

## Information and political security of the democratic state - world experience and Russia

Ilya Leonidovich Morozov

Russian Presidential Academy of National Economy and Public Administration, Volgograd Branch.  
Gagarin Str., 8, Volgograd, 400131, Russia

**Abstract.** The article analyzes transformation of the new threat in the information area. The author requests for discussion the various models of information security of Russia in the modern world. The article includes recommendations and proposals aimed at strengthening the security of the democratic state. Of particular importance is information transparency of government organizations, support social movements, the strengthening of international cooperation.

[Morozov I.L. **Information and political security of the democratic state - world experience and Russia.** *Life Sci J* 2014;11(11s):620-623] (ISSN:1097-8135). <http://www.lifesciencesite.com>. 141

**Keywords:** Information theory, state security, political communication, Russia, confrontation, political extremism, discourse.

### Introduction

The first decade of the XXI century became a decisive moment in the pull-down confrontation between the authoritarian and democratic trends in the world arena. Despite the fact that under the collapse of bipolar international system the Western civilization managed to overcome the identity crisis, and to save the military-political infrastructure [1], the threat of the authoritarian political regimes proliferation remains relevant. The image of democracy has problems with attractiveness to the European citizens [2], and Russia is, also, experiencing the special political difficulties, even despite the best efforts of recent decades, it failed to integrate into the Western civilization structure. As a result of collapse of the political regime of Viktor Yanukovych in Ukraine in February 2014 a new conflict field has appeared between Russia and the West, so called the threat of direct confrontation. The destructive political forces, including the extremist and terrorist organizations in Russian and beyond its borders, will try to turn to advantage this escalated international situation. The information confrontation and the desire to take control of the political consciousness of citizens are of key importance. The danger of this process is that the probability of coming into the power of radical, populist, revolutionary wing leaders rises. As noted by Professor Jeff Colgan, such leaders with a high probability will pose a danger to the surrounding states: "Once in power, the leaders of revolutionary type lean towards the aggressive style and thus provoke the international conflict much more often than the leaders of conservative states." [3] Originality of information and political confrontation at the present stage, new threats and challenges, with which the democratic countries are faced - it's a subject field of this research.

### Methods

Research of the subject field of this article is made on the basis of a systematic approach to the consideration of information and political security problem of the State [4]. Key findings were obtained taking into account the analysis of expert and analytical and research and theoretical literature on information political security, empirical (statistical) data. The historical and retrospective and comparative study of political practices of applying the information technologies by extremist forces was carried out, as well as the methods to counter them by the Russian government.

### Main body

The significant difference of modern strategies aimed to undermine the state institutions stability in a democratic system is the steady increase of the non-military component's role in the extremists' activities. At the first stage they implement the information and communicative contour destabilization in the political system of the State-opponent. This is followed by the political regime dismantling, what, in the modern conditions, can't be performed without the active role of cohesive, mobilized irreconcilable opponents of the authority. As noted by the Professor S.V. Anufrienko: "To achieve its goals, the contemporary terrorism can dispense with the communicative component only." [5]

Schematically, the modern postindustrial war model against the democratic political regime can be represented in three stages:

- informational suppression of communication resources of the regime government, both within the state and beyond its borders;
- activation of the intrastate irreconcilable opposition by using the information and financial

instruments and radicalization of its activities aimed at the political regime destabilizing;

- external intervention by the neighboring aggressive authoritarian state in conjunction with the "fifth column" and the ruling regime overthrow.

The resulting component at the output in this model will be inevitably the application of military force, but the consistent success in all three stages of confrontation can only be achieved with the active use of information methods.

Strategy for the information and ideological defense of state infrastructure seems to be optimal to classify by the dominant nature of actions: passive security model, active security model, combined security model.

Passive model is based on the reflexive principle - response to the challenges and threats by the very fact of their manifestation. Strategy of the state infrastructure protection from the informational pressure by their opponents is predicated on a system of prohibitions, blocking access to the "undesirable" information, detection and suppression of generators and disseminators of such information (repressive persecution, defamation, social and psychological isolation, etc.).

Active model is based on the pre-emptive actions, both on its own information field, and on the promotion of its ideological concepts and information and political codes on the opponent's information field. With this approach the government services, by involving the public organizations and movements as widely as possible deploy a system of communications work and taking into account the principles of network communications, debate with the most dangerous political opponents in public in order to attract their former supporters into its ranks and to implement the unconditional interception of impact on the neutral part of mass audience.

Combined model is based on a combination of the above principles - when you selectively block only the most radical and socially unacceptable (rejected by the overwhelming majority of citizens of the State) generators of political ideologems on the background of information pluralism towards different opposing actors of the political and communication process.

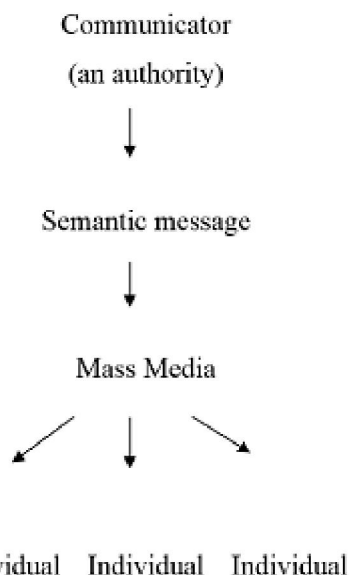
The modern Russian political elite have realized the importance of information as a factor of international and internal conflicts in the contemporary world. Already in the early presidency years of V.V. Putin a number of fundamental documents governing the policy of Russia in the field of information security were adopted [6]. However, in those years the process of building the really efficient information security system of the

individual, State and society was not implemented [7].

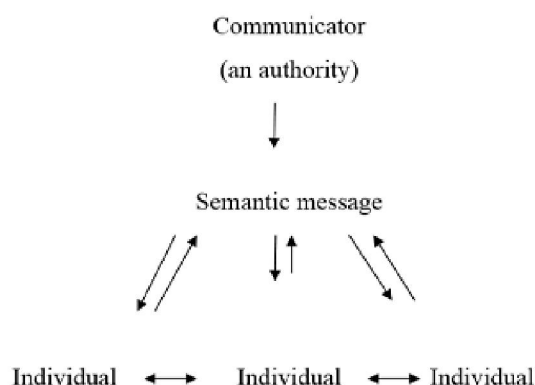
A system error of the Russian political elite that is capable to lead to the long-term negative consequences is a consistent desire for the implementation of the passive model of information and communicative security of the State system as the least costly financially, the simplest in terms of semantic content and practical realization, understandable in the performance for the bureaucratic apparatus, power structures, and all other institutions of civil service. This model can only work in the conditions of complete indifference, political apathy of citizens, simplified social and political consciousness and the lack of professionalism on the part of opponents, Eastern authoritarian type. In such societies, the popular protest can be kept at a latent level quite a long time by force and prohibitive measures, and the growing points of the opposition's activities can be passed off as the terrorist enclaves and eliminated without much public outcry. However, according to some researchers: M. Libicki [8], L. Davis [9], B. Hoffman [10], and S. Bodrunova [11], a temporary preservation of potential extremist threats will only make the situation worse.

Building up the political communications by the passive model, the state authority is derived from the traditional principle of private monopoly to generate the political ideologems and the right to control not only the communication channels between the institutions, but also between all the citizens (Figure 1). In this approach the public sphere in the information space is either absent, or is nominal, and for the representative of authority the ideal individual is that one, who assimilates the information codes and evaluative attitudes broadcasted by the State mass media and interacted with the authority on the "linear" information scheme.

In the coordinates of globalization and information "transparency" of the world the Russian society evolution gradually generates the rejection of prohibitive and force approach to the information and communication sphere. The legislative initiatives to prohibit the access of ordinary citizens to the "inconvenient" political information, according to the ruling class (Figure 2), only stimulate the protest mood.



**Figure 1. Political communications in the industrial society**



**Figure 2. Political communications in the postindustrial society**

### Conclusion.

In the contemporary world that prompts the person to the personal development, expansion and diversification of social contacts (at least in virtual form), the citizens can no longer be satisfied with the role of passive consumer of information generated by the authorities. Now, the ideologemes, received from the authorities, are actively discussed and criticized at the level of citizens' network interaction out of the traditional mass media, and the social network develops its own world view, which is often mismatched with the officially recommended. The numerous dos and don'ts, even at the criminal

legislation level, can't stop such civil communications process.

### Findings.

If there is no political communications security, the democratic state can't effectively counter the extremist challenges and threats in the contemporary world [12]. To implement this problem in relation to the modern Russia it's recommended:

1. To organize and systemize the mass training of civilian personnel in the field of information countermeasures of the foreign and domestic policy threats by introducing a system of relevant specialized training courses in the field of Public Service and Administration into the higher education institutions.

2. To optimize the legislative framework in the field of information security in terms of the latest information threats detailed elaboration, and the legal field creation to interact with the public organizations and popular movements.

3. To activate the spiritual and moral work on the Russian national ideology revival, using the personnel potential of the domestic research and development centers with a focus on the specific result. In the conditions of spiritual and ideological vacuum that emerged in the Russian socium in the 90-ies of XX century, it's impossible to counteract the modern information methods of the political system disintegration.

### Corresponding Author:

Dr. Morozov Ilya Leonidovich  
Russian Presidential Academy of National Economy and Public Administration, Volgograd Branch.  
Gagarin Str., 8, Volgograd, 400131, Russia.

### References

1. Huntington, S. P., 2004. Who Are We? The Challenges to America's National Identity. Simon and Schuster, Rockefeller Center, New York, pp.: 8-24.
2. Laqueur, W., 2012. After the Fall: The End of the European Dream and the Decline of a Continent. New York, pp.: 14-19.
3. Colgan, J. D., 2013. Domestic Revolutionary Leaders and International Conflict. World Politics, 65(04): 656.
4. Gunnell, J. G., 2013. The Reconstitution of Political Theory: David Easton, Behavioralism, and the Long Road to System. Journal of the History of the Behavioral Sciences, 49(2): 190-210.
5. Anufrienko, S. V., 2013. Mass Media as a Vital Element of Modern Terrorism. Middle-East Journal of Scientific Research, 18(2): 206.

6. Doktrina informazionnoy bezopasnosti. The Law of the Russian Federation "On education" of 9.11.2000 #1895.
7. Morozov, I. L., 2002. Informazionnaya bezopasnost politicheskoy sistemi. Politicheskije issledovaniya (Polis), 5: 134-145.
8. Libicki, M. C., 2007. Conquest in Cyberspace. National Security and Information Warfare. Cambridge University Press, pp: 23-24.
9. Davis, L. M., D. Golinelli, and R. Beckman, 2008. National computer security survey: final methodology. The RAND Corporation Press, pp.: 6-75.
10. Hoffman, B., 2006. Inside Terrorism. Columbia University Press, pp.: 78-93.
11. Bodrunova, S., 2014. Media and Public Sphere. Russian Federation 2014: Short-Term Prognosis, University of Tartu, pp.: 49-52.
12. Bodrunova, S. S., and A. A. Litvinenko, 2013. New media and the political protest: the formation of a public counter-sphere in Russia of 2008-12. Russia's Changing Economic and Political Regimes: The Putin Years and Afterwards. London: Routledge, pp.: 29-65.

7/16/2014