ИНТЕРНЕТ-СТРУКТУРЫ В КОНТЕКСТЕ ПОСТДЕМОКРАТИИ И ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

Гагик Арутюнян[*]

Первоначально созданный для общения профессионалов, Интернет всего за несколько десятилетий (а по несколько иным критериям отсчета – за неполных двадцать лет) стал доступен миллиардам, а внутри него начали создаваться социальные структуры с различной функциональной нагрузкой. Все это – очередной виток перманентной информационной революции, со всеми вытекающими из этого сложного понятия последствиями позитивного и негативного характера. Следует также констатировать, что Интернет, особенно с имплантированными соцсетями и блогосферой, уже не является пассивным информационно-коммуникативным, социально-психологическим и бизнес-сервисным феноменом. Он все больше выходит за пределы мониторов наших компьютеров и становится реальным, крайне важным общественным и военно-политическим фактором.

Мы придерживаемся того мнения, что всемирная паутина стала составной частью окружающей нас среды, и поэтому давать однозначные оценки тому или иному явлению в Интернете не совсем корректно. Исследователи должны расширить свои представления об этом феномене и попытаться разобраться в механизме его динамики. Это в определенной мере позволит, с точки зрения защиты интересов общества, содействовать желательным тенденциям или же противодействовать не совсем желательным.

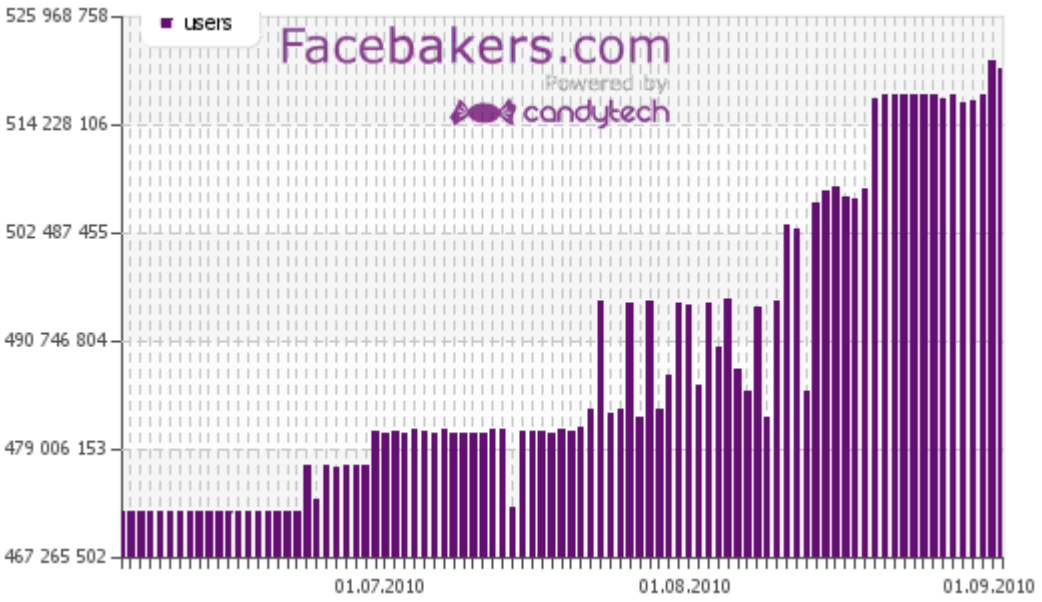
В данной статье мы попытаемся представить Интернет (в комплексе с соцсетевым сообществом и блогосферой) как новую, виртуальную, но действенную форму демократии, которая в социальном плане вступает в конфликт с реалиями современной демократии, весьма метко определяемой термином «постдемократия». Вместе с тем мы также рассмотрим роль Интернета и соцсетей в терминах информационной безопасности, так как этот комплекс является весьма мощным оружием современных информационных сетецентричных войн и геополитического противостояния в целом.

[1] Доклад, прочитанный на всемирном общественном форуме «Диалог цивилизаций», Родосский форум, VIII ежегодняя сессия, октябрь 7-11, 2010, Родос (Греция).

[*] Директор НОФ «Нораванк».

Социальные сети в Интернете. Известно, что соцсети и блоги являются наиболее бурно развивающимся сегментом Интернета. По некоторым оценкам, сегодня более 70% аудитории Интернета посещает эти структуры. Время, которое интернет-пользователи провели в 2009г. в социальных сетях, согласно данным компании *Nielsen,* по сравнению с 2008г. увеличилось на 82%. Рост посещаемости социальных сетей впечатляет: в 2007г. – 210 млн., в 2008г. – 242 млн., а в декабре 2009г. соцсети посетили более 307 млн. пользователей. *Facebook* попрежнему остается мировым лидером среди социальных сетей: его аудитория в декабре 2009г. превысила 206 млн. человек (67% всех пользователей соцсетей в мире). Но уже в 2010г. эта цифра выросла, как следует из *рис. 1*, до 520 млн., причем 50-миллионное увеличение зафиксировано за 3 летних месяца этого года[1], а капитализация компании выросла на треть (составила около $34 млрд.) и обогнала тем самым *Google*.

Рис. 1



Появление этих новых форм – соцсетей и блогосферы – превратило Интернет из полезного, но пассивного инструмента получения информационных услуг в интерактивную информационную социальную среду, которая не только приводит к локализации и изоляции от реальной жизни (многие исследователи отмечают «уход из реальности» определенного сегмента сетевой аудитории), но и имеет тенденцию войти во взаимодействие, порой – весьма бурно, с реальной окружающей средой. В этом контексте небезынтересно, какой именно является эта среда в настоящее время.

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

Демократии: реальная и виртуальная. Английский социолог Колин Крауч в своем недавно вышедшем на русском труде «Постдемократия» определяет нынешнюю эпоху – как бы вслед за постмодерном – как «постдемократическую» [1]. В такой системе политики замкнуты в своей собственной среде и поддерживают связь с обществом посредством начиненного манипулятивными технологиями *PR*–а. При этом сохраняется вся формальная демократическая атрибутика: выборы, разделение ветвей власти и т.д., однако в постдемократическом обществе, как в додемократические времена, всеми делами вершит симбиозная политическая и финансовая элита, причем доминирующей является последняя составляющая. Характерно, что некоторые комментаторы окрестили подобную формацию «новым тоталитаризмом».

Скепсис относительно адекватности нынешних демократических обществ классическим определениям демократии естественным образом возникал у многих исследователей (мы, например, иногда пользовались термином *квазидемократия*). Но похоже, что Крауч не только подобрал очень удачный термин, но и дал научное обоснование всему этому. В частности, он считает, что современные представления о демократии подразумевают «ограниченные возможности правительства в неограниченной экономике» и сводят демократическую составляющую к проведению выборов, которые, к тому же, можно назвать таковыми лишь с большой натяжкой. В этих условиях «правительство становится своего рода институциональным идиотом», которого все время обвиняют в невозможности реализовать эффективную политику, приписывая такую возможность лишь «частному бизнесу». Заметим, что подобная ситуация по своей сути во многом приравнивает так называемые страны с «развитой» демократией к тем, в которых демократические институты в современной интерпретации имеют недолгую историю.

В отличие от постдемократических реалий в виртуальном мире, где нет четко выраженных иерархических структур управления и соблюдается известная анонимность граждан, вроде бы царят классические, протодемократические нравы (но это – лишь в определенной мере, и к этому мы еще вернемся) типа тех, что, возможно, имели место в античных Афинах.

Между тем «граждане виртуально демократического общества», при всех своих известных и не совсем известных особенностях, являются производными от реального мира, и поэтому определенное взаимодействие и даже конфликт между виртуальным и реальным обществами неизбежны. Это особенно характерно для тех сетевых структур, которые формируются по идейным интересам. Насколько нам известно, первый конфликт такого рода с вынесением обвинительного приговора в России (за высказывания в блоге о милиции) произошел в

2008г., но сейчас такие конфликты стали почти обыденными [2]. Наверное, нет смысла вдаваться в подробности известного всем «Химкинского дела» в Москве или же реального участия в ликвидации пожаров в России посредством соцсети *Пожар_ру.* Нечто подобное имело место и в Ереване, когда против сноса представляющего архитектурную ценность кинотеатра, а затем и против закона о реформировании образования была собрана масса подписей в блогосфере с последующим переносом «дела» в *Facebook*, что и вынудило властей поменять или же отредактировать свои первоначальные решения.

Примеров консолидации и «материализации» – с тем или иным успехом – «виртуальных граждан» для протестных действий в реальном мире – множество, причем специально оговорим, что мы не рассматриваем проявления «экологического» терроризма. Наши социологические оценки по Армении показывают, что наиболее эффективно и конструктивно в этом плане функционируют организации по охране окружающей среды и памятников культуры, что, как правило, очень доброжелательно воспринимается «реальным обществом». В таком контексте действия сетевых сообществ можно представить как некий механизм для компенсации дефицита демократии в условиях «постдемократии». Подобные акции соцсетей фактически укрепляют пошатнувшиеся демократические институты. Это может показаться странным, но, выступая против властей, соцсети в некотором смысле укрепляют институты «национального государства» в «постдемократических условиях» в его отношениях с наднациональным капиталом (если, конечно, у властей на то имеется желание и воля). Вместе с тем виртуальные сообщества занимаются не только вопросами культуры и экологии.

Совсем недавно как реальное, так и виртуальное сообщества были взбудоражены акцией расположенного в исландском «информационном офшоре» ресурса *WikiLeaks*, на сайте которого было представлено более 75 тысяч секретных документов Пентагона о ходе военной кампании в Афганистане. Известно, что после этого начались преследования: в различных странах, с не особенно скрываемой подачи военного ведомства США и, скорее всего, по надуманным обвинениям, были выданы ордера на аресты, вызваны на допрос сотрудники *WikiLeaks*.

Заметим, что вряд ли в свое время движение против войны во Вьетнаме могло бы собрать хоть небольшую часть той массовой аудитории и столько антивоенных аргументов против американского правительства, как это сделал *WikiLeaks*. Известно также, что, несмотря на непопулярность войн в Афганистане и Ираке (а в последнем она продолжается вопреки декларированию ее окончания), в целом реальный мир достаточно вяло реагирует на эти процессы. Причин тому много, но большей частью они лежат в плоскости той же «постдемократии» с искусным манипулированием обществом (возможная при нынеш-

нем симбиозе СМИ, власти и олигархата глобально-тотальная пропаганда, большие денежные компенсации семьям погибших военнослужащих и т.д.) [3].

Вместе с тем, и это может прозвучать несколько странно, скорее всего именно манипулятивная природа изрядной доли современных *СМИ,* в том числе виртуальных, позволяет некоторым аналитикам выдвинуть версию, что действия *WikiLeaks* являются частью масштабной и хорошо спланированной информационной операции. Тем самым публикация секретных документов, в интерпретации нынешних властей, никак не противоречит национальным интересам США, которые сегодня пытаются избавиться хотя бы от части неоконсервативного наследия администрации Дж.Буша. Между тем такая постановка вопроса актуализирует тему соцсетей и блогосферы в терминах информационных войн и информационной безопасности.

Сетевые структуры и сетецентричные войны в контексте проблем информационной безопасности. Не требует особых комментариев тот факт, что формирование в начале девяностых годов прошлого века концептуальных основ информационных войн *(ИВ)* и информационных операций (*ИО*) совпало, а скорее всего было обусловлено, именно появлением *Интернета*.

Теория и практика *ИВ* и *ИО,* как и Интернет в целом, развиваются весьма динамично. В 90-х годах прошлого века экспертами *RAND* были разработаны концепции «информационных войн» (*ИВ*) и «сетецентричных войн» (*СВ*) [4]. Понятие «сеть» предполагает отказ от метода иерархического правления «центр – периферия» и формирование не имеющей четкой структуры, т.е. неструктурированной системы, подчиняемой логике саморазвития и нелинейных процессов. В подобной системе «центр» формально отсутствует, однако каждое из входящих в систему звеньев может взять на себя функции руководящего «центра».

В основе концепций *ИВ* лежат представления, согласно которым могущество государства в первую очередь зависит от возможности быть осведомленным, получить информацию и адекватно на нее реагировать. Цель *ИВ* – «убедить или принудить целевую аудиторию к принятию решений, способствующих продвижению собственных национальных интересов», а задача *ИЦВ* некоторыми аналитиками интерпретируется как «имплантация своего культурного кода в социуме условного друга или конкурента».

Однако отметим, что *ИСВ* является инструментом, которым могут пользоваться далеко не все, т.к. для его эффективного применения подразумевается:

- наличие системы с высокоинтеллектуальными ресурсами и притягательной идеологической средой, компоненты которой могут полноценно осведомляться, а также быстро и адекватно реагировать на полученную информацию;

- осознание военной обстановки (широко интерпретируя это понятие и не имея в виду чисто военное положение) и соответствующий мобилизационный стиль работы и действий [5].

Новые концепции привлекли внимание политических и военных стратегов. Очень скоро *ИВ* и *ИСВ* стали одним из краеугольных элементов современной внешней и военной политики США и других ведущих государств. В этом аспекте нетрудно заметить, что виртуальные социальные сети во многих своих проявлениях могут послужить инструментом для ведения *ИВ* и *ИСВ.*

Это проявляется в мирное время, когда виртуальные соцсети осуществляют, например, информационно-организационное обеспечение «цветных революций» (как это недавно имело место в Иране). Соцсети играют активную роль и во время боевых действий: например, по ходу израильско-палестинского или же армяно-азербайджанского вооруженного противостояния. Таким образом, соцсети являются инструментом *ИВ,* и для их обсуждения уместна терминология из сферы информационной безопасности *(ИБ),* в которой различают технический и контентный сегменты.

Приоритетной задачей технической части *ИБ* считается обеспечение безопасности так называемых «*критических инфраструктур*» – систем управления, энерго- и водоснабжения, коммуникационно-информационных, финансовых и других систем. Представляется, что в этот список следует включить также и соцсети. В частности, согласно данным *Ponemon Institute*, порядка 65% участников опроса – пользователей социальных веб-сайтов не используют настройки безопасности и приватности, 90% регистрируются в сети, не удосуживаясь ознакомиться с ее политикой безопасности, а 40% указывают при регистрации настоящий домашний адрес и столько же нарушают тайну пароля. Естественно, что в такой обстановке криминал в соцсетях процветает, как в лучшие для гангстеров времена в Чикаго. Заметим также, что базы данных в соцсетях представляют интерес не только для криминальных структур, но также и для мало-мальски уважающих себя спецслужб. Не говоря уже о том, что остается весьма проблемной фигура администратора, который постепенно приобретает статус оруэлловского «Большого Брата».

Намного сложнее, как нам кажется, обеспечение защиты контентного сегмента, в котором уровень *ИБ* во многом определяется способностью общества отстаивать свои базовые ценности. Это особенно важно в контексте принципа *СВ* – «имплантация своего культурного кода в социуме условного друга или конкурента». В качестве методики защиты, по аналогии с принятыми в техническом сегменте *ИБ* определениями, как нам представляется, следует устанав-

ливать также и не всегда очевидные «*критические инфраструктуры*» контента. В практике это означает, что из системы национальных ценностей должны выбираться и стать предметом особого внимания и защиты те тезисы, искажение которых может привести к национальной деморализации и деградации.

Возможные сценарии и комментарии. В последнее время появилось множество прогнозов относительно развития Интернета, и это относится как к технической сфере, так и к социальной. В частности, эксперты *Cisco и Monitor Group* полагают, что в ближайшие 15 лет интернет-аудитория будет расти в основном за счет жителей развивающихся стран, а границы Интернета будут размыты[1]. В этом случае пользователи по всему миру смогут выходить в Сеть с большого количества доступных устройств, а Интернет станет центром для оказания услуг. Вместе с тем Интернет ждет превращение в небезопасную сеть из-за возрастающего числа кибератак, и, как следствие, у него могут появиться безопасные аналоги, доступ к которым будет недешев. В этом аспекте любопытно, что в США не исключают возможности нанесения военного удара в ответ на кибератаки[2], т.е. действия в Интернете могут послужить *casus belli*, а возникшие войны могут в принципе привести к тотальному разрушению как реального, так и виртуального миров.

По прогнозам шведских исследователей развитие интернет-сетей в итоге приведет к формированию интеллектуальной *net* элиты, которая, собственно, и будет управлять реальным глобализованным обществом [6]. Между тем интеллектуальный уровень современных соцсетей не всегда располагает к оптимизму, и это относится не только к повальному увлечению разного рода играми, что приводит к своеобразной инфантилизации *net* сообщества [см., например, 7]. Вслед за выражением *easy music* можно ввести в оборот термин *easy information,* которая к тому же передается на весьма упрощенном, «глобализованном» языке [8]. Этой *легкой информации* свойствен определенный синергизм, так как она, в отличие от профессиональной – *сложной информации*, обладает определенной сверхтекучестью[3] и легко резонирует с себе подобными, разветвляется, а в итоге получаем синергетический, но не всегда утешительный эффект.

Некоторые выводы. Можно констатировать, что сегодня происходит интенсивное взаимодействие между реальным и информационно-виртуальным мирами. Граница между ними становится условной, а понятие «виртуальный»

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

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

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

теряет свой первоначальный смысл. Этому особо способствует бурное развитие соцсетей и блогосферы в Интернете, что содержит в себе как большие возможности, так и серьезные риски, из которых отметим следующие:

Социальные сети и блогосфера в Интернете способны, как минимум, тормозить процессы *дедемократизации*, столь характерные для современных *постдемократических* обществ. В определенных случаях – в контексте тенденции к доминированию наднационального капитала на государственном и глобальном уровнях – действия подобных структур могут быть направлены на защиту «национального государства» и цивилизационных ценностей общества. Таким образом, при определенных сценариях развития интернет-структуры способны стать глобальными демократическими институтами.

Социальные сети и блогосфера в Интернете являются инструментом для ведения информационно-сетецентрических войн, т.е. в известных обстоятельствах эти структуры являются в некотором смысле оружием массового поражения, обладание которым увеличивает искушение проведения экспансионистской политики. В этом контексте очевидно, что интернет-структуры и их действия следует изучать и оценивать также и в терминах информационной безопасности, с использованием методик по определению и защиты *критических инфраструктур технического и контентного сегментов*.

Сентябрь, 2010г.

Источники и литература

1. *Крауч К.,* Постдемократия. М.: Гос.ун-т, Высшая школа экономики, 2010.
2. *Таратуга 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.

INTERNET STRUCTURES IN THE CONTEXT OF POST-DEMOCRACY AND INFORMATION SECURITY

Gagik Harutyunyan

Resume

It can be stated that today intensive interaction between real and information-virtual worlds is taking place. The border between them becomes conventional and such a concept as "virtual" loses its original tenor. This is particularly boosted by the rapid development of social networks and blogosphere and this process contains both great possibilities and serious risks among which the following should be mentioned:

- Social networks and blogosphere can at least hamper the processes of de-democratization which are so characteristic of *post-democratic* societies. In some cases, in the context of the tendencies to the domination of the supranational capital on state and global levels. Thus, in case of certain scenarios of development, internet structures can become a global democratic institution.
- Social networks and blogosphere are tools for the information and network-centric wars, i.e. under some circumstances those structures are a kind of a weapon of mass distraction, possession of which increases temptation of carrying out policy of expansion. In this context it is obvious that internet structures and their activities should be studied and evaluated in terms of information security, using the methods of defining and protection of *critical infrastructures of technical and content segments.*