominent intermediaries and practically shape the financial system. But banks are costly and the *elimination of intermediaries* grants cost advantages to the cryptocurrency system. Moreover, in recent years and due to repeating financial crises, banks have been losing their biggest asset, clients' trust. Banks failed to maintain their position as an institution of trust by conducting extremely risky investment strategies and initiating financial bubbles.

The system so far has ensured a high level of security by eliminating the possibility of duplicating virtual coins and by encrypting every transaction. There is no evidence of duplication of personal data, either. *Anonymity* is on a much more advanced level than any other form of payment and users of cryptocurrencies may be tracked only by the IP addresses or the algorithms used in the public ledgers.

Macro implications and policy options

If the use of cryptocurrency and their value continue to grow, financial institutions, whether they are regulatory bodies or intermediaries, will be forced to adapt to the new realities and perform their main duties of protecting consumers and acting as institutions of trust and transparency. Even though the impact of cryptocurrencies may be huge in many areas, this paper focuses on the impact on financial structures and anonymity.

a) Regulatory implications

A market is an environment where supply meets demand. The money market is, as any other market, also dependent on the movements in supply and demand. Looking at the way in which Bitcoins are generated, it is easily noticeable that the supply is fixed, while the demand for cryptocurrencies remains unknown. The volatility index depends on the movements of supply and demand. The current volatility index of bitcoins stands at 3.90. Traditional currencies also face the problems with volatility since the concept of the perfect market is utopian, but in this case central banks and secondary banks take all necessary actions to stabilize the market. In the cryptocurrency world, the market itself must drive this process.

Apart from a possible bubble affect, the main threat from using cryptocurrencies is related to the shift of decision-making power from the central banks. Until now, the central banks have had a monopoly in deciding and shaping monetary policy. In a decentralized system, national policy makers are challenged to define the role of regulators responsible for monitoring the system. Regulators have the duty and legal responsibility to ensure the stability of the financial system, identify and mitigate the risks, and protect the consumers, clients or investors participating in the system. It is inevitable that in the future cryptocurrencies will be under regulatory pressure, especially if this technology minimises the role of traditional currency or fiat money. The more the cryptocurrency will minimise or even substitute fiat money, the more national regulators will try to monitor and mitigate the risk associated with it.

Secondary banks are embracing the opportunities that the new technology is offering. Banks and other financial institutions have prepared special programmes and research in order to better assess these opportunities. A group led by Swiss banking giant UBS and ten other companies plans to develop its own digital currency. (World Economic Forum, 2017). Other banks like Barclays and BNY are involved in similar projects, which is a clear signal for the central banks. In 2016, there were 26,885 projects based on the use of blockchain, but only 8% of those projects are still implemented and they are characterized by a short lifespan of 1.22 years. The geographical leader when it comes to such projects is San Francisco, which houses 101 organisations with 1279 users. London takes second place, with 858 users and 61 organisations, and New York is third, with 725 users and 49 organisations. (Jesus Leal Trujillo, 2017)

At the country level, Finland is giving refugees bankcards based on blockchain technology. This technology gives refugees a secure digital ID so the new arrivals can pay bills and receive wages. According to the World Economic Forum, the card has a unique digital ID stored in a blockchain, which means that the government doesn't need to go through a traditional bank. The refugees generally lack documents and without an authenticated digital identity it's difficult to get a job or a bank account. The United Nations is also analysing whether or not it could solve many refugees' problems by using blockchain credit cards. (World Economic Forum, 2017)

Considering the special role of Central Banks as institutions that guarantee and back the value of the currency as well as the role of regulators, several attempts have been made to study, analyse and assess the impact of cryptocurrencies. (Barrdear J, 2016). A global survey launched by the Financial Stability Board's Fintech Issues Group in February 2017 indicates that 20 of 26 jurisdictions that were contacted have already taken some measures to respond to fintech, with five additional jurisdictions planning to follow suit. (Financial Stability Board, 2017). On one hand, they have to protect the participants and inventors from risks, but on the other hand, they are responsible for enabling and supporting the development of the financial market. It is an ongoing debate between regulators and industry about how much to regulate without overregulating.

How regulators will treat and face the challenges coming from the growing effects of the cryptocurrencies will shape their future development. Moreover, if this technology continues to expand in the upcoming years, regulators will need to even legally redefine the functions, duties and responsibilities of concepts such as money, a unit of value, the payment system, and actors participating in the financial system.

One of the greatest challenges that regulators face is how to ensure financial stability in a developing environment in which the risks and participants are still to be defined. The stability of a financial system relies on certain pillars, such as a sound monetary policy, an efficient system of payment, and smoothing the shocks and mitigating the risk. New technologies directly and indirectly impact all of those pillars, so regulators would have to adjust their actions accordingly.

International associations or institutions dedicated to supervisory authorities such as the Bank for International Settlement, ESMA, IAIS, IOSCO, several banks' associations but also the IMF and World Bank should play an active role in fostering collaboration within supervisory bodies in order to reach a certain level of global harmonisation of rules and actions and avoiding "paradise" spots in which such initiatives may develop. (IOSCO, 2017) (International Monetary Fund , 2017) (Basel Committee on Banking Supervision, 2017) (Dong, 2016) (He, et al., 2017)

b) The implication of anonymity

Anonymity is a threat that may have an impact in the further development of bitcoin and cryptocurrencies, especially in relation to the use of this technology for criminal activity or money laundering. The regulators are taking action and are including blockchain and bitcoin transactions within the regulatory framework for anti-money laundering. The European Commission has already taken some steps forward in this regards by expressing the need to apply AML legislation to businesses that use cryptocurrency. (European Commission).

Although other cryptocurrencies are being developed, the case of bitcoin is more advanced in the legislative framework. In the United States, virtual currency is treated as property for tax purposes. This also suggests that compulsory monitoring and reporting to the tax authortities will need to be introduced. Additionally, there is a special status for the exchange as Money Service Businesses, which must be licensed and comply with very specific requirements. Nevertheless, most of the juridictions are still starting out when it comes to understanding the new technology and defining cryptocurriencies and their functions. It would be a very limited worldview that considers cryptocurrencies to be property alone. Their functions are much more complex because they simultaneously act as a property, a payment system and a digital token simultanously. Once the parties and their duties, as well as the legal status of cryptocurencies have been defined, decisions will need to be made as to the anonymity of participants, in order to protect the system against risks.

Conclusion and recommendations

The continuous increase of usage of cryptocurrencies results from three main factors. The first factor is the development of new technologies that enabled the creation of virtual cash and the encryption of data. The second factor is related to the tendency to innovate in financial services in order to increase profits. The third factor is strongly related to the aim of improving client experience and access in the financial system and in the usage of financial instruments.

The financial system and its participants will be affected if the use of cryptocurrencies continues to grow. We will be forced to redefine the functions of regulatory bodies and intermediaries that will inevitably arise.

The use of blockchain cryptocurrency opens the door to new opportunities not only in the financial market but also in other areas of activity. They have the power and the potential to transform and develop new business models and create innovative solutions. Although the new technology represents a world of opportunities, there are many risks and threats that should be taken into account. One of them is the level of anonymity technology guarantees to users, which in turn creates a very fertile ground for money laundering and criminal activities. There is an urgent need for further legal initiatives in this area from the regulatory bodies in order to protect the investors and the payment system.

If the new technology continues to develop, banks will need to adapt to new realities where they will not only operate as intermediaries. In order to survive in the new system, banks should innovate or implement the new technologies. Some large banks are already implementing and preparing adaptation programs and others should follow them before it is too late. The winners are always the ones who embrace and welcome innovations.

Considering the high interconnectedness of the financial system, regulators and policy makers must coordinate their activities and share experiences.

The number of bitcoins is limited, so the future supply is somehow fixed, while the demand remains unknown. If there are imbalances, they will affect not only the value of bitcoins, but might be accompanied by transaction costs. After all, this is what Satoshi Nakamoto had in mind when designing a system that would resemble the mining of gold, a precious metal with an eternal influence on the history of money.

Bibliography

Books

Mishkin Frederic S. 2004, T*he economics of Money and Banking and Financial Markets*. New York: Pearson.

Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S, 2016, *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University Press.

Wash Carl E, 2010. *Monetary Policy and Theory*. Cambridge: MIT Press.

Research Papers

Barrdear J, Kumhof M. 2016. Staff Working Paper No. 605. *The macroeconomics of central bank issued digital currencies*. London: Bank of England.

Basel Committee on Banking Supervision, 2017, *Sound Practices: Implications of Fintech Developments for Banks and Bank Supervisors*. Basel: Bank for International Settlement.

Brito J, O'Sullivan A. 2016. *Bitcoin: A Primer for Policymakers*. Fairfax, Virginia: The Mercatus Center at George Mason University.

Dong He, Karl Habermeier, Ross Leckow, Vikram Haksar, Yasmin Almeida, Mikari Kashima, Nadim Kyriakos-Saad, Hiroko Oura, Tahsin Saadi Sedik, Natalia Stetsenko, Concepcion Verdugo-Yepes. 2016. *Virtual Currencies and Beyond: Initial Considerations*. IMF Staff Disscusion Note.

Dong He, Ross Leckow, Vikram Haksar, Tommaso ManciniGriffoli, Nigel Jenkinson, Mikari Kashima, Tanai Khiaonarong, Céline Rochon, and Hervé Tourpe. 2017. *Fintech and Financial Services: Initial Considerations*. IMF Staff Disscusion Note.

Alex Biryukov, Dmitry Khovratovich. 2016. "*Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem*", University of Luxembourg.
https://www.cryptolux.org/images/b/b9/Equihash.pdf

Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities' Attention. 2017. Financial Stability Board.
http://www.fsb.org/wp-content/uploads/R270617.pdf

International Monetary Fund. 2017. *Global Financial Stability Report: Getting the Policy Mix Right.*

IOSCO, 2017, IOSCO Research Report on Financial Technologies (Fintech).

Iwamura M, Kitamura Y, Matsumoto T, Saito K. 2014. *Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money.* Institute of Economic Research, Hitotsubashi University.

"*The Pulse of Fintech Q4 2016: Global Analysis of Investment in Fintech.*" 2017. KPMG.

Satoshi Nakamato. 2008. "*Bitcoin: A Peer to Peer Electronic Cash System*"
https://bitcoin.org/bitcoin.pdf

Trujillo J. L, Fromhart S., Srinivas V. 2017. "*Evolution of blockchain technology Insights from the GitHub platform*".
https://dupress.deloitte.com/dup-us-en/industry/financial-services/evolution-of-blockchain-github-platform.html

Web pages

European Commission. *Legislative Proposals on Financial Crime.*
http://ec.europa.eu/justice/civil/financial-crime/applying-legislation/index_en.htm

World Economic Forum. *Banks are finally starting to adopt cryptocurrencies.*
https://www.weforum.org/agenda/2017/09/banks-are-finally-starting-to-adopt-cryptocurrencies

World Economic Forum. *Sweden is on its way to becoming a cashless society.*
https://www.weforum.org/agenda/2017/09/sweden-becoming-cashless-society

Information Operations in the Hybrid/Non-Linear Warfare

Nurlan Aliyev

Nurlan Aliyev is a PhD Candidate/Researcher at the Institute of International Relations of the University of Warsaw. From 2000 to 2017, he has worked as an expert at various government, non-government and international institutions. His research focuses on political and social processes in Central and Eastern Europe, post-Soviet countries, regional security, and also strategic communication and asymmetric warfare threats.

Introduction

In hybrid/ non-linear warfare, any means can be used in order to reach the final goal. This becomes possible as the main players are getting hidden behind the smaller players. The main strength of this war manifests itself in remaining hidden as much as possible. The key player seeks to divert the 'fire', and to direct it against smaller players activated by the strength of the former. Consequently, it is not the key player itself, but the smaller players that are struggling to overcome the attacks. All these require the strengthening of information 'forces' to the maximum. ***Hybrid/ non-linear or asymmetric warfare relies on a combination non-military and military tools in conflict situations.*** However, the successful use of these tools depends on the efficient management of information warfare supported with special operations coordinated by those who conduct the non-linear warfare.

Non-linear warfare itself incorporates many of the political and economic elements of conventional and irregular war. Still, after a certain level, its success is contingent on the initial information operations used in special operations (Pocheptsov, 2015). Such information operations use disinformation, fake news and also, psychological warfare (psychological control operation) tactics as their main tools. Information operations are employed together with cyber operations.

This article analyses the informational effects of hybrid operations carried out by Russia, and investigates the application of information attacks over Bulgaria and Ukraine and the use of some political groups, in this particular case radical right forces, as propaganda tools in France and Italy. Ways of using disinformation, fake news, false narratives, trolls and far-right political groups in information operations are analysed in the article. Possible activities for preventing and deterring information interventions based on disinformation campaign are recommended.

The Government Betrayal disinformation operation – The Bulgarian Case

Bulgaria celebrates its Freedom Day on March 3rd every year, remembering how it gained its independence from the Ottoman Empire on that day in 1878. On the eve of Bulgaria's Freedom Day in 2016, the spread of contradictory information about the holiday caused concerns in society. The reason was that *The Bulgarian Times*, a local news portal, reported that the government of Bulgaria had issued an invitation for the participation of Recep Tayyip Erdogan, Turkey's now President and former Prime Minister, at the festive event on March 3, while similar invitation letter had not been sent to the Russian President Vladimir Putin (Bultimes.com, 2016). Bulgarian society has strong opinions on the role that Russia played in the country's nineteenth century rise to independence. The Treaty of San Stefano is a peace agreement signed on 3 March 1878 after a year-long war between Russia and the Ottoman Empire. Following the "The Bulgarian Times", the Russia news media started to re-publish this piece of news. Commenting on the issue, the Russian President's press secretary Dmitry Peskov said that the invitation for the 138th anniversary of independence of Bulgaria from the Ottoman Empire's occupation had not been sent to President Vladimir Putin by the Bulgarian government. Bulgaria's Foreign Ministry's official Betina Joteva said that none of the foreign heads of state had been invited to attend the events in Sofia, since the invitations had been sent only to foreign diplomats based in the country.

Russia has been frequently using its historical, religious and cultural ties with Bulgaria as leverage, to ensure that its interests are represented within. Such same attempts have been made in the context of the South Stream pipeline project, the opening of NATO's command centre in the country, and Bulgaria's refusal to allow Russia to use its airspace for military air transport. This led to the protests and information campaigns organised by the country's pro-Russian forces.

Apart from above-mentioned cases, following the shooting of the Russia's Su-24 aircraft at the end of 2015, tension was generated within the *Rights and Freedoms Movement* (RFM), also known as a Turkish minority party. Thus, Lutvi Mastan, the pro-Turkey chairman of the movement, resigned due to his statements in support of Turkey in connection with the shooting down of the Russian military aircraft. His statement was questioned by a pro-Russian group led by Ahmed Dogan, the party's founder and honorary chairman. Russia's relations with Turkey are a sensitive topic in Bulgaria, and many citizens feel that they are used as leverage against the pro-Western Bulgarian government. ***The seriousness of the issue following the events which took place in the RFM pushed the Bulgarian Parliament to establish a temporary commission to determine the impact of Russian and Turkish propaganda in the country.*** In this regard, the Russian Foreign Ministry immediately issued a harsh statement recalling the Russia's role in the liberation of Bulgaria from Turkish and fascist occupation and saying that the Kremlin was concerned about a strengthening 'neo-McCarthyism' in the Bulgarian community (Mid.ru, 2016). In response, the Bulgarian Foreign Ministry declared that no country has the right to interfere in the internal affairs of another. A few days later, the Russian Foreign Ministry's spokesman strongly reacted to an article by the Bulgarian Foreign Minister Daniel Mitov which was published in the local press on the same subject and stated that accusations against Russia 'belong to the individual politicians' and these initiatives 'could not change the Bulgarian people's historical memory' (Sofia News Agency, 2016). The false information given on the unknown Internet portals may seem insignificant at first glance, but it could lead to broad public debate and diplomatic tensions. This case is an operation of the hybrid nature conducted by Russia against the Bulgarian government and the media attack was one of the main parts of this operation. **The incident concerning the "Freedom Day" activities in Bulgaria must be viewed within the context of the information warfare.**

First of all, any false information posted on the internet portal it was created for similar purposes. For instance, the above-mentioned *The Bulgarian Times* disseminates news related to euro-sceptic and anti-immigrant trends. The site declared that it had obtained the information related to Freedom Day from podoko.eu, an unrecognized local website. The editor of podoko.eu is Nikolai Ivanov, a member of the pro-Russian and opposition Social Democratic Party (Chursin, 2016). ***Although such Internet portals are not well recognized, they have many "followers" on social networking sites. Usually most of the "followers" are fake profiles of paid employees-trolls registered on social networks. In order to make the fake information convincing, that source usually refers to a blog, politician or public figure and well-known media outlet. The main purpose of such operations is to spread information as widely and quickly as possible. Therefore, such fake outlets have a large number of troll-followers on social networks. Although the false information was later denied in a consistent way, it had already fulfilled its mission.*** Thus, according to the public relations rules, the main job in the transmission of information to the audience is to be the first one to do so. Although that information is later proved to be false, it may leave some impact on the target audience and create suspicions. Additionally, the parties that disseminate false information may use it for their own purposes.

For example, in the case of Bulgaria, the aim may consist of the following facts:

1. To persuade public opinion of a new idea or to strengthen already established ideas. In this case, this idea centred on politicians sacrificing the country's national interests to 'historical enemies' by inviting Turkey, the Ottoman Empire's successor, to the celebration, rather than Russia, which is supposed to be a 'saviour of the country'. This was quite a sensitive issue in the Bulgarian society.
2. To create a narrative which can be used by Bulgaria's pro-Russian forces future electoral campaigns against the current government.

This is not a one-time event and should be considered as a part of long-term trend of information warfare. Russia's modern information operations reflect the elements of propaganda, counter-propaganda and disinformation. These operations may have a convincing or confusing character, in accordance with their objectives. The Bulgarian case mentioned above bears the signs of information warfare and information operations, which are considered to be a major organising factor of hybrid warfare.

Designing false narratives before occupation and using soft power as a tool in information operations – the Ukrainian Case

Russia's successful information operations were observed during the armed conflict in Ukraine. British experts divided Russia's information warfare in Crimea and Donbas into the following phases:

1. creation of loyalty through cultivating the cultural, linguistic and ideological ties of Russian minorities and Russian-speaking communities of these regions towards Russia;
2. spreading fear among the population about a supposed government crackdown against them. This phase included a strong emphasis on the Soviet army's role in liberating those areas from the Nazi German occupation during World War II;
3. defence of these regions by the Russian military or civilian forces and the 'humanitarian intervention', with the aim of encouraging those regions to join Russia (Thornton 2015, 45).

Russian information attacks in Crimea and Donbas started even before the 2014 events. Those effects first began to look like a regular and active information operation during the first Maidan events (2004). Since the majority of the population in these areas is Russian-speaking and have close historical, cultural and economic ties with Russia, Moscow could successfully carry out information operations there. In addition to the media institutions, Russia also used educational and cultural institutions for propaganda in Crimea. The local branch of the Moscow State University (MSU) played an important role in spreading propaganda among the local youth. The MSU's branch, which worked independently in the early years following its inauguration, was known as an educational institution that brought international experts for lectures and organised high-quality educational programmes. However, the management of the branch was changed later on and the institution has become an instrument for 'brainwashing'. Afterwards, the MSU's branch started to invite only Russian experts, notably the propagandists of Russkiy Mir (Russian World) to deliver a lecture. Next, local businessmen closely tied to Russia began to organize charity events, such as creating and renovating museums, galleries, and exhibitions of the Great Patriotic War. Those businessmen played an important role in the promotion of so-called George's ribbons. Local experts who witnessed those events listed the following five reasons due to which Russia's media operation on Crimea was successful (Aliyev, 2016):

1. The ethnic factor - Crimean Tatars and their non-Slavic roots were presented as a threat;
2. The failure of Ukraine's policy (working with the media, counter-propaganda, poor sociocultural awareness) aimed at the Russian-speaking population;
3. The failure of Ukrainian nationalist ideas in Crimea where a large proportion of the Russian-speaking population lives;
4. The presence of strong local self-identity;
5. The promotion of the idea [before the invasion of Crimea] that Ukraine could collapse just as the Soviet Union did (this action envisaged the 'legalization' of the idea of Crimean secession among the local population).

Russia created an alternative reality in the information space by using historical factors (the 'Russification' of these regions during the Russian Empire and the USSR) formed in Donetsk and Luhansk many years ago. These factors resulted in a type of historical weakness when it comes to the identification of Donbas's population with Ukraine. Both during the Soviet period and since independence, the negligent attitude of official Kyiv towards the eastern regions has played a role in creating those conditions. In addition to other factors, the lack of sufficient Ukrainian content in these Russian-speaking regions (as happened in Crimea) and the activities of *Russkiy Mir* (Russian World) have played important role in the formation of an alternative reality. When the active phase of Russia's activities began, Kyiv's lack of understanding when it came to information policy and a lack of timely measures for accurate directions became a serious problems. In this phase, civil society became the main actor taking measures against information war. The information operations carried out by Russia widely used narratives tjat were popular during the Soviet period and shortly after independence. According to such narratives, the Eastern regions 'supply the entire country with basic products'. The overthrow of Yanukovych did, on the other hand, have a huge psychological impact in the country's eastern regions and was used to that effect. Thus, during the rule of Yanukovych, who is originally from Eastern Ukraine, these regions regarded themselves as necessary and important provinces. Yanukovych's resignation gave rise to a so-called 'abandoned child syndrome' in these regions. ***The regional factor, which was widely used for the political struggle in Ukraine during the years of independence, played in favour of Russia while it carried out its information operations against Ukraine. This allowed Russia to maximise its psychological impact on the eve of the beginning of the conflict. In fact, the approach created by the Ukrainian political circles at that time was now used against them and the country.***

Another narrative which was used for psychological impact in the information operations consisted of inconceivable 'facts' such as a 'Nazi attack against the civilian population in these regions'. The Nazi terminology in the Russian propaganda is used to refer to the country's far-right nationalist organizations (especially the *Right Sector*) and generally to Western Ukraine. The journalists and civil society activists captured by the separatists' military forces were tortured and forced to make false confessions (for the purpose of generating hatred and using them as anti-heroes), which were techniques widely used by Russia in the information warfare (Strategy XXI, 2016).

The majority of audiences' trust in the accuracy of this type of false information can be explained by several factors:

1. This type of information propaganda is of a confusing nature and it is continues non-stop, making it impossible for an unprepared person to deeply understand and analyse the information received;
2. Quantitative factors – the amount of interconnected information was very high. In this case, the majority of people is inclined to subconsciously believe in the

pieces of information connected to each other and of the same type;

3. The factor of trust in broadcasting – this feature is applicable to the most of population groups in the former Soviet Union (especially among the middle-aged and the older generation). This approach can be summarised as 'if the TV says so, then it must be true';
4. Limited or no access to alternative sources of information;
5. The education level of the population (it is mainly poorly educated people who tend to believe false information of propaganda purposes).

The last two factors play an important part in counter-measure efforts in the information war. ***A domination of the information space, a reflection of different views to make the population believe the media, and the education level of the population are of great importance in the information war***. Latvia, for example, encouraged the opening of local media in the Russian language to protect the Russian-speaking community in this country from the influence of a Russian propaganda-style media sphere. Despite the fact that some local Russian-language websites have sharply criticized the Latvian government, such approaches and measures prevent the outburst of the "negative energies" of Russian-speaking people and minimise the chance of Russia benefitting from this outburst.

Active civil society can play an important role in the information wars. In the first period of the Ukraine crisis, civil society actively fought against the information attacks of Russia. In order to combat fake news and propaganda disseminated by the Russian information TV channels, the StopFake.org Internet portal generated by journalists did important work in this area.

Use of far-right political organizations and individuals as means of propaganda in the European Union

A majority of anti-immigrant and populist political organisations operating in the have connections to Russia, as do their leaders (Polyakova, 2016). Some Moscow-controlled media outlets (such as RT and Sputnik) support these organisations. So far, Russia has indirectly provided financial assistance to the radical political organizations operating in the EU (Re:Baltica 2015), including to the France's National Front, of which there is proof.

FN accepted a €9.4m ($10.6m) loan from First Czech Russian Bank, a lender with indirect links to the Kremlin (The Economist, 2015). Russia does not simply provide press support for these organizations. In some cases, the Kremlin indirectly grants financial support for individuals of radical political groups in the EU member countries for the creation of media tools. It is possible to witness such activities in case of France and Italy.

In case of France, persons close to the National Front (FN) and other radical organizations have implemented media projects with the financial support of Russia.

Gilles Arnaud, the FN's former regional adviser and member of the French far-right Party (*Parti de la France*, PDF, 2009) heads a media association called *French Association Groupe EDH Communication*. This association includes media entities such as *Agence-2-Presse, TV Norman Channel* and *Editions d'Heligoland*. Gilles Arnaud, who attended an international summit entitled *Global Media: challenges of the XXI* century held in Moscow in July 2012 established a relationship with the management of the *ITAR-TASS* news agency and the *Voice of Russia*. Consequently, *Groupe EDH Communication* received funding from Russia for the creation of a new television channel. Allegedly, Alexander Orlov, Russia's Ambassador to France assisted in signing the contract between Arnaud and the Russian state media. Arnaud opened the *ProRussia.TV* web TV in September 2012 with the funds (115.000 euros) obtained according to the agreement. According to the agreement, he was to receive additional 300.000 euros for the next year for his television activities (Jauvert, 2014). *ProRussia.TV* was realised in co-operation with *Agence2Presse, ITAR-TASS, Interfax* (the Russian news agency), *Voice of Russia* and the Iranian *Mehr News Agency* (ProRussia TV). The channel operated until the summer of 2014. The main subjects of channel were pro-Russian, anti-American broadcasts and those that dealt with the suppression of democracy in the EU. Television allocated extensive broadcasting time for radical right-wing leaders in Europe as well as to Russian nationalists. Later, Arnaud in cooperation with Philippe Milliau, a radical nationalist politician and a co-founder of *Réseau Identites* (Identity Network) opened a new television channel known as *Notre Antenne TV*. However, that television project did not last long and Philippe Milliau abandoned the idea. Although Philippe Milliau justified this step with his reluctance to be directly dependent on Russia, many experts say that he merely aimed to wipe his traces. It is noteworthy that, after a short period, Philippe Milliau along with several other radical nationalists opened a new TV channel. At the beginning of 2014, Philippe Milliau, together with Yvan Blot, Le Gallou and other radical nationalist politicians, introduced *TV Libertes*, a new channel. Apart from the above-mentioned radical nationalists, Robert Menara, a co-founder of Reporters Without Borders (*Reporters Sans Frontières*) and a mayor of Béziers (elected with the support of the National Front in 2014) participated in this project. Although *TV Libertes* did not openly support the Moscow's policy as directly as *ProRussia.TV* did, television broadcasts reflected the pro-Russian orientation too. This channel was the only French TV broadcasting an event organized in the Russian Embassy in 2014 dedicated to the visit of now former State Duma's speaker Sergei Naryshkin. It also provided positive and extensive coverage of the elections held by separatist regimes in Donetsk and Luhansk (Clemenceau, 2014).

Russia's media operation carried out in Italy is similar to that in France. Representatives of the nationalist *Northern League* have acted as local partners for Russia. The website of the Lombardy-Russian Cultural Association (*Associazione Culturale Lombardia-Russia*, ACLR, 2014) is working closely with official Russian media. The information of the website is not lagging behind the propaganda news broadcast by Russian media.

The initiator of ACLR is Max Ferrari, a member of the Northern League and an employee of the Italian branch of the *Voice of Russia*. The President of the Association is Gianluca Savoini, a spokesman of Matteo Salvi, leader of the Northern League party. The Honourary President of Association is Alexei Komov, Russian representative of the *World Congress of Families*. Komov is considered to be close to Konstantin Malofeyev, a radical nationalist and oligarch known for his close ties to the Kremlin. It is also possible that Malofeyev indirectly finances the Northern League. Malofeyev openly declares his desire to restore the Russian empire (Weaver 2014). The co-chairman of Piedmont-Russian Cultural Association (*Associazione Culturale Piemonte Russia*), which is a branch of ACLR, is Alexander Dugin. Dugin declared that Matteo Salvinini was an only politician representing the true interests of the people of Italy. In October 2014, the Northern League party and the ACLR's delegation paid a visit to Crimea. During the visit a cooperation agreement on the 'exchange of information' was signed between the 'Ministry of Information and

Communication' of Crimea, the *Krιminform* news agency and ACLR (Lombardiarussia.org, 2014).

Moscow has two main objectives in providing support for the creation of media in these countries:

1. to provide information in the local language on sensitive issues from Russia point of view and use it to pressure local authorities (including on issues related to Middle Eastern migrants);
2. to provide indirect financial assistance to these political groups under the guise of creating media institutions and using these financed individuals as agents (like in France and Italy).

As mentioned above, the Kremlin is eager to develop relations with far-right political groups in France, Italy and throughout Europe. Their main goal in this is to establish and support Russia- friendly groups and individuals with the aim of using them for the Kremlin's influence activities. Such groups might be used as channels for spreading news that would be in the interest of the Kremlin. Although such channels may not seem so influential in formulating public opinion, they might be useful as separate parts of a communication strategy. And Moscow has used such groups as part of its communication influence activities towards the EU.

Conclusion

In hybrid/non-linear warfare, information plays a major role. This is because events change quickly, which leads to a constant interpretation and re-interpretation of facts, as well as a constant need for propaganda and counter-propaganda due to the discrepancy between the 'created information' and the real situation. ***The main feature forming the basis of hybrid warfare is that the aggressor state seeks to shake the victim-state from the inside through the complex use of non-military and military force (political, economic, military, humanitarian, etc.), i.e. mainly not through military operations, but by weakening the socio-economic foundations through exploiting some external and chiefly internal factors***. The ultimate goal of the attacker is to achieve internal selfdestruction of the selected object. In this case, both the external influences as well as open military intervention act as auxiliary means.

An aggressive government uses information operations and propaganda to describe such impacts as an 'internal conflict' to a domestic audience, the government, and the foreign community. ***In this situation, the ultimate goal of information operations is to create uncertainty. Even if the uncertainty lasts for a short period of time, it allows the attacker to interpret the events in a desired form, to confuse the object-country including its public, decision-makers, as well as foreign circles, and make them take the wrong decisions.***

Information warfare during the Cold War was understood as justification of propaganda or counter-propaganda activities between Russia (formerly the Soviet Union) and the West in order to convince the other party of its wickedness and political problems. At present, this method of struggle is based on fuzzy logic, rather than on a (previous) coherent logical explanation. In modern times an audience (of any nationality) exposed to information warfare is not aware of an ongoing information attack most of the time. As a result, the attacked state does not use the mechanisms in its disposal. Thus, it establishes the foundation of future defeats. While you are directly affected by the use of different military arms and military tactics in conventional war, information war implies the use of more flexible, more diverse and often unpredictable means. The direction and tools of attack in information wars are often unpredictable. According to Stephan Lewandowsky, a cognitive scientist at the University of Bristol who studies the persistence and spread of misinformation, having a large number of people in a society who are misinformed and have their own set of facts is absolutely devastating and extremely difficult to cope with (Gray, 2017).

Information security, which is the pinnacle of national and public security, must be protected not only by technological and cyber tools, but also by narratives and other strategic communication methods. Technical solutions are not enough to ensure information security in the modern world where countless of websites, social media accounts and trolls armed with a plethora of fake news stories and alternative facts continue their subversive activities (Aliyev, 2017). Any state should implement the following to be ready for information warfare:

1. establish structures that focus on analysis, communication and psychology, staffed by qualified professionals;
2. pay attention to the development of local media and information spaces. Such spaces should be open to different opinions in order to minimize the effects of alternative information obtained by the country's citizens from the other states' news outlets that is differ from the information presented in the official news. It is important to stress that in the modern, highly precarious world, correctly informed citizens play a huge role in the security and prosperity of states and nations.

Bibliography

Aliyev. 2017. “*The Art of Communication during Migrant Crisis*”. Visegrad Insight.
http://visegradinsight.eu/the-art-of-communication-during-migrant-crisis/

Aliyev. 2016. Interviews and discussions with local experts, media representatives and activists in Ukraine (include from Donbas and Crimea), July - August, 2016

Bultimes.com. 2016. “*За 3-ти Март на Шипка не каним Путин, но каним Ердоган*”. Bultimes.com.
http://bultimes.com/za-3-ti-mart-na-shipka-ne-kanim-putin-no-kanim-erdogan/

Clemenceau. 2014. “*Ce lobby qui défend Poutine*”. Lejdd.fr.
http://www.lejdd.fr/International/Europe/Ce-lobby-qui-defend-Poutine-685316

Chursin. 2016. “*«Эрдоган вместо Путина» -российские СМИ опять муссируют фейк»*”. Новая Газета.
http://www.novayagazeta.ru/politics/72120.html

Gray.2017. “*Lies, propaganda and fake news: A challenge for our age*”. BBC.
http://www.bbc.com/future/story/20170301-lies-propaganda-and-fake-news-a-grand-challenge-of-our-age

Jauvert. 2014. “*Poutine et le FN : révélations sur les réseaux russes des Le Pen*”. Nouvelobs.com.
http://tempsreel.nouvelobs.com/politique/20141024.OBS3131/poutine-et-le-fn-revelations-sur-les-reseaux-russes-des-le-pen.html

Lombardiarussia.org. 2014. “*Соглашение о сотрудничестве с Министерством внутренней политики, информации и связи Республики Крым и агентством новостей Крым Информ*”. Lombardiarussia.org.
http://ru.lombardiarussia.org/index.php/component/content/article/57-categoria-home-/257-2014-11-11-12-44-23

Mid.ru. 2016. “*Брифинг официального представителя МИД России М.В.Захаровой- О создании в болгарском парламенте Временной комиссии по изучению фактов и обстоятельств, связанных с утверждениями о вмешательстве Российской Федерации и Турецкой Республики во внутренние дела Болгарии*”.
http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2111747#12

Pocheptsov. 2015. “*Роль информации в гибридных войнах*”. Prportal.com.ua.
http://prportal.com.ua/Peredovitsa/rol-informacii-v-gibridnyh-voynah

Polyakova, Laruelle, Meister, and Barnett. 2016. “*The Kremlin’s Trojan Horses*”. The Atlantic Council.

http://www.atlanticcouncil.org/publications/reports/kremlin-trojan-horses

ProRussia TV. Accessed November 10, 2017.
http://original.livestream.com/prorussiatv

Re:Baltica. 2015. "*Kremlin's millions: How Russia funds NGOs in Baltics*". Delfi.
http://m.en.delfi.lt/article.php?id=68908408

Strategy XXI. 2016. "*«Гибрессия Путина. Невоенные аспекты войн нового поколения». Центр глобалистики «Стратегия XXI».*"
http://geostrategy.org.ua/images/Hybression_finversion.pdf

Sofia News Agency. 2016. "*Russia Lashes Out at Bulgaria FM*".
http://www.novinite.com/articles/173500/Russia+Lashes+Out+at+Bulgaria+FM+over+Article

Thornton, 2015. "*The Changing Nature of Modern Warfare -Responding to Russian Information Warfare*". The RUSI Journal, Volume 160, Issue 4: 40-48.
http://www.tandfonline.com/doi/abs/10.1080/03071847.2015.1079047

The Economist. 2015. "*In the Kremlin's pocket*". The Economist.
https://www.economist.com/news/briefing/21643222-who-backs-putin-and-why-kremlins-pocket?fsrc=scn%2Ffb%2Fte%2Fpe%2Fed%2Finthekrlemlinspocket

Weaver. 2014. "*Malofeev: the Russian billionaire linking Moscow to the rebels*" The Financial Times.
https://www.ft.com/content/84481538-1103-11e4-94f3-00144feabdc0

Evaluation of the Ukrainian Internet Governance Eco-System as a key element for inter-stakeholder strategic communication

Oleksandr Tsaruk

Introduction

Nowadays, the multistakeholder model of Internet governance is considered to be the best mechanism for maintaining an open, resilient, and secure Internet because, among other things, it is based on equal participation of all interested parties – including businesses, technical experts, civil society, academia and governments – who adopt mutually significant decisions by consensus through a bottom-up process. This is the process that is used to elaborate on policies affecting the underlying functioning of the Internet domain system.

However, there are a lot of aspects, fields, communities and states where a multistakeholder model of Internet governance has not yet proved to be successful/to be working.

The main question which this research trying to answer is what the place of Ukraine in global internet governance ecosystem is and what actions are needed to develop the mechanism locally.

Background and statement of the problem

Governments and private sector usually deal with the ‘digital divide’ - the gap between socio-demographic groups and regions that have access to modern information and communication technologies (ICTs), and those that do not or only have restricted access. ICTs include the telephone, television, personal computers and the Internet, as well as all the related software and applications.

In its early development, the Internet would often be assessed from a technological perspective. However, during the last decade, other issues, often qualified as “soft”, have emerged focusing on topics such as human rights, democracy, privacy, social equity, inclusion, local content creation, interdependence, and other cultural, educational, economic and political aspects of Internet use.

Such discussions have been ongoing since the creation of the Internet Governance Forum (IGF), which resulted from the two World Summits on the Information Society (WSIS in Geneva, 2003, and Tunis, 2005) and the WSIS+10 Review Process and outcomes. In this context, ‘language’ separation and English-language content monopolism is increasingly recognized as an issue. (*World Summit on the Information Society 2012*)

Today, the international community has several multi-stakeholder mechanisms for discussions on and implementation of solutions on Internet governance issues. The WSIS events and IGFs are among the major ones. To participate in international multi-stakeholder processes, countries and their national representatives need to be equipped with proper language skills and tools that facilitate understanding, cooperation and coordination.

For quite long, Ukraine was not a part of the global process of internet governance development. Only single players were present on the global level.

Therefore, communications between basic stakeholders were not visible and still remain fragmented in Ukraine. The local Internet governance eco-system is probably missing some principal elements and this research is going to uncover it.

Research question or hypothesis, aim and objectives

We consider Internet governance as a process aimed at the development and application by governments, private sector, and civil society in their respective roles of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

The **Aim** of the research is to evaluate the maturity level of the Ukrainian Internet Governance Eco-System and draft recommendations for improvement of inter-stakeholder strategic communications based thereof.

The main **hypothesis**, which will be verified, is: Ukraine's Internet Governance Eco-System is missing a representation of the Internet Users' community as a principal stakeholder. Without this community, the multi-stakeholder mechanism cannot legitimise any consensual decisions.

Roots of multi-stakeholder Internet Governance

Conversations regarding the Internet governance model have long expressed tension between stakeholders advocating for greater government supervision of the Internet and those advocating for a coordinating structure distributed across many actors — including international organizations, governments, the private sector, civil society. The best examples of the latter model are global institutions, such as the Internet Corporation for Assigned Names and Numbers (ICANN). What is this multi-stakeholder model and who are the stakeholders? How should power be distributed across various coordinating entities, and who decides on that? Is there something unique about this framework of governance or are there analogies in other areas of society?

Governance of the Internet is not a single-issue area. The governance encompasses a wide range of administrative and technical coordinating tasks necessary to keep the Internet operational and to enact related public policy. The tasks range from technical protocols and the administration of domain names and numbers to setting policies related to cybersecurity and human rights. As the Internet has evolved, many of these functions have been carried out by the private sector — such as private telecommunications companies that make contractual decisions to interconnect their networks, and information intermediaries that establish policy via terms of service with end-users — and by the Internet's technical community — which includes the Internet Engineering Task Force (IETF) and its institutional home, the Internet Society; the World Wide Web Consortium; regional Internet registries; and ICANN.

Tensions between multilateral and multi-stakeholder oversight can be seen in many of the global policy disputes around the Internet, ranging from long-standing questions about how to transition US oversight of Internet names and numbers to debates about types of interconnection that arose at the World Conference on International Telecommunications that convened in Dubai in 2012. Tensions between governments and the private sector are also evident in debates about encryption that mediate competing values in cyberspace, such as law enforcement and national security versus individual privacy and economic security. This collection of research lays out some of these controversies, seeks to explain the "multi-stakeholder model" of Internet governance and makes recommendations about the types of governance innovations necessary to maintain both Internet freedom and Internet stability in the coming years.

Therefore, we see Internet governance phenomena as a complex eco-system of interests carried out by many groups constrained by context-specific policies, markets and norms. Joseph S. Nye, Jr., a globally recognized researcher best known for his analyses of soft power, considers (2014) that "the emergence of a unitary cyber regime is improbable because of the different values and norms that exist around issues like cyber security and because of global disputes over cyber power (DeNardis, 2017)" Nye considers the structures underlying cyber governance a regime complex, with "a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages (DeNardis, 2017)" . Within this regime complex, governance approaches to issues take various forms.

"Multi-stakeholder" is a term used to describe how the administration of the Internet works in practice, but also often without explaining its actual meaning. What is this institutional form called multi-stakeholder governance and how does it connect to or differentiate from multilateralism? Various researchers still cannot agree on an answer to this question.

Key issues for discussion on the Internet Governance approach in Ukraine

The latest analytical observations of local researchers such as Olga Kyryliuk (Freedom of Expression in Times of Conflict: Ukrainian Realities, 2017) and range of the reports of international nongovernmental organisations with the focus on the protection of and respect for the freedom of expression in different countries confirmed that Ukraine "was traditionally ranked somewhere in-between, gradually improving its positions during each subsequent reporting period. Freedom of expression directly depends on the political and socio-economic climate in the country. Therefore, changing of peacetime realities, the annexation of Crimea and the protracted conflict in the East of Ukraine have led to the deterioration of the state's positions in international rankings (Kyryliuk, 2017)". According to the independent international Institute for Economics and Peace, Ukraine was ranked 156th in Global Peace Index 2016 and turned out to be in the group of countries with the lowest level of security.

"Finding a proper balance between protecting national security, including its information component, and ensuring freedom of expression in times of the most difficult trials for the country is a huge challenge and a test for democratic governance of the state and its orientation towards the protection of human rights." (Kyryliuk, 2017) suggests.

The observations argue that Ukraine was unprepared to resist information attacks from aggression in cyberspace and consequently was gradually closing its information space from external influence and trying to regulate its fillings. This caused some concerns among human rights activists and an international community but even "blocking" some resources on the Internet (which is technically impossible) did not find huge resonance among internet users, who have a variety of tools that allow them to circumvent such obstacles.

Regional cybersecurity trends as a threat to human rights

The President of Ukraine issued an order enacting the decision of the National Security and Defence Council of Ukraine (NSDC) "On the Information Security Doctrine of Ukraine" on 25 February 2017. The aim of that is to counter destructive information influence in a form of hybrid war. Definitions provided in the document are quite broad and may further lead to qualification of any nonconformist opinions as a threat to national security. It was also proposed that a specification for a mechanism that would block and take down Internet content which threatens national sovereignty or promotes some totalitarian regimes and their symbols be drafted at the legislative level. Internet users may therefore be held responsible/brought to justice upon the suspicion of acting against Ukraine.

Key institutional obstacles for implementing multi-stakeholder model of Internet governance

As a multi-stakeholder model is about inter-group strategic communication, it involves having a continual dialogue and finding solutions beneficial for all parties, or at least sharing awareness on common issues.

One of the first and most popular places for conducting such a dialogue is the Internet Governance Forum (IGF), a multi-stakeholder forum for policy dialogue on issues of Internet governance. It brings together all stakeholders in the Internet governance debate, whether they represent governments, the private sector, or civil society, including the technical and academic community, on an equal basis and through an open and inclusive process. The establishment of the IGF was formally announced by the United Nations Secretary-General in July 2006. It was first convened in October–November 2006 and has been holding annual meetings since then.

The first Ukrainian Internet Governance Forum (IGF-UA) was held in September 2010 in Kyiv. Since that time, the annual IGF-UA has been a continuation of the world series of Forums devoted to discussing the most important issues of the information society development, consolidation of efforts of state bodies, businesses, the online community, professional and academic elites in order to accelerate the implementation of the

IT-capabilities, creating conditions for the comprehensive development of Internet technologies for the public interest.

IGF-UA gathers participants from different countries who represent international organizations, governmental agencies, non-governmental and commercial organizations in the field of ICT and media. The 8th Ukrainian Internet Governance Forum IGF-UA was held on October 6, 2017.

About 150 participants attended the event from Ukraine and other states, representing government agencies, international organizations, the private sector, civil society, academic and technical community, the media. Some number of participants took part in the IGF-UA remotely.

The evaluation of Ukrainian Internet Governance Eco-System and its stakeholder's structure was done using data collected by questionnaire and survey shared among participants of IGF-UA in October 2017 in an online form. The following figures show the stakeholder and gender balance between the global IGF 2016 and IGF-UA 2017 (*Figure 1-2*).

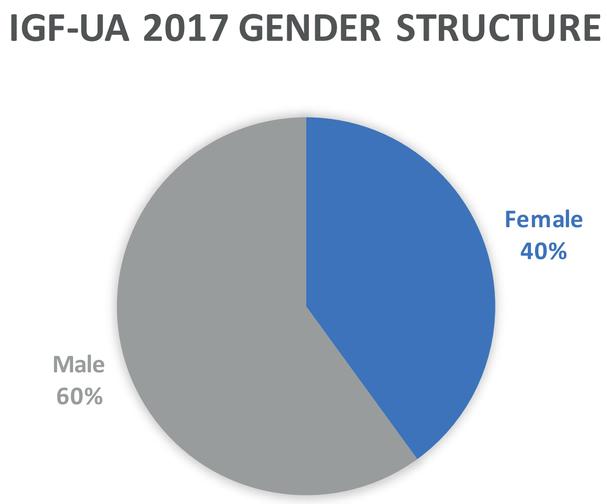


Figure 1. IGF 2016 Gender Structure

(source: igf-ua.org, intgovforum.org)

According to the announced results of the IGF-UA 2017 and IGF 2016, the proportion of the male to female on-site participation is the same – around 60% to 40%, respectively. The main difference is in the number of participants, which rose from 151 to 2066 persons.

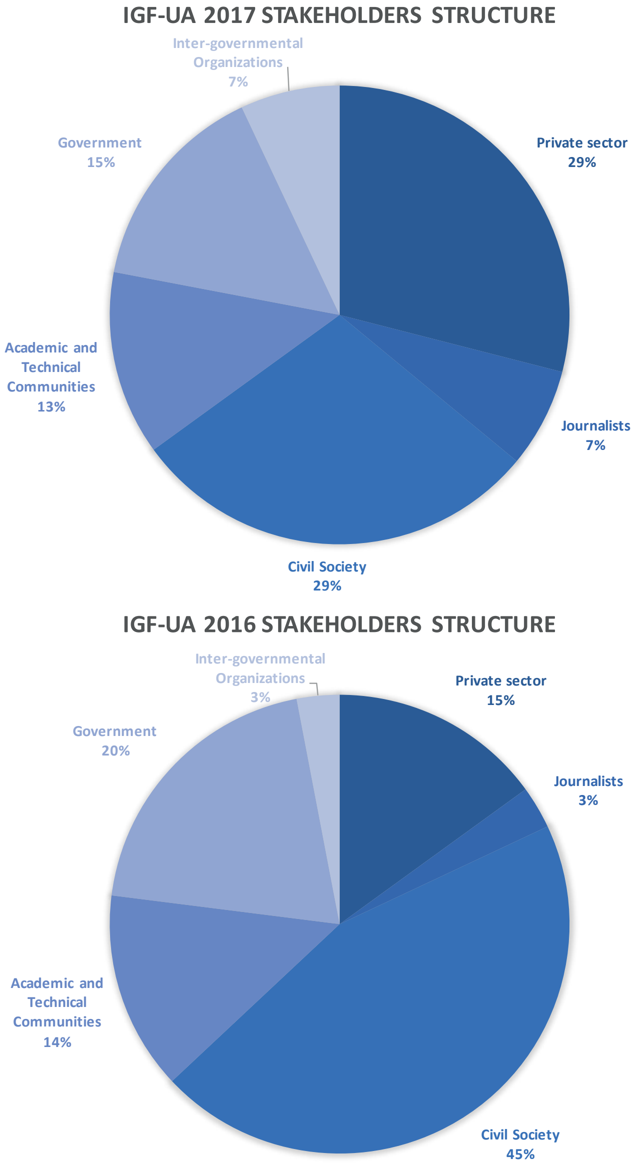


Figure 2. IGF Stakeholders Structure

(source: igf-ua.org, intgovforum.org)

As for the stakeholder structure of the IGFs on-site visitors, it is totally different. And at first glance, it might be considered that IGF-UA has a more balanced structure. Only the academic and technical group had a similar representation in 2016 and 2017, as did the government group. There is, however, a clearly visible difference in civil society with 45% taking part at a global level and 29% at a local level. When it comes to the private sector, 15% took part globally and 29% locally. The media sector, meanwhile, represented 3% of all participants in the first case and 7% in the second. This data suggests that Civil Society is playing a dominant role atthe global level but the Private sector is dominating locally, presumably because of closer interests. Civil Society can very often be affected by business, and be dependent on local projects, as can the government stakeholder, so the dominance of Private sector on local IGFs needs to be balanced by the influence of Civil Society at global level.

The issues of representation of the "Internet users" stakeholder group was raised during IGF-UA steering committee meetings, but as the global IGF does not have such a unit, the share of independent participants on local and global IGFs remains unmeasured and this group is probably not even represented by Civil Society in some countries, many of which even do not have an ISOC chapter like Ukraine does. Consequently, the role of representing interests of consumers of telecom services and Internet users tends to be fulfilled by the Government in many countries.

Outcomes and research impact

It can be observed that Ukrainian Internet governance eco-system can be affected by short and long-term possible impacts, and our research gives some reasons for this development. It also recommends the following policies:

In the short term, there is a big need to raise awareness of the real state of the internet governance ecosystem among active professionals in Ukraine.

In the long term, there is a need to create an analytical basis for a well-functioning system of internet governance in Ukraine. This could, for example, include creating an organisation that represents users and civil society and forms an integral part of the internet governance ecosystem.

The private sector will continue to dominate on the local level. Civil Society will remain influenced by international organizations. Some appropriate level of balance will therefore need to be found on the local IGF level as to legitimise the multi-stakeholder mechanism in Ukraine.

Bibliography

DeNardis, Laura. 2017. "Introduction". *Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance GCIG Research Volume Two Series.* https://www.cigionline.org/publications/who-runs-internet-global-multi-stakeholder-model-internet-governance

"*Why a Summit on the Information Society*". World Summit on the Information Society, International Telecommunication Union. 26 March 2008. Retrieved 26 May 2012. http://www.itu.int/net/wsis/basic/why.html

Kyryliuk, Olga. 2017. "*Freedom of Expression in Times of Conflict: UKRAINIAN REALITIES.*" http://cedem.org.ua/en/library/freedom-of-expression-in-times-of-conflict-ukrainian-realities/

E-governance in Ukraine: The digital-by-default principle in action

Olga Zykova

As Ukraine seeks to break away from the dysfunctional post-Soviet era and integrate into the European community, people increasingly turn to digital technologies. They are increasingly seen as a fast track to economic, political and social modernization. The introduction of e-Government initiatives is regarded as a way of improving the Ukrainian economy and standards of living, as well as reducing bureaucracy and cutting down on opportunities for corruption. E-Government can play a key role in Ukraine's transformation into a competitive economy and modern European society.

The processes that are currently starting to take place in the Ukrainian society were described as "a magnificent information and communication revolution" in the World Bank's (2016) "Digital dividends" report. Ukraine's main "weapons" include knowledge, innovation, technology, uninterrupted access to information.

One of the indicators which make it possible to measure the global spread of digital technologies is the Digital Adoption Index (DAI) (United Nations, 2016). The DAI is a composite index that measures the depth and breadth of adoption of digital technologies in 171 countries, spanning every region and income group. It is "based on three sectoral sub-indices covering businesses, people, and governments, with each sub-index assigned an equal weight". According to the World Bank Report, Ukraine's DAI is higher than in lower middle-income countries of the region and amounts to 0.51.

Over the past five years, Ukraine has seen an increase in the development of new e-government tools. This trend accelerated especially after the 2014 Revolution of Dignity. Social media continued to play a pivotal role throughout the Revolution, and steady advocacy campaigns by civil society since 2014 have prompted series of reforms. These include the introduction of e-petitions (the first time in Ukraine's history this has happened), open budgeting, mandatory online asset declarations and ambitious open data and e-procurement agendas. The country's progressive advances in e-government and e-democracy did not go unnoticed in 2016. Since 2014, Ukraine has significantly improved its global ranking:

- by 45 positions, up to 32nd place, in the UN E-Government Survey;
- by 30 steps, up to 24th place, in the Global Open Data Index; and
- by 18 positions, up to 44th place, in the Open Data Barometer ranking.

The UN E-Government Survey, which presents a systematic assessment of the use and potential of information and communication technologies to transform the public sector by enhancing efficiency, effectiveness, transparency, accountability, access to public services and citizen participation, showed the sufficient development of e-governance components in Ukraine (United Nations, 2016). For instance, one of the components of the E-Government Development Index is the Online Service Index, which measures the use of ICT by governments to deliver public services at national level. Ukraine has experienced a substantial progress in online service delivery: in 2016, it was ranked as a high-index country under the assessment of Online Service Index among 193 UN member states, belonging to 56 countries (29%) with high-OSI values (between 0.50 to 0.75)[1]. In general, Ukraine was ranked by E-Government Development Index (EGDI) levels as High-EGDI country in 2016 (36% of the countries) (United Nations, 2016).

[1] The 2016 Survey shows continued effort by most countries to build and maintain national portals and back-end systems to automate core administrative tasks, to improve the delivery of public services and promote transparency and accountability.

In this regard, one of the basic prerequisites for Ukraine's success is the creation of an effective governance system capable of supporting the introduction of systemic reforms in Ukraine, including e-governance reform, based on the principles of democracy, rule of law, human rights and gender equality, inclusivity and engagement. The structure and operation of government machinery must ensure the timely provision of public services with efficient use of public resources and in a way that is transparent and accountable to the public.

In April 2017, the Cabinet of Ministers of Ukraine approved the Medium-Term Action Plan, which contains essential priorities of the Government's activities for the next three years, up to 2020. It determines the principal directions of work that aims to build a new model of development of Ukraine's economy, one that differs from the commodity-based economy and is capable of ensuring sustainable growth through effective privatization, upgrade of infrastructure, modernization of energy system, pension reform, land reform, judicial reform, as well as reforms in education and healthcare sectors. The outlined priorities were designed to ensure sustained economic upturn and for solving social problems, effective fighting against poverty, among them – economic growth, human resource capacity development, the rule of law, the fight against corruption, security and defense, and effective governance.

Key priorities under the effective governance objective are as follows:

- Public administration reform, with introduction of new public policy-making and coordination principles, policy-based strategic planning standards; insurance of the accountability of public administrative bodies and the delegation of relevant powers to local authorities via decentralization.
- Decentralization – to promote the creation of viable territorial communities and to support their development; to delegate maximum powers to local authorities and to ensure they are able to exercise the delegated powers in practice, with the creation of a modern local self-government system and of a territorial organization of power with due regard to distinctive Ukrainian features and traditions and based on European local democracy values, and the European Charter of Local

Self-Government in particular.

- Public finance management reform, with an efficient and transparent use of public finances and introduction of full-scale medium-term budget planning in order to improve the effectiveness and high quality of public services. It is aimed at building a modern and effective public finance management system, which would serve as a basis for sustainable economic growth and quality service provision by effectively accumulating public resources and allocating them strictly in accordance with medium-term national development priorities.
- E-government tools implementation as an important factor for the country's competitiveness and investment appeal and an essential prerequisite for effective public administration today. They will include introduction of the priority e-services in all areas of public life, publication of high-quality data sets available as open data in accordance with the public interests, world best practice and specified requirements with regard to openness and transparency of activities, introduction of the electronic network links between various public information e-resources; and a set up of e-document management.

The Medium-Term Action Plan 2020 also specifies the following key performance indicators and respective objectives to be achieved by 2020:

- Government Effectiveness (World Governance Indicators) – higher than in 50% of countries;
- Public Sector Performance (Global Competitiveness Index of the World Economic Forum) – top-50 countries;
- E-Government Development Index (United Nations E-government Survey) – top-40 countries;
- Open Budget Index (OBI) (International Budget Partnership) – top-50 countries;
- The level of public budget deficit should fall to 2.1% of the gross domestic product.

In 2016, E-governance in the broadest sense became a household term in Ukraine. Ukraine has already made significant steps towards using ICTs to make governance more transparent, efficient, and bringing it closer to citizens. While promoting democratic and transparent governance in a safe and secure electronic environment is an end in itself, it is also very important to establish how and whether developing e-governance will serve the EU integration goals of Ukraine.

To date, the necessary conditions for the development of E-Government have already been met in Ukraine, in particular:

- the Unified State Administrative Services Portal has been launched, with the introduction of around 30 pilot e-services;
- the Unified State Open Data Portal has been introduced;
- an electronic document exchange system between central executive authorities was launched
- interoperability between basic state registers was enabled, and the development of alternative electronic means of identification and E-Democracy tools was initiated.

Development of the electronic open-source data infrastructure

In general, e-government corresponds to an open government, which embraces the use of modern ICT and data as resources and tools to create more meaningful interactions between citizens and governments. It is a new culture transformation on how government and citizens interact and cooperate towards to a "Government of the people, by the people, for the people". The precondition for any e-Government policy is an open data system. This is for several reasons, as such a system allows for a:

- well-informed public;
- more transparent and accountable government;
- a base to mitigate corruption and rebuild trust in public institutions.
- better data management and data sharing;
- evidence-based decision-making within government;
- creation of innovations.

E-government supports effective policy integration. The data system that is typically a corollary of e-government offers particular benefits for enhancing this integration and should be strengthened. According to the UN E-Government Survey 2016, the number of countries with Open Government Data catalogues more than doubled in 2016 compared to 2014, with 106 out of 193 countries offering Open Government Data catalogues, compared to 46 countries in 2014. This is a significant increase and shows that many countries are investing in releasing open government data.

Under the initiative to develop electronic infrastructure for open-source data, and due to the fact that data enables more informed decision making, increased efficiency, improved measurement and greater transparency, e-data.gov.ua , a unified web portal on public spending, was launched in Ukraine on September 15, 2015. This was governed by the law on the open use of public funds (Zakon Ukrainy "Pro Vidkrytist' Vykorystannia Publicznych Koshtiv" 2015). "E-data" is the biggest open public finance database, which makes the use of public funds transparent, satisfies the public interest and right to receive reliable information on government transactions. For Ukraine, it is a revolutionary IT platform, which contributes to combating corruption.

This is the biggest web resource in Ukraine which fully complies with the international OpenData standards, i.e. contains information in the format suitable for machine-reading, and makes data easy to search and comprehend.

The Ministry of Finance is the authorized body responsible for open source data within the system of central executive authorities. Its duties include maintaining of the state web portal of open source data, checking whether the dataset conforms to the set requirements for data submitted to further hosting at the portal, providing methodological assistance, implementation of monitoring, and analysing the disclosures and delivery of open source data.

Structurally and functionally, E-data.gov.ua is an "umbrella" for two modules: Spending and Open Budget. The first module provides access to complete information about the sources, distribution and spending of public funds, while the "Open Budget" module, upon being launched in full-scale regime, will contain more information on state budget revenues and a detailed breakdown by budget lines and programs, ensuring the transparency of budgetary procedures. The tool for evaluating the public finance management effectiveness will become a ready-to-use system when the abovementioned two modules start to operate in consolidation.

The launch of the E-Data portal enabled the public to gain direct control over the public funds. It reveals information on the use of funds from the state budget as well as local budgets. As of 10/18/2017, the portal contains data of 65570609 transactions of the State Treasury of Ukraine totaling at about 5 trillion UAH (equivalent to 186.8 mln. USD) and more than 20.6 million contracts, protocols and reports of entities managing public funds. The number of visitors of this web portal has risen from 0.5 million in 2015 to 11 million in 2017.

During 2017 the E-Data team conducted trainings in 23 regions of Ukraine not only to educate the managing entities, which are obliged to upload the relevant information, but also to train journalists and civil activists to use this e-tool in their professional activities, as the portal is a reliable resource for investigations on the use of public funds. Within the project, another initiative, known as the E-Investigation contest, is constantly being hosted to promote the use of e-data.gov.ua and other open public data resources to disclose cases of corruption. The E-Data Rating competition is also taking place right now, and it aims to encourage city mayors to make their data public and format it properly.

Furthermore, by 2018 the integrated information and analytical system known as Open Budget should become fully operational. This system will introduce changes in the budget processes at the Ministry of Finance, bring automation to the State Fiscal Services and State Treasury systems, and allow forthe automation of records and reporting systems at local level.

Another successful project, which has recently become a globally recognized e-tool, is Prozorro – one of the most innovative procurement systems in the world . As a fully online public procurement platform, Prozorro is a collaboration environment that ensures open access to public procurement (tenders) in Ukraine. All public tender information in

Ukrainian and procurement announcements in English over certain price thresholds are available on the portal. In this way, Prozorro ensures transparent and efficient spending of public funds by simplifying oversight opportunities for civil society and enabling enhanced, open competition among businesses that aim to supply goods and services to government entities in Ukraine.

Fully implemented in 2016 as a hybrid system (both centralized public and decentralized private market places), it has since been globally recognized as one of the most innovative public procurement systems delivering government services in a stakeholder-focused, transparent, effective, fair and low-cost way. As of August 2017, the portal has had one million tenders and 27,800 purchasing entities in its internal systems.

It is important not to leave aside the fact that the new public finance management strategy of Ukraine for 2017-2021 involves, among other steps, the integration of the e-data portal with the systems of the State Treasury and Prozorro, which will facilitate covering the entire cycle of the respective contract ranging from the tender bid and contract works to acceptance certificates and agreed bank accounts.

What is more, integration with other systems and subsequent development of E-Data can further improve the performance of Ukraine in international ratings. The full-scale launch of e-data.gov.ua will let Ukraine qualify for the top 20 countries in the 2018 Global Open Data Index.

Under the open-data strategy, a tech NGO known as the 1991 Open Data Incubator, a tech NGO and Ukraine's first incubator for open data projects was launched in partnership with the Ukrainian government, Western NIS Enterprise Fund and Microsoft Ukraine . It aims to create socially oriented services and applications based on government open data. The project is a contribution to improving the economy and state management and developing anti-corruption analytical systems. The incubator will support projects in the following four directions:

- industry solutions for infrastructure, agribusiness and energy sectors;

- electronic services for citizens, essentially via public-private partnerships;
- analytical systems for government bodies;
- Smart Cities solutions for local authorities.

The program mainly targets startups using open data from the state and corporate sectors.

The ambitious open data agenda, led by the State Agency for E-governance on the government side and by the 1991 Open Data Incubator and TAPAS, a new USAID donor program, on the civil society side, has evolved into a multi-partner ecosystem. It aims to both motivate government agencies to publish their data online free for public usage and to instruct the public on how to effectively use the data. So far, several hackathons have been supported by 4 regional EGAP Program's Challenges, the 1991 Open Data Incubator and Apps4Cities to stimulate IT and social innovation in Ukraine. (Tomkova and Konashevych 2016).

The digital revolution offers unprecedented opportunities for improving virtually all forms of public service delivery. On September 20, 2017, the Cabinet of Ministers of Ukraine approved the concept of development of the e-governance in Ukraine until 2020 . Currently, Ukraine provides 30 electronic services. By the end of 2017, this amount will have increased to 100 services. In addition, mobile identification will be implemented by the end of the year. This is an integral part of the implementation of reforms in Ukraine. The main tasks of the concept of the e-governance development in Ukraine include modernization of public services, improvement of quality and maintenance of openness in servicing Ukrainian citizens and business, modernization of public administration.

Priority is given to activities in three main areas:

- modernization of public services, which involves the introduction of the hundred most important online administrative services for citizens and business through a single electronic resource, as well as introduction of electronic contracts and promotion of all services;
- modernization of public administration, which includes the implementation of the

interaction of state registries, the launch of approval of regulatory legal act drafts by state authorities in an electronic form, the creation of the electronic archive and the development of internal systems of document circulation;
- management of e-governance development, implemented by the Interagency Council for the development of e-governance through the coordination of the implementation of the Concept and the mutual harmonization of all tasks, taking into account international experience.

By the end of 2017, electronic services will be introduced for the following:

- The initial registration of cars;
- obtaining a license and permission for transportation;
- licenses for tobacco and alcohol;
- police clearance certificates;
- declarations of conformity (the State Emergency Service of Ukraine);
- introduction of the e-interaction system and the connection of 10 basic state registries,
- introduction of thethe MobileID electronic identification system;
- approval of regulatory legal act drafts in e-form;
- e-contracts.

E-democracy concept

One of the integral parts of e-governance development is e-democracy, (both of) which have overlapping areas. The essence of e-democracy lies in the support and enhancement of democratic processes and democratic institutions by means of technology. It offers citizens an additional opportunity to participate in political processes.
Democratic political participation should involve the means to be informed, the mechanisms to take part in decision-making and the ability to contribute and influence the policy agenda. The concept of e-democracy can refer to the following stages:

- E-information (online provision of information): a one-way relation in which the government produces and delivers information in its online channels for public use by citizens. It covers both "passive" access to information upon demand by citizens and "active" measures by government to disseminate information.

- E-consultation: a two-way relation in which citizens provide feedback to government using online tools. It is based on the prior definition by government of the issue on which citizens' views are being sought and requires provision of information.
- Active e-participation or e-partnership: a relation based on partnership with government, in which citizens actively engage in the policy-making process via different online-tools. It acknowledges a role for citizens in proposing policy options and shaping the policy dialogue – although the responsibility for the final decision or policy formulation rests with government (OECD, 2001).

Under this three-level model of e-participation and according to the UN E-Government Survey 2016, Ukraine took the 32nd position among the top fify performers in the e-participation index. The report also concluded that all the countries that exhibited significant advances in their e-participation ranking have expanded their e-consultation activities, among others: Azerbaijan – from 5% to 74%, Uzbekistan – from 18% to 58% and Ukraine – from 27% to 84%. This was also coupled with moderate progress in e-information. Continued progress in the provision of public information remains fundamental for progress in e-participation.

Moreover, the holistic governmental approach in the area of e-democracy is now gradually being developed in Ukraine through the development of the E-democracy Concept Paper:

- The active civil society of Ukraine should continue performing its proactive role in the development of e-democracy.
- All e-democracy initiatives have to be accompanied by awareness raising campaigns and education programmes. The case of Prozorro is a good example of how this kind of awareness raising and training helps to establish a good environment for an e-initiative and make it sustainable.
- Public awareness must be increased, in part through concrete community projects

where different stakeholders are working towards a common agenda. Such projects could enhance the creation of a culture of dialogue and, consequently, help Ukrainian e-democracy to flourish.

Legislative developments linked to e-democracy in Ukraine indicated a turning point in 2014, with visible and sufficient changes (Tomkova and Konashevych 2016).

One of the key pre-2014 milestones was the adoption of the Law on Access to Public Information passed in 2011, which enabled citizens to access public information through government websites as well as obliged state institutions to reply to public queries. One of the most prominent achievements in post-2014 period were the amendments to the Law on Access to Public Information and Cabinet of Ministers Resolution on the Approval of Regulation on Datasets to be Published in Open Data Format, which opened more than 300 public registries. The state web portal data.gov.ua was created to host the released datasets. Additionally, the Law on the Open Use of Public Funds, passed in 2015, obliges all state bodies, organizations and enterprises to publish their expenditures in an open data format at the portal spending.gov.ua. Furthermore, the legislation on public procurement and online public procurement portal Prozorro was approved in 2015 and was another step towards enhancing transparency. The Law on Citizens' Petitions could be regarded as a breakthrough in the field of e-participation in Ukraine. Ukrainian citizens could send their petitions online to state bodies at national as well as local levels.

In 2014-2015, a series of policy papers in the field of e-governance was produced, which mostly defined the government's agenda, with e-democracy area being only partially and sometimes indirectly referred to. Those paper include the Digital Agenda for Ukraine 2015 (by the Ministry of Economic Development and Trade and the State Agency for E-Governance), the Green Paper for the Electronic Governance in Ukraine (by a Working Group for the Public Policy on e-governance at the Ministry of Regional Development and Municipal Economies), the White Paper for the Policy on Electronic Democracy (Pantsyr 2015) by the Strategic Advisory Group on Electronic Governance at the State Agency for Electronic Governance in Ukraine. The 2014-2015 policy papers highlighted some directions, but in practice the developments were far from systematically planned, and were rather unrelated initiatives.

For the development of infrastructural and institutional capacities, in late 2016-early 2017, the Digital Agenda for Ukraine 2020 was created (HiTech Office 2016). It is promoted by the Economic Development and Trade Ministry, and a wide group of stakeholders from business, civil society, and authorities. Regarding transparency, in early 2017 a debate started around the Draft Roadmap for the Development of Open Data in Ukraine. The most recent and the most comprehensive strategic document in the field of e-democracy is the Concept Paper and the Action Plan for the Development of Electronic Democracy in Ukraine, developed by the State Agency for Electronic Governance in Ukraine. This is also one of the commitments of Ukraine for Open Government Partnership. The Concept Paper covers the period of 2017-2020, while the Action Plan is targeted for 2017–2018. In the governmental sector, the State Agency for Electronic Governance in Ukraine plays a major role in the development of e-democracy. One of the Agency's main achievements in this area is that many more now understand what is happening in the sector. Additionally, the cooperation experience with civil society within the framework of the E-democracy Coalition is seen as successful and important.

The Maidan revolution triggered a wave of civic activism and different civic movements; this is where the kick-start of Ukrainian e-democracy took place and numerous e-democracy programs started to emerge. However, the low level of enforcement of existing legislation as well as weak institutionalized mechanism and regulation of e-participation constitute substantial barriers to coherent e-democracy implementation in the region. Bringing e-governance issues under the control of higher executive levels could be beneficial. The State Agency for Electronic Governance of Ukraine sets an important precedent by establishing a strategic framework and a mandate for e-democracy development at national level.

It should also be underlined that the e-democracy is not linked so much to technologies as to the political and cultural choices of every country in terms of the level of involvement of the citizens in political spheres, the level of accountability and openness.

E-governance as the way forward

Great attention should be paid to ensuring interoperability and e-interaction between the information systems established and used by public authorities.
Due to unrestricted information interchange between various public authorities, integrated systems may penetrate through departmental isolation. They would also allow for better dissemination and reuse of information, while its ability for further multi-purpose uses. For average citizens it would mean that they would provide their personal data for public authorities only once and not every time they apply to public services. Public authorities would be able to reuse the acquired data without any additional requirements or inconveniences for those applying to them for a service.

As of today, Ukraine, as well as many European countries, face difficulties in implementing e-governance projects at both national and local level, as well as similar interagency projects, which require serious effort to integrate certain data and programs.

The major point is that they should organize the process of approval, use of related standards, formats, and coordinate the architecture of information technologies of various organizations and agencies rather than use specific technologies. European experiences show that national frames of interoperability are key to ensuring effective e-governance. Generally speaking, such a national frame is a regulatory document of organizational and technical nature, setting and describing specific organizational and technical requirements to projects and systems of public authorities within the e-governance sphere.

In the context of further integration with the EU, eIDAS (the European Parliament and the Council of the European Union requirements on electronic identification and trust services for electronic transactions at the internal market) and EIF (European Interoperability Framework) conformity should be of high importance. This would further allow and ensure the cross-border e-interaction and delivery of cross-border e-services.

Moreover, digitizing a government requires paying attention to two major considerations.

The first one is the core capabilities that governments use to engage citizens and businesses and carry out their work: the methods and tools they use to provide services, the processes they implement, their approach to making decisions, and their sharing and publishing of useful data. The other consideration is the organizational enablers that support governments in delivering these capabilities: strategy; governance and organization; leadership, talent, and culture; and technology (exhibit). These elements make up a framework that governments can use to set their priorities for a comprehensive digital transformation that boosts the efficiency, responsiveness, and quality of government activity and helps improve quality of life.

Regardless of how digitally sophisticated a government might be, it can always take another step forward. One of the key examples for Ukraine to take into consideration while developing its own digital way is the Estonian e-governance model (e-Governance Academy 2016).

Estonia, having a highly (if not the highest) digitised government, has pushed the boundaries of digital service delivery beyond its own borders, with its Country-as-a-Service concept (a holistic approach to transform all administrative acts into digital services), the once-only principle as part of the shared data infrastructure X-Road, which allows citizens to enter their data once and then share it with other government agencies, and an e-Residency programme, through which international entrepreneurs become "quasi citizens" and can easily set up their online business in Estonia ("Estonia 2020 Action Plan 2017-2020" 2017).

The Estonian e-Governance Academy carried out a procurement in the EGOV4UKRAINE project of the U-LEAD support program of the Ukrainian administrative reform, according to which Ukraine's intergovernmental secure data exchange solution will be created by an Estonian-Ukrainian business consortium, including Cybernetica AS and Soft Xpansion Ukraine. The data exchange solution will guarantee state institutions and service centers access to information in national registers and give opportunity to provide/deliver fast and good-quality public services. The data exchange solution will be introduced by the end of 2017.

To conclude, Ukraine has achieved a great deal in terms of technical preconditions and legislative framework for e-government, which enables the government to offer a variety of traditional services online as well as to function much more efficiently and effectively. It is also important to ensure sharing best practices in these areas, and addressing bottlenecks so that the existing positive developments may continue in the future. The implementation of certain e-governance measures will be a significant step towards providing the transparency and efficiency of interaction between business entities and individuals and public authorities. It will also significantly simplify and speed up the procedure for obtaining administrative services under the implementation of a digital by default principle. Implementing new standards for legal-regulatory and technical documents and their further harmonization with European analogues is the major prerequisite for systematic e-governance development in Ukraine.

Bibliography

"*Digital Agenda For Ukraine*". Kyiv: 2015.
https://www.slideshare.net/KyivSchoolofEconomics/da-event-ver5-02-042015

e-Governance Academy. 2016. "*Welcome To E-Estonia*".
http://ega.ee/wp-content/uploads/2016/09/eGA-esitlus-eEstonia_2016_PDF.pdf

"*Estonia 2020 Action Plan 2017-2020*". 2017.
https://ec.europa.eu/info/sites/info/files/2017-european-semester-national-reform-programme-estonia-en.pdf

HiTech Office. 2016. "*Tsyfrova Adgenda Ukrainy - 2020*". Kyiv: HiTech Office.
https://drive.google.com/drive/folders/0B8Oa6Q2zfKDSN2Q2MnNJd1NXa0U

"*Komponent 4. Natsionalna Polityka.| EGAP – Innovatsii, Tekhnologii, Ludy, Demokratiya*".
http://egap.in.ua/natsionalna-polityka/

OECD. 2001. "*Citizens As Partners: OECD Handbook On Information, Consultation And Public Participation In Decision-Making*". Paris.
https://www.internationalbudget.org/wp-content/uploads/Citizens-as-Partners-OECD-Handbook.pdf

Pantsyr, S. 2015. "*Elektronna Demokratiya. Bila Knyha Derzhavnoyi Polityky*". Kyiv.
http://www.frgn.mk.ua/wp-content/uploads/2015/11/WB_eDem_1.0.docx

The World Bank. 2016. "*Digital Dividends*". Washington, DC.
http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf

United Nations. 2016. "*United Nations E-Government Survey*". New York.
http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf

Zakon Ukrainy "*Pro Vidkrytist' Vykorystannia Publicznych Koshtiv*". 2015. Kyiv: Verkhovna Rada Ukrainy.

The Glass Man identity created by normative virtuality

Alexei Krivolap

This paper examines the communication problem with creating online identity and saving private space in the era of data turn when every step and click is recorded and stored in databases. This article aims to present a new concept of human identification – the Glass man identity. The problem arises in the field of virtual communication when users have to be visible for the Other, i.e. a machine, and when everybody can be described in terms of database content and algorithms. The Glass man identity highlights the impact of social norms on the transformation from the cultural vision of self-representation in virtual space to surveillance culture. This concept is presented in the historical perspective on the Russian case of the normative use of language and phenomena of power as abilities to re-establish norms including moral ones. This study attempts to reveal the current trend of the ongoing changes both in human identity and ethics in the era of data turn. Glass man identity means a new type of human, a new type of balance between control and power. Glass man means a person who does not need to hide anything. Nothing to hide, nothing to be ashamed of – this is a new mode of communication and power. When Big Brother isn't just a metaphor anymore.

The case of Glass man identity means transparency by default. A tightening control over virtual space is accompanied by the steady growth of the number of Internet users in Russia. The appearance of SORM-1, SORM-2, and SORM-3 (Lewis, 2014) has not affected the growth of the audience (SORM is an abbreviation for System for Operative Investigative Activities). It is possible that users perceive control as an access condition. They believe having access to the internet automatically means being controlled or monitored. Documents published by Wikileaks (Wikileaks, 2017) describe in detail the mechanisms for implementing this control.

It seems to me that it is not possible to use the two basic ways to control communication (namely restricted access and surveillance of access) at the same time. A choice needs to be made and it was made. In 2014, an idea to create Cheburashka, their own internal Russian network to reduce dependence on western technologies and influence, was presented. The project was not, however, implemented. This logic fits the understanding of the danger and vulnerability to external influence (Balashova, 2017). RosKomNadzor (a Unified Register of the domain names, website references and network addresses that allow state bodies to identify websites containing information which it is forbidden to circulate in the Russian Federation) is responsible for maintaining blacklists with forbidden sites.

Glass man identity signifies a new type of human being. It can be an ethical issue. For Jean-François Lyotard the critically important question was: "Who will know?" (Lyotard, 1984, 6). Now this question can be rephrased: Who will know tomorrow what you said (wrote, liked, commented…) yesterday? We need to remember, and we lost a right to forget. How to push such a "troubled identity" (Donskis, 2009) into a tiny national framework, especially in Russia, where, for example, it's hard to distinguish between Russian citizens (Rossijane) and the Russian ethnic majority?

Gianni Vattimo described this new condition of the post-modernity as the "transparent society" (Vattimo, 1992). It occurs when the decision-making process needs to be more transparent and it is possible to understand how the society itself functions. And human identity isn't fixed by default. Zygmunt Bauman proposed the concept of liquid modernity: "To put it in a nutshell, 'individualization' consists of transforming human 'identity' from a 'given' into a 'task' and charging the actors with the responsibility for performing that task and for the consequences (also the side-effects) of their performance" (Bauman, 2013, 31-32). And it is a challenge for everyone to create their own identity. However, transparent society will require transparent individuals, and this process will take place by re-establishing normative practice.

For the Russian case, it is the metaphor of the glass that has its own historical and literary context. I am referring to We, a dystopian novel by Yevgeny Zamyatin (1921), in which all houses are built of glass, and people are always exposed to control/monitoring. His text was the "first novel of warning that admonished humanity about where modernity would lead if no one stopped its totalitarian and totally emancipated version, with its system of complete surveillance, transparent glass buildings, the demise of the family and the end of the humanities in their world of human studies: all this issuing in a society governed like a technological project from which what early modernity knew as love and friendship had vanished" (Bauman & Donskis, 2013, 195).

This article is about radical changes in the condition of access to the Internet in Russia and inevitable challenges in the role of its users. There is absolute transparency and a total lack of privacy in the era of a Big Brother that watches you, serving as a metaphor for global surveillance culture. Still, as Kammerer argues, "as important as Big Brother may be for an analysis of our contemporary culture, the difference between television entertainment and social reality must not be forgotten" (Kammerer, 2012, 104). The Big Brother concept has gone a long way from being a utopia in the glass to representing the politics of transparency (McQuire, 2013, 106-109). Big Brother invades a closed and limited private space, and a glass man in a glass-walled house is simply deprived of privacy by default. The Western model of Big Brother suggests a Panopticon, voyeurism, surveillance, and the like. This is where we find ourselves now, under surveillance that may seem benign enough but which nonetheless asserts a dark, controlling power over us, the watched (Preston, 2014). In other words, it can be a question of re-establishing of norms or just normativity.

Normative Virtuality

Nowadays, critical theory offers a wide range of explanations about how privacy has become impossible. From my point of view, we need to pay attention to several specific practices of online media consumption. Glass man identity is created by the new normative practice, when a person needs to be online. Normative virtuality can be interpreted as the next step in the development of network sociality (Wittel, 2001) when part of the social life moved to the virtual space. As Wittel argues, the "concept of a network sociality: it is a sociality based on individualization and deeply embedded in technology; it is informational, ephemeral but intense, and it is characterized by an assimilation of work and play" (Wittel, 2001, 71). Also, it is about establishing new normative practices for being online.

The concept of normative virtuality has its own previous history from pre-internet times. Then, virtuality was practically synonymous with fantasy, fictional universe, or something not directly set in our reality, and this is part of the process of building the cultural identity. Roland Barthes, writing in his article entitled Language and Clothing (Barthes, 1959), made a reference to Principles of Phonology, a text by Nikolay Trubetzkoy (Trubetskoi, 1958) and underlined, that "Trubetzkoy suggests applying the Saussurian distinction between language and parole to clothing; like language, clothing would be an institutional system, abstract and defined by its functions, and from which the individual wearer would draw their apparel, each time actualizing a normative virtuality" (Barthes 2013, 25). Normative usage of language means the normative vision of social reality since we need a language to understand social space.

Jean Piaget in 1970 repeated the term "normative virtuality" in the introduction to the French version of Main research areas of social and human sciences: "It goes without saying that in so far as man is no longer conceived as given once and for all from an absolute beginning, all the problems concerning his activities arise in entirely new terms: instead of being able to refer to an initial status concerning (in the preformed or predetermined state) the set of normative virtualities that determine human nature..." (Piaget, 1970, 12).

We consume media content and produce our own symbolic representation to construct ourselves in the eyes of Others. In the 1980s Alan Toffler proposed a term "prosumer" (Toffler, 1981) and at the beginning of 21st century, Christian Fuchs (Fuchs, 2011) adopted and conceptualized it to describe the condition of current virtual social networks. Now it's harder and harder to reject an invitation to be online as it is a new restriction from virtual normativity. The need to be in the Internet, to create a log and trace of your presence online and to be visible, is a new norm, which is required by normative virtuality. And at the same time, it does not require any moral choices as to which information to consume and which to reject.

Point of the Glass Man

I propose using the metaphor of Glass man to explain the condition of the current cultural identification process. In Russian this term came from medical terminology, where it means "Imperfect osteogenesis" when bones are weak and are not able to provide the needed level of support. The body lacks the stamina and resistance needed to function properly.

The rise of a new kind of human identity – the Glass man identity – will be seen, firstly by discussing the "eroding" changes (Opsahl, 2010) in private space and then, examining the concept of normative virtuality. In many cases we cannot say "no" to corporations, because we need to continue to use this service. Today web browsers are designed like credit cards. They make it easy to "swipe" the credit card for our time and take out a loan against our future selves (Harris, 2014). Even more, Tristian Harris proposes ten cases of "hijacking people's minds" while surfing in virtual space (Harris 2016). We have the ostensibly "free" choice to be presented online, but the corporations need to keep our attention for as long as possible. "Technology will not allow you to remain on the sidelines. 'I can' transmutes into 'I must'. I can, therefore I must. No dilemmas permitted. We live in a reality of possibilities, not one of dilemmas. This is something akin to the ethics of WikiLeaks, where there is no morality left. It is obligatory to spy and to leak, though it's unclear for what reason and to what end" (Bauman & Donskis, 2013, 6-7). This phenomenon can be understood in ethical terms of moral blindness, when "nobody has a monopoly on truth in politics, and the same applies to virtue and ethics in general" (Bauman & Donskis, 2013, 76).

Glass man is a person without the need to hide anything. Nothing to hide, nothing to shame – it's a new mode of communication, without taboos and ethical limits in topics of conversation.

But Glass man identity means transparency not for a person but for a corporation which acts into the mediated public space. We are able to hide something about ourselves from other users, but not from service owners. We need a medium to be presented in this new virtual public space or inside the "culture of connectivity" (van Dijck, 2013).

Glass man means a life without the backbone of hidden past, in sense of "skeletons in the closet". We cannot be flexible anymore because we are like glass: coded and fixed in a hard form. Our history is the history of tracking our external skeleton. And we cannot change or modify it. We have no total control over the representation of ourselves any more. The psychological mechanism of deleting "bad" uncomfortable memories, when we were able to forget them, does not work anymore now. After the data turn, we are not able to forget any facts in our life. Blockchain technologies take control of our memory of our own past and impact ethical issues. The metadata and algorithms of our online behavior tell about us more than about ourselves than we personally know. And according to algorithmic identity, "cybernetic categorization provides an elastic relationship to power, one that uses the capacity of suggestion to softly persuade users towards models of normalized behavior and identity through the constant redefinition of categories of identity" (Cheney-Lippold, 2011, 177). Metadata defines who we are.

User verification has become the norm in professional environments, and now this rule applies to all users in general. Everything can be verified in a couple of clicks; the past cannot be changed or reinvented. In Russia (and worldwide) users of telecommunication technologies can be transparent for providers accumulating metadata and contents. This refers not only to the Internet but mobile communication and public Wi-Fi, too. A Foucauldian Panopticon occurs when we are visible and controlled by disciplinary practices. The Glass man identity is based on the lack of dilution – there is no trust anymore.

The focus of the text is not on an individual level, since everybody faces the problem of identification. And it is not about a group or collective identity. It is about how a corporation looks at us, how a corporation sees a human. There is a steady trend of growth of internet users in Russia. In this case, user's communication activities after July 2018 (when new restriction according to Yarovaya-Ozerov Law will be adopted) will be completely different in comparison with users ten years ago in the sense of understanding privacy and anonymity values. Maybe this shift will be the starting point of creation of Glass man identity? Now we can only try to anticipate the scale of the changes. However, judging by the Draft of the Order with the description of the strict requirements for the equipment and transmitted data in Internet (Regulation.gov.ru, 2017) submitted for public discussion, they will be significant. Together with the resumed user names, IP-addresses, and email, they will accumulate data on the languages the user owns, passport data, and even the list of the user's relatives.

It is possible to argue that the old technical ways to guarantee anonymity on the network: TOR, VPN, ssh-tunnels, proxy, and the like are still there. But in June 2017, the State Duma of Russia began to discuss a draft law that would oblige the owners of anonymizers, VPN, and other services to block access to prohibited sites, and the owners of search engines to remove links to prohibited sites. If this law is adopted, Russian users may be banned from being anonymous when surfing online. Advanced users will still resist turning into a glass man, but most users will not notice the transformation. In other words, it is as if residents of a glass house were forbidden to use curtains. New media, Big Data, and the like turn us into transparent "creatures" for the view of the Other. The Other isn't meant to be a real human being as usual. It is a corporate machine-based approach to supervise human activities. How can we change our ideas about what is ethical, and what is not in such a situation? Who can perform the function of an external conscience (moral measure) for an individual? What will be the morality of the new glass man, which cannot have included any secrets? Or can it be outsourced like any other hard task? All those quantitative benchmarks from different methods of calculation of users and their online activity didn't capture the current transformation in the human identification process. We are identified with our history of purchase or consumption. And there are cases when this consumer logic can be interesting not only for the corporation but for the state as well. We can mention a Chinese experiment that looked at the creation and implementation of a system of social credit or social trust. This system would, "with the help of artificial intelligence technologies and Big Data, [...] analyse data of every official such as party attendance, education, marital status. The system will compare data on the incomes of the official and members of their family with data on purchased real estate and luxury goods. [It will make such calculations] based on these data, as well as information on the trustworthiness [of the official]" (Kovachich 2017). In a society in which ethical boundaries are constantly blurred, individual identity is disintegrated. No trust, no moral doubt. Only records in databases make sense and bring profit.

Conclusion

Users accept new terms of services because they need to be online. Today in Russia (and beyond), normative virtuality means a need to be online and the impossibility of not being there. "Tracks" of normative virtuality have to be collected in databases. And we see the birth of a new type of human identity worldwide and among Russian Internet users – such a Glass man is as transparent as glass, hard, but simultaneously fragile. He is not ashamed and/or has nothing to hide. And it is not our own decision; sometimes it may be the law. One of the possible reasons for this is the lack of ability for users to monitor their own data. Electronic traces of our activities do not belong to us but are a commodity (object of purchase and sale) for marketers and data brokers. The identity of Internet users will be lost, as will privacy as a characteristic by default when all information about users will be stored in databases. There will be absolute transparency and total lack of privacy. If the Big Brother invades a closed and limited private space, then the Glass man will simply be deprived of privacy by default. And at the same time, the ethical question can be outsourced. Prosumers will be able just to click 'like' or 'dislike' without moral troubles. We know that they know what we know.

Bibliography

Balashova, Anna. 2017. "Pomochnik presidenta – RBC: "*Nash Internet uyazvim k vneshnemu vozdeistviju*"." [Title in English: Assistant of the President - RBC: "*Our Internet is vulnerable to external influences*"]. RBC. http://www.rbc.ru/interview/technology_and_media/27/03/2017/58d3bc559a79471ca8c1fbbd

Barthes, Roland. 2013. *The Language of Fashion*. A&C Black.

Bauman, Zygmunt, and Donskis, Leonidas. 2013. *Moral blindness: The loss of sensitivity in liquid modernity*. John Wiley & Sons.

Bauman, Zygmunt. 2013. *Liquid modernity*. John Wiley & Sons.

Cheney-Lippold, John. "*A new algorithmic identity: Soft biopolitics and the modulation of control*." Theory, Culture & Society 28, no. 6 (2011): 164-181.

Donskis, Leonidas. 2009. *Troubled identity and the modern world*. Springer.

Regulation.gov.ru. 2017. "*Draft of the Order with a description of the strict requirements for the equipment and transmitted data in Internet…*" [Proekt Prikaza ob utverzhdenii Trebovanij k oborudovaniju i programmno-tehnicheskim sredstvam, ispol'zuemym organizatorom rasprostranenija informacii v seti «Internet» v jekspluatiruemyh im informacionnyh sistemah, obespechivajushhih vypolnenie ustanovlennyh dejstvij pri provedenii operativno-razysknyh meroprijatij, vkljuchaja sistemu hranenija, in Russian] *Federal Portal Of The Projects Of Normative Legal Acts*.
http://regulation.gov.ru/projects#npa=18013

Fuchs, Christian. 2011 Web 2.0, *Prosumption, and Surveillance Surveillance & Society*. No 3 (8), 288–309.

Harris, Tristian. 2016 "*How Technology Hijacks People's Minds — from a Magician and Google's Design Ethicist*" TristanHarris.com.
http://www.tristanharris.com/2016/05/how-technology-hijacks-peoples-minds%e2%80%8a-%e2%80%8afrom-a-magician-and-googles-design-ethicist/

Harris, Tristian. 2014 "*Is your web browser a credit card for your time?*" TristanHarris.com.
http://www.tristanharris.com/2014/08/is-your-web-browser-a-credit-card-for-your-time/

Kammerer, Dietmar. 2012. "*Surveillance in literature, film and television*." Routledge handbook of surveillance studies, 99-106.

Kien, Grant. 2013. "*Media memes and prosumerist ethics: Notes toward a theoretical examination of memetic audience behavior.*" Cultural Studies – Critical Methodologies, 13(6), 554-561.

Kovachich, Leonid. 2017. "*Bolshoi Brat 2.0. Kak Kitai stroit cifrovuju diktaturu*" [Big Brother 2.0. How China builds a digital dictatorship, in Russian]. Carnegie Moscow Center.
http://carnegie.ru/commentary/71546

Lewis, James Andrew. 2014. "*Reference Note on Russian Communications Surveillance.*" Center for Strategic & International Studies (CSIS)
https://www.csis.org/analysis/reference-note-russian-communications-surveillance

Lyotard, Jean-François 1984. T*he postmodern condition: A report on knowledge (Vol. 10)*. U of Minnesota Press.

McQuire, Scott. 2013. "*From glass architecture to Big Brother: Scenes from a cultural history of transparency*". Cultural Studies Review, 9(1), 103-123.

Opsahl, Kurt. 2010. "*Facebook's eroding privacy policy: A timeline*". EFF Deeplinks Blog. (April 28, 2010)
https://www.eff.org/deeplinks/2010/04/facebook-timeline

Piaget, Jean. 1970 "*La situation des sciences de l'homme dans le système des sciences." Tendances principales de la recherche dans les sciences sociales et humaines. Première partie: Sciences sociales*" Mouton.: 1-65.

Preston, Alex. 2014. "*The death of privacy*". The Guardian. (August 3, 2014).
https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

Yandex. 2016. "*Razvitie interneta v regionah Rosii*" [Title in English: *The development of the Internet in the regions of Russia*]: Accessed November 14, 2017
https://yandex.ru/company/researches/2016/ya_internet_regions_2016

WikiLeaks. 2017 "Spy Files Russia". Last modified September 19, 2017
https://wikileaks.org/spyfiles/russia/releases/

Toffler, Alvin. 1981. *The third wave*. Bantam books.

Trubetskoi, Nikolai Sergeevich. 1958. *Grundzüge der phonologie. Vandenhoeck & Ruprecht.* (In English - Trubetzkoy, Nikolai Sergeevich. 1969. *Principles of phonology.*)

Van Dijck, José. 2013. *The culture of connectivity: A critical history of social media*. Oxford: Oxford University Press.

Vattimo, Gianni. 1992. *The transparent society*. Cambridge: Polity Press.

Wittel, Andreas. 2001. "*Toward a Network Sociality*". Theory, Culture & Society, 18(6), 51–76.

Zamyatin, Yevgeny. 1921 *We*. Translated by. Natasha Randall. New York: Modern Library (2006).