

Флиши де ла Невиль Т.,
штатный сотрудник кафедры геополитики
и бизнеса Реннской школы бизнеса
(Франция)
**ЦИФРОВИЗАЦИЯ МИРА:
ЭПОХА НЕЗРИМОЙ ВЛАСТИ**

DOI: 10.31249/rimm/2020.03.02

Нет сомнений, что вступление мира в цифровую эпоху, когда человек и машина тесно связаны, является важным переходным процессом в истории нашей цивилизации. Цифровой формат меняет способы осуществления власти, частично скрывая ее от глаз общественности. Сайты, собирающие данные пользователей без их ведома, подвергаются атакам действующих анонимно¹ хакеров. Таким образом, в кибернетическую эпоху власть становится менее ощутимой², что, в свою очередь, делает изучение текущего технологического изменения чрезвычайно важным. Тем не менее в этом начинании присутствует и доля риска: существует опасность, что мы ошибочно принимаем достижения в области цифровых технологий за действительную жизнеспособность цивилизации, опирающейся на возможность вдохнуть новую жизнь во все части общества³. Возникающий в настоящий момент гибридный реального и виртуального миров порождает опасения, что человек предпочтет технологии реальной жизни. Вместе с тем существует

¹ Идея всех систем анонимизации состоит в том, чтобы слить воедино данные разных пользователей Сети, делая их неотделимыми друг от друга. Таким образом, становится невозможным установить соответствие между данными и конкретной личностью.

² Сегодня кибератаки стали настолько изощренными, что стало невозможно определить, где именно находятся преступники. Это затрудняет реализацию агрессивной тактики, рекомендованной в последней правительственной «белой книге» по киберстратегии.

³ Арнольд Тойнби писал, что, «рассматривая историю военных технологий в рамках греческой истории, мы бы увидели непрерывное развитие от начала и вплоть до самого конца: до, во время и даже после периода роста. Мы бы также заметили, что каждый шаг на пути прогресса был простимулирован событиями, которые в противном случае погубили бы эллинскую цивилизацию». Арнольд Тойнби. *L'histoire* (Paris: Gallimard, 1951), с. 219. Перевод с английского, выполненного по французскому оригиналу.

надежда, что возникнет некая форма цифрового гуманизма. Незримую власть¹ не так-то просто заметить. Одной из дилемм в исследовании кибербезопасности является то, что большая часть данных находится в закрытом доступе. В этой сложной области исследования можно разобраться лишь при помощи технических возможностей армии или разведывательных служб. Изучение разных источников информации, содержащих точки зрения сторонников и противников цифровизации, может помочь преодолеть это препятствие. Ряды противников составляют те немногие философы, которые критически размышляют о цифровом мире. Так, французский философ Бернар Стиглер считает, что Интернет – это разрушительная технология², поскольку цифровая автоматизация ведет к уклонению от уплаты налогов и безработице. Писатель Эрик Садин приписывает искусственному интеллекту (ИИ) своего рода разумность, которая позволяет в реальном времени оценивать различные обстоятельства, непрерывно предлагая услуги и продукты. Подобный технолиберализм направлен на формирование поведения человека. Наконец, профессор компьютерных наук Каве Саламатин представляет Интернет в виде чудовища с множеством щупалец и сердцем, рассчитанным на обслуживание большого количества пользователей, чья подводная инфраструктура дает представление о положении дел в цифровой геополитике³. В поддержку выступают различные блоги и сайты, свидетельствующие о нынешней жизнеспособности технологий. Представляется полезным сравнить сайт о технологиях Wired.com, ориентированный на неспециалистов, с французскими сайтами InternetActu.net и Reflets.info, которые предлагают более аналитическое понимание предмета. Кроме того, различные онлайн-инструменты позволяют нам оценивать эволюцию цифровых технологий, начиная с карт подводной сети кабелей, по которой передаются 99% интернет-данных⁴,

¹ Большинство пользователей не подозревают, как именно работает поисковая система Google.

² Мировой судья и специалист по кибертехнологиям Мириам Кеменер исследует изменения во французском законодательстве в ответ на оказывающие подрывное действие цифровые технологии.

³ Суэцкий канал и Малаккский пролив являются важными в стратегическом отношении пунктами для подводных кабелей. Вместе с тем лишь четыре пункта связывают Китай с остальным миром.

⁴ Кабель связи MAREA, состоящий из кабелей толщиной не больше шланга, был проложен в 2017 г. Он связывает Вирджинию с Бильбао и в настоящее время передает 75% мирового онлайн-трафика.

и заканчивая картами пользователей TensorFlow или Shodan.io, предоставляющими обзор подключенных устройств. Также можно обратиться к представителям сообщества геймеров-хакеров¹, которые согласны обсудить свою подпольную деятельность² (правда, IT-специалисты могут неохотно вступать в контакт с миром, в корне отличным от их собственного)³. Однако информационные источники в поддержку любой из сторон не учитывают географическое положение. Поэтому представление о цифровой геополитике с поправкой на определенное место мы получаем из программ для мониторинга, таких как TadaWeb.com, и сопоставительных анализаторов, таких как Gephi.org. Вопреки логике, при всей своей незаметности цифровым мощностям не присуще лишать данные подключенных к Сети пользователей индивидуальности. Цифровизация процветает благодаря массовому сбору персональных данных, а это, в свою очередь, означает деление общества на предопределенные микрогруппы. Включение групп людей в онлайн-базы является необходимым условием для эффективного персонализированного маркетинга, ответвлением которого является электронный маркетинг⁴. Как это ни парадоксально, при цифровизации человеческих обществ их индивидуальность проявляется до такой степени, что микрогруппы подключенных к Сети одиночек начинают конфликтовать друг с другом⁵. При более пристальном рас-

¹ К примеру, сайт Pastebin публикует информацию о самых недавних хакерских операциях.

² Tim Jordan and Paul Taylor. A Sociology of Hackers // The Sociological Review. Vol. 46. N 4. November 1998. P. 757–780.

³ Люди с синдромом Аспергера (форма аутизма, при которой наблюдаются трудности в общении) часто бывают особенно успешны в IT-профессиях. См.: Steve Silberman. The Geek Syndrome // Science. 12 January 2001.

⁴ Одним из флагманских продуктов Quantcube Technology является Global Macro Smart Data, прогнозирующая в режиме реального времени платформа, требующая от пользователей ежегодного продления лицензии. С мая 2013 г. Quantcube Technology предсказала 21 результат выборов с точностью до 92% еще за несколько недель до открытия избирательных участков. Среди прочего этот стартап в 2016 г. предсказал, что Великобритания проголосует за выход из ЕС и что Дональд Трамп победит на президентских выборах в США (во втором случае за две недели до выборов). Также были предсказаны итоги первого тура президентских выборов во Франции в 2017 г. и промежуточных выборов в США в 2018 г.

⁵ Главным инструментом сокращения трений между пользователями на больших цифровых платформах является модерация пользовательских сообщений. Эта скрытая от глаз задача потребляет огромное количество ресурсов. Глобальные платформы используют автоматизированные инструменты модерации

смотреии непрерывное подключение к Сети, контролируемое вездесущими алгоритмами, производит впечатление инструмента скорее разобщения, нежели объединения¹. Чтобы разобраться в этом и наметить потенциальные геополитические последствия, необходимо изучить механизм цифровой революции.

Коммерческая сторона цифровой революции

Стремясь заменить непредсказуемость человека искусственным интеллектом, цифровая революция использует каптологию для монополизации внимания потребителей, при этом почти не подвергаясь кибердисфункциям.

Искусственный интеллект: троянский конь, призванный лишить людей независимости. В ближайшие годы развитие искусственного интеллекта будет идти в ногу с развитием 5G и квантовым компьютером. 5G в сто раз быстрее 4G и устанавливает взаимосвязь людей с цифровыми устройствами. Мобильная связь пятого поколения создает условия для всего, начиная от умных городов и заканчивая автоматизированным окружением. 5G разработан специально для «интернета вещей», таких как умные автомобили и дроны. С самого начала лидирующую позицию в этой области заняла Швейцария, запустив 17 апреля 2019 г. 338 вышек 5G. Однако эта технология не лишена элемента риска, поскольку требует установки ретрансляторов через каждые 800 м из-за непостоянства высокочастотных волн. Ряд патентов, связанных с технологией 5G, принадлежит Китаю. В мае 2019 г. президент США Дональд Трамп запретил американским телекоммуникационным сетям закупать оборудование Huawei. Правительство США выразило опасения по поводу широкомасштабного шпионажа и надавило на своих союзников, чтобы те прекратили сотрудничество с китайской компанией. Однако если компании Huawei и другим китайским компаниям не удастся развернуть 5G в Европе, то европейские телекоммуникационные операторы потеряют 1,5 года, а расходы составят 55 млрд евро. Также с новыми квантовыми компьютерами (и, в частности,

контента. Задача модерации как таковой состоит из выявления и удаления оскорбительного или неприемлемого контента. См.: Tarleton Gillespie. The Custodians of the Internet // Yale University Press. 2018. P. 296.

¹ Если, конечно, эти виртуальные конфронтации не угрожают кибербезопасности, от которой зависят иностранные инвестиции.

IBM Q) действующие криптографические протоколы теряют свою актуальность. Тем не менее около десяти существующих в настоящее время квантовых компьютеров все еще находятся на стадии эксперимента. В ближайшие годы ИИ разовьется до такой степени, что не только сможет формировать выбор потребителей, но и реформировать государственный аппарат¹. Для этого была разработана новая наука – каптология.

Каптология: искусство незримой манипуляции. Искусственный интеллект главным образом завязан на эмоциях². Чтобы завладеть нашим вниманием, алгоритмы переводят наше ментальное пространство в код. Основы каптологии были заложены в работе Б.Дж. Фогга из Стэнфордского университета, который в 2003 г. опубликовал книгу *Persuasive Technology: Using Computers to Change What We Think and Do* («Технология убеждения: компьютер как средство для изменения наших мыслей и действий»). Технологии убеждения, разработанные специалистами в области архитектуры выбора, направлены на то, чтобы подтолкнуть людей к определенному выбору. Укоренившись в поведенческой экономике и нейромаркетинге, они предоставляют реальную власть алгоритмам. Эта новая экономика рассматривает продолжительность концентрации внимания как редкий и ценный ресурс, который можно использовать в интересах бизнеса, сосредоточивая это внимание на информации, вызывающей, в свою очередь, определенное действие. Философ Бернар Стиглер отрицательно высказывался о замыкающей внимание психотехнологии, как и до этого лингвист Ноам Хомский и экономист Эдвард С. Херман, критиковавшие роль массмедиа в производстве согласия. Каптология может также играть на искусственно созданных тревогах, например на «страхе что-либо упустить». Этот страх во многом подогревается определенными атрибутами современных технологий, такими как мобильные телефоны и социальные сети (например, Facebook и Twitter), которые дают пользователям возможность постоянно

¹ Правительственные стартапы могут оказаться в авангарде государственных реформ.

² По мнению французского IT-бизнесмена Пьера Беллангера, «программное обеспечение и алгоритмы – это человеческая мысль в коде. Лишь третья часть нашего мозга посвящена рациональному мышлению. Если большая часть наших мыслей возникает из бессознательного, то с развитием сетей наше мышление оказывается в отрыве от здравомыслия, контроля и какого бы то ни было понимания наших собственных целей. Интернет кодирует и формирует наши мечты». Перевод с английского, выполненного по французскому оригиналу.

сравнивать свои профили. По мере роста использования Интернета в мире у части населения разовьется психологическая зависимость от онлайн, и пребывание офлайн будет вызывать у них чувство тревожности.

Низкое влияние киберпреступности на глобализацию. Несмотря на рост¹ киберпреступности в мире, особенно в развивающихся странах², хакерам редко удастся парализовать корпорации или государства на сколько-нибудь длительное время. В действительности же кибератаки (которые часто поддерживаются государствами³) являются более изощренной версией применяемых издревле практик: саботажа, шпионажа и диверсии. Хотя затраты на эти операции сильно сократились, область применения киберсаботажа по-прежнему ограничена. Ущерб можно нанести различными способами: взорвать трубопровод, сломать плотину, взломать радар самолета, задержать ядерную программу, закрыть банк, перехватить управление автомобилем⁴ или убить кого-то, заминировав мобильный телефон. У кибершпионажа большой потенциал: шпионы, перегруженные огромным количеством предлагаемых украденных данных, оказываются неспособными обработать весь объем этой вырванной из культурного контекста информации. В шпионском мире атаки становятся все более изощренными. Например, некоторые вирусы сами себя стирают, что делает невозможным отследить их источник⁵. Они даже могут мутировать,

¹ Наиболее эффективно действуют хакеры из Израиля и Индии.

² Очагами киберпреступности главным образом являются развивающиеся страны, которые в последнее время стали значительной силой в области мошеннических операций. Хакерские атаки из Бразилии продолжают усиливаться, делая ее одной из пяти самых активных «горячих точек» киберпреступности в мире.

³ Программное обеспечение Тог, распространяемое через даркнет, использует технологию так называемой луковой маршрутизации, которая была разработана ВМС США в 1990-х годах. Эта военная технология по большей части финансировалась правительством США для продвижения идей демократии во всем мире. До 2017 г. правительство США переводило почти все свое финансирование через ВМС США, Государственный департамент и Совет управляющих по вопросам вещания, сформированного ЦРУ. В результате крупнейшие спецслужбы могут отменить процесс анонимизации данных, раскрыв личности пользователей Тог.

⁴ Хакеры могут управлять автоматическими окнами и индикаторами на приборной панели или даже вызвать поломку двигателя.

⁵ Согласно прогнозам «Лаборатории Касперского» по целенаправленным атакам в 2019 г., в будущем вирусы будут действовать незаметно.

как и биологические вирусы¹. Что касается диверсии, несмотря на то что протестное движение легко запустить онлайн, его очень сложно поддерживать на длинной дистанции. Таким образом, саботаж на время усложняет использование цифровых технологий, а шпионаж пожинает плоды нашего постоянного подключения к Сети. В конечном итоге лишь некоммерческая диверсия может представлять реальную угрозу происходящему в настоящее время переходу на цифру, однако для этого она применяется недостаточно часто.

Глобальная цифровизация коренится в динамике развития рынка и позволяет незримо влиять на подключенных к Интернету людей. С помощью этого финансовый капитализм прокладывает себе дорогу к новой международной геополитической позиции.

Цифровые империи против цифровых вассальных государств

Тремя главными тенденциями, определяющими геополитику в цифровом мире, являются уменьшение мощи США, возрастание мощи Китая и конкуренция между ними за цифровую колонизацию остального мира.

Ослабление цифровой мощи Америки. Америка приобрела влияние в виртуальном мире благодаря олигополии, известной как GAFAM. Акроним GAFAM используется для описания пяти крупнейших компаний – Google, Apple, Facebook, Amazon и Microsoft, – которые были основаны бывшими хакерами². Эти компании физически хранят данные³. Таким образом, у США и их британской ретрансляционной станции имеется доступ к огромному объему

¹ Для размножения вирусы используют нестабильные энзимы. Поскольку не существует системы корректирования, которая бы могла в этом случае прийти на помощь, ошибка остается в геноме. Это происходит примерно в одном из десяти тысяч случаев. Именно поэтому вирусы имеют такое разнообразие.

² Среди них Стив Джобс (Apple), Марк Цукерберг (Facebook), Билл Гейтс (Microsoft) и Линус Торвалдс (Linux).

³ Инфраструктура Интернета главным образом состоит из подводных оптоволоконных кабелей большой проводимости, соединенных с наземными кабелями и маршрутизаторами. Для Европы наиболее важными являются кабели, соединяющие континент с Британскими островами, а оттуда – с Соединенными Штатами через Атлантический океан.

данных¹; через Соединенные Штаты идет 80% всех данных. Прослушивающие станции размещаются неподалеку от места выхода подводных кабелей на сушу². Кабельная геополитика отражает напряженность в китайско-американских отношениях³, как и борьбу Португалии и Бразилии за контроль над экономическим рынком бывших португальских колоний⁴. Кабели связи могут способствовать росту зависимости заморских территорий, удаленных от крупных населенных пунктов⁵. Поскольку поведение GAFAM аналогично поведению государств, в 2017 г. Дания направила в группу компаний своего посла. На самом же деле это больше похоже на клептократию, существующую за счет украденных данных⁶. Ее гибридная система убеждений имеет черты как левого либертарианства, так и правого технологического детерминизма. Возникшее в результате техно-либертарианство нашло последователей в лице харизматичных провидцев-основателей, которые генерируют неизменно технологически авангардные инновационные коммерческие предложения. В 2016 г. при поддержке инвестиционных фондов «Большая пятерка» потратила на исследования и разработки 58 млрд долл. В какой-то мере своей монополией она обязана

¹ Чтобы избежать американского надзора, Бразилия проложила собственный подводный кабель в Испанию. Китай также проложил кабель Sea-me-we 5, соединяющий его с Ближним Востоком, а оттуда – с Европой. Huawei Marine Group продолжает активную укладку кабелей связи, например, между Бразилией и Камеруном.

² В прошлом подводные кабели помогли Британской империи нарастить финансовую мощь. Первый полностью рабочий кабель был проложен в 1851 г. между побережьями Франции и Англии для передачи телеграфных сообщений с биржевой информацией. Сегодня консорциум Seaborn Networks начал прокладку подводного волоконно-оптического кабеля, соединяющего бразильскую Форталезу с Уолл-стрит. В проекте, известном как Seabras-1, заложена установка связи с африканскими финансовыми рынками через Южную Африку.

³ Соединенные Штаты решительно прореагировали на неуклонно растущую цифровую мощь Китая. В 2013 г. американская администрация сорвала планы китайской компании Huawei по прокладке нового трансатлантического кабеля между Нью-Йорком и Лондоном.

⁴ С февраля 2019 г. кабель SACS соединяет Анголу с Бразилией, а ELLALINK – Португалию с Бразилией через Кабо-Верде.

⁵ С 2009 г. кабель Gondwana-1 соединяет Новую Каледонию с Австралией, что обеспечивает ей максимально быструю связь. Компания Orange также планирует соединить Французскую Гвиану с Карибским бассейном.

⁶ У GAFAM имеется исторический аналог – чрезвычайно мобильная венецианская гондольерная компания, передававшая до жу информации, которой делились путешественники.

блестящим китайским и индийским специалистам, работающим в Кремниевой долине. Однако соперничество GAFAM с Китаем, который пытается помешать их дальнейшему развитию, продолжается¹. Для сохранения доминирующей позиции США должны ускорить промышленную интеграцию с Европой². В свою очередь, если Европа надеется восстановить свою цифровую независимость, она должна вкладывать в разработки в два раза больше усилий и средств. Если этого не произойдет, вынужденное заключение стратегических альянсов сделает ее не более чем цифровым вассалом.

Приход Китая к кибернетической власти как индикатор редких ресурсов. Демографический коллапс в Китае заставил набирающую силу державу сконцентрироваться на технологиях. В настоящее время Интернет в Китае имеет огромное распространение, и более половины его населения находятся онлайн с 2017 г. К примеру, 400 млн китайцев играют в онлайн-игры. Китай стремится провести четкую границу между «китайским Интернетом» и «глобальным Интернетом» и, бойкотируя многосторонние встречи, пытается освободиться от ICANN – регулирующего Интернет правового органа, базирующегося в Калифорнии. В попытке «очистить» Интернет Коммунистическая партия Китая долго искала способы взять в тиски то, что она называет информационным загрязнением и «электронным опиумом»³. В среднем китайские интернет-пользователи находятся в Сети около трех часов в день, и более половины этого времени приходится на мобильные устройства. Они пролистывают сайты и смотрят онлайн-видео в дороге, предпочитая свободу передвижения экранам телевизоров. В отношении ИИ китайцы превзошли американцев. Искусственный интеллект процветает благодаря собираемой в огромном количестве информации, что предоставляет в распоряжение Китая колоссальные объемы однородных данных, позволяя опережать США. Система «социального кредитования», присуждающая каждому граж-

¹ Есть определенное сходство между устремлениями Китая и попытками США не допустить СССР к ядерной и аэрокосмической промышленности в 1950-х годах.

² Следует отметить, что, несмотря на правовую стабильность и привлекательность, за последние 20 лет Франция не может похвастаться какими-либо инновациями из-за жестких законов о труде.

³ Интернет-зависимые люди воспринимаются одновременно как «девианты», нуждающиеся в коррекции поведения, и «нездоровые пациенты», которым требуется медицинская помощь.

данину определенное количество баллов, позволит собирать огромные объемы данных¹; она готовится к запуску в стране в 2020 г. Таким образом, существует два аналогичных режима: с одной стороны, GAFAM ворует наши данные, а с другой – китайское правительство ворует данные своих граждан. Китайцы располагают данными, но у американцев есть алгоритмы, поэтому Китаю жизненно необходимо либо воровать у американцев алгоритмы, либо привлекать самых лучших инженеров. Жесточайшая конкуренция в этой сфере оставила позади Индию, которая отвечает только за разработку существующих программ. Чтобы сохранить свою цифровую независимость, Китай ограничивает экспорт и применение своих редких металлов, поскольку они используются для производства мобильных телефонов. По мнению журналиста Гийома Питрона, специализирующегося на сырьевой геополитике, битва за редкие металлы является скрытой стороной цифровой революции. На целевых для киберколонистов территориях градус напряженности будет особенно высоким.

Основные державы, соперничающие за цифровую колонизацию Африки. Если бы процесс цифровой колонизации был смоделирован по алгоритму, она бы происходила следующим образом: сначала организовать кибератаку на телекоммуникационную сеть целевого государства и предстать его спасителем; затем подключить страну к Интернету, обеспечить безопасность ее стратегических сетей и перетянуть на свою сторону местную киберэлиту, запустив магистерскую программу обучения в сфере цифровизации; после этого украсть данные, захватить потребительский рынок и, наконец, прибегнуть к электоральному маркетингу, чтобы сохранить контроль над завоеванным рынком. Частота использования Интернета в Африке быстро растет. Только в 2018 г. в Сеть выходили 35,2% африканцев против 16% в 2012 г. Китай занял очень неординарную позицию в отношении Африки. Прежде всего, китайские компании предоставили континенту технологии по весьма конкурентоспособным ценам. Например, базирующийся в Шэньчжэне производитель электроники Huawei осуществляет свою деятельность в Африке с 1999 г. Еще в 2013 г. он заключил партнерство с Microsoft для завоевания африканского рынка смартфонов и теперь в этом секторе опережает калифорнийского гиганта. Сегодня компания Huawei стремится продавать телефоны

¹ Она основана на анкетировании, которое используют некоторые американские страховые компании.

премиум-класса африканскому среднему классу для улучшения качества обслуживания. Тем не менее существуют значительные различия между странами Северной Африки¹ и Сахельского региона².

Ближний Восток: цифровые островки и большие прибыли. На Ближнем Востоке есть два противоборствующих, но вместе с тем зеркально отражающих друг друга цифровых «островка»: Иран и Израиль. Израиль обеспечивает 7% мировой кибербезопасности. Большие инвестиции³ в эту отрасль направлены на защиту лишенной стратегического значения территории и разработку инноваций на экспорт.

6 мая 2019 г. после одной из кибератак израильские военные разбомбили здание в секторе Газа, в котором укрывались хакеры ХАМАС. Это стало предупреждением всем действующим из-за границы хакерам. Тем не менее это не мешает Израилю вербовать хакеров, которые не прочь поработать на правительство за весьма щедрую плату. На самом деле хакеров очень привлекают, а в Дубае даже провели хакерскую ярмарку! В 2016 г. для работы в этой области три бывших сотрудника израильской разведки основали ХМ Cyber. Как цифровой островок, Израиль находится в оппозиции

¹ В 2017 г. Алжиру (по оценкам, страна с наиболее низким уровнем кибербезопасности) пришлось пригласить специалистов из киберполиции для мониторинга экзаменов на степень бакалавра. Британцы, также проявляющие заинтересованность в этом перспективном рынке, в 2018 г. провели киберфорум. В 2019 г. компания Orange создала в Марокко дочернюю компанию под названием Orange Cyberdefense, специализирующуюся на кибербезопасности; она начала работу в Касабланке 16 апреля 2019 г. В рамках сотрудничества с Политехническим университетом Франции (фр. – Université Polytechnique Hauts-de-France) в Валансьене, чтобы привлечь местных специалистов и дать старт их карьере, была открыта магистерская программа в области кибербезопасности. Также французские компании уже давно присутствуют в Ливии: в 2007 г. Amesys – французская дочерняя компания Bull – продала свою программу Eagle для отслеживания противников правительства Каддафи. Сменив название на Advanced Middle East Systems, компания продала Египту аналогичную систему, известную как Cerebro.

² В Сахельском регионе практика отличается, поскольку интернет-кафе предлагают скорее более высокую скорость Интернета, чем доступ к компьютерам. Французская армия провела несколько курсов по кибербезопасности, в том числе с 29 января по 3 февраля 2018 г. в Ниамее, Нигерия, и с 10 по 13 сентября того же года в Нуакшоте, Мавритания.

³ 800 млн долл. в 2017 г.

к Ирану, стране с аналогичным уровнем технической мысли¹, но не получающей западные денежные вливания. По всей вероятности, именно Иран стоял за кибератаками на несколько британских банков в декабре 2018 г. Примененные тогда вирусы (Shamoon 1, 2 и 3) также использовались для атаки на нефтяную инфраструктуру нефтедобывающих монархий Персидского залива². Турецкие хакеры из националистической группировки Cyber-Warrior Akıncılar взламывали всех, кто, по их мнению, выступает против интересов Турции и ислама³. Ряд израильских фирм, специализирующихся на кибербезопасности, к услугам которых прибегала Саудовская Аравия, использовали свое положение для сбора данных о деятельности элиты⁴ или оппозиции⁵ в стране. Несмотря на обеспечиваемую израильскими компаниями защиту, из всех стран на Ближнем Востоке Саудовская Аравия в настоящее время наиболее часто подвергается кибератакам⁶, целью которых в большинстве случаев является кража данных из информационных систем частных и правительственных учреждений.

Рост цифрового могущества неточно отражает реальную мощь каждого государства: взлет GAFAM скрывает геополитический спад США, в то время как технологическая мощь Китая прикрывает его демографическую неустойчивость. В свою очередь, как в Африке, так и на Ближнем Востоке хакерские операции, направленные на кражу цифровых или финансовых ресурсов, обнажают слабые стороны внешне могущественных сил.

¹ Слово «алгоритм» было придумано персидским математиком аль-Хорезми в IX в.

² В некоторых случаях киберпреступность может быть альтернативой военным действиям. Так, целью иранских кибератак было ослабить давление на страну во время эмбарго.

³ Например, в 2011 г. они взломали сайт Charlie Hebdo.

⁴ В 2017 г. представители компании NSO Group Technologies, базирующейся в Герцлии, провели серию встреч в Вене и, как минимум, в одной из стран Персидского залива, в ходе которых был подписан контракт на сумму 55 млн долл. на поставку в Саудовскую Аравию известного шпионского ПО Pegasus.

⁵ Джамаль Хашогги и Омар Абдулазиз хотели создать кибероппозиционное движение.

⁶ Отсутствие должной локальной подготовки и общая неосведомленность об опасности кибератак сделали Королевство уязвимым.

Заключение

Таким образом, уровень социальной цифровизации лучше отражает реальные возможности, а не потенциальные. Среди конкурирующих экономических держав ведется жесткая борьба за Интернет, целью которой, по сути, является приватизация пространства, которое пока еще для пользователей бесплатно. Постоянная интернет-связь мгновенно поглощает данные и соединяет объекты и людей, а тех, кто отказывается подключиться к Сети, маркирует как подозрительных. В будущем государства и отдельные лица в качестве акта неповиновения будут создавать завесу неправильных данных, чтобы скрыть себя в Интернете¹. В довершение всего, цифровизация вызывает неожиданные геополитические изменения. В конечном итоге она уничтожит работу, требующую повторения одних и тех же действий, и временно сосредоточит власть в сфере инноваций, предоставив государствам и предприятиям возможность с помощью сопоставительного анализа определять лидеров общественного мнения. И наконец, цифровизация позволит военачальникам приказывать роботам, распознающим лица с помощью ИИ, уничтожать цели. Мы находимся на пороге гибридной цивилизации.

*Автор перевода с английского
на русский яз.: Атамали К.Е.*

*Статья предоставлена автором для публикации
в бюллетене «Россия и мусульманский мир»*

¹ Голосовое клонирование уже стало реальностью. Имея всего лишь одну минуту записи голоса, Lyrebird и Wave Net может воссоздать голос человека в цифровой форме и вложить в «уста» нужные слова. Аналогично Стэнфордский университет продемонстрировал технику захвата лица, с помощью которой мимика человека записывается в режиме реального времени, а компьютер мгновенно воспроизводит ее, «накладывая» на целевое лицо. Такие дипфейки могут быть использованы против отдельных людей, организаций и даже государств. Университетский колледж Лондона разработал программу My Text in Your Handwriting (рус. – Я пишу вашим почерком), способную точно воспроизвести почерк любого человека на основе образца. Говорящий робот по имени Лука, обработав диалоги из первого сезона сериала «Кремниевая долина», способен симитировать персонажей. Робот отвечает на вопросы, генерируя новые фразы на основе имеющихся моделей. Есть мнение, что в 2022 г. население развитых стран будет читать больше фейковых новостей, чем подлинной информации. Программы, автоматически генерирующие текст, изображение и аудио, могут заразить всю коммуникационную сеть человечества. Уже сейчас 8,5% Twitter-аккаунтов ведут боты.