Кибервойна и противоборство в цифровом информационном пространстве

ЛЕОНОВА Ольга Георгиевна
Доктор политических наук, доцент, профессор кафедры глобалистики факультета глобальных процессов МГУ им. М.В. Ломоносова

Аннотация
Информационный кибертерроризм – это форма политически мотивированного информационного насилия по отношению к стране-мишени. Он имеет определенные виды, типы и специфические характеристики. Информационное противоборство в цифровом информационном пространстве является частью кибервойны, что делает необходимым контроль и регулирование информационного потока со стороны государства.

Ключевые слова:
кибервойна, информационный кибертерроризм, дезинформация, фейковые новости, информационные диверсия, атака, вброс.

Кибервойна становится одной из самых актуальных и обсуждаемых проблем в современном политическом дискурсе.

Все технологии кибервойны можно разделить на *жесткие*, которые имеют целью разрушение сетей управления инфраструктурой страны, что может привести к фактически уничтожению государства, и *мягкие*, проявляющиеся как информационное противоборство в цифровом информационном пространстве. В данной статье речь пойдет именно о мягких технологиях проявления кибервойны.

Прозрачность и публичность всех событий, происходящих в стране или мире, которую обеспечивает и гарантирует интернет, сегодня оборачивается другой стороной. Свобода мнений и точек зрения, демократичность распространения и получения информации, как оказалось, имеет и ряд негативных последствий, которые несут непосредственную угрозу безопасности страны. Поэтому многие политики, эксперты, общественные лидеры и бизнесмены высказывают озабоченность проблемой кибербезопасности и кибертерроризма, которые начинают угрожать политической и экономической стабильности государства.

Такая дестабилизация может быть спровоцирована навязыванием стране дебатов на основе фейковых новостей, дезинформации и предвзятых (заказных) онлайн комментариев подставными «экспертами», которые могут привести к расколу общества и гражданскому противостоянию.

Есть **три уровня анализа** информационного кибертерроризма.

Первый — *теоретико-методологический уровень* предполагает анализ и уточнение категориального аппарата исследования данного феномена, критерий его выделения среди других видов международного терроризма, (к которому также относятся государственный, ядерный, уголовный, религиозный, биотерроризм и др.), создание классификации (–ий) его видов и подвидов.

Второй уровень анализа — *концептуальный*, который позволяет выявлять основные формы, механизмы, алгоритмы, методы и инструменты информационного кибертерроризма, выделять специфические его особенности, создавать классификацию (классификации) его видов и подвидов.

Третий уровень — *технологический*, целью которого является изучение «материальной» составляющей информационных потоков и виртуальной коммуникации, а также поиск механизмов противодействия угрозам информационного кибертерроризма.

Сегодня на Западе озабочены отсутствием общей терминологии в области исследования кибервойны. Так Брюс Макклинток пишет: «Необходимо выработать четкий консенсус, что считать проявлением кибер-насилия... Сегодня нет общепринятых определений для кибер-терминов — в разных странах и организациях они понимаются по-разному». (*Перевод автора*). Он упоминает, что зато есть около двадцати определений понятия «кибер-атака», смысл которых весьма варьируется. Отсутствие ясности в терминологии тормозит прогресс в создании национальных стратегий и международных стандартов противодействия кибер-войне. Макклинток полагает, что достижение согласия по поводу трактовки определений необходимо, т.к. это поможет принять решение о применении существующего международного права в области киберпространства. [2]

Мы полагаем, **что информационный кибертерроризм является одной из разновидностей международного терроризма**.

Сегодня все чаще говорят об информационном оружии и возможности террористических актов с использованием информационных систем.

Информационным оружием являются компьютерные вирусы, программные закладные устройства (так называемые «логические бомбы»), сознательно внедренные в программное обеспечение ошибки, манипулирование информацией.

Дезинформация, фейковые новости, манипулирование ими по степени опасности для общества также можно отнести к *информационному* оружию. По своим разрушительным последствиям для общества и отдельных граждан действия по применению такого и*нформационного* оружия можно приравнять к понятию терроризм. А поскольку это происходит в виртуальном *информационном* поле, следует уточнить, что данное явление представляет собой *информационный* терроризм.

Исследуя данное явление в рамках именно интернет-пространства, данный феномен следует определить как цифровой информационный терроризм или информационный кибертерроризм.

Информационный кибертерроризм сегодня становится средством политической борьбы против существующей социально-экономической и политической системы страны-мишени отдельных ангажированных (или неангажированных) личностей, групп хакеров и анонимусов, специальных подразделений и структур, финансируемых на деньги частных акторов или за счет федерального бюджета, а также отдельных государств. Это есть экстремистская форма проявления информационного насилия и манипулирования сознанием потребителя информации, имеющее целью дестабилизацию, а впоследствии и трансформацию социально-экономической и политической системы страны-мишени.

Анализируя и суммируя различные характеристики *информационной* террористической деятельности, её цели и задачи, можно дать ей следующее **определение:** *информационный кибертерроризм* — это инструмент и форма политически мотивированного информационного насилия по отношению

к стране-мишени, систем жизнедеятельности общества и отдельных граждан, реализуемая *субъектами различного организационного и идеологического статуса*.

Информационный кибертерроризм — это специфическая политическая технология реализации поставленных целей и достижения задач посредством управления информационным потоком и создания информационных полей с заранее заданными свойствами.

Информационный кибертерроризм — специфический вид деятельности в цифровом информационном пространстве, имеющий **целью** расшатывание социально-экономических и политических устоев общества; дестабилизацию, а впоследствии и трансформацию социально-экономической и политической системы страны-мишени.

Задачами информационного кибертерроризма являются: навязывание воли, мнений, взглядов и точек зрения субъекта информационных кибератак; создание утопической социальной реальности; навязывание дискуссий и дебатов в обществе по заранее спровоцированной тематике и с заранее предсказуемым результатом.

К появлению информационного кибертерроризма привели некоторые негативные процессы, происходящие в цифровом информационном пространстве. Современные информационные и коммуникационные технологии создают новые возможности для цифрового информационного терроризма.

Факторами, обусловившими появление информационного терроризма, являются процессы информационной глобализации, технологический прогресс в информационной и коммуникационной сферах, усиление геополитической конкуренции в глобальном мире.

Если попытаться **классифицировать** информационный кибертерроризм по степени опасности для социально-политической стабильности страны, то можно выделить следующие его *виды*: искусственная информационная перегрузка потребителя информации, дезинформация, информационный вброс, информационная диверсия, информационная атака.

С точки зрения *тактики* реализации можно классифицировать следующие *типы* цифрового информационного терроризма: превентивный; провокационный; селективный; средовой (объектом которого в интернет-среде становятся группы по интересам, возрасту, социальной или половой принадлежности); вирусный; «слепой».

Информационный кибертерроризм имеет свои **специфические характеристики**.

Во-первых, корыстные, но тщательно скрываемые от потребителей информации цели субъектов терроризма.

Во-вторых, данные цели не обязательно имеют в своей основе экономическую или финансовую корысть, но чаще всего они мотивированны политическими интересами.

В-третьих, видимая легитимность деятельности, вполне правомочное использование свободы слова и информации в интернет-пространстве.

В-четвертых, его запланированным следствием является дестабилизация политической и социально-экономической системы общества, разрушение его традиционной культуры, психологические, этические, ментальные сбои у потребителей информации.

Если признать информационное противоборство в цифровом информационном пространстве как часть кибервойны, то это делает возможным и необходимым вмешательство государства, а именно контроль и регулирование информационного потока, а также корректировку информационного поля.

Однако такое вмешательство государства порождает ряд юридических, политических и социальных проблем. Сегодня международное сообщество озабочено поиском путей решения этих проблем и возможных мер противодействия дезинформации, фейковым новостям и фальсификациям информации.

ЛИТЕРАТУРА

1. **Combating Online Information Operations.** (Стенограмма телепередачи. December 6, 2017). URL: https://www.cfr.org/event/combating-online-information-operations

2. MCCLINTOCK B. **Russian Information Warfare: A Reality That Needs a Response. Commentary** (U. S. News & World Report). July 21, 2017. URL: https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html

3. **Stateless Attribution. Toward International Accountability in Cyberspace.** Ed. by John S. Davis II, Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern, Michael S. Chase. Santa Monica, Calif. Published by the RAND Corporation.2017. 57 p. URL: https://www.rand.org/pubs/research_reports/RR2081.html

4. **Tactical Cyber. Building a Strategy for Cyber Support to Corps and Below.** Ed. by Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, Drew Herrick. Santa Monica, Calif. Published by the RAND Corporation, 2017. 83p. URL: https://www.rand.org/pubs/research_reports/RR1600.html

5. **The Hacked Elections, Online Influence Operations, and the Threat to Democracy symposium.** December 6, 2017. (Стенограмма симпозиума). URL: https://www.cfr.org/hacked-elections-online-influence-operations-and-threat-democracy

6. WIENER M., WIENER C. **Cybersecurity Threats: How Vulnerable Is the United States?** Annual Lecture on Science and Technology. June 19, 2017. URL: https://www.cfr.org/event/cybersecurity-threats-how-vulnerable-united-states

Россия оцифровывается

Объем цифровой экономики в России вырос в пять раз до 4,3 трлн руб. за последние пять лет. Если в 2012 г. на цифровую экономику приходился 1% ВВП России, то по итогам 2017 г. этот показатель увеличился до 5%. Об этом сообщил глава Министерства связи и массовых коммуникаций РФ Николай Никифоров на расширенном заседании коллегии Минкомсвязи. При этом объемы связанных с Интернетом рынков выросли с 10% ВВП в 2012 г. до 24% в 2017 г.

Цифровая экономика

Николай Никифоров (на фото) начал свое выступление на итоговом заседании коллегии Минкомсвязи с заявления о том, что Россия переходит на цифровую экономику. Если в 2012 г. цифровая экономика давала чуть больше 1% ВВП РФ, то в 2017 г. — в пять раз больше — 4,3 трлн руб. Он также отметил, что объемы рынков, которые связаны с Интернетом, выросли с 10% ВВП до 24%. При этом количество граждан, занятых в интернет-экономике, увеличилось с 700 тыс. человек до 2,3 млн человек.

Аудитория российского Интернета увеличилась с 59 млн человек в 2012 г. до почти 88 млн в 2017 г. В 2012 г. только 12% пользовались мобильным способом доступа в Интернет, а в данный момент — это уже 70%. При этом объем мобильного трафика увеличился на 90%. Однако стоимость мобильного трафика в РФ в 10 раз дешевле, чем в США, в три раза дешевле, чем Германии, в два раза дешевле, чем в ЮАР.

Сети третьего и четвертого поколений

Николай Никифоров обратил внимание на то, что, следуя цифровой экономике, всего за шесть лет удалось пройти путь от запуска первых сегментов сетей связи четвертого поколения к полноценному использованию этого стандарта.

По его словам, этому способствовал введенный принцип технологической нейтральности сотовых сетей и реформа процедуры выделения радиочастот. За пять лет изменились принципы оплаты радиочастотного спектра: операторы стали платить не за число базовых станций, а за объем используемого ресурса. "Разрешили операторам совместно использовать инфраструктуру связи и радиочастоты", — сказал чиновник.

Николай Никифоров также напомнил, что до 2015 г. частоты выделялись без дополнительных финансовых условий. "Мы ввели конкурентную процедуру, абсолютно прозрачную, которая предусматривает проведение торгов за частоты в форме аукциона. Первые же аукционы принесли в бюджет 15 млрд руб.", — сказал министр связи.

Он отметил, что в данный момент уже больше трети базовых станций (БС) сотовой связи в России работают в стандарте 4G. Николай Никифоров

уточнил, что это более 160 тыс. БС по всей стране, включая Крым. Он напомнил, что в 2012 г. их было 2000.

Заместитель председателя правительства РФ Аркадий Дворкович, комментируя итоги пятилетней деятельности Минкомсвязи, сказал, что по инфраструктуре связи удалось достичь плановых показателей. Что касается мобильной связи, покрытие связью в стандартах 3G и 4G на текущий момент составляет 80% и 40% соответственно.

С декабря 2017 г. в три-пять раз в зависимости от тарифных планов снизилась стоимость сотовой связи в роуминге, как для жителей Крыма, так и для граждан, приезжающих на отдых в Крым. Процесс снижения цен будет продолжаться и дальше. Николай Никифоров упомянул в своей речи, что полная отмена внутрисетевого роуминга в РФ должна произойти в первом полугодии 2018 г.

Перспективы 5G

Николай Никифоров напомнил о том, что менее месяца назад ПАО "Ростелеком", Nokia и фонд "Сколково" запустили первую в России открытую опытную зону фрагмента перспективной сети мобильной связи стандарта 5G/IMT 2020. Опытная зона позволит показать перспективы новейших технологий связи на основе 5G для их дальнейшего использования в разных отраслях экономики. ПАО "Ростелеком" проведет исследование возможности применения отдельных участков полос радиочастот в диапазоне 3400–3800 МГц совместно с ПАО "МегаФон".

Комментируя это событие, министр связи отметил, что таким образом РФ шагнула в новое технологическое будущее мобильной связи. "Сети 5G станут основой построения цифровой экономики, курс на развитие которой поставил президент РФ Владимир Путин в своем ежегодном послании в декабре 2016 г. Без 5G невозможен ни Интернет вещей, ни умный город, ни умное производство, ни умный дом, ни умный транспорт",— подчеркнул он.

Аркадий Дворкович добавил, что в данный момент готовятся конкурсы по предоставлению частот под распространение инфраструктуры 5G. Николай Никифоров после заседания коллегии Минкомсвязи рассказал журналистам, что проведение аукционов запланировано на конец 2018 г. "Подготовительная работа по этому идет. Сама процедура регламентирована нормативной базой, она занимает от семи до девяти месяцев. Пока выделение таких частот возможно лишь путем аукциона",— сказал он.

https://www.comnews.ru/content/112613/2018-04-10/rossiya-ocifrovyvaetsya