НЕЖЕЛЬСКИЙ Александр Александрович – аспирант Национального исследовательского института мировой экономики и международных отношений им. Е.М. Примакова РАН (117997, Россия, г. Москва. Профсоюзная ул., 23); аналитик данных в АО «Лаборатория Касперского» (125121, Россия, г. Москва, Ленинградское ш., 39А, стр. 3; nejel@mail.ru)

ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ СФЕРЫ КИБЕРБЕЗОПАСНОСТИ: ПРОБЛЕМЫ АТРИБУЦИИ АТАК И ЛОКАЛИЗАЦИИ ДАННЫХ

Аннотация. *В статье автор рассматривает государственное регулирование сферы кибербезопасности, исследует вопрос о терминологических расхождениях в российском и американском подходе к определению кибербезопасности. В статье приводятся три возможных сценария развития государственного регулирования, выделяется наиболее актуальный на данный момент сценарий для России.*
Ключевые слова: *кибербезопасность, информационная безопасность, атрибуция кибератак, локализация данных, международные отношения*

Термин «кибербезопасность» (*cybersecurity*) получил распространение в середине 1990-х гг. сначала в США, затем в Европе, а позднее – и в других странах. Оригинальное понятие отсылает нас к термину «киберпространство» (*cyberspace*) – виртуальная среда в рамках технологического информационно-коммуникационного пространства, в которой любой человек может передавать данные и получать их. В ноябре 2005 г. во время тунисской встречи на высшем уровне по вопросам информационного общества (ВВУИО) было принято решение не присваивать понятие киберпространства какой-то конкретной территории, а считать ее атомарной сущностью, распространяющейся глобально. Из этого следует, что логика государственного суверенитета и государственного администрирования неприменима к киберпространству.

Россия, однако, наряду с некоторыми другими странами – участницами ВВУИО, ратует за введение понятия локального суверенитета в вопросах управления Глобальной сетью, считая, что решения по вопросам Интернета на глобальной арене должны принимать лишь правительства стран, но никак не бизнес или заинтересованные группы интернет-пользователей.

Начиная с 1990-х гг. в ряде стран и организаций, в т.ч. в России, получает развитие альтернативная концепция, в основе которой лежат совершенно другие термины. В наиболее широком виде данная терминология может быть найдена в конвенции об обеспечении международной информационной безопасности (МИБ). Позже концепция МИБ получила распространение в странах – членах ШОС, а затем ОДКБ и СНГ. В основе концепции МИБ лежит идея, что суверенитет и законы распространяются на информационную инфраструктуру, расположенную на территории государства, и находятся под его юрисдикцией. Таким образом, по разные стороны океана сформировались два семантически противоположных определения.

В 1998 г. произошло первое столкновение двух противоречивых подходов. Дипломатические и организационные усилия России по продвижению концепции МИБ столкнулись с противодействием со стороны бизнеса, международных организаций и правительств развитых стран. Оппоненты настаивали на неприменимости российского подхода к сформировавшимся практикам, сложившимся на тот момент в международном сообществе. И если в 1998 г. конфликт скорее был похож на небольшие терминологические расхождения, то

сегодня он играет определяющую роль в поддержании международной информационной безопасности.

На текущей стадии развития межгосударственных и международных отношений важность информационного противоборства продолжает расти. Информация сегодня играет все большую роль в процессе принятия решений, стратегического планирования и сбора разведданных. Ее особая роль в современных внешнеполитических конфликтах заставляет нас переосмыслить сам подход к обеим сущностям: 1) к информации как таковой; 2) к международным конфликтам.

Как следует из доклада Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (принят резолюцией Генеральной Ассамблеи ООН A/68/150 от 30.07.2013 г.), ИКТ являются технологиями двойного назначения, которые могут использоваться как в законных, так и в злонамеренных целях. Любое устройство ИКТ может стать источником или объектом злонамеренных действий. Злонамеренное использование ИКТ легко скрыть, а выявление конкретного злоумышленника может быть сопряжено с трудностями, в связи с чем злоумышленники, которые нередко действуют в условиях безнаказанности, могут осуществлять все более сложные вредоносные действия. Эту проблему также усугубляет глобальный охват сетей ИКТ. Свойство глобальной доступности, уязвимые технологии и фактор анонимности облегчают использование ИКТ для осуществления противоправной деятельности.

Конфликт между концепциями кибербезопасности и МИБ повлиял на проблемы регулирования и на внутрироссийском уровне. В 2012–2013 гг. в Совете Федерации России была предпринята попытка привлечь экспертов к составлению единого доктринального документа – концепции стратегии кибербезопасности Российской Федерации. В ходе попытки составления документа была обнаружена необходимость четко определить, что же такое кибербезопасность (ранее в государственных документах эта категория никак не выделялась). Определение кибербезопасности должно было способствовать переходу к единой терминологии и разрешению конфликта между концепциями МИБ и кибербезопасности.

Хотя документ и оценивается экспертами как очень прогрессивный для своего времени, он получил немало негативных отзывов, преимущественно со стороны российских государственных органов – МИДа, Совета безопасности РФ, ФСБ.

В качестве критики концепции стратегии кибербезопасности РФ часто упоминается тот факт, что категориальный аппарат концепции шел вразрез с ранее изданными нормативными актами и доктринальными документами (к примеру, с Доктриной информационной безопасности РФ от 2000 г. и принятыми в 2013 г. Основами государственной политики России в области международной информационной безопасности до 2020 г.). Все это лишь усугубило конфликт в вопросе о категориях, перенося его уже на внутрироссийскую действительность.

Раскрытие Эдвардом Сноуденом в 2013 г. информации о многочисленных формах слежки спецслужбами США за гражданами различных стран продемонстрировало глубокий кризис доверия как между правительствами различных стран, так и между правительствами и их собственными гражданами.

Глобальный Интернет сегодня является не только средством доступа ко все большему объему информации о гражданах по всему миру, но и удобным средством контроля над людьми со стороны государства. В противовес контролю со стороны государства гражданское общество также получает возможность кон-

тролировать деятельность государства через размещенную в Глобальной сети информацию о выборах, чиновниках, закупках, а также другие открытые данные. Кроме того, по мере развития новых медиа (социальные сети, видеоблоги, сервисы потокового видеовещания) граждане государства получают новые способы свободно и неподконтрольно для государства делиться и обмениваться информацией (в т.ч. и ложной).

Таким образом формируется причудливая двусторонняя зависимость между государством, которое находится во все большей зависимости от раскрываемых перед гражданами данных, с одной стороны, и гражданами, которые находятся во все большей зависимости от государства, имеющего де-факто неограниченные ресурсы по сбору и анализу их персональных данных, – с другой.

Другим важным вопросом являются особенности хранения и обработки пользовательских данных. За последнее десятилетие обмен данными стал новой парадигмой понимания социального поведения. С появлением *Web* 2.0 и социальных сетей многие аспекты социальной жизни, которые раньше не приходилось оценивать количественно, такие как дружба, любовь, предпочтения, оказались частично или полностью оцифрованными. Значительная часть человечества переместила бóльшую часть своего социального взаимодействия в веб-среды. *Twitte*r и *Facebook* перевернули общественное представление о таких явлениях, как дружба и симпатия, добавив в него влияние алгоритмов. Цифровая трансформация социальности породила индустрию, которая строит свой бизнес на ценности данных и метаданных. Метаданные, не так давно считавшиеся бесполезным побочным продуктом, который производят пользователи в ходе работы с веб-порталами, постепенно превращаются в «новое золото», которое можно добывать, обогащать, продавать и многократно использовать в цифровых продуктах.

Исследователи все чаще используют масштабную оценку твитов как термометр для измерения настроения общества по тем или иным вопросам. Предположение основано на идее, что онлайн-социальный трафик течет по свободным технологическим каналам, а люди высказываются в псевдоанонимной интернет-среде более свободно. Явление роста и изменения самой исследовательской парадигмы, ее переход на *data-driven* рельсы получили название *datafication*.

Существует несколько крайне интересных случаев манипуляции данными с целью оказания влияния на общественное сознание. Помимо очевидных отключений Интернета и массовой пропаганды, стоит отметить случай поведения поисковых алгоритмов *Google*. В ходе выборной кампании президента США 2017 г. пользователи отмечали, что на одни и те же запросы поисковый алгоритм *Google* выдавал разным пользователям совершенно разные результаты. По комментариям самой *Google*, данный факт был связан с более оптимальной работой алгоритма, который учитывал портрет пользователя, чтобы показать ему наиболее релевантную информацию. Но далеко не все исследователи согласны с данной позицией. Даже если в данном конкретном случае манипуляции не было, сама возможность такой манипуляции поисковыми результатами для формирования общественного мнения видится весьма реальной.

В результате перед гражданским обществом встает вопрос, от ответа на который напрямую зависит развитие информационной безопасности государства и его граждан: является ли масштабный государственный шпионаж в сети «случайным» злоупотреблением отдельных разведок и правительств, или же это системное свойство нынешней модели управления Интернетом.

Ответ на этот вопрос не так очевиден, как может показаться на первый взгляд. Даже наличие серьезных случаев масштабной слежки за гражданами со сто-

роны государства еще не говорит о системности этого явления и дисфункциональности любых попыток регулирования этого вопроса, как наличие крупных ДТП не говорит о бесполезности правил дорожного движения.

В зависимости от ответа мы можем наметить два метасценария. Если мы исходим из того, что слежка является «случайным сбоем», должны ли мы реагировать на это? Если мы исходим из того, что слежка является системным явлением, способны ли мы принять меры к исправлению ситуации, и какие именно институциональные и технические шаги помогут в исправлении ситуации?

Попытаемся ответить на вопрос о системности слежки с применением акторно-сетевого анализа. При ближайшем рассмотрении мы можем обнаружить множество фактов использования шпионажа со стороны государства за последние 17 лет.

Кибероружием пользуются страны-изгои (к примеру, КНДР), преследующие свои локальные цели, традиционные страны «первого мира», а также ключевые игроки международной арены (создание кибервойск в Китае). Наиболее активно пользуется им единственная сверхдержава – США (проект *PRISM* и другие разоблачения Э. Сноудена). На приведенных выше примерах становится понятно, что государственный шпионаж и использование сомнительных схем работы в области кибербезопасности – *modus operandi* любого государства вне зависимости от его экономической и военной мощи, политического режима или провозглашаемых ценностей. Все акторы в получившейся модели пространства информационной безопасности применяют шпионаж и недобросовестные методы влияния в целях разведки, сбора компрометирующих сведений и проведения военных операций (*Stuxnet*). Отличаются только масштабы и задачи. Если одни государства сконцентрированы на собственных гражданах (вероятно, из-за дефицита ресурсов или боязни быть замеченными в Глобальной сети), то иные также осваивают проведение экстерриториальных операций.

Изучив информацию из открытых источников, можно прийти к выводу, что на сегодняшний день ИКТ превратились в объективную часть национального оборонительного потенциала множества государств, а их военные доктрины и развитие инфраструктуры в сторону создания кибероружия уже приняли крайне серьезный характер. Данная тенденция подтверждается как наблюдениями независимых исследователей, так и заявлениями официальных лиц. У технологически развитых государств уже сформирован потенциал для применения ИКТ в целях обороны, разведки, проведения специальных операций.

Более того, потенциал ИКТ в области разведки и военных операций зачастую закреплен в качестве превентивной меры, силы, которую можно применить в мирное время. Это является своеобразным следствием специфики информационного нападения (оно не связано с человеческими жертвами). Развитие наступательного потенциала ИКТ усугубляется его асимметричной природой. В большинстве случаев конкретное государство не знает, в каком состоянии находятся разработки потенциальных противников (равно как и союзников), а также о самом факте наличия/отсутствия таких разработок. Это дополнительно эскалирует желание вести разработку такого рода «информационного оружия» внутри государственных структур, связанных с безопасностью (разведывательное сообщество, силовые структуры, армия). Таким образом, менее развитые государства тоже втягиваются в цифровую гонку вооружений в надежде получить преимущества и предотвратить риски со стороны более развитых держав.

Угроза, исходящая от потенциального применения «информационного оружия», приводит к снижению значения традиционных атрибутов безопасности и военной мощи государств: у них появляется принципиально новая плоскость

соперничества (или еще одна «шахматная доска», в терминах З. Бжезинского). Отличительной особенностью «информационного оружия» является его, в подавляющем большинстве случаев, бескровность. Несмотря на весь имиджевый, экономический, политический и иной ущерб, в ходе «информационных операций» все же не гибнут живые люди. Это создает противоречивый эффект: с одной стороны, склоняет государства к использованию такого вида оружия, с другой – приводит к эрозии самой природы конфликтности. Создаются новые ступени эскалации напряженности международных конфликтов – возможности информационного нападения, которые могут спровоцировать симметричный или асимметричный ответ. Высокая сложность атрибуции кибератак, являющейся неотъемлемым свойством киберпространства, склоняет государства к применению кибероружия. На фоне растущей роли информационного оружия оружие ядерное уже не выглядит столь ультимативным, а значит, создается все больше предпосылок к реформе Совета Безопасности ООН.

По словам А.В. Крутских, специального представителя России по вопросам международного сотрудничества в области информационной безопасности, по состоянию на 2015 г. деятельность по созданию «информационного оружия» вели более 140 стран мира.

Ключевая проблема текущей международной ситуации заключается в отсутствии на международном уровне функционирующих механизмов предупреждения и сдерживания конфликтов. Действующая система международного права не адаптирована к реальности использования ИКТ в политических и военных целях. Такая ситуация является следствием двух производных:

– использование ИКТ никак не подпадает под юрисдикцию действующих систем международных договоров, конвенций и иных соглашений;

– использование ИКТ в военно-оборонительных целях не охвачено какой-либо системой международных договоров, конвенций и иных соглашений.

Как следствие, отсутствуют международные организации, которые вели бы контроль и мониторинг деятельности государств в части использования ИКТ в военно-политических целях, а также осуществляли верификацию в части соблюдения ограничений в этой сфере. Неоднократно высказанная представителями различных организаций и стран (включая генерального директора «Лаборатории Касперского» Е.В. Касперского) идея «МАГАТЭ для киберпространства» пока не получила реального развития.

Одной из наиболее острых сторон проблемы является тот факт, что даже существующий корпус норм международного права, регулирующих конфликты и войны вне зависимости от типов используемого оружия, не может применяться к сфере ИКТ в формате «как есть» в силу ее технологических особенностей. Речь идет о нормах международного гуманитарного права (*jus in bello*) и права вооруженного конфликта (*jus ad bellum*), которые кодифицированы в таких актах, как Гаагская конвенция 1899 г., Гаагская конвенция 1907 г., Женевская конвенция 1928 г., Женевские конвенции I–IV 1949 г., и Дополнительные протоколы I–III 1977, 1997 и 2005 гг. к Женевским конвенциям I–IV.

Применение указанных документов к вопросам использования ИКТ в военно-политических целях требует единообразной, юридически закрепленной международной интерпретации, которая на текущий момент отсутствует. Выработка такой интерпретации с учетом отмеченных негативных тенденций в сфере международной безопасности в части наращивания военно-политического потенциала ИКТ видится одним из возможных приоритетов для мирового сообщества на ближайшие годы.

Таким образом, можно выделить несколько возможных сценариев дальнейшего развития событий в области регулирования кибербезопасности.

Первый сценарий. Поиск общих точек соприкосновения в вопросах о регулировании кибербезопасности. В странах Азии аналогичный подход получил название «управляемая анархия» (*Governing Anarchy*). Подвижки в сторону данного сценария предпринимались в ходе президентского срока Д.А. Медведева, однако ощутимых плодов не принесли. Данный подход, судя по всему, лежит за пределами логики действующего правительства, поэтому развитие данного сценария пока что видится маловероятным.

Второй сценарий. Изоляционистский сценарий («Китайский путь»). Предполагает дальнейшее развитие запретительных мер, законодательных и технических ограничений на трансграничную передачу данных. В последнее десятилетие принято немало законов и подзаконных актов, которые создают видимость развития России именно по этому сценарию. Наиболее заметными среди них стали ФЗ-152[1] и законопроект о «суверенном Интернете»[2]. Тем не менее все эти меры встречают энергичное сопротивление населения, а технологическое развитие интернет-сервисов не позволяет заблокировать что-либо окончательно. В случае продолжающегося и углубляющегося конфликта с Западом развитие сценария видится вполне возможным, но, судя по всему, реализовать его в полном объеме не получится.

Третий сценарий. Сценарий развития собственной методологии, в основе которой будут лежать распространенные в России понятия государственного сетевого суверенитета и международной информационной безопасности. Начиная с 1998 г. Россия периодически пытается отстаивать свою концепцию регулирования. Данный сценарий видится компромисом между первым и вторым, однако его реализация потребует гораздо более значительных ресурсов во многих областях, таких как законодательное регулирование, технический надзор, административное содействие, экономическая поддержка, дипломатические усилия для продвижения своей парадигмы и повестки дня среди дружественных стран.

В контексте всего описанного выше наиболее реалистичным для России на сегодняшний момент видится некий промежуточный сценарий между сценариями 2 и 3, возможно, при официальном декларировании сценария 3. Причины просты: реализовать каждый из них в полном объеме достаточно тяжело, а вот продавить и реализовать отдельные меры каждого из подходов – вполне реально. Кроме того, это хорошо укладывается в саму природу среды ИКТ: полностью защититься от киберрисков невозможно, а вот меры защиты можно осваивать бесконечно. Это также обеспечит негласный компромисс с протестным потенциалом населения: те, кто заинтересован в доступе к запрещенным ресурсам, будут получать его в обход официальных блокировок, а силовые структуры получат дополнительный рычаг давления на политических активистов.

Данный подход причудливым образом позволяет минимизировать риски всем участникам российской киберэкосистемы:

– государство в лице высших чинов правительства секьюритизирует проблему потенциального кибернападения и минимизирует риск такого нападения, а также сможет защищаться от кампаний общественного политического давления (см. запрет «умного голосования» за неправильный сбор и хранение персональных данных);

---

[1] Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (последняя редакция). Доступ: http://www.consultant.ru/document/cons_doc_LAW_61801/ (проверено 15.07.2019).

[2] http://duma.gov.ru/news/29748/ (проверено 15.07.2019).

– государство в лице силовых структур минимизирует риск информационных утечек (все ресурсы можно запретить);

– пользователи Рунета будут развивать сервисы анонимизации и обхода блокировок и минимизировать риски от соприкосновения с опасной государственной машиной.

Однако не стоит забывать, что технологии ИКТ – символическое отражение будущего. В то же время правовое регулирование – символическое отражение прошлого. Опасно пребывать в уверенности, что сфера ИКТ и все акторы в ней поддаются законодательному регулированию.

Использованная литература

Armacost M. 1996. *Friends or Rivals? The Insiders' Account of US – Japan Relations*. N.Y.: Columbia University Press. 271 p.

Demidov O. 2019. Operationalizing Norms with the Private Sector and Technical Communities. – *Cyber Stability Conference of UNIDIR*. Vol. 1. No. 1. P. 2.

Kennet W. 1959. *Man, the State, and War*. N.Y.: Columbia University Press. viii + 263 p.

NEZHEL'SKY Aleksandr Aleksandrovich, *postgraduate student at the Institute of World Economy and International Relations, Russian Academy of Sciences (23 Profsoyuznaya St, Moscow, Russia, 117997); Data Analyst in JSC «Kaspersky Lab» (bld. 3, 39a Leningradskoye Highway, Moscow, Russia, 125121; nejel@mail.ru)*

STATE REGULATION IN THE SPHERE OF CYBERSECURITY: THE PROBLEM OF ATTRIBUTION OF ATTACKS AND DATA LOCALIZATION

Abstract. *The author considers the state regulation of the sphere of cybersecurity and investigates the question of terminological differences in the Russian and American approaches to the definition of cybersecurity. The article gives three possible scenarios of the development of state regulation and allocates the actual scenario for Russia nowadays.*

Keywords: *cybersecurity, information security, attribution of cyberattacks, data localization, international relations*