Доктор Пётр Лучук

От пропаганды до троллинга – теория заговора или прелюдия гибридной войны?

Ещё в 1993 году американский социолог и футуролог Алвин Тоффлер (Alvin Toffler) в своей знаменитой книге „Война и антивойна” очень образно описал, как будут возникать войны в киберпространстве (2006, с. 170). Он предостерегал, что игнорирование этой угрозы может привести к ситуации, когда группа профессиональных хакеров будет в состоянии привести страну на край финансовой пропасти и анархии, которая постепенно распространится на весь мир. Тоффлер был также убеждён, что вместе с развитием технологий террорист из любой точки на земле сможет принести значительно больше вреда, пользуясь только клавиатурой компьютера, чем бомбой или карабином. Как учёный, Тоффлер одним из первых ещё в начале 90-х предвидел начало нового вида войны и появление нового вида солдат. А главную роль на этом глобальном поле сражений должна была играть именно информация (там же, с. 170-171).

На протяжении последних лет можна наблюдать немало примеров, которые однозначно подтверждают, что перенос военных действий в киберпространство – это не фикция. Методы ведения гибридной войны опираются в огромной степени на разведовательные действия и на контрразведку. Гораздо важнее, чем уничтожить инфраструктуру врага, получить информацию о нём и благодаря этому уничтожить его систему безопасности. В разведдеятельности именно поиск информации является самым ценным умением. Независимо от своего содержания, каждая информация может пригодиться в самый неожиданный момент. Именно поэтому во времена холодной войны шпионы с риском для жизни изучали даже ритм жизни своих „объектов” и собирали на их тему всю доступную и менее доступную информацию. Сейчас шпионские забавы переместились в интернет, где в огромной степени сами пользователи провоцируют их активность.

Американский эксперт в делах раздведдеятельности Роберт Д. Стиль (Robert D. Steele), на которого ссылается Тоффлер, считает, что именно разведка должна являться вершиной информационной инфраструктуры (там же). По его мнению, агенты и аналитики должны пользоваться как явными, так и тайными источниками информации, а эффекты их работы должны быть общедоступными. Но не становимся ли мы в эпоху интенсивного развития технологий, эпоху Facebooka и продвигаемого WikiLeaks опубликования всех архивов всё больше похожи на героев романа „1984” Джорджа Оруелла, и не живём и мы уже под внимательным наблюдением Большого Брата?

Война за информацию или информационная война?

Не подлегает сомнению, что всякого рода социальные сети являются богатейшим источником информации для агентов разведок отдельных стран. Когда-то поиск такого рода информации требовал огромных усилий и был очень рискованным занятием. Сейчас мы по собственной воле размещаем в публичном пространстве все „оперативные сведения” о себе. На основании нескольких информаций и популярных в последнее время апликаций геолокализации достаточно несколько минут, чтобы выстроить цепочку контактов, связей и знакомств любого конкретного человека или определить его актуальное местонахождение с точностью до нескольких метров. Для хорошего хакера умение перехватить пароль, личные данные или банковские реквизиты не является проблемой, поскольку большинство интернет-пользователей пренебрегает даже основными средствами безопасности в своей жизнедеятельности в сети. Именно на эти угрозы обращает особое внимание Европейская комиссия, описывая европейский подход к умениям и навыкам пользования медиа в цифровом пространстве (2007).

Опасности, связанные с нарастанием пропагандных действий, и первые проявления информационной войны, направленные против конкретных стран Евросоюза, Евросоюз определил как вражескую пропаганду прочих стран-членов ЕС, которая приобрела новые формы и способы в контексте новой геополитической специфики. Одним из самых популярных действий такого типа является интернет-троллинг, а также – использование fake news – препарированных новостей, которые ведут к дезинформации общества, а в результате – к углублению различий и разноголосий в структурах ЕС и к разрыву связей стратегических партнёров на линии Евросоюз – США, а также внутри самого Евросоюза.

Сегодня не секрет, что киберпространство и технологические новинки активно использует пропаганда. Кроме непосредственных кибер-атак на информатические структуры, серверы и даже на информационные сервисы, именно пропаганда в интернете является основным орудием новой военной доктрины – в войне гибридной. И хоть о интернет-троллях и о пропаганде говорится довольно давно, настоящий перелом в этом вопросе произошёл несколько месяцев назад. В 2015 году СМИ облетела сенсационная новость: открыто функционирование „фабрики троллей" в Петербурге. Официально там действовало Агентство интернет-исследований, руководил которым олигарх Евгений Пригожин – частно близкий знакомый Владимира Путина. В действительности же в агенстве трудилось более 300 „блогеров", заданием которых было на протяжении „рабочего дня" опубликовать до 30 тысяч восхваляющих Россию и самого Путина постов в фейсбуке, твиттере и на интернет-порталах как в самой России, так и за её границами. После этого открытия исчезли последние сомнения в том, что таких мест только на территории России гораздо больше (Лучук, 2017, с. 58).

Тролли не только в сказках

Нарастающая интенсивность действий Кремля на поле информационной войны, проводимой против стран Евросоюза, обратила на себя внимание также авторов Резолюции Европейского Парламента, которая концентрируется на вопросах стратегической коммуникации с целью противостояния вражеской пропаганде третьих стран (2016, s. 5-7). Кремль владеет множеством каналов дезинформации, начиная от групп консультантов и фондов (например, Русский мир) и до специальных органов (Россотрудничество), телеканалами на разных языках (например, RT), пропагандными информационными агентствами (Спутник) и армией интернет-троллей (там же, с. 5).

Принимая во внимание широкую палитру пропагандистских действий, ведущихся при помощи интернета, особенно следует обратить внимание на различие двух основных групп так называемых интернет-троллей. Первая из них – это **интернауты, выполняюшие свои задания на заказ и за оплату.** К их обязанностям относится, например, размещение постов и комментариев, цель которых – показать своего заказчика в позитивном свете, опираясь в основном на факты, правда, на соответственно подобранные и сманипулированные. Вторая группа - это **интернауты, называемые „полезными идиотами" (useful idiots).** Их задание - создавать профили в социальных сетях и вести блоги, в которых должны соответственно появляться подготовленные и препарированные информации. К этой группе относятся также все те люди, которые, не сознавая всей операционной системы, доверяют искуственным блогерам, укрепляя тем самым доверие к ним и в глазах общественного мнения.

Организация CERT.GOV.PL предупреждала, что как социальные медиа так и весь интернет очень охотно используют для своих целей милитаристские, разведовательные и пропагандистские системы. Анализируя подобные случаи, администраторы социальных сервисов и крупнейших информационных порталов в Польше заметили, что в большинстве случаев записи, появляющиеся в интернете, были как две капли воды похожи на появляющиеся на других порталах, как будто их писали под копирку. Причём все публикации появлялись почти одновременно. Поначалу эти записи, написанные неграмотным польским языком, пользователи интернета высмеивали, но со временем их качество очень улучшилось. CERT.GOV.PL била тревогу, что рост записей такого типа давно перешёл границы

допустимого и становится всё более серьёзной угрозой в информационной войне (2014, с. 48-49).

Настоящей сенсацией стало открытие „фабрики троллей" в Петербурге. Полный механизм профинансированных Кремлём действий интернет-троллей довольно прост: сотрудники, которые официально работали как блогеры, должны были создавать фиктивные аккаунты на различных порталах и в социальных сетях. Потом они начинали свою деятельность в интернете, используя различные фиктивные аккаунты и личности, и размещали множество постов и комментариев, создавая и наращивая информационный шум вокруг избранной темы. Очень важно знать, что тролли соединялись с интернетом при помощи системы серверов proxy, что должно было стать гарантией анонимности, а в самом худшем случае - успешно затереть следы к источникам информации. Использование proxy должно было создавать впечатление, что записи, которые публиковались, не имеют никакого отношения к России, а авторы не находятся на территории этой страны. С точки зрения обычного пользователя, не осознающего механизмов машины пропаганды, всё выглядело так, как будто авторы находились в стране, по отношению к которой и предпринимались пропагандистские действия. Работающие как хорошо отлаженные фирмы маркетинга, „фабрики троллей" были в состоянии целыми сутками заливать интернет пророссийскими комментариями различной степени эмоциональной окраски. Часто для большей правдоподобности отдельные тролли даже вступали между собой в полемику. Типичным действием были также массовые жалобы администраторам порталов социальных сеток на якобы нарушения и требования заблокировать или удалить записи, не совпадающие с линией пропаганды (Лучук, ст., цит. с. 59).

К сожалению, отличить записи авторства троллей, действующих на заказ, от записей, которые пишут обычные, и часто наивные, пользователи социальных сетей, со временем становится всё труднее. Непросто было также найти веские доказательства присутствия действий пропаганды, манипуляций и информационной войны в польском интернете. Занялся этим Анджей Голось, социолог маркетинг-агенства „ARC Rynek i Opinia", который решил рассмотреть проблему с научной точки зрения (2014).

Голось начал с попытки измерить реальное присутствие российского влияния в польском интернете. Он проанализировал ряд идущих там дискуссий и содержание сотен комментариев. В результате ему удалось найти определённые закономерности. Оказалось, что пророссийские записи составляли 39 процентов, а под популярными статьями на российско-украинскую тему их количество увеличивалось до 70 процентов. Анализируя все записи, автор пришёл к выводу, что среди всех записей проукраинские составляли 32 процента, а в 10 самых популярных статьях их было только 17 процентов. Такую же схему можно было увидеть в дискуссиях, идущих в социальных сетках. Как только там появлялись проукраинские записи, немедленно начиналась лавина пророссийских голосов. Через несколько часов атака заканчивалась, и всё возвращалось в норму (там же, с. 9-15).

Подобные выводы касались также аназила записей под текстами о России на интернет-страницах CNN и BBC. Этот механизм обозначает, что на войну в киберпространстве брошены многочисленные силы, задача которых – подготовить почву для возможных последующих волн гибридной войны. Наивно было бы утверждать, что так скоординированные действия – всего лишь случайность.

В свою очередь Роберт Горва, аналитик из Оксфорда, в своей аналитической работе описал механизмы создания в интернете фиктивных аккаунтов с целью расширения пропагандистский действий в массовом масштабе (2017). Горва опирается на информации, полученные от специалиста коммуникации и маркетинга из Польши, который по понятным причинам остался анонимным. Как сотрудник фирмы, которая годами специализируется в создании фальшивых аккаунтов и цельных образов в интернете, этот источник информации обладает исключительно ценными знаниями в области использования механизмов подобного типа в различных областях маркетинга – от торговли до политики. Оказалось, что только одна эта фирма на протяжении 10 лет была в состоянии создать и поддерживать почти 40

тысяч искуственных аккаунтов. Следует отметить, что каждый такой искусственный аккаунт имел определённую историю в интернете, свои черты характера, соответствуюшие группы по интересам в социальных сетках. Фальшивым пользователям присваивались также уникальные адреса IP, чтобы их действия в интернете не будили ничьих подозрений и как две капли воды напоминали стандартную активность в сети (там же, с. 16).

Сценарий манипуляции

В контексте реальных возможностей и результатов проведения на широком уровне пропагандистских действий особого внимания заслуживает модель манипуляции общественным мнением, обработанная Trend Micro – международной фирмой, которая специализируется в системах безопасности сектора IT (2017, с.62-64). Она состоит из восьми основных этапов:

Этап 1 – разведка

В его основе лежит сбор информации на тему запланированной акции и анализ адресатов этой акции. В рамках этих действий собираются информации о лицах, потенциально заинтересованных тематикой действий, их лояльности, а также знаний в данной области.

Этап 2 – вооружение

Второй этап предусматриавет приготовление, спрепарирование ключевой истории и собственной версии фактов, которые в будущем планируется передать целевым адресатам. Также на этом этапе происходит приготовление дополнительных fake news, вспомогающих ключевую историю, и обработка различных „альтернативных версий" данного события. Это ведёт к созданию информационного шума вокруг данной темы и дословно – заливания интернета сманипулированными информациями.

Этап 3 – доставка адресатам

Этот этап предусматривает распространение приготовленных заранее и препарированных материалов и fake news при помощи определённых каналов связи, например, социальных сеток или традиционных СМИ. Кроме того, действия на этом уровне предполагают также возможности использования всех возможных каналов fake news, причём, в первую очередь, манипуляции и дезинформации при помощи сети ботов и ферм интернет-троллей.

Этап 4 – эксплуатация

Предусматривает постоянное подогревание темы в социальных сетках и укрепление достоверности fake news при помощи подогревания настроений конкретных социальных групп и приверженцев и активистов, отождествляющих себя с распространяемой идеей.

Этап 5 – закрепление

Один их ключевых шагов, цель которого – укрепить достоверность всей пропагандистской акции. Предусматривает контакт с максимально крупной группой адресатов, в том числе - настроенных критически. Основная цель на этом этапе – это в некотором смысле требование от пользователей интеракции и так называемого вирусного эффекта. Чем больше людей будет говорить и писать на данную тему, тем больше людей прочитает о ней и услышит, а следовательно – геометрически увеличится количество людей, потенциально заинтересованных идеей, или тех, кто, не вникая в детали, просто поверит в пропагандированный таким образом fake news. Здесь часто используется впечатление ссоры на данную тему и препарируются записи как позитивного, так и негативного значения, цель которых – поднять ранг fake news и обратить внимание людей, изначально настроенных критически.

Этап 6 – поддержка заинтересования

На этом этапе в игру входят приготовленные заранее „истории поддержки" и подогревание активности на максимально высоком уровне.

Этап 7 – переход от слов к делу

Предполагает реализацию действий, запланированных в самом начале акции. Это может привести к дополнительной стимуляции целевой групы и спрвоцировать, например, реализацию действий, продуманных инциаторами заранее: организации манифестации,

марша поддержки, открытого письма и тд.

Этап 8 – вытирание следов

Здесь происходит как можно более быстрое отвлекание внимание общественного мнения от данной проблемы и перенаправление его на соответственно направленные другие темы. В крайних случаях этот этап связан даже с полным замалчиванием и утратой памяти о всех предыдущих событиях с целью успокоения общественных настроений. Такия действия обеспечивают полных контроль над ситуацией и дают возможность эффективного „переключения" внимания общественного мнения на иные рельсы, с возможностью очередной активизации целевой группы, если в будущем такая потребность возникнет.

Выводы

Последовательная реализация всех пунктов этого сценария означает, что информационная война, направленная на европейские страны, уже идёт. Не подлежит также сомнению, что социальные сетки и СМИ имеют огромное влияние на реальность, а то, что происходит в виртуальном пространстве, всё чаще и всё сильнее влияет на целые общества. Факты всё больше теряют своё значение в ситуациях, когда вместо объективных информаций в ходу находятся спрепарированные и базирующиеся на эмоциях фейки. Именно это соединение интернета и теории манипуляции обшественным мнением даёт самые твёрдые и пугающие эффекты, особенно если всё это опирается на мир политики.

Доктор Пётр Лучук
Журналист и теолог. Преподаватель кафедры интернета и цифровых коммуникаций института медиа-образования и журналистики UKSW. Автор разработок на тему кибер-безопасности, информационной войны и влияния современных технологий на общественные связи.

Bibliografia:

CERT.GOV.PL, Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku, dostępny na stronie internetowej: http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html.

Gorwa, R.: Computational Propaganda in Poland:
False Amplifiers and the Digital Public
Sphere
, dostępne na stronie internetowej:
http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Poland.pdf

Gu, L., Kropotov, V., Yarochkin
, F.: The Fake News Machine. How Propagandists Abuse the Internet and Manipulate the Public
, dostępne na stronie internetowej: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf?_ga=2.58817832.485134583.1503746972-1268436894.1503494608

Komisja Wspólnot Europejskich (2007): *Europejskie podejście do umiejętności korzystania z mediów w środowisku cyfrowym*, dostępne na stronie internetowej: http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52007DC0833&from=PL.

Łuczuk, P.: Nie karmić trolla! Kulisy wojny w internecie. w: Wpis 7-8 (81-82 2017), s. 57-60.

Parlament Europejski (2016): *Rezolucja Parlamentu Europejskiego z dnia 23 listopada 2016 r. w sprawie unijnej komunikacji strategicznej w celu przeciwdziałania wrogiej propagandzie stron trzecich*, dostępne na stronie internetowej:
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0441&language=PL.

Toffler A., Wojna i antywojna, Poznań 2006.