УДК 32:316.62; 004.514.6

ЭЛЕКТОРАЛЬНОЕ ХАКЕРСТВО И «ЦИФРОВОЙ ПОВОРОТ» «МЯГКОЙ СИЛЫ»

Реут Олег Чеславович,

Северо-западный институт управления РАНХиГС,
кандидат технических наук,
Санкт-Петербург, Россия,
E-mail: olegreut@sampo.ru

Аннотация

Рассматриваются возможности и ограничения применения концепции «мягкой силы» в обстоятельствах её «цифрового поворота» для исследования принципиально нового феномена электорального хакерства.

Ключевые понятия:

«мягкая сила», электоральное хакерство, «цифровой поворот».

Большинство современных политологических теорий рассматривают потребность в безопасности граждан в рамках договорных отношений «человек – общество – государство», которые являются одними из центральных оснований появления политики как универсального ресурса, обеспечивающего функционирование и развитие социума и политикума. Актуальные исследовательские задачи предопределяют дифференциацию категорий безопасности, что, с одной стороны, вызвано расширением предметного поля за счёт включения новых видов военных и невоенных угроз, а с другой – определяется обстоятельствами, в которых эти угрозы репрезентируются. В особую группу оформляется такой вид безопасности, как безопасность информационная, который в соответствии с пространственным измерением контекста взаимодействия политических акторов дифференцируется по уровням – от индивидуального до глобального.

Информационная безопасность представляет собой состояние, при котором сохраняется целостность, устойчивость и способность к эффективному

саморегулированию, несмотря на неблагоприятное внешнее информационно-коммуникационное воздействие. В целях обеспечения информационной безопасности политические акторы используют различные методы, которые могут быть ориентированы на применение насилия или на использование средств косвенного воздействия. Считается, что задействование потенциала инструментов «мягкой силы» (*soft power*), реализуемых посредством информационно-коммуникационных технологий, надлежит определять как нетрадиционные. Однако такое представление не является в полной мере корректным для ситуаций электорального хакерства, с которым столкнулись на протяжении последнего года ряд государств.

При этом важно отметить, что сама проблематика хакерства находится в довольно сложных взаимоотношениях с концептуальным оформлением вопросов безопасности, что становится очевидным при рассмотрении характера и стилей принятия политических решений; роли институтов государства, гражданского общества и индивида в обеспечении безопасности; в выборе соотношения методов и средств обеспечения. Более того, многократное усложнение природы такого феномена современности, как информационные войны, приводит к переформатированию репрезентации ненасильственного воздействия на противника.

Ранее считалось, что в ходе информационного противоборства политические акторы концентрируют свои усилия на создании двух образов, или имиджей: негативного – врага, и позитивного – своего государства. Сами же имиджи транслируются как на граждан своей страны, соседние государства, так и на потенциального противника. В последние годы основной вектор формирования репрезентационной картины выстраивается в направлении выявления скрываемой от аудитории информации. Это могут быть скандальные шпионские досье, взломанные материалы почтовых сервисов, результаты журналистских расследований. При этом сами хакеры позиционируются не как маргинальные кибер-агрессоры, а в качестве разоблачителей государственных или корпоративных афер. Конечно, хакинг остаётся в тёмно-серой области спектра политических действий, но его последствия вполне претендуют быть представленными обществу как ответ на социальный запрос, направленный на преодоление фальшивых новостей (*fake news*), генерируемых традиционными средствами массовой информации.

Чёткое терминологическое оформление категории «электоральное хакерство» выступает довольно нетривиальной задачей, поскольку её решение призвано объединить в некоторую совокупность разные проявления принципиально нового феномена – от утечек социально и политически значимой информации до выстраивания так называемого «искусственного общественного мнения», от повышения уязвимости (вплоть до выведения из строя) сложных инженерно-технических и информационных систем до фальсификации итогов голосования на выборах и референдумах. Одновременно с этим электоральное хакерство концентрируется на использовании потенциала Интернет-технологий, хотя и не ограничивается ими. И, вне сомнений, отдельную сложность в описании рассматриваемых феноменов представляет собой транснациональный характер хакерских групп, к которым лишь частично применимы

подходы, выработанные в отношении, например, частных военных компаний. Это «работает» только в ситуации, когда хакерские коллективы выступают контракторами, наёмными исполнителями воли государственных заказчиков, т. е. тех, кто действует в интересах отдельного государства или их группы. При этом существуют и всё больше заявляют о себе абсолютно самостоятельные группы, которые, в отличие от хакеров в погонах, имеют практически невыявляемую и склонную к постоянным изменениям систему целеполагания [2].

Именно в этом контексте представляется ограниченно возможным расширить применимость сложившегося категориального аппарата, оперирующего вышеназванным понятием «мягкая сила». Исходя из классификации природы воздействия, предложенной в ставших классическими работах Джозефа Ная [4], «мягкая сила» вполне корректно описывает совокупность ресурсов, находящихся за пределами пространств применения принуждения – как военных, так и экономических (прежде всего, санкционных). При этом она оперирует такими единицами анализа, как «массовая культура» и «политические ценности», которые конструируются социально и (вос) производятся в «потоке практик» различных акторов. В данном прочтении исходной точкой рассуждений выступает оппозиция «объективное / социально сконструированное», пришедшая в социально-гуманитарных науках на смену классической дихотомии «объективное / субъективное».

Применительно к электоральному хакерству довольно сложно не заметить различия в языках описания, которые используют не только политологи и международники, но, например, социологи, специалисты в области систем информационной безопасности, культурных (*cultural*) или медиаисследований. Очевидно, что представители разных областей знания оперируют разными аксиоматическими допущениями и, что более значимо, разными описательными метафорами, которые вполне обоснованно были объединены Ричардом Рорти при объяснении введённого им [3] понятия «конечный словарь». Естественно, «конечный словарь» является «начальным словарём», поскольку указывает на всю совокупность риторических элементов той или иной исследовательской программы: от базовых категорий и концептуализаций до первоначальных образных сравнений, задействованных той или иной дисциплиной. «Словарь» – потому что эта совокупность доступна кодификации. «Конечный» (по Рорти) – потому что исследовательская оптика представляет собой «замкнутую систему»; каждому новому феномену она будет подбирать описания из уже имеющихся ресурсов воображения. В некотором смысле, такой словарь есть арсенал всех доступных исследователю способов описания своего объекта.

Первичное описание, как правило, глубоко метафорично – даже само помещение слов «электоральный» и «хакерство» (как, впрочем, «мягкая» и «сила») в одно словосочетание надлежит рассматривать как подобный приём, именно поэтому задача последующей концептуализации представима как превращение метафор в концепты. Однако уже на стадии начала повествования требуется построение эксплицитной объяснительной модели или, другими словами, повествование использует имплицитные объяснительные схемы, встроенные (более или менее искусным образом) в само описание.

В какой степени электоральное хакерство корректно представлять, например, через категориальную сетку политических ценностей? Поиск ответа на этот вопрос может, пожалуй, лишь воспроизвести полемику о герметичности объяснительных моделей, инициированную следованием или отказом от следования дюркгеймовским принципам «объяснения социального социальным». Жанр функционального оперирования «мягкой властью» куда менее требователен в этом отношении, что определяется не только опорой на методологию конструктивизма, но и адаптивностью «цифрового поворота» в политологическом знании, считающейся одним из признаков трансформации исследовательских парадигм, когда приходит осознание необходимости изучать процессы, сопутствующие появлению тех или иных коллективно разделяемых смыслов.

Хотя конечные словари концепций «мягкой власти» и «электорального хакерства» – пересекающиеся множества, применение «воздействия привлекательности» выстраивается в совершенно нетождественной, а порой и в прямо противоположной логике. По-разному и выстраивается состав субъектов, и происходит артикуляция внешнеполитических интересов, и действуют механизмы убеждения.

Не менее важно и то, что институты, занимающиеся имплементацией «мягкой силы», не только не успевают перестраиваться в соответствии с теми требованиями, которые необходимо учитывать, применяя данную концепцию в обстоятельствах «цифрового поворота» (*digital turn*), но и испытывают определённую растерянность в формулировании отношения к хакингу, конструирование привлекательности которого объективно затруднено устойчивостью фобий Интернет-пользователей.

Так, например, по данным Лаборатории Касперского за 2016 год, 23% россиян заклеивают веб-камеры персональных компьютеров, поскольку боятся спецслужб и хакеров [1]. Отчасти это указывает на возможность восприятия «мягкой силы» в качестве инструмента внутренней политики, что требует «перезагрузки» аксиоматических допущений не только по поводу экспортного продвижения национальных интересов и политических ценностей, которые они манифестируют, но и в отношении более фундаментальных подходов, связанных с функциями современного государства, обеспечением информационной безопасности и даже возможностью информационной гражданской войны.

С одной стороны, новый угол зрения позволяет расширить теоретическую основу концепции «мягкой силы», но с другой – ставит под сомнение сложившийся категориальный аппарат, оперирующий данным понятием, что в свою очередь формулирует основания для возможного «перехода» к концепциям «умной силы» (*smart power*) и «тёмной силы» (*dark power*). В таких обстоятельствах целесообразно вернуться к базовым положениям разработанной Наем теоретической конструкции.

По его мнению, государства могут добиваться решения ряда проблем через формирование и продвижение своей привлекательности. В условиях трансграничных вызовов и угроз противостояние им оказывается более эффективным при включении в систему ценностных, идеологических и культурных

регуляторов, выгодно позиционирующих государство в сравнении с другими членам международного сообщества. «Мягкая сила», таким образом, в отличие от «жёсткой», склоняющей другое государство, чужих граждан и иных акторов мировой политики к принятию тех или иных действий через навязывание своей воли, основывается на способности формировать предпочтения других. В последнем аспекте «мягкая сила» в определённой мере вписывается в рамки публичной дипломатии, в т. ч. в рамки оформившегося сравнительно недавно направления цифровой публичной дипломатии.

Ответ на вопрос «Является ли хакерство привлекательным?» скорее отрицательный. Но останется ли он прежним при добавлении уточнения о том, что в результате, например, установлена фальшивость социально (и политически) значимых новостей, генерируемых традиционными средствами массовой информации, либо выявлена государственная или корпоративная афёра, либо разоблачена неискренность политика – кандидата на выборную должность? Парадоксальность ситуации заключается в том, что сами добавляемые уточнения являются социально конструируемыми. Более того, они конструируются традиционными средствами массовой информации, государственными или корпоративными институциями, политиками – лидерами общественного мнения. Происходит секьюритизация хакерства, дискурсивно оно оформляется в категориях информационно-коммуникационной опасности. Восприятие хакерства как угрозы легитимирует необходимость его контроля и регулирования.

Последнее наблюдение, тем не менее, не является универсальным. В ряде случаев субъекты политики исходят из того, что отсутствие контроля и регулирования в сфере цифрового взаимодействия выступает не меньшей ценностью, чем адекватное ограничение открытости и прозрачности. Очевидно, что разноречивое прочтение контекста затрудняет формулирование механизмов «создания привлекательности».

Вполне вероятно, что именно в этой точке размышлений первостепенной оказывается важность терминологического оформления привлекательности. Если привлекательность является необходимым элементом «мягкой силы», то верно ли утверждать, что она создаётся исключительно при коммуникативном обмене, в которой одна из интерпретаций «правды» одерживает верх над другими, а генерирование симпатии, сочувствия и благодарности происходит в отношении действий, рассматриваемых как законные и заслуживающие доверия? Означает ли это, что электоральное хакерство, изначально помещённое за пределы законности и доверия, не может претендовать на субъектность в создании привлекательности?

Открытость ответа на последний вопрос может быть охарактеризована в качестве проблемы методологической интервенции, т. е. операции по переносу языков описания и объяснения из концепции «мягкой силы» в сферу информационно-коммуникационной безопасности с последующей проблематизацией аксиоматического ядра реципиента. Здесь стоит признать, что разносторонность эмпирической базы исследования электорального хакинга и пока недостаточно высокая степень её критической проработанности не позволяют выстроить стройную логику преодоления изоляционистских

конвенций. Вне сомнений, формирование большинства современных политологических теорий, помещающих в центр своего внимания проблематику обеспечения информационной безопасности, представляет собой процесс непрерывного обмена концептами, аксиоматическими допущениями и объяснительными моделями. При этом в связи с усложнением и динамизмом практик информационно-коммуникационного взаимодействия назревает необходимость содержательного переосмысления концептуального оформления «мягкой силы», обнаруживаемой в обстоятельствах «цифрового поворота».

В означенном контексте нуждается в обсуждении и вопрос о том, «работают» ли предложенные Наем теоретические идеи, возможна ли их адаптация, переосмысление и модификация в исследованиях с учетом современных общественно-политических реалий. Не менее продуктивным представляется обсуждение вопроса о том, какие исследовательские метафоры и концептуальные сюжеты содержатся в новых теоретических конструкциях, появившихся в последние годы в общественно-гуманитарной мысли, какие методологические ракурсы они открывают в актуальных прикладных исследованиях.

1. Кочергина Е. Заклей меня полностью: фотопроект о пластыре на камере ноутбука, 5 июня 2017 г. http://batenka.ru/protection/no-camera.

2. Реут О.Ч. Страна электоральных хакеров – новый образ России? // Имидж страны как фактор «мягкой силы» в международных отношениях: история и современность. Материалы Интернет-конференции, 2017. http://ashpi.asu.ru/ic/?p=4100.

3. Рорти Р. Случайность, ирония и солидарность / Пер. с англ. М.: Русское феноменологическое общество, 1996. 282 с.

4. Nye J. Bound to Lead: The Changing Nature of American Power. NY: Basic Books, 1990. 336 p.

References

1. Kochergina E. Zaklej menya polnost'yu: fotoproekt o plastyre na kamere noutbuka, 5 iyunya 2017 g. http://batenka.ru/protection/no-camera.

2. Reut O.Ch. Strana e'lektoral'nyx xakerov – novyj obraz Rossii? // Imidzh strany kak faktor «myagkoj sily» v mezhdunarodnyx otnosheniyax: istoriya i sovremennost'. Materialy Internet-konferencii, 2017. http://ashpi.asu.ru/ic/?p=4100.

3. Rorti R. Sluchajnost', ironiya i solidarnost' / Per. s angl. M.: Russkoe fenomenologicheskoe obshhestvo, 1996. 282 s.

4. Nye J. Bound to Lead: The Changing Nature of American Power. NY: Basic Books, 1990. 336 p.

UDC 32:316.62; 004.514.6

ELECTORAL HACKING AND THE DIGITAL TURN OF SOFT POWER

Reut Oleg Cheslavovich,

North-West Institute of Management, branch of RANEPA,
St.-Petersburg, Russia,
E-mail: olegreut@sampo.ru

Annotation

The article considers opportunities and limitations of the application of the soft power concept in the circumstances of its digital turn for studying a fundamentally new phenomenon of electoral hacking.

Key concepts:

soft power, electoral hacking, digital turn.