Введение в кибергеополитику

Леонид Савин

главный редактор журнала «Геополитика» и интернет портала Geopolitica.ru, руководитель администрации МОД «Евразийское движение».

В последнее время все чаще приходится слышать о возрастающей роли киберпространства в качестве инструмента политики, либо той сферы, где разворачивается противоборство между различными политическими организациями, странами и даже альянсами государств. Инцидент с Эдвардом Сноуденом является показательным фактом того, насколько Интернет коммуникации и взаимозависимость социальной среды с политикой, экономикой и военным сектором стали важны и влияют как на текущую повестку дня, так и на стратегическое планирование лидеров ведущих держав мира.

Если в геополитике уже достаточно разработан научный аппарат и дефиниции, которыми оперируют политики, эксперты и ученые, то киберпространство в какой-то мере представляет собой «terra incognita». И за обладание этим пространством ведется довольно активная борьба. Крайне показательным является то противостояние, которое заняли в отношении регулирования Интернет пространства различные государства. Дихотомия буквально повторяет тот мегацивилизационный раздел, который пролег между странами и народами, относящимися к Sea Power и Land Power. США, страны ЕС и их сателлиты выступают за полную свободу действий в Интернет, что является явным лицемерием[1], в то время как Россия, Иран, Китай, Индия и ряд других государств требуют того, чтобы Интернет был суверенным и находился под юрисдикцией норм международного права, точнее Международного Союза Электросвязи, входящего в Организацию Объединенных Наций. Саммит по вопросам киберпространства, прошедший в декабре 2012 г. в Дубаи показал усугубляющиеся противоречия, связанные с международными телекоммуникациями, когда США отказались подписать новый договор, регламентирующий право всех государств заниматься управлением Интернета. Данное разделение четко вписывается в схему Карла Шмитта, которая является надежным показателем Политического — это дуальные категории друг и враг. Данные категории не являются моральными, а представляют технические функции, которые проявились и в позициях по поводу взгляда на функционирование Интернет пространства.

[1] Достаточно посмотреть на то, как власти этих стран контролируют с помощью Интернет и социальных сетей своих граждан и собирают информацию об их частной жизни, а также как используются спецслужбами западных стран Интернет технологии для подрывной деятельности и шпионажа.

География киберпространства

Для начала нужно дать определение термину киберпространство. Исследователи приписывают авторство этого слова писателю-фантасту Уильяму Гибсону, который использовал его в рассказе «Burning Chrome», опубликованном в 1982 г. Два года спустя он развил эту тему и в своем знаменитом киберпанковском романе 1984 г. под названием «Neuromancer» — автор описал киберпространство как «всеобщую галлюцинацию»[1]. Киберпространство имеет существенное отличие от наземного, морского, воздушного и космического пространств — оно создано не природой, а является искусственной конструкцией, имеющей компоненты, которые могут меняться с течением времени.

В различных странах есть свои определения киберпространства. В США в документе по национальной стратегии в отношении кибербезопасности от 2003 г. было указано, что «киберпространство состоит из сотен тысяч соединенных между собой компьютеров, серверов, маршрутизаторов, коммутаторов и волоконно-оптические кабелей, которые позволяют нашей критической инфраструктуре работать. Таким образом, нормальное функционирование киберпространства имеет важное значение для нашей экономики и нашей национальной безопасности»[2].

Отсюда видно, что киберпространство напрямую связано с реальной географией, которая вместе с политикой является основным элементом науки геополитики.

Во-первых, все маршруты коммуникации, сервера и технические узлы, которые связаны как с Интернет, имеют географическую локализацию. Во-вторых, киберзоны имеют национальную идентификацию в смысле доменных зон, государственного контроля и используемого языка. В-третьих, киберпространство подчеркивает физическую географию особенным образом — датчики различных служб, навигационные устройства, технические гаджеты и мобильные устройства воплощают собой интерактивную карту с перекрестными потоками информации, техники и людей.

Хотя основной трафик идет по подводным кабелям, ряд государств все же напрямую несет ответственность за происходящее в киберпространстве, так как маршруты коммуникаций проходят через их национальные территории. Как справедливо заметил Мака Аалтола в отношении Финляндии и региона, Балтийское море является основным проводником данных, через которое проходят подводные кабели, соединяющие вместе важный перекресток глобального киберпространства. Для Финляндии самые стратегически важные связи - это два северных кабеля BCS, которые связывают Россию со Швецией и далее за их пределами с

[1] William Gibson, Neuromancer. New York: Ace Books, 1984.

[2] The National Strategy to Secure Cyberspace, Washington, DC: White House, 2003.

помощью финских узловых точек. В результате основная часть киберпотока из России в остальной мир проходит через Финляндию. В случае, если какой-либо внешний актор попытается шпионить за этим трафиком данных, это может привести к недоверию. Россия может затем рассмотреть меры по противодействию или попытаться обойти в Финляндию с ее системой коммуникаций. Основные проблемы, следовательно, существуют, и на них Финляндия должна найти стратегические ответы. С одной стороны, она должна стремиться обеспечить надежные и безопасные инвестиции, связанные киберпространством. С другой стороны, она должна обеспечить свою собственную кибербезопасность. В некоторой степени, эти цели могут быть даже противоречивыми.[1] Действительно, это серьезная дилемма, учитывая, что этот регион является привлекательным для инвестиций в области высоких технологий. В Финляндии нет тектонической активности и крайне низка вероятность природных катастроф. Ее умеренный климат естественно охлаждает компьютерные парки облачных вычислений. Компания Google уже вложила сотни миллионов евро в свой центр обработки данных в г. Хамина на южном побережье Финляндии.

Еще один важный фактор, актуальный для нынешней геополитики — это глобальность. Киберпространство по-особому фиксирует и гомогенизирует физическое пространство — таким образом, с помощью GPS технологии и других инструментов глобализация добирается в самые укромные уголки планеты.

При этом цифровые технологии реконфигурируют опыт картирования в нечто другое, что Бруно Латур и его коллеги называют навигационной платформой (navigational platform), характеризуемой присутствием:

- Банка данных;
- Определенного интерфейса для управления данными, т.е. подсчета, обработки и поиска;
- Инструментальной панели для взаимосвязи с пользователями;
- Множества различных выходов, сделанных для огромного количества пользователей - и один из них имеет выход на печатное устройство[2].

Традиционная роль карты пересматривается, появляются различные школы, связанные с описаниями политических и институциональных отношений картирования, перформативным использованием и пониманием карт как эмерджентности, возникающей через разнотипный набор практик.

Картографирование Интернет пространства становится приоритетной задачей ряда исследовательских центров и университетов. Пока еще в достаточно ограниченном количестве, но с каждым годом все больше и больше — специализированные издания, работа кафедр и подразделений в различных think-tanks

[1] Mika Aaltola. Finland should aim to be a cyber connector. FIAA Comment, № 15, November 2013.

[2] Valerie November, Eduardo Camacho-Hubner, Bruno Latour. Entering a risky territory: space in the age of digital navigation. Environment and Planning D: Society and Space 2010, volume 28, p.583.

ведут мониторинг киберпространства и фиксируют его изменения — будь то появление новых технических узлов, издание новых законопроектов или противоправная деятельность в сети.

Исходя из вышеуказанного, мы видим, что киберпространство не однородно и имеет несколько уровней.

Дэвид Кларк предложил модель, в которой существует четыре уровня киберпространства[1].

1. Физический уровень содержит все аппаратные устройства, которые включают маршрутизаторы, переключатели, носители и спутники, датчики и другие технические соединители, как проводные, так и беспроводные. Физическая инфраструктура географически расположена в «реальном пространстве», и, таким образом, является предметом различных национальных юрисдикций.

2. Логический уровень в целом относится к коду, который включает в себя как программное обеспечение, так и протоколы, которые включены в него.

3. Уровень контента описывает всю созданную, взятую, хранящуюся и обрабатывающуюся информацию в киберпространстве. Информация определяется как «знания, касающиеся объектов, например, факты, события, вещи, процессы или идеи»[2].

4. Социальный уровень, состоящий из всех людей, использующих и формирующих характер киберпространства. Это фактический Интернет людей и потенциальные отношения, а не подразумеваемый Интернет аппаратных средств и программного обеспечения. По сути, социальный

слой включает правительства, частный сектор, гражданское общество и субъекты технического сообщества. Тем не менее, всех их объединяет специфика: если в «реальной» жизни (экстра киберпространство) люди могут в конечном счете быть идентифицированы по их уникальным кодам ДНК, атрибуция в сети гораздо сложнее (внутри киберпространства). В отличие от «плотского» мира, люди в киберпространстве облегчают создание множественной идентичности для пользователя. И в альтернативе, одна виртуальная личность может иметь несколько человеческих пользователей (например, тот же онлайн-аккаунт офиса газеты «Нью-Йорк Таймс» используется разными сотрудниками). Это имеет не только важное значение с точки зрения защиты безопасности или авторских прав, но также поднимает интересные вопросы о том, как кибер-мир играет в реальном мире.[3]

[1] David Clark, Characterizing cyberspace: past, present and future, MIT/CSAIL Working Paper, [1]2 March 2010.

[2] ISO/IEC 2382-1:1993, Information technology — Vocabulary — Part 1: Fundamental terms.

[3] Alexander Klimburg, Philipp Mirtl. Cyberspace and Governance — A Primer. The Austrian Institute for International Affairs, Working Paper 65 / September 2012.

Четвертый уровень и является локомотивом геополитики в киберпространстве. Именно Man Power — что не является абстрактной величиной, т.е. люди, а не машины принимают решения по политическим вопросам, включая действия, связанные с Интернет пространством.

Кроме того, терминология, используемая ранее в кибернетике, также адекватна и для геополитики киберпространства. До настоящего момента было принято говорить о двух кибернетиках — первого и второго порядка. Если кибернетика первого порядка была связана с наблюдаемыми системами, то кибернетика второго порядка — это кибернетика наблюдающих систем[1]. Данная ремарка указывает на высокий организационный характер новой волны кибернетики, хотя некоторые дефиниции довольно сильно напоминают геополитические теории и науки о власти.

Интернет политика

Если говорить о киберпространстве как политической деятельности, то на данный момент есть две основные модели, связанные с этим новым ареалом человеческой активности. Первая — это электронное правительство. Под данным термином следует понимать создание специальных сервисов, которые облегчают взаимоотношения населения с представителями власти и получение от них различных услуг. Электронные платежи, виртуальные приемные, обработка запросов в удаленном доступе — все эти действия призваны облегчить и упростить жизнь налогоплательщиков в странах, где начинают применять современные коммуникационные технологии.

Второе — это использование киберпространства в качестве среды и инструмента для распространения определенной политической культуры.

Крайне показательными в этом отношении являются усилия США, где правительство использует Интернет как новое средство для достижения своих целей. При этом задействуется не только гражданский сектор, но и силовые ведомства.

В 2011 г. стало известно, что военные в США запустили программу, связанную с манипуляциями в социальных сетях. Она подразумевала создание не существующих онлайн-личностей, которые должны обладать правдоподобным прошлым и историей, и что любой из 50 управляющих личностями сможет оперировать фальшивыми онлайн-личностями со своих рабочих компьютеров «без страха быть раскрытыми хитрыми противниками». Как заявил один из представителей компании, разрабатывавшей программный продукт: «Технология позволяет вести секретную деятельность в блогах на иностранных языках, которая позволит

[1] Heinz von Foerster. Cybernetics of Cybernetics. University of Illinois, Urbana 1979

Центральному командованию Минобороны США противостоять экстремистам и вражеской пропаганде за пределами США»[1].

А в конце 2011 г. в Белом доме заявили о создании виртуального посольства в Иране для «укрепления связей с иранским народом»: http://iran.usembassy.gov/[2]. Показательно, что в это же время Конгресс США принимает различные меры по ослаблению связей с иранскими чиновниками и введением санкций наносит ущерб иранской экономике. А до этого США уже открыли виртуальное консульство для Сектора Газы[3].

По мнению Н.А. Цветковой «существует несколько терминов, используемых американским правительством для обозначения инновационного способа оказания влияния на зарубежное общество при помощи Интернета: цифровая дипломатия (digital diplomacy), интернет-дипломатия (Internet diplomacy), дипломатия социальных сетей (Twitter diplomacy) и публичная дипломатия Web 2.0. (public diplomacy Web 2.0.)»[4]. Наиболее распространенным термином среди руководства США, занимающегося вопросами внешней политики и установления влияния в других странах, является последний.

Технология Web 2.0, рассчитанная на взаимодействие политических активистов посредством интернет технологий, доказала свою эффективность и в ходе массовых протестов в Тунисе и Египте, а также координации оппозиции и самоорганизации различных групп политической направленности в России.

Угрозы киберпространства

Как видим, киберпространство не является утопией, о чем ранее говорили писатели-фантасты. Это новая сфера человеческой активности, где существуют свои ограничения, катаклизмы, эпидемии и изъяны, хотя они не затрагивают напрямую жизни людей — все во многом зависит от выбора самого индивидуума. Если кто-то настолько увлекся компьютерными играми, что стал неадекватно воспринимать реальность — разве это не бич киберпространства, наподобие наркомании в реальном мире?[5] Киберзависимость связана не только с профессиональными обязанностями или развлечениями, такова сама природа Интернет. Современный американский философ Джон Зерзан, например, отмечал, что пси-

[1] Ник Филдинг, Иан Кобэйн. Военные США будут манипулировать социальными сетями.// ИноСМИ http://www.inosmi.ru/usa/20110318/167469729.html

[2] Mutter, Paul. Few Virtues to "Virtual Embassy in Iran". December 23, 2011. http://www.fpif.org/blog/few_virtues_to_virtual_embassy_in_iran

[3] http://gaza.usvpp.gov/about_econsulate.html

[4] Цветкова Н.А. Программы Web 2.0 в публичной дипломатии США. 13.04.2011 http://www.ushistory.ru/stati/559-programmy-web-20-v-publichnoj-diplomatii-ssha.html

[5] Dene Grigar. Lara Croft: Cyber Heroine. Leonardo June 2006, Vol. 39, No. 3, Pages 269-270.

хика человека, который хотя бы раз воспользовался Интернет, подвержена необратимым последствиям[1].

Аналогично и с «болезнями» в этом «мире». В 1983 г. Фред Коэн намеренно разработал программы, которые могут «заразить другие программы, модифицируя их посредством возможного включения своей эволюционированной копии», как он выразился в своей диссертации. Опираясь на биологическую аналогию, он назвал новую программу вирусом.

Термин «червь» был придуман Джоном Бруннером в романе 1975 г. Shockwave Rider. В то время как вирусы просто заражали компьютерную программу (или файлы), черви «ползли» дальше, копируя себя между системами. Использование уязвимости компьютеров, известные как задние двери, черви распространяются без помощи невнимательных пользователей. В 1988 г. червь Морриса проник и инфицировал около 60000 хостов зарождающейся сети Arpanet, которая являлась прототипом нынешнего Интернет. Сам Роберт Моррис, создатель червя, был первым человеком, привлеченным к ответственности и осужденным в соответствии с законом о компьютерном мошенничестве 1986 г.[2]

Если в физическом мире есть карантин в отношении опасных болезней и даже бывают межгосударственные конфликты, связанные с эпидемиями или целенаправленным инфицированием (биологическое оружие), разве не должно этого быть в киберпространстве? История последнего десятилетия свидетельствует и о таком феномене. Наиболее показательными случаями были:

Кибератаки в 2007 г. на правительственные сайты Эстонии;

Действия хактивистов в августе 2008 г. во время оккупации Грузией Южной Осетии и миротворческой операции со стороны России;

Внедрение американскими и израильскими спецслужбами компьютерного червя Stuxnet на иранскую атомную станцию.

По мнению специалистов в будущем количество таких атак будет только возрастать, а методы работы хакеров совершенствоваться. Это вынуждает правительства многих стран пересмотреть свою политику в отношении Интернет и принимать особые меры по охране этого пространства.

Индийский опыт

На примере нескольких конкретных случаев, произошедших в Индии, рассмотрим как именно киберпространство взаимосвязано с реальной жизнью. При этом мы будем рассматривать спектр угроз для граждан и государства, а не широких возможностей, связанных с новыми технологиями.

[1] Зерзан Джон. Закат эры машин.// Глобальный дискурс. Под ред. Савина Л.В. Сумы: Университетская книга, 2003. http://dglobal.narod.ru/twilight.html

[2] A Better Way to Battle Malware. November 22, 2011. Winter 2011, Issue 65. http://www.strategy-business.com/article/11403?pg=all

Первое явление — это терроризм. Наиболее крупные теракты за последнее время были совершены в г. Ахмедабад в июле 2008 г. и в г. Мумбаи в ноябре этого же года. В обоих случаях террористы использовали Интернет для координации своих действий и даже после них. В частности, как указано в издании Times of India от 10 января 2009 г., члены террористической группировки Indian Mujahideen использовали неконтролируемые сети Wi-Fi для рассылки сообщений полицейским, которые занимались расследованием этих инцидентов. В письмах содержались угрозы в адрес работников правоохранительных органов. Данный инцидент вынудил индийскую полицию обратиться к правительству для издания постановления об уголовном преследовании для тех компаний, которые в будущем не будут защищать свои Wi-Fi. Аналогичная ситуация прослеживается и в других странах. Как правило, антиправительственные элементы всегда находятся на несколько шагов впереди, и исследователям остается только констатировать постфактум об их методах работы, включая использование систем Linux, программ P2P и пр.

Следующее явление — сепаратизм и антигосударственная деятельность.

В Индии сепаратисты Кашмира регулярно используют Интернет для антигосударственной деятельности. Точкой отсчета считается 2010 г., когда появилось новое поколение киберактивистов, начавших осваивать альтернативное пространство для выражения своих политических пристрастий. В связи с цензурой на местных медиа, контролем за смс и телефонными линиями в этом конфликтном регионе, Интернет остается единственным инструментов для ангажирования в политический дискурс. Вместе с тем, по словам одного из активистов, с 2010 г. возросла и деятельность правительственных служб, занимающихся контролем и наблюдением за коммуникациями. При этом полиция использует ложные аккаунты в социальных сетях, специальные программы для анализа протокола данных и пр., что позволяет им тоже иметь продвинутую стратегию[1].

Представитель отдела полиции, занимающийся киберпреступлениями штата Джамму и Кашмир в апреле 2012 г. заявил, что они раскрыли группу молодежи, которая на протяжении нескольких лет занималась антинациональной политикой в Интернет с помощью социальных сетей и управлении веб сайтами. По данным полиции страницы 'Freedom of Dawn', 'Balai Khuda', 'Aalov' и 'We love Syed Ali Shah Geelani' поддерживали сепаратистские настроения, а также подстрекали к погромам во время беспорядков летом 2010 г.[2] Как указывает издание Press Trust

[1] Uzma Falak. India clamps down on Kashmir's online dissenters. August 14, 2012 http://www.newint.org/blog/2012/08/14/kashmir-teenage-cyberactivist/?utm_medium=ni-email&utm_source=message&utm_campaign=-enews-2012-08-23

[2] J-K cops crack 'anti-national' network. Apr 16 2012 http://www.indianexpress.com/news/jk-cops-crack-antinational-network/937240/

of India, при расследовании было определено, что многие сепаратистские сайты управлялись из таких стран как США, Великобритания, Пакистан и ОАЭ.

Непосредственно внешнее управление конфликтами — это третий случай рассматриваемой нами темы. Что касается Индии, то второй половине августа 2012 г. в Индии с помощью Интернета в социальных сетях и на мобильных телефонах были распространены фотографии изуродованных тел с угрозами, что индийские мусульмане планируют совершить нападения на жителей северо–восточного региона страны, которые не принадлежат к мусульманскому вероисповеданию. В послании было сказано, что готовящиеся акции задуманы как ответное действие на смерти мусульман, которые произошли в результате длительного спора между бенгальскими мусульманами и коренными племенами бодо в штате Ассам. Этот многолетний спор, связанный с этнической принадлежностью, земельными участками, рабочими местами и политической властью привел к гибели 70 человек и спонтанной миграции с мест своего проживания более 300 тысяч человек с июля 2012 г.[1]

Распространение сообщения о мести со стороны мусульман коснулось не только штата Ассам, но также вызвало панику среди рабочих и студентов этого региона, которые находились в этот момент в южной Индии. Они посчитали себя в роли потенциальных жертв и поспешно на автобусах и поездах ринулись домой. Все же панику с трудом удалось остановить.

Индийское правительство заявило, что эти изображения изуродованных тел имеют пакистанское происхождение. В результате расследования и профилактических мер было закрыло около 300 сайтов и вынесено предупреждение Интернет провайдерам об ответственности.

Что характерно, именно социальные сети, которые зарегистрированы в США и тесно сотрудничают с Белым домом и Пентагоном, не захотели пойти на встречу пожеланиям индийских властей. Секретарь Индии по телекоммуникациям Чандрашехар заявил о том, что Facebook и Twitter могут столкнуться с правовыми действиями, так как они не пошли на встречу требованиям правительства снять материалы или проследить источники данного сообщения. В верхах даже предположили, что доступ к Twitter вообще может быть полностью закрыт в Индии.

Наверняка центры мировой социальной паутины будут давать отказы на подобные запросы в будущем, мотивируя это свободой слова демократией в киберпространстве.

И последний случай, — это когда социальные медиа в комбинации с телевизионным освещением дают беспрецедентные возможности для трудно предсказуемых политических движений.

[1] Jonah Force Hill. India's Internet Freedom Nightmare.// The Diplomat, August 25, 2012 http://thediplomat.com/2012/08/25/indias-internet-freedom-nightmare/?all=true

Казалось бы, толчком послужил обычный криминальный случай — 16 декабря 2012 г. в столице Индии была изнасилована 23-летняя девушка, но именно с помощью социальных сетей весть об этом вызвала общественный резонанс, — и тысячи сторонников наказания виновных (а заодно и улучшения прав женщин) вышли на улицы Нью–Дели.

Следует отметить, что для страны с населением свыше 1,2 млрд. человек единичный акт насилия или убийства не является чем-то из ряда вон выходящим. Достаточно в течение определенного времени помониторить индийскую региональную прессу, и неискушенный читатель обнаружит много шокирующих наше представление фактов. Во время поездки по Индии автор публикации неоднократно узнавал о том, как в одном месте полицейский изнасиловал школьницу, в другом поклонники культа богини Кали совершили кровавый ритуал на кладбище, который включал эксгумацию трупа и его расчленение и т.п. Что касается аварий и катастроф, то согласно статистике каждый день в Индии происходит инцидент с жертвами на железной дороге, а время от времени переворачивается грузовик со свадебным кортежем (естественно, с летальным исходом для многих пассажиров). Для традиционного индусского сознания с понятием кармы и кастовой системы такие инциденты, вероятно, являются нормальным ходом вещей. Что же побудило огромные массы выйти на улицы Нью-Дели и драться с полицией?

Являлся ли выход масс на улицы индийской столицы спонтанной реакцией, где местные кибератвисты стали катализатором протеста или запланированной акцией, предусматривающей, например, срыв визита Президента РФ Владимира Путина в Индию, который все же состоялся, несмотря не неспокойную обстановку? Однозначно, кое-кому было бы на руку сорвать многомиллионные контракты Нью-Дели и Москвы, подписанные руководством обеих стран. По крайней мере, американские аналитики сильно занервничали из–за того, что Россия начала серьезно конкурировать с США на рынке вооружений, где Индия является одним из важных покупателей. Например, заголовок одной статьи в издании Wired по поводу военных контрактов России с другими странами, где освещался и недавний визит в Индию, звучит не иначе как «Путинские торговцы оружием наращивают поставки отвратительным негодяям»[1].

В общем, мы видим, что катализатором широкомасштабных протестов становятся социальные сети, которые превращаются в первоклассный инструмент для провокаций или цветных революций в стиле Web 2.0 (подтверждением чему являются и недавние события в Киеве). И при наличии огромных людских масс в сочетании с доступностью Интернет и мобильной связи (программа всеобщей

[1] Beckhusen R. Putin's Arms Dealers Are Selling More Weapons to More Dirtbags Than Ever.// Wired magazine, 12.12.12. http://www.wired.com/dangerroom/2012/12/russia-exports/

интернетизации страны была завершена в Индии еще около десяти лет назад) последствия таких акций могут быть довольно серьезными.

Поэтому правительство Индии сейчас столкнулось с дилеммой выбора — как наиболее адекватным способом решить эту проблему. Дело в том, что для властей этой страны Интернет всегда являлся инструментом для организации лучшего управления, и его применение было сугубо техническим. Технократы, в частности, работали с электронным управлением e-governance. А тех сил, которые работают в области безопасности киберпространства, явно не хватает. Национальная организация по техническим исследованиям National Technical Research Organization, которая работает при советнике по национальной безопасности, имеет в своем штате всего 50 человек, занимающихся мониторингом медиа, и даже не имеет официальной лицензии в качестве мониторингового агентства.

А, по мнению экспертов Института оборонных исследований и анализа из Нью-Дели, цензура и другие подобные меры могут быть только временным решением. Следовательно, необходимо создать некую альтернативную модель[1].

И, конечно же, учесть разницу в подходах к киберпространству, где на одной стороне оказались США и их сателлиты, а на другой — Россия, Китай, Иран и другие страны, настаивающие на распространение суверенитета в киберпространстве. Так что, возможно, опыт Индии или коллективные решения (например, на очередном саммите БРИКС) в этом вопросе будут весьма кстати и затребованы в самое ближайшее время.

Киберконфликты и реакция США

Конечно же, киберпространство является одновременно средой для конфликта и его инструментом. Если классическая геополитика использует понятия могущества посредством моря (Sea Power) и могущества посредством суши (Land Power), а позже появилось могущество посредством воздуха и могущество посредством космоса, с недавнего времени заговорили и о новом домене — могуществе посредством киберпространства (Cyber Power). Военные США придают ему особое значение. Офицер ВВС США Роберт Ли указывает, что «кибермогущество будет такой же революционной для войны как и военно-воздушные силы, но текущая векторизация этой области будет определять, какая нация достигнет кибергосподства и с какой целью. На раннем этапе появления киберпространства Соединенные Штаты в первую очередь рассматривали кибермогущество как средство налаживания широких возможностей командования и управления через боевые зоны. Киберпространство сосредоточено на связи, да и оперативный успех зависел от

[1] Shruti Pandalai. Don't Shoot the Messenger: The 'Un-Social' Strategy. August 28, 2012.
[b]ttp://www.idsa.in/idsacomments/DontShoottheMessengerTheUnSocialStrategy_spandalai_280812

поддержания линий коммуникации. Так как эта область расширялась, она взяла на себя дополнительные роли по обеспечению поддержки сил традиционных военных операций, в то время как эксперты исследовали другие роли — это процесс, который произошел на самом высоком уровне

секретности. Многие из первых лидеров киберпространства поняли, что кибератаки предлагают ряд вариантов для атаки, защиты, и эксплуатации, которые никогда прежде не были возможны для военачальников. В очень взаимосвязанном мире, где существенные достижения в области технологии были обычным делом, возможности и оружие в киберпространстве стали еще более впечатляющими»[1].

Кибероперации могут быть проведены во всех областях ведения боевых действий: в воздухе, космосе, киберпространстве, на суше и море. Кроме того, несмотря на незрелость оперативных доктрин для киберпространства, доктрины для воздуха и космического пространства остаются актуальными и применимыми к сфере киберпространства. «Кибероперации — это просто еще один набор инструментов из арсенала командира».[2]

США первым создало Киберкомандование в 2010 г., хотя внимание этой новой сфере начали придавать и ранее. Например, в декабре 2005 кибероперации были включены в основное положение о службе и миссии ВВС США.[3] Китай, Иран и другие страны тоже поспешили обзавестись своими кибервойсками с соответствующими доктринами и стратегиями. Бюджеты на кибербезопасность также начинают стремительно увеличиваться. Руководство киберкомандования США в январе 2013 г. заявило, что штат этого рода войск будет увеличен в пять раз. Британия тоже спешит произвести апгрейд своих кибервозможностей, обосновывая это необходимостью безопасности сети, в связи с тем, что 6% ВВП Британии зарабатывается с помощью манипуляций, которые так или иначе связаны с Интернет.

Известный специалист по сетевым войнам Джон Аркилла пишет, что «подвиги кибервойн малого масштаба (Аркилла приводит в пример атаки на правительственные сайты Эстонии в 2007 г. и соответствующую инфраструктуру Грузии в августе 2008 г., приписывая данную инициативу российской стороне, а также инцидент с вирусом Stuxnet на иранских ядерных объектах — Л.С.) в конечном итоге могут достичь больших размеров, учитывая явные уязвимости передовых военных и различных систем связи, которые с каждым днем все больше охватыва-

[1] Robert M. Lee. The Interim Years of Cyberspace.// Air & Space Power Journal, January–February 2013, P. 58

[2] Eric D. Trias, Bryan M. Bell. Cyber This, Cyber That . . . So What?//Air & Space Power Journal. Spring 2010, P. 91.

[3] Hon. Michael W. Wynne, Flying and Fighting in Cyberspace, Air and Space Power Journal 21, no. 1, Spring 2007: 3, http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/spr07.pdf

ют мир. Вот почему я думаю, что кибервойнам суждено сыграть более заметную роль в будущих войнах»[1].

Аркилла считает, что есть возможность выработать определенный код поведения, например, не применять кибератаки против исключительно гражданских объектов, по крайней мере, такая договоренность возможна между государствами. Некоторые теневые сети, т.е. радикальные политические группировки также могут следовать некоему кодексу. Второй тезис мало вероятен, так как в случае терроризма целью действий подобных групп является запугивание населения для достижения своих политических целей, и киберпространство представляет для этого хорошую возможность.

Поскольку кибермогущество может быстро и особым образом поражать сети и информационные системы по всему миру, размывая линию боевого сражения, эта особенность в сочетании с его разрушительной силой, порождает страх перед его возможностями среди населения - такой же сильный, как и от террористических атак[2]. Следовательно, недооценивать его силу влияния на общественное мнение и политику будет серьезной ошибкой. Даже если рассматривать исключительно военную сторону киберконфликтов, они сильно отличаются от войны на суше, море, в воздухе и космосе. «Свобода действий — это характеристика превосходства в киберпространстве... Приблизительным резюме для превосходства в киберпространстве может быть «свобода действий в течение атаки» (т.е. возможность действовать даже во время атаки и после нее)»[3].

Но есть и другая точка зрения, согласно которой, наоборот, кибервозможности применительно к конфликтам «смягчают» их природу и минимизируют ущерб как противника, так и затраты атакующей стороны. Профессор Военно-морской школы США Дороти Деннинг считает, что «если вы можете достичь того же эффекта с кибероружием вместо кинетического оружия, часто этот вариант этически предпочтительнее... Если операция нравственно оправданна, то кибер маршрут вероятно предпочтительнее, потому что он вызывает меньше вреда»[4]. К вопросу этики в киберпространстве можно отнести и применение беспилотных летательных аппаратов, что стало темой широкой дискуссии в США. Сторонники более массированного применения БПЛА в США указывают на три основных причины, из-за которых нужно развивать эту отрасль: 1) БПЛА смогут выполнять задачи, на которые не способны люди из психологических ограничений

[1] Arquilla J. Cyberwar Is Already Upon Us. MarchH/April 2012. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

[2] Robert M. Lee. The Interim Years of Cyberspace.// Air & Space Power Journal, January–February 2013, P. 63.

[3] Eric D. Trias, Bryan M. Bell. Cyber This, Cyber That . . . So What?//Air & Space Power Journal. Spring 2010, P. 96-67.

[4] Kenneth Stewart. Cyber Security Hall of Famer Discusses Ethics of Cyber Warfare. America's Navy, 6/4/2013 http://www.navy.mil/submit/display.asp?story_id=74613

(например, длительность проведения операций и экстремальные маневры); 2) сохранение жизни пилотов во время выполнения опасных миссий и снижение политического риска, который имеет случай быть, если пилот попадает в плен; 3) снижение затрат в связи с отказом от применения систем, необходимых для поддержания функций пилота (кислород, контроль климата, катапультируемое кресло и т.п.) и возможности применения дизайна отличного от того, который нужен для самолетов, предназначенных для эксплуатации вместе с командой на борту[1]. Есть тенденция, что беспилотники в будущем смогут заменить даже действующие стратегические бомбардировщики.

Другая часть считает, что применение дронов противоречит нормам международного права и приводит к огромному количеству жертв среди мирного населения.

В докладе New American Foundation указано, что за два года, в течение которых Обама был президентом, было произведено в четыре раза больше боевых вылетов БПЛА, чем за восемь лет президентства Дж. Буша. В данном отчете дается примерное количество убитых в Пакистане - от 1489 до 2297 (данные на апрель 2012 г.)[2].

В начале 2013 г. правозащитники привели следующую статистику убитых американскими дронами лиц:

Атаки дронов в Пакистане, которые подотчетны ЦРУ, 2004–2013 гг.:

- Всего: 362
- При Обаме: 310
- Убито всего: 2,629-3,461
- Среди них гражданских лиц: 475-891
- Среди них детей: 176
- Всего ранено: 1,267-1,431

Тайные операции США в Йемене 2002–2013:

- Всего подтвержденных операций: 54-64
- Всего подтвержденных применений дронов: 42-52
- Возможные дополнительные операции: 135-157
- Возможное дополнительное применение дронов: 77-93
- Убито всего: 374-1,112

Среди них гражданских лиц: 72-177

Среди них детей: 27-37

Тайные операции США в Сомали 2007–2013:

- Всего: 10-23

[1] Policy Options for Unmanned Aircraft Systems. A CBO Study. June 2011. Congress of U.S. Congressional Budget Office. P. 3.

[2] Masters, Jonathan. Targeted Killings.// CFR, April 25, 2012. http://www.cfr.org/counterterrorism/targeted-killings/p9627?cid=nlc-dailybrief-daily_news_brief-link14-20120426

Всего применений дронов: 3-9

- Убито всего: 58-170
- Среди них гражданских лиц: 11-57
- Среди них детей: 1-3

Бюро журналистских расследований на своем сайте также приводит интерактивные карты (можно сказать, что это своего рода кибер в квадрате - применение киберпространства для мониторинга киберактивности!), где отмечены места атак американских БПЛА и статистические данные, включая имена убитых граждан[1]. Показательным является тот факт, что сенатор Линдси Грэм в своем выступлении в феврале 2013 г. заявил, что число убитых американскими БПЛА лиц составляет 4700 человек, что примерно на 1000 человек больше, чем в докладе Совета по международным отношениям, посвященном БПЛА, который вышел месяцем ранее[2].

Применение БПЛА ширится — 13 января 2012 г. армия США издала директиву, согласно которой БПЛА будут использоваться внутри США для тренировочных миссий и «внутренних операций»[3].

Так или иначе, этот смертоносный интерфейс человека и машины наиболее наглядным образом показывает, куда могут завести кибервозможности в военных целях.

Впрочем, нужно отдавать отчет, что кибероружие как таковое не является чем-то новым, как некоторые себе представляют. Электронное подавление новейшей модификации применялось при атаке на инфраструктуру Ливии в 2011 г. и при налете израильских ВВС на научный объект в Сирии в 2007 г. Обнародованные документы Национального агентства безопасности США свидетельствуют, что кибератаки против компьютерных сетей других государств планировались еще в 2007 г.[4] Речь шла не об эксплуатации и защите, а именно об атаках!

Большое количество акторов, использующих киберпространство для своих целей также привносит некоторую путаницу для тех, кто пытается создать досье на киберактивистов в широком смысле этого слова. В 2009 г. подполковник армии США в отставке и бывший директор по безопасности цифровой продукции в Intel Дэвид Джонсон предложил реализовать шесть пунктов, которые бы могли помочь систематизировать всех акторов, действующих в киберпространстве и выработать общую стратегию, направленную на укрепление безопасности государства. Для этого необходимо:

[1] См. Interactive map. August 10th, 2011 http://www.thebureauinvestigates.com/2011/08/10/google-map/

[2] Ingersoll, Geoffrey. US Senator: 'We've Killed 4,700' People With Drones. Feb. 20, 2013, [h]ttp://www.businessinsider.com/graham-weve-killed-4700-people-with-drones-2013-2#ixzz2LZWjk8fW

[3] http://www.fas.org/irp/doddir/army/ad2012_02.

[4] Byrne M., Richelson J. When America Became a Cyberwarrior.// Foreign Policy, April 26, 2013 http://www.foreignpolicy.com/articles/2013/04/26/when_america_became_a_cyberwarrior_nsa_declassified

- Создание совместной стратегии по киберпространству, направленную на выявление общих интересов в родах войск, невоенных правительственных органов и партнеров из частного сектора, с учетом, что координации между этими группами не требует централизованной командной структуры, непригодной к проблемам кибербезопасности.
- Перспективная (а не ретроспективная) оценка рисков в области безопасности, которая, скорее всего, будет принята через пять, десять, или двадцать лет в будущем, такие вербовка, обучение и доктрина, которые могут быть согласованы с будущими потребностями.
- Разработка набора показателей для отслеживания и указания намерений и возможностей акторов в киберпространстве, а также для оценки внутренних (инсайдерских) рисков.
- Изучение социальной динамики в хакерском обществе, для того, чтобы иметь возможность влиять на ключевые отдельные лица или группы, которые активно воздействуют на общие мнения и обсуждения.
- Анализ топологии криминальных сетей, действующих в качестве специальных групп по развитию и рекрутировки, а также тактических групп и резервных сил для противоборствующих государств или негосударственных акторов с целью изоляции ключевых узлов, в том числе финансовых сетей, коммуникационных технологий, либо сайтов.
- Обзор слабых мест при нынешней подготовке в сфере безопасности военных кадров, федеральных государственных служащих и государственных подрядчиков, с тем, чтобы расширить осведомленность по технологии безопасности как неотъемлемой части своей работы и снизить риск социальных инженерных атак.[1]

Подобные рациональные предложения могли бы быть востребованы не только в США, хотя правительство этой страны уже адаптировало большое количество межведомственных инициатив и проектов для защиты киберпространства США, как общественного, так и частного. Только один Пентагон имеет около 15 тыс. сетей для обеспечения своей безопасности.

Но помимо национальной безопасности есть и глобальный уровень киберконфликта. На стратегическом уровне киберконфликт становится новым измерением межгосударственной войны. Усилия по противодействию и подготовке к такой конфронтации возложена на Киберкомандование США и Национальный совет по безопасности в Белом доме.

По мнению Роберта Мэннинга, «если употреблять несовершенную аналогию, стратегическая киберугроза имеет много общего с ядерными угрозами. Обе они построены на атаке, обе могут быть причиной огромного разрушения, которое

[1] David Johnson, Ian Crone. The Human Terrain of Cyberspace// Defense Concepts, Vol. 4, Ed. 3. Fall 2009. P.38

выведет из строя необходимую национальную инфраструктуру и нанесет ущерб или ослепит вооруженные силы, которые зависят от электроники»[1]. В США также появился нарратив «Электронный Перл-Харбор», который используют алармисты и паникеры для обоснования увеличения расходов в этой области.

Все эти факторы позволяют говорить о том, что геополитика как таковая обрела еще одну сферу — кибернетическую, на которую распространились ее основные аксиомы, но, вместе с тем, которая является реальностью другого уровня, где действуют новые правила.

[1] Robert A. Manning. ENVISIONING 2030: US Strategy for a Post-Western World. Atlantic Council. Washington DC, 2012, P. 56.