Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Уильям Ким, *Connections QJ* 17, № 2 (2018): 5-19
https://doi.org/10.11610/Connections.rus.17.2.01

Рецензированная статья

Цифровое пробуждение России

Уильям Ким

Джорджтаунский университет, https://www.georgetown.edu/

Резюме: После распада Советского Союза Россия беспрецедентным образом начала использовать современные технологии при осуществлении своей внешней политики и разведывательной деятельности. В этой статье исследуется отношение России к интернету и компьютерным технологиям, подробно рассматривая рост популярности технологий среди российской общественности и российского руководства, начиная с начала 1990-х и вплоть до 2017 года. Особое внимание обращено на умение, с которым российские нелиберальные политические институции и службы безопасности пользуются неурегулированным характером интернета и манипулируемостью современных технологий и СМИ, а также на то, как и почему Запад и США не смогли спрогнозировать восход России в качестве цифровой сверхсилы и продолжают не успевать противодействовать ее доминированию.

Ключевые слова: Россия, кибербезопасность, кибервойна, разведка, внешняя политика, информационные операции, Восточная Европа.

В известном анекдоте о современной России говорится, что после Холодной войны Российская Федерация до последнего настолько отставала в своем экономическом и технологическом развитии, что очень немногие русские понимали вообще что-нибудь в интернете и в компьютерах. Это несколько преувеличенное утверждение, которое оправдывает себя в редких комедийных моментах, как когда во время визита в головной офис Твиттера в 2010 году бывший в то время президентом Дмитрий Медведев сделал свой первый неуклюжий твит и выглядел очаровательно запутавшимся в новой технологии. Дальше в анекдоте говорится, что в России еще несколько лет назад не знали, что такое блог, но сейчас Россия имеет весьма существен-

ное присутствие в сети, и Кремль превратил интернет во впечатляюще могущественное кибероружие. За последние 20 лет российское руководство научилось искусно использовать технологию и интернет для достижения своих масштабных политических целей. Российское кибер доминирование является прямым результатом российской театральной политической культуры и истории, а также богатого разведывательного технологического инструментария в сфере дезинформации и обмана. Русская политическая культура прекрасно подходит для эпохи интернета и дает России уникальную способность более умело манипулировать потенциалом интернета, чем другие основные кибер акторы. США просмотрели появление превосходства России и могут многому научиться, изучая киберполитику России, в том числе как лучше противодействовать России и как разрабатывать более согласованную собственную киберполитику.

Чтобы понять центральное значение киберспособностей для российской политики и для российского руководства, надо рассмотреть развитие ее современной политической культуры и основные достижения ее киберполитики: осуществление ранних кибероперациий за границей, слияние группировок организованной преступности и хактивистских групп со службами государственной безопасности и общая аура отрицания и обмана относительно кибер эффективности России. Перечисление этих основных пунктов бросает свет на то, почему Россия очень успешно перешла в эпоху интернета, и как Соединенные Штаты могут адаптироваться и действовать в ответ на российское доминирование.

Обращение России к интернету и технологиям в качестве ключевого элемента при проецировании ею политической и военной силы было предсказуемым заключением, если взглянуть на богатую историю советской разведки и политики по национальной безопасности. Многие западные знатоки и аналитики сегодня делают упор на то, что они называют «новые» российские способности для ведения «гибридной войны», в частности, российские информационные операции на Украине и в Соединенных Штатах в течение нескольких последних лет.[1] Однако, все еще ведутся споры о термине «гибридная война» (и это только одна из нескольких похожих концепций, касающихся одного сложного явления), но использование Россией сочетания политических, военных, экономических и информационных приемов принуждения не является каким-то новым явлением – критически важный момент, который отсутствует во многих популярных анализах.

Советская стратегия «активных мероприятий» является предвестником того, что сегодня известно как гибридная война. Этот термин используется для обозначения советских действий политического воздействия, используемых для оказания влияния на курс мировых событий, в том числе под-

[1] Molly K. McKew, "The Gerasimov Doctrine," *Politico*, September/October 2017, https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538.

держку групп коммунистической и социалистической оппозиции, революционные конфликты в других странах, террористические и преступные группировки и действия, направленные на западные институции в целом. Бывший генерал-майор КГБ Олег Калугин называл активные мероприятия «сердцем и душой советской разведки».[2] Активные мероприятия направлены на осуществление «подрыва и мер для ослабления Запада, вбивания клиньев между членами союзов Западного сообщества, в особенности НАТО, создания разногласий между союзниками, ослабления США и подготовки почвы на случай, если война в самом деле начнется».[3] Бывший информатор КГБ Юрий Безменов считает, что в 1970-х активные мероприятия составляли 85 % всей деятельности КГБ, но эти программы привлекали гораздо меньше внимания международного сообщества, чем более известные концепции шпионажа и разведывательной деятельности.[4] Активные мероприятия были направлены на использование асимметрий противника – признавая неспособность собственного государства победить в конвенциональном конфликте, находить те места, где у оппонента были непропорциональные слабости, которые можно было эффективно использовать. Для Советского Союза открытость западных СМИ, политики и культуры были первейшей мишенью для дестабилизации путем дезинформации и манипулирования. Это остается верным и сегодня, с той лишь разницей, что сейчас Россия располагает гораздо большим числом инструментов для достижения тех же целей.

Учитывая историю советских активных мероприятий, впечатляющий переход России в эпоху интернета вполне объясним и является модернизацией советской политики. Просто стратегия активных мероприятий переносится в цифровой век, и ее технологии усиливаются благодаря огромной анонимности и манипулируемости интернета. Поскольку активные мероприятия в советское время включали широкий набор информационных операций, манипуляций СМИ, дезинформаций, фальсификаций, оказания поддержки повстанцам или оппозиционным политическим движениям и т.д., эти кампании требовали значительно больше усилий, времени и финансирования в период Холодной войны, чем в 21-ом веке. Россия быстро поняла, что расширение глобализации и взаимосвязанности технологий через интернет может облегчить использование активных мероприятий в попытках России восстановить свое присутствие в мировых делах после падения

---

[2] Oleg Kalugin, “Inside the KGB: An Interview with Retired KGB Maj. Gen. Oleg Kalugin,” *Cold War Experience*, *CNN*, January 1998, http://web.archive.org/web/20070627183623/ and http://www3.cnn.com/SPECIALS/cold.war/episodes/21/interviews/kalugin.

[3] Kalugin, “Inside the KGB.”

[4] Yuri Bezmenov and G. Edward Griffin, *Soviet Subversion of the Free World Press: A Conversation with Yuri Bezmenov, former propagandist for the KGB* (Westlake Village, CA: American Media, 1984), www.youtube.com/watch?v=RzKl6OF9yvM.

Советского Союза. Открытое формулирование этой политики двумя ближайшими советниками Путина после 1999 года определило однозначно техно-центрический подход России к проецированию силы и влияния по всему миру.

Хотя русские активные мероприятия не новое явление, сделать киберспособности центральным элементом большой стратегии Кремля способствовали два официальных представителя российских властей – Владислав Сурков и Начальник генерального штаба вооруженных сил России, Валерий Герасимов. В 2013 году Герасимов опубликовал статью в журнале Академии военных наук Российской Федерации *Военно-промышленный курьер*, озаглавленную «Ценность науки в предвидении», в которой он обосновал необходимость укрепления и развития существующей политики в отношении конфликтов 21-го века.[5] Герасимов пишет: «В 21-ом веке мы наблюдаем тенденцию размывания линий разграничения между состояниями войны и мира. Войны уже не объявляют, а когда они начинаются, то следуют незнакомым стереотипам».[6] Герасимов предлагает отношение невоенных к военным мерам 4 к 1, подчеркивая значение политических, экономических и социальных мероприятий для формирования ландшафта целевого государства путем подрывной деятельности, шпионажа и пропаганды в согласовании с кибератаками.[7] Классическая советская доктрина маскировки, сфокусированная на отрицании и обмане, снова оказывается на переднем крае и в центре работ Герасимова с тем, чтобы держать оппонентов в состоянии неопределенности и колебаний в результате отрицания русского участия в продолжающихся операциях.[8]

Схожим образом, для одного из главных ассистентов Путина, Владислава Суркова, основным достижением является мастерское сочетание политики и театра, возможно, это одна из основных отличительных черт эпохи Путина, а также разработка его идеологии «суверенной демократии» и осуществление этой политики, среди прочего, в Чечне и на Украине. Сурков был главным идеологом Кремля в начале 2000-х, который сформулировал русскую версию «управляемой демократии» в которой государство называет себя демократическим, но на практике в большей степени демонстрирует авторитарные черты.[9] «Суверенная демократия» Суркова позволила

---

5 Mary Ellen Connell and Ryan Evans, “Russia’s ‘Ambiguous Warfare’ and Implications for the U.S. Marine Corps,” Occasional Paper (Arlington, VA: Center for Naval Analyses, May 2015), 3, https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf, по состоянию на 18 мая 2018.

6 Connell and Evans, “Russia’s ‘Ambiguous Warfare’.”

7 Connell and Evans, “Russia’s ‘Ambiguous Warfare’,” с. 4.

8 Connell and Evans, “Russia’s ‘Ambiguous Warfare’.”

9 Julia Ioffe, “Kremlin Henchman: The Only Thing I Like About America is Tupac (And Sanctions Won’t Keep Me from Listening),” *New Republic*, March 17, 2014, https://newrepublic.com/article/117053/vladislav-surkov-responds-sanctions-will-miss-tupac-shakur.

Кремлю добиваться своих целей по консолидации власти подавлением гражданского общества, свободной прессы и либерализма под знаком этой иллюзорной демократии. Он также разработал современную политику Кремля привлечения, маргинализации и манипуляции политических оппонентов, в соответствии с которой российские власти не закрывают оппозиционные медиа порталы, а устанавливают контроль над всем медиа циклом, и вытесняя оппозиционные группы в маргинальное пространство, эффективно обезоруживают их, сохраняя возможность правдоподобного отрицания.[10]

Сурков также сформулировал стратегию Кремля дестабилизации Украины путем негласной поддержки сепаратистов в Донбасском регионе, чему существенно способствует манипулирование международными СМИ в рамках широкой информационной кампании для распространения неопределенности об идентичности повстанческих сил в регионе.[11] Сурков комбинировал использование новых технологий и интернета с традиционными русскими формами принуждения и контроля – на практике он модернизовал политические махинации советской эпохи для 21-го века.

Хотя работа этих двух лиц как будто и не имеет прямого влияния на кибер присутствие России, их вклад в политику национальной безопасности России на деле сыграл критически важную роль для сегодняшней доминирующей позиции России. Герасимов был прав, указав, что современные конфликты уже не имеют конкретного начала и конкретного конца, и эта точка зрения оказала влияние на участие России в украинском конфликте, на ее продолжающуюся агрессивность в отношении Соединенных Штатов и на другие кампании политической дестабилизации по всей Европе. Приверженность Герасимова и Суркова к заблуждению и обману является основным моментом в российской киберстратегии создания широкомасштабного замешательства относительно намерений России и всеобъемлющей неопределенности о том, что является фактом и что – вымыслом. Предположительно Россия достигла больше, чем любая другая страна в деле использования интернета как оружия экономически эффективным и результативным способом. «Управляемая демократия» Суркова позволяет Кремлю заново установить централизованную власть и контроль над Россией, а также утвердить новорожденное интернет присутствие, приведшее к печально известным программам наблюдения и перехвата коммуникаций.

Российская Система оперативно-розыскных мероприятий (СОРМ), созданная Федеральной службой безопасности (ФСБ) в 1995 году, является государственной официальной системой для мониторинга частных коммуникаций в России. Хотя на бумаге доступ ФСБ к коммуникационным данным

---

[10] Ioffe, “Kremlin Henchman: The Only Thing I Like About America is Tupac.”

[11] Reid Standish, “Hacked: Putin Aide’s Emails Detail Alleged Plot to Destabilize Ukraine,” *Foreign Policy*, October 25, 2016, https://foreignpolicy.com/2016/10/25/hacked-putin-aides-emails-detail-alleged-plot-to-destabilize-kiev-surkov-ukraine-leaks/.

разрешен только при наличии ордера, СОРМ потребовала установление «черного ящика» для перемаршрутизации в оборудовании каждого интернет-провайдера (ИП), который направляет трафик данных через ФСБ, и на практике дает службе полный доступ ко всем коммуникациям независимо от юридической процедуры.[12] В 2017 году скептики могли не воспринимать идею, что российская СОРМ чем-то хуже, чем китайская *Великая стена* или печально известная система PRISM США, но аналитики, следящие за СОРМ, описывают ее как «PRISM на стероидах» из-за ее все более инвазивного развития после 1995 года.[13]

К 2017 году СОРМ-3 позволяет осуществлять следующее: мониторинг телефонных звонков, трафика электронной почты, просмотра веб-страниц, IP адресов, всех транзакций по кредитным картам, мониторинг всех сайтов социальных сетей, требует от них устанавливать черные ящики для следящих систем и предоставлять телефонные номера, электронные адреса пользователей и располагает способностью осуществлять глубокую проверку пакетов (ГПП). Способность ГПП имеет существенное значение, поскольку она позволяет чтение не только метаданных или заголовка посылаемых и принимаемых информационных пакетов, но также само содержание пакетов.[14] Также, охват закона быстро был расширен в сторону предоставления доступа к мониторингу российской налоговой полиции, охранительным службам Кремля/Думы/Президента, пограничной охране и служителям таможни.[15] В этом году, совсем недавно Путин окончательно решился на запрет использования прокси серверов, виртуальных частных сетей (ВЧС) и приложения для анонимных сообщений в попытке еще больше ограничить инакомыслие.[16]

Легко можно сказать, что СОРМ – это капля в море российского авторитаризма, но она является ключевой для российского кибер-присутствия и весьма важным инструментом Кремля для обезоруживания и преследования оппозиционных лидеров и врагов.[17] Именно режим Путина установил контроль и доминирование над «российским интернетом» и над внутренней российской связанностью и внутренними коммуникациям в конце

---

[12] Jen Tracy, "New KGB Takes Internet by SORM," *Mother Jones,* February 4, 2000, http://www.motherjones.com/politics/2000/02/new-kgb-takes-internet-sorm/.

[13] Nick Shchetko, "Forget its Hotels, Sochi's Tech Has Been Up for the Olympic Challenge," *Ars Technica*, February 20, 2014, https://arstechnica.com/information-technology/2014/02/forget-its-hotels-sochis-tech-has-been-up-for-the-olympic-challenge/.

[14] Marechal, "Networked Authoritarianism and the Geopolitics of Information."

[15] Tracy, "New KGB Takes Internet by SORM."

[16] Harriet Sinclair, "Putin Bans VPNs in Crackdown on Anonymous Internet Use in Russia," *Newsweek*, July 31, 2017, http://www.newsweek.com/putin-bans-vpns-crackdown-anonymous-internet-use-russia-644136.

[17] Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal* September 12, 2013, www.worldpolicy.org/journal/fall2013/Russia-surveillance.

1990-х и начале 2000-х. Исходя из этого, по мере того, как власть начала понимать, что интернет мог бы функционировать в качестве усилителя российского влияния и проецирования силы, Кремль начал экспериментировать с использованием кибератак для дестабилизации своих соседей.

Эпоха быстрого технологического развития в 21-м веке, начиная с появления интернета, всегда изобиловала проблемами, касающимися атрибуции и анонимности. Профессионалы в сфере безопасности давно пытаются преодолеть проблему установления авторства кибер-вмешательств и кибератак, так же как доказать атрибуцию и как подобающим образом на них реагировать. Однако, за последние десять лет мир стал еще более взаимосвязанным благодаря развитию смартфонов, социальных медиа и Интернета вещей (ИВ), так как большинство персональных устройств стали сетевыми и стали частью более широкого интернета. Сегодня мы находимся в периоде, когда имеется сверхизобилие информации, доступной каждому и в любое время. В 2017 году люди создали и сохраняют больше информации и данных, чем созданные за все предыдущие 5000 лет человеческой истории.[18]

Сегодня мир такой, что у среднего человека каждый день имеется доступ к ошеломляющему количество информации, новостей и контента, и никакие существенные барьеры не мешают публиковать в интернете. Это, однако, обоюдоострый меч – интернет обеспечил беспрецедентный прогресс в сфере образования, исследований и разработок, и социальные связи между людьми по всему миру. Те, кто стремились к тому, чтобы интернет был свободным и честным рынком идей, распространяли доступную, правдивую информацию так, чтобы другие могли учиться и расти. Однако, из-за неограниченного характера интернета, распространения социальных медиа и анонимности, есть много людей с нечистыми намерениями, которые пытаются затопить кибер-рынок идей преднамеренной дезинформацией и намеренно затруднить определение истины и, в конечном итоге, сделать ее бессодержательной. Можно определенно утверждать, что объективные факты и правда утратили свою силу в качестве фундамента общества по мере того, как интернет, образно говоря, превращался в зал кривых зеркал, где информация искривляется, и определение объективных фактов становится почти невозможным. Отрицание и дезинформация являются двумя ключевыми последствиями бесконтрольного распространения информации, которые были использованы Российской Федерацией в качестве оружия.

Впервые Россия опробовала свои кибер-способности в нескольких кампаниях кибератак в Эстонии в 2007 году, и с тех пор инкорпорировала в свои кибер-мероприятия и другие аспекты традиционного контроля Кремля, как

[18] Richard Harris, “More Data Will Be Created in 2017 than the Previous 5,000 Years of Humanity,” *App Developer Magazine,* December 23, 2016, https://appdevelopermagazine.com/4773/2016/12/23/more-data-will-be-created-in-2017-than-the-previous-5,000-years-of-humanity-/.

частную индустрию и российскую организованную преступность. Организованные русские атаки типа распределенного Отказа в Обслуживании (DDoS) против эстонского государства и гражданской инфраструктуры были первым широкомасштабным использованием кибер-способностей Россией для достижения стратегической цели в отношении соседнего государства, предположительно в ответ на дипломатическую перепалку по поводу переноса статуи Советского солдата в Таллине.[19] Эстонские атаки были дебютом для российских кибер-способностей, и они были успешными в расстройстве работы эстонских вебсайтов и другой технологической инфраструктуры более чем на месяц, что можно считать существенным уроном для страны, которая считает себя технологически передовой и имеет почти безбумажную администрацию.[20] Исполнители атак, в число которых входили группы организованной преступности и частные хакерские группы, использовали ботнеты с компьютеров по всему свету, чтобы подавить эстонские серверы, в том числе серверы государственных организаций, банков, политических партий и большинства вебсайтов новостных медиа. На деле, российская власть аплодировала хакерам и поощряла их, но отрицала какое-либо участие в этих атаках.[21]

Хотя эстонские атаки достигли малого в плане конкретной пользы для России, они были критически важными для демонстрирования эффективности простых, широкомасштабных кибератак, особенно в сочетании с другими средствами экономического и политического принуждения. Хотя после атак НАТО создало в Таллине Кооперативный центр передового опыта по кибер-защите, толерантная международная реакция и возможность России отрицать свою причастность и отклонять обвинения в участии придали Кремлю уверенность для еще более широкого использования кибер-нападений. Россия продолжила использование сочетания кибер-операций с кинетическими военными операциями в Грузинской войне в 2008 году, первый комбинированный кибер-военный конфликт такого типа, и продолжила использовать дестабилизирующие кибер-атаки в Украине, начиная с 2014 года. Ключом к успеху была способность России притворяться невиновной, используя в своих операциях одновременно службы безопасности и криминальных хакеров.

Всемирная оценка угроз Разведывательного сообщества США от 2015 года содержит вывод, что Россия и Китай являются «наиболее опытными игроками, являющиеся национальными государствами» в технологиях кибер-войны, и что русские хакеры «являются ведущими в плане квалификации, программистских способностей и изобретательности», – и эта оценка

[19] Michael Connell and Sarah Vogler, “Russia’s Approach to Cyber Warfare,” Occasional Paper (Arlington, VA: Center for Naval Analyses, March 2017), с. 13, https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

[20] Connell and Vogler, “Russia’s Approach to Cyber Warfare,” с. 13.

[21] Connell and Vogler, “Russia’s Approach to Cyber Warfare,” с. 14.

остается верной и по сей день.[22] Похоже, что Россия при Путине вложила много усилий для развития кадровых хакеров на государственной службе, часто привлекая людей из рядов уголовного подземного мира. Аналитик по кибер-угрозам компании FireEye Джонатан Ролстэд пришел к выводу, что Россия поддерживает «симбиотические отношения» с синдикатами организованной преступности как минимум «уже 10 лет, если не дольше», развивая связи типа «услуга за услугу», при которых незаконченные уголовные дела против хакеров таинственным образом распадались в обмен на содействие службам безопасности.[23] Кремль получает команды хакеров высшей квалификации, а также «лучшие образцы вредоносного программного обеспечения» и, что самое важное, получает возможность правдоподобно открещиваться от деятельности привлеченных групп».[24] Такая практика идет рука об руку с традиционными российскими и советскими активными мероприятиями и дымовыми завесами, предназначенными для выведения противника из равновесия, создания замешательства и разногласий.

Далее, способность России кооптировать частный бизнес и частную промышленность в свою сеть служб безопасности тоже оказалась эффективным тактическим приемом для расширения кибер-охвата на глобальный уровень. Ничто лучше не демонстрирует эту постановку, чем Лаборатория Касперского, российская компания, занимающаяся кибер-безопасностью и антивирусными программами, очень популярными во всем мире, которую давно подозревают в связях с российскими службами безопасности и разведывательными ведомствами. Хотя было время, когда имя Касперский было уважаемым в сфере персональной кибер-безопасности и его антивирусные продукты использовались сотнями миллионами потребителями по всему миру, в том числе, государственными ведомствами США, в последние годы возникли вопросы относительно связей (добровольных или вынужденных) компании с российским государством. Компания всегда отвергала такие вопросы как необоснованные и абсурдные, но в стране, в которой СОРМ и ФСБ существенным образом мониторят российский интернет, они определенно не лишены оснований. Те, кто изучали операции Касперского, были вознаграждены в 2017 году, когда вытекшие в сеть электронные письма и детали хакерских атак с упоминанием Касперского раскрыли близкие отношения компании с ФСБ, причем Касперский напрямую разрабатывал технологии безопасности для ведомства и работал над совместными

[22] Owen Matthews, “Russia’s Greatest Weapon May Be Its Hackers,” *Newsweek*, May 7, 2015, http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html.

[23] Cory Bennett, “Kremlin’s Ties to Russian Cyber Gangs Sow US Concerns,” *The Hill*, October 11, 2015, http://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns.

[24] Bennett, “Kremlin’s Ties to Russian Cyber Gangs Sow US Concerns.”

проектами.[25] Отношения еще больше были раскрыты при привлекшем большое внимание взломе персонального компьютера контрактора Агентства национальной безопасности, который неправомерно хранил секретные документы АНБ, – АНБ установила, что контрактор имел на своем компьютере программное обеспечение от Касперского, которое играло активную роль при поиске секретных американских файлов и передавало их либо российским хакерам (связанными или не связанными с государством), или напрямую российской разведке.[26]

Можно предположить, что российские власти имели длительные и плодотворные отношения с Касперским, предоставляющим технически легальный инструмент для того, чтобы шпионить за противниками России – но с уверенностью можно сказать, что эти отношения идут к концу, поскольку сейчас репутация Касперского падает, и власти США запретили использование программ Касперского. Сейчас Касперский завел дело против властей США по поводу запрета, дело, которое само по себе можно рассматривать как продолжение российских операций, поскольку оно, вероятно, вовлечет США (по крайней мере, в некоторой степени) в досадную юридическую битву по доказательству двойственности Касперского.[27] Тем не менее, наше утверждение остается в силе – Россия показала себя мастером при нахождении креативных способов утверждения влияния Кремля на все грани русского киберпространства в осуществлении своих политических и разведывательных целей по всему свету. Цифровое путешествие России, возможно, достигло своей кульминационной точки при создании «Агентства интернет-исследований» и при дестабилизации политической системы Соединенных Штатов.

В статье газеты Нью-Йорк Таймс от июня 2015 года, озаглавленной «Агентство», представлен пророческий взгляд на русские «фабрики троллей» и дезинформационные кампании задолго до того, как такие операции получили всемирную известность в 2016 году. В одной из первых серьезных публикаций, раскрывающих российские кибер информационные операции, подробно рассказывается о том, что известно об «Агентстве интернет-исследований», организации, располагающейся в невзрачном административном комплексе в Санкт-Петербурге, в которой работают несколько сотен сотрудников, чья задача состоит в ведении «информационной войны» –

---

[25] Jordan Robertson and Michael Riley, “Kaspersky Lab Has Been Working with Russian Intelligence,” *Bloomberg Businessweek*, July 11, 2017, по состоянию на 28 мая 2018, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence.

[26] Nicole Perlroth and Scott Shane, “How Israel Caught Russian Hackers Scouring the World for U.S. Secrets,” *New York Times*, October 10, 2017, www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html.

[27] Dustin Volz and Jim Finkle, “Kaspersky Lab Asks Court to Overturn U.S. Government Software Ban,” *Reuters*, December 18, 2017, https://www.reuters.com/article/us-usa-cyber-kasperskylab/kaspersky-lab-asks-court-to-overturn-u-s-government-software-ban-idUSKBN1EC2CK.

распространении разрозненных и фальшивых нарративов по множеству политических и социальных вопросов по всему миру с целью размыть грань между правдой и ложью на пользу Кремля.[28] В статье четко показано, что является предвестником российской информационной операции в США в 2016 году, но не показана связь между феноменом финансируемых государством дезинформационных кампаний и тем, насколько уязвимыми были и остаются США к такой общей стратегии. Статья «Агентство» показательна для настроений и взглядов американской администрации и американской публики в 2015 году – отражены множество деталей об этом опасном феномене, но недостаточно хорошо объяснено, почему Россия делает это и каков ее полный потенциал. Можно провести прямую линию между описанными в статье операциями к кампании Кремля по дестабилизации выборов в США в 2016 году, которая принесла Путину ошеломляющий результат при предполагаемых расходах, не превышающих 500 000 долларов.[29] Всего через два года после этого статья «Агентство» уже устарела и выглядит наивной на фоне последних мировых событий. Это остается прекрасным примером отсутствия воображения у властей США, что касается кибер-способностей и показывает некоторые из качеств, которые позволили российскому руководству и российской разведке так быстро развернуться в киберпространстве.

Кибер развитие России с конца 1990-х до сегодняшнего времени показывает последовательную схему умелой адаптации к меняющимся реалиям мира и четкое приспосабливание традиционной советской разведывательной стратегии и приемов к новой технологии. Можно с уверенностью утверждать, что подъем России к высотам кибер распространения и доминирования обусловлено по большей части уникальными особенностями исторического, культурного и политического характера России. Хотя вначале Россия медленно осознала возможности интернета и технологии 21 века, в конечном итоге сделала кибер-технологию ключевым элементом своей политики национальной безопасности и своей внешней политики в такой степени, в которой это не сделали даже Китай и Соединенные Штаты. Считается, что использование кибер-технологий в качестве основного инструмента для проецирования силы и для вмешательства в дела иностранных государств чаще всего возможно в таких авторитарных государствах, как Россия, которая в конце 1990-х и начале 2000-х быстро рецентрализовала власть в руках Путина и Кремля и ограничила свободу СМИ и интернета образом, который дал огромные полномочия службам безопасности и администрации. Российское государство, несмотря на громкие заявления Владимира Путина и других представителей российского руководства, по сути

[28] Adrian Chen, “The Agency,” *New York Times*, June 2, 2015, www.nytimes.com/2015/06/07/magazine/the-agency.html.

[29] Greg Miller, Greg Jaffe, and Philip Rucker, “Doubting the intelligence, Trump Pursues Putin and Leaves a Russian Threat Unchecked,” *The Denver Post*, December 14, 2017, https://www.denverpost.com/2017/12/14/trump-pursues-putin.

своей неморально, что позволяет ему полностью использовать политический и подрывной потенциал интернета и современных технологий, не заморачиваясь моральными и этическими затруднениями, присущими таким технологиям.

Россия также выигрывает от самой природы глобальной технической индустрии – Кремниевая долина и другие технологические центры продолжают не понимать, что платформы и приложения, которые они разработали, располагают потенциалом быть использованными неэтическим образом для создания политического и экономического хаоса, опущение, которое играет на руку группам и государствам, как Россия. И опять же, к этому привел не только провал в прогнозировании того, как враждебные государства и негосударственные группы могут взять под свой контроль социальные медиа, журналистику и кибер-инфраструктуру для дестабилизации целых государств, но отсутствие морального сознания у Кремниевой долины и намеренный отказ принять реалию, что технология не является этически нейтральной. Для такого государства, как Россия, чье правительство не обременено такими соображениями при преследовании основанных на реалполитике целей по достижению международного могущества, близорукость американских и западных технологических компаний является одним из самих больших подарков России и другим подобным государствам. Только после событий, связанных с выборами в 2016 году в США, американское общество начинает понимать эти вопросы и начинает спрашивать, как технология оказывает влияние и формирует американскую демократию и американское общество.[30]

И наконец, Россия так же умело приспосабливается к эпохе интернета благодаря тому, что ее культура анонимности, двойственности и искривления в совершенстве подходит для богатой российской истории обмана и запутывания в сердцевине ее политической культуры. Основной характерной чертой активных мероприятий Советского Союза было создание массового замешательства и неопределенности в отношении глобальной деятельности, политических позиций и целей России, запутать массовые восприятия других государств и породить широкую политическую и экономическую нестабильность. Сам характер технологии 21-го века и интернет работают как мультипликатор для этих целей. Не следует переоценивать Россию – вряд ли Россия действительно предвидела такое будущее и специально делала планы для реальности, в которой глобальное население перегружено информацией и дезинформацией и простые, недорогостоящие информационные операции окажутся удивительно эффективными для достижения больших политических целей. Однако, определенно не было сложным предсказать такое будущее, поскольку авторы как Олдос Хаксли, написавший в 1932 году *О дивный новый мир,* предчувствовали мрачное будущее, в котором

[30] Irina Raicu, “Rethinking Ethics Training in Silicon Valley,” *The Atlantic*, May 26, 2017, https://www.theatlantic.com/technology/archive/2017/05/rethinking-ethics-training-in-silicon-valley/525456/.

«правда утоплена в море нерелевантности», а не лишенное информации общество из *1984* Джорджа Оруэлла.[31] Позже Хаксли в своем последующем эссе *Возвращение в дивный новый мир* от 1958 года сам отмечает, что «Развитие огромной индустрии массовых коммуникаций, которая интересуется в основном не истиной и ложью, а нереальным, является более или менее полностью неадекватным. В двух словах, они не учли почти бесконечный аппетит человека к развлечениям».[32] Нетрудно увидеть, насколько сегодня общество напоминает это предсказанное будущее, и как такие государства как Россия используют в огромной степени лавину информации и шума, с которой сталкиваются люди ежедневно. Сотрудник Гаагского центра стратегических исследований Александр Климбург описывает киберпространство сегодня как «Европа в 1914 году, до начала Первой мировой войны – правительства, как сомнамбулы, они не понимают силу новой технологии и последствия непонимания взаимных действий».[33] Эта реальность вряд ли скоро изменится – кибер превосходство России это подтверждает и использует. Остается посмотреть, как Соединенные Штаты и соседи России ответят на этот вызов.

Кибер разведка США в 21-м веке должна признать наличие реалий постоянно меняющегося настоящего, к которым следует адаптироваться и разработать эффективную политику реагирования на действия таких стран, как Россия. Разведывательное сообщество США (РССША) обязано по серьезному отнестись к слабостям, органически присущим потребительской технологии по всему миру – Россия уже показала огромную хаотическую силу социальных медиа, а Кремниевая долина все еще не воспринимает эту проблему серьезно и не рассматривает способы, которыми ее продукты могут использоваться вредоносно злонамеренными акторами. Затруднительно считать, что РССША должно вмешиваться в целостность частной технологической индустрии, но необходимо сотрудничество с властями США для того, чтобы гарантировать, что события, как вмешательство в выборах в 2016 году, не будут повторяться. Некоторые аналитики считают, что «Лучшая защита – это нападение», и что США должны выдвинуть вперед свои наступательные кибер-способности.[34] Это несколько неправильно – хотя глупо оспаривать, что наступление не должно быть в фокусе кибер-политики США, опыт кибератак российских властей (и других государств и групп) показывает, что кибер-война настоящего и будущего атакует политическую, экономическую и социальную инфраструктуру стран через их слабую оборону и культурные характеристики прозрачности и свободного обмена. Это и есть

[31] Neil Postman, *Amusing Ourselves to Death* (Upper Saddle River, NJ: Pearson Education, 2007), xix.

[32] Aldous Huxley, *Brave New World Revisited* (New York: RosettaBooks, 2000), 31.

[33] Matthews, “Russia’s Greatest Weapon May Be Its Hackers.”

[34] Gillian Rich, “As Russia Hacks, Is the Best Cyber Defense a Terrifying Cyber Offense?” *Investor’s Business Daily*, December 19, 2016, https://www.investors.com/news/preventing-cyberattacks-is-the-best-defense-an-almighty-offense/.

части американского общества, которым в наибольшей степени нужна надежная кибер-защита. Конечно, США должны защищать конкретную инфраструктуру, границы и располагать кинетическими сдерживающими способностями, но как показал 2016 год, манипулирование информацией и общественными восприятиями может быть гораздо эффективнее пуль и бомб.

Однако, как и для большинства вещей, имеющих отношение к современной России и к ее нынешнему восстановлению, есть ограниченное время действия российского кибер превосходства, о котором Кремль должен знать. У России сегодня есть много серьезных политических, экономических и демографических проблем, которые будут играть важную роль в способности страны демонстрировать силу даже в экономически эффективных кибер-атаках и отношениях с уголовными группами хакеров. Есть большая опасность в том, чтобы работать с негосударственными акторами и группами, у которых нет опыта и темперамента представителей администрации и военных – любая ошибка хакерских групп может быстро и опасно эскалировать в ситуацию, которая выйдет из-под контроля Кремля.[35] Кремль также рискует, связываясь «слишком тесно» с уголовными группами, которые он может оказаться не в состоянии контролировать. Путин неожиданно успел передефинировать русскую политическую и культурную идентичность на основе его концепции национализма и консерватизма, что привлекло «патриотических хакеров», желающих внести свой вклад в восстановление России – патриотически настроенные русские способствовали работе ботнетов, нацеленных на Грузию в 2008 году. Но национализм вряд ли будет достаточен для того, чтобы привязать частных хакеров к российскому государству в долгосрочном плане – мрачные экономические перспективы России из-за чрезмерной зависимости от нефти и газа, стареющего населения страны и утечки мозгов в конечном итоге лишат Кремля его элитных криминальных хакеров.[36] Учитывая, что хакерство становится все более глобализованным и широко распространенным уголовным феноменом, и с появлением криптовалют российские хакеры в конце концов не будут нуждаться в услугах Кремля по отмыванию своих незаконно приобретенных денег, и многие, вероятно, уедут за границу вне досягаемости кремлевского принуждения.[37]

Российский кибер-голиаф сейчас выглядит неодолимой проблемой, и если в 2017 году Россия была на вершине кибер превосходства, то последует неизбежный спад. Российское превосходство неустойчиво как из-за

---

[35] Cyberreason Intel Team, “Russia and Nation-State Hacking Tactics: A Report from Cyberreason Intelligence Group,” *Cyberreason.com*, June 5, 2017, https://www.cybereason.com/blog/blog-russia-nation-state-hacking-the-countrys-dedicated-policy-of-strategic-ambiguity.

[36] Cyberreason Intel Team, “Russia and Nation-State Hacking Tactics.”

[37] John Leyden, “Russia is struggling to keep its cybercrime groups on a tight leash,” *The Register*, June 6, 2017, https://www.theregister.co.uk/2017/06/06/russia_cyber_militia_analysis/.

внутренних экономических, политических и демографических проблем, так и из-за факта, что мир открыл глаза, и такие страны как США и Китай наращивают свои кибер-стратегии и свою кибер-готовность. Однако, Кремль тоже понимает, что его превосходство имеет временный характер, и по этой причине политики и сотрудники разведки должны ожидать, что Россия будет использовать свою огромную мощь с некоторой наглой импульсивностью, пока это еще возможно, особенно с учетом того, что режим Путина начинает слабеть. Хотя разные факторы могут оказать влияние на темп изменений и позволят России еще некоторое время оставаться на верху. Факт, который мир должен был заметить еще раньше, остается – интернет и глобализованные технологии в их современном виде являются идеальным инструментом для современной России с ее длинной историей мастерского использования двойственности и заблуждения. Признание факта, что Россия выигрывает у мира и понимание того, как это происходит, являются первыми шагами к тому, чтобы остановить Кремль.

Об авторе

Уильям КИМ в данное время является студентом магистерской программы по исследованиям безопасности при Школе иностранной службы им. Уолша Джорджтаунского университета. У него степень бакалавра, полученная в Университете Пенсильвании. Он специализируется на политических анализах России и ее внешней политики, а также на исследованиях в сфере разведки. В число других его академических интересов входят исследования Балканского региона и этические аспекты национальной безопасности и разведывательной деятельности. Раньше он работал в Государственном департаменте США и был интерном при Колледже международной безопасности Национального университета обороны США.
E-mail: wm.a.chim@gmail.com.