HOMO VIRTUALICUS IN THE CONTEXT OF POST-DEMOCRACY AND INFORMATION SECURITY[1]

Gagik Harutyunyan[*]

Initially created for interaction between professionals, Internet became accessible to billions of people in a matter of a few decades (by some criteria in less than 20 years), and special structures with various functionality began to appear inside it. All of this represents just another cycle of the permanent information revolution, a complicated concept with all the positive and negative ramifications stemming from it. It has to be noted that Internet, especially with its embedded social networks and blogosphere, is no longer a passive information/communication, socio-psychological and business service phenomenon. It gradually crosses the boundaries of our computer screens and becomes a real, crucially important societal, political and military factor.

We believe the World Wide Web has become an integral part of the environment around us, and hence it would not be quite appropriate to pass unequivocal judgments on this or that happening in the Internet. Researchers should widen their understanding of this phenomenon and try to figure out its dynamic mechanisms. To some extent this would enable supporting the desirable trends and/or countering the detrimental ones, from perspective of the public interests protection.

In this paper we contemplate the Internet (along with social networking community and blogosphere) as a new, virtual, but effective form of democracy, which clashes in social sense with the realities of the modern democracy quite aptly defined by the term "post-democracy." We shall also examine the role of Internet and social networks in terms of information security, since this system is a rather powerful weapon in modern network-centric information warfare, as well as in geopolitical confrontation as a whole.

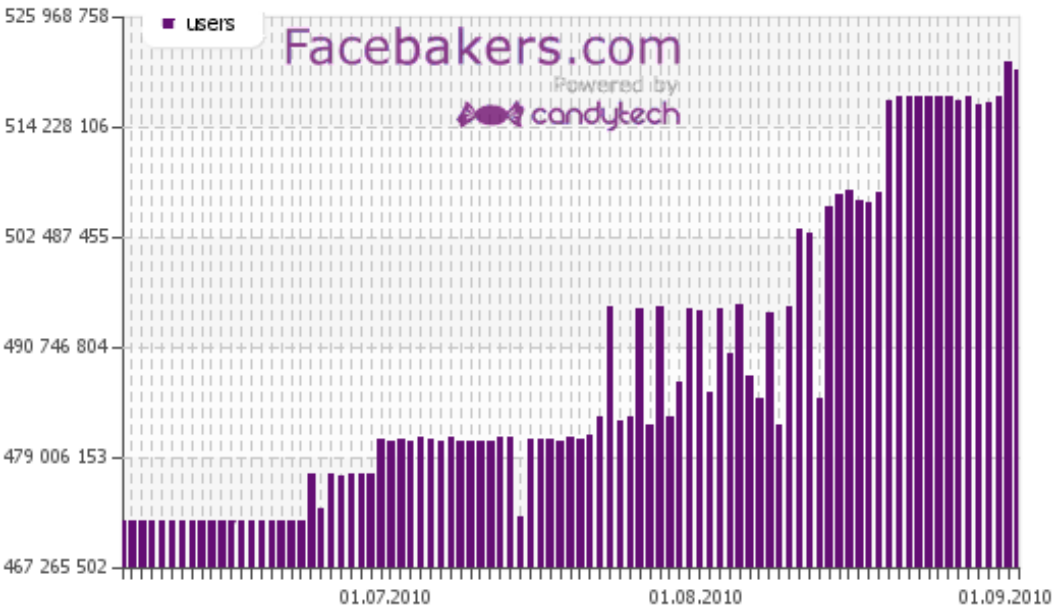
---

[1] A paper presented at World Public Forum "Dialogue of Civilizations," Rhodes Forum, VIII Annual Session, October 7 – 11, 2010; Rhodes, Greece.

[*] Executive Director, Noravank Foundation.

Social networking in the Internet. It is known that social media and blogs are the most burgeoning segment of the Internet. By some accounts over 70% of Internet users visit these websites. According to *Nielsen Media Research* the time spent by internet users in social networks in December 2009 increased by 82% compared to the same time in 2008. The growing traffic of social networking sites is impressive: 210 million in 2007, 242M in 2008, and 307M unique visitors in December 2009. *Facebook* continued to be the No. 1 global social networking destination in December 2009 and 67% of global social media users visited the site during the month. By 2010 this number had already grown to 520 million as seen in Fig. 1; an increase of 50 million was recorded in three summer months of that year[1] and the market capitalization of the company rose by one-third (amounting to about $34 billion), surpassing that of Google.

Figure 1



Emergence of these new forms, social media and blogosphere, transformed the Internet from a useful but passive instrument for consuming information services into an interactive informational social venue, which not just leads to localization and isolation from the real life (many researchers note the "evasion of reality" among a certain segment of Internet users), but also tends to interact with the real environment, sometimes quite actively. In this context it is interesting to know what exactly this medium is at present.

[1] http://www.facebakers.com/countries-with-facebook/

Actual and virtual democracies. Colin Crouch, a British sociologist, in his *Post-Democracy* defines the current epoch as "post-democratic", kind of following the postmodern [1]. In such system politicians retire to their own world and keep in touch with the public through PR laden with manipulative technologies. Meanwhile, all formal democratic attributes remain; including elections, separation of powers, etc., however in the post-democratic society akin to pre-democratic times, power is focused in the hands of symbiotic political and financial elites, the latter being predominant. Interestingly, some commentators have dubbed such formation a "new totalitarianism."

Many researchers inherently developed skepticism regarding adequacy of the modern democratic societies relative to the classical definitions of democracy (for instance, we have sometimes used the term *quasi-democracy*). Nonetheless, it appears Crouch not only has coined a suitable term, but also has scientifically rationalized all these matters. In particular, he contends that current ideas about democracy imply "limited government within an unrestrained economy," narrowing the democratic component down to holding elections, which in their turn can be considered as such with great reserve. In these conditions "government becomes a kind of institutional idiot" blamed for inability to implement effective policies, with "private business" alone being credited for such ability. It has to be noted that a situation like this essentially equalizes the countries with so-called "developed" democracy with those where democratic institutions in their contemporary interpretation have a short history.

Unlike the post-democratic realities, in the virtual world, where no distinct hierarchic structures of governance exist and anonymity is reasonably maintained, pro-democratic mores appear to reign, (though only to a certain extent, which we shall expound on later) similar to those conceivably commonplace in ancient Athens.

Meanwhile, the "citizens of the virtual democratic society," given their well-known and not-so-known peculiarities, are still derivatives of the real world and hence, some interaction and even conflicts between the virtual and actual societies are inevitable. This is especially typical for network structures formed along the lines of the interests to ideas. As far as we know, the first conflict of this kind occurred in 2008 in Russia, and ended up with a guilty verdict (for blogging statements about police) [2], though currently such conflicts have become almost routine. Perhaps it would make no sense to elaborate on the notorious "Khimki case" in Moscow or actual participation in firefighting in Russia through online social network *Pozar_ru*. Something like that occurred in Yerevan, Armenia as well, when scores of signatures were collected in blogosphere against demolition of a movie theater building with architectural value and later also against an education reform law, which were then

followed by transferring the "case" to *Facebook,* eventually compelling the authorities to cancel or amend their initial decisions.

There are many examples of consolidation and "materialization" of "virtual citizens" for protest actions, with various degrees of success, and it needs to be mentioned that we do not include here manifestations of the "environmental" terrorism. Our sociologic assessments for Armenia suggest that the most efficient and constructive organizations in these terms are those involved in protection of environment and cultural monuments, which as a rule are perceived in a very positive light by the "real society." Against this backdrop the activities of online communities can be pictured as a mechanism of sorts to compensate the lack of democracy in "post-democracy" settings. However strange it may seem, the actions of social networks against the authorities in some sense strengthen the institutes of the "nation state" in "post-democracy settings" in the state's relations with transnational capital (of course, if the authorities have such wish and will). At the same time, problems of culture and environment are not the only ones the virtual communities get involved with.

Quite recently both the virtual and actual communities were galvanized by actions of *WikiLeaks*, a resource hosted in the Icelandic "informational offshore." The site presented 75,000 secret documents of Pentagon regarding the military campaign in Afghanistan. As known, reprisals followed: in different countries *WikiLeaks* employees were summoned for questioning, arrest warrants were issued based on most likely unsubstantiated accusations and under barely disguised patronage of the US DOD.

One may contend that opposition to the United States involvement in the Vietnam War at the time hardly had been able to mobilize even a fraction of the mass audience and countless anti-war arguments that *WikiLeaks* managed to. It is also commonly known that despite the ill repute of wars in Afghanistan and Iraq (which in the latter case continues notwithstanding the assertions about its end), the response of the real world as a whole to these processes is rather tepid. There are many reasons for this, but they mostly fall along the lines of the same "post-democracy" with crafty manipulation of the public (including the global and total propaganda enabled by virtue of the current symbiosis between mass media, powers-that-be and oligarchs, sizable monetary compensations to the families of those killed in action, etc.) [3].

At the same time, as odd as it may appear, this very manipulative nature of a significant share of modern mass media (including the virtual media) was most likely the reason why some analysts argued that the *WikiLeaks* actions were part of a large-scale and well-plotted informational operation. The point is that the publica-

tion of these classified documents in no way contradicts the US national interests from perspective of the current American authorities, which now try to get rid of at least some of the G. W. Bush administration's neoconservative legacy. Meanwhile, a problem statement like that makes the topic of social networking and blogosphere relevant in terms of information warfare and information security.

Network structures and network-centric warfare in the context of information security matters. Perhaps, no special comments are needed about the fact that emergence of the Internet coincided with, or rather, set conditions for establishment of conceptual basis for information warfare (*IW*) and information operations (*IO*) back in 1990s.

Theory and practice of *IW* and *IO*, along with the Internet as a whole, develop in a quite dynamic manner. In 1990s *RAND* experts worked out the concepts of "information warfare" and "network-centric warfare" (*NCW*) [4]. The notion of "network" implies abandoning the "center to periphery" hierarchic management method and forming a system with no clear-cut structure, i.e. a non-structured system subject to the logic of self-development and nonlinear processes. In such a system there is no formal "center," yet each of the units in the system may assume the responsibilities of a managing "center."

The underlying concepts of *IW* entail the idea that the strength of a state primarily depends on its capability to be aware, obtain information and adequately respond to it. The goal of the *IW* is to "convince or force the target audience to make decisions that promote advancement of one's own national interests," whereas the *NCW* is interpreted by some analysts as "implanting one's own cultural code in the society of the potential ally or adversary".

However, let us point out that not everyone is capable of applying *NCW* as a tool, because its effective use entails the following:

- Existence of a system with intellectual resources and attractive ideological settings, with system components capable of obtaining full information and adequately responding to it.
- Comprehension of military situation (in its wider interpretation rather than in purely military terms) and appropriate mobilizing style of work and actions [5].

These new concepts have attracted the attention of political and military strategists. Before long, *IW* and *NCW* found their place among the cornerstones of current foreign and military policies of the USA and other leading countries. In this sense it can be readily appreciated that virtual social networking in many of its manifestations may serve as a tool for carrying out *IW* and *NCW*.

This is exhibited in peacetime, when for instance, online social networks provide informational and organizational support to "color revolutions" (as they did during the recent events in Iran). Social networks play an active role in wars as well, as it happened during Israeli-Palestinian or Armenian-Azerbaijani military confrontations. Thus, social networks are *IW* instruments, and the information security (*IS*) terminology with its distinct technical and content-related segments is applicable for their discussion.

The priority objective of *IS*'s technical part is ensuring the security of the so-called "*critical infrastructure*" – management systems, energy and water supply structures, information/communication, financial and other systems. It appears social networking needs to be included in this list, too. In particular, studies by the *Ponemon Institute* indicated that approximately 65 percent of users do not set high privacy or security settings in their social media sites, 90 percent do not review a given website's privacy policy before engaging in use, 40 percent of users share their physical home address through social media applications and the same percentage use a password known to individuals other than themselves. Naturally, under such circumstances crime is widespread in social media like in heydays of the Chicago gangsters. Let us note that data in online social network databases are of interest not only for criminals, but for any self-respecting intelligence service. On the top of that, the role of administrator remains quite problematic, gradually heading towards a status of the Orwellian Big Brother.

In our viewpoint it is even more difficult to protect of the content segment, in which *IS* largely depends on the public's ability to stand up for their fundamental values. This is especially important against the backdrop of *NCW* principle of "implanting one's own cultural code in the society of the potential ally or adversary." It seems that by analogy of common definitions in the *IS*'s technical segment, one of the protection techniques, inter alia, should be determining the content's "*critical infrastructures*", which are not always too apparent. In practice this implies that the theses, distortion of which may lead to national demoralization and degradation, must be selected within the system of national values and must become a subject for special attention and protection.

Possible scenarios and comments. Lately there have been many forecasts regarding Internet developments both in technical and social directions. Particularly, *Cisco* and *Monitor Group* experts believe that most growth in the Internet-related market in the coming 15 years will occur in developing countries and Internet frontiers will become fluid[1]. "Digital natives" around the world will relate to the Internet

[1] http://lenta.ru/news/2010/08/26/future/

in markedly different ways and through a number of different devices, and Internet will become a service-providing hub. At the same time, relentless cyber attacks will turn Internet into an insecure network, and consequently, secure alternatives may emerge, but access to them would be expensive. Interestingly, in this regard the USA do not rule out the option of a military strike in response to cyber attacks[1], i.e. actions in Internet might become a *casus belli*, and hypothetically, the ensuing wars might result in total destruction of both the actual and virtual worlds.

Swedish researchers predict that evolution of the Internet networks will eventually lead to creation of an intellectual *net-elite*, which actually, will rule the globalized real world [6]. However, the intellectual level of the modern social networks does not inspire optimism, and this is not only about the widespread crush on all sorts of games, which results in infantilization of the *net-community* [for instance, see 7]. After *easy music,* the phrasing *easy information* can be introduced, which incidentally, is communicated in the simplified "Globish" language [8]. Certain synergism is characteristic to this *easy information*, because unlike the professional *complicated information,* it is superfluid[2] and easily reverberates with the likes of itself, branches out and ultimately produces a synergetic effect which is not always reassuring.

Some conclusions. One may state that currently an intensive interaction occurs between the real and informational-virtual worlds. The border between them becomes conditional and the concept of "virtual" loses its original meaning. The rapid development of social networking and blogosphere particularly contributes to this process that contains both great opportunities and serious risks, among which the following should be mentioned:

- Social media and blogosphere on the Internet are capable of at least hampering the processes of de-democratization, which are so characteristic of *post-democratic* societies. In some cases, given the trends of the supranational capital domination at the state and global levels, activities of these structures may be directed to protection of the "nation-state" and civilizational values of the society. Thus, in certain development scenarios, internet structures may become global democratic institutions.
- Social networks and blogosphere are tools for the information and network-centric wars, i.e. under some circumstances these structures are, in a way, weapons of mass destruction, possession of which increases temptation to implement expansionist policies. In this context it is obvious that internet struc-

[1] Зарубежное военное обозрение, #6, с. 96, 2010.

[2] *Самвел Мартиросян,* Сверхтекучесть информации в социальных сетях, http://www.noravank.am/rus/articles/detail.php?ELEMENT_ID=4810&sphrase_id=1076

tures and their activities should be studied and evaluated in terms of information security, using the techniques for determining and protecting the *critical infrastructures of the technical and content segments.*

September, 2010

References and Literature

1. *Крауч К.,* Постдемократия. М.: Гос.ун-т, Высшая школа экономики, 2010.
2. *Таратута Ю., Зыгарь М.,* Вы у нас еще попишите. Русский Newsweek, #18-19, (287), с. 13, 2010.
3. *Арутюнян Г.,* О некоторых задачах стратегии США в контексте Иракской проблемы. «21 Век», #3(5), с.105, 2004 (на арм. языке); *Арутюнян Г.*, Переходное состояние: геоидеологический фактор в глобальных развитиях. «21-й Век», #2, с. 3, 2005.
4. *Гриняев С.*, Поле битвы – киберпространство. Мн.: Харвест, 2004.
5. *Арутюнян Г.*, Проблемы информационной безопасности и цивилизационный фактор // кн. «О некоторых проблемах информационной безопасности». НОФ «Нораванк», Ереван, 2009, с. 5.
6. *Берд А., Зондерквист Я.,* Netokratia. Новая правящая элита и жизнь после капитализма. Стокгольмская школа экономики, СПб, 2005.
7. *Павловский Г.*, Интернет есть, счастья нет. Эксперт, # 30-31,(715), с. 15, 2010.
8. *McCrum R.,* Globish. London/New York City.: Viking/Norton, 2010.