DOI 10.31162/2618-9569-2019-12-1-95-110
УДК 94(5-011)+327(5-011)+28+004.777+004.056.53

Original Paper
Оригинальная статья

Исламский мир в условиях цифровых угроз XXI века

Г. Н. Валиахметова
Уральский федеральный университет им. первого Президента России Б. Н. Ельцина, г. Екатеринбург, Российская Федерация
e-mail: vgulnara@mail.ru

Резюме: в статье рассматриваются этапы и причины погружения исламского мира в цифровые войны и гонку кибервооружений. Носителями цифровых угроз выступают не только мусульманские государства, претендующие на региональное лидерство на Ближнем Востоке, в Южной и Юго-Восточной Азии, но также негосударственные акторы – группы высококвалифицированных хакеров, хактивисты, хакеры-одиночки, радикально-экстремистские группировки исламистского толка. Реалии цифровой эпохи значительно усиливают разнородность и противоречивость современного исламского мира. Это ставит в международную повестку дня вопрос о координации усилий всех участников мирового сообщества в деле контроля за кибервооружениями и урегулирования актуальных проблем развития мусульманских стран и сообществ.

Ключевые слова: Ближний Восток; гонка кибервооружений; история международных отношений; кибербезопасность; кибервойны; киберугрозы; мусульманские страны; хакеры

Благодарности: основные положения и выводы статьи были представлены в виде доклада на Международной научной конференции «Ислам в современном мире: вероучение и община», проводившейся 27–28 октября 2018 г. в рамках юбилейных мероприятий, посвященных 200-летию Института востоковедения РАН.

Для цитирования: Валиахметова Г. Н. Исламский мир в условиях цифровых угроз XXI века. *Minbar. Islamic Studies.* 2019;12(1):95–110. DOI: 10.31162/2618-9569-2019-12-1-95-110.

The Islamic World and Digital Threats of the 21st Century

G. N. Valiakhmetova
Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg, Russian Federation
e-mail: vgulnara@mail.ru

Abstract: the article analyzes the stages and reasons for involvement of the Islamic world in digital wars and the cyber arms race. Digital threats are carried not only by Muslim states that claim to be regional leaders in the Middle East, South and Southeast Asia, but also by non-state actors – groups of highly skilled hackers, hacktivists, «lone wolves», radical

extremist Islamist groups. The realities of the digital age significantly enhance the heterogeneity and inconsistency of the modern Islamic world. It puts on the international agenda the question of increasing global cooperation in the cyber arm control process as well as the settlement of the most pressing issues of Muslim countries and communities.

Keywords: cyber arms race; cyber security; cyber threats; cyber wars; hackers; history of international relations; Middle East; the Muslim countries

Acknowledgements: the key provisions and findings of the paper were presented at the international conference «Islam in the Modern World: Doctrine and Community», held on October 27–28, 2018 as part of anniversary events dedicated to the 200th anniversary of the Institute of Oriental Studies.

For citation: Valiakhmetova G. N. The Islamic World and Digital Threats of the 21st Century. *Minbar. Islamic Studies.* 2019;12(1):95–110. (In Russ.) DOI: 10.31162/2618-9569-2019-12-1-95-110.

Введение

Современный исламский мир формируют весьма разнородные государства и негосударственные акторы мировой политики, в том числе вне- и антисистемные. В совокупности с издержками догоняющего развития это порождает в мусульманских сообществах и за их пределами целый комплекс противоречий и конфликтов, которые зачастую воспринимаются на Западе как «исламская» угроза глобальному миропорядку. Особую актуальность проблема встраивания мусульманских стран в глобальные процессы современности приобретает в условиях «осыпающегося» мира, когда «развилка формирования эффективно функционирующего международного порядка на основе глобального управления пройдена... прежний мировой порядок уже не существует, а нового нет и пока не понятно, каким ему быть»[1]. Данный глобальный тренд ведет к очевидному сужению поля безопасности на всех уровнях жизни современного общества – от международного и национального до корпоративного и индивидуального. Весьма противоречивое воздействие на переформатирование глобальной мировой системы и ее региональных подсистем оказывает стремительное развитие информационно-коммуникационных технологий (ИКТ), усиливая взаимозависимость и уязвимость мира перед лицом традиционных и новых угроз.

Процесс накопления знаний в сфере цифровой проблематики демонстрирует много общего с процессом осмысления роли и места исламского фактора в мировой политике: относительно короткая история (с распада биполярной системы и начала цифровой революции); одновременное формирование предмета исследования и выработки подходов к его изучению; внушительная и разнообразная по характеру и направлениям историография; многочисленные научные дискуссии, которые порождают больше вопросов, чем ответов; высокая степень политизированности изучаемых проблем и, как следствие, отсутствие единого методологического инструментария, прежде всего в сфере понятийного аппарата.

[1] *Жизнь в осыпающемся мире. Доклад Международного дискуссионного клуба «Валдай»*. Октябрь, 2018. Режим доступа: http://ru.valdaiclub.com/files/22596/ [Дата обращения: 18.10.2018].

В подобных условиях сопряжение этих двух весьма противоречивых полей исследования (ИКТ и исламского фактора), как правило, превращается для исследователя в уравнение со многими неизвестными. Данный факт, однако, не снижает востребованности исследований, выполненных в рамках case-studies, которые позволяют подготовить основу для последующего общетеоретического дискурса.

Изучение влияния цифровых технологий на мусульманский мир предполагает, кроме того, объединение усилий представителей различных научных школ и направлений – исламоведов, ИТ-экспертов, международников-политологов, правоведов, специалистов в области военных наук, культурологов и т.д. Это тоже задача на долгосрочную перспективу. В данной статье предпринимается попытка в рамках междисциплинарного подхода систематизировать цифровые угрозы, с которыми сталкиваются современные мусульманские сообщества, и тем самым внести определенный вклад в осмысление проблем, связанных с адаптацией мусульманского мира к реалиям информационной эпохи.

Ближний Восток – испытательный полигон для цифровых вооружений

С Ближним Востоком, который является историко-культурным, политическим и экономическим центром мусульманского мира, связаны все крупные международные конфликты современности. Утрата управляемости международными процессами, кризис и разрушение национальных государств и идентичностей, обострение и растекание конфликтов, гуманитарные катастрофы, экспансия терроризма, повышение в мировой политике роли факторов силы и случайности – сегодня Ближний Восток не только демонстрирует эти и другие тренды глобального развития, но и сам в немалой степени генерирует их[2]. Незавершенность и противоречивость процесса переформатирования геополитического пространства Ближнего Востока в XXI в. создали благоприятные условия для превращения региона в масштабный полигон для испытаний цифровых вооружений.

Первым признаком погружения региона в новую реальность – цифровые войны[3] – стал рост политически мотивированного хакинга. Первая волна хакер-

[2] *Ближний Восток в эпоху испытаний: травмы прошлого и вызовы будущего. Доклад Международного дискуссионного клуба «Валдай»*. Август 2016. Режим доступа: http://valdaiclub.com/files/11593/ [Дата обращения: 18.10.2018].

[3] В рамках данного исследования под цифровой войной (кибервойной) понимается комплексное информационное воздействие на систему государственного и военного управления противника с одновременным обеспечением надежной защиты собственной национальной информационной инфраструктуры. Инструментом ведения такой войны является кибероружие – совокупность новейших ИКТ и средств, которые позволяют получить несанкционированный доступ к информации и возможность ее целенаправленно видоизменять (искажать, блокировать, копировать, уничтожать), взламывать системы защиты, ограничивать допуск законных пользователей, осуществлять дезинформацию, препятствовать функционированию носителей информации, технических средств, компьютерных систем и информационно-коммуникационных сетей. Кибероружие также может выступать в качестве инструмента политического давления или сдерживания, обеспечивая имеющим его государствам политические и военно-стратегические преимущества. Подробнее см.: [1].

ских атак была зафиксирована после начала «интифады Аль-Акса» (сентябрь 2000 г.), вторая – после терактов в США 11 сентября 2001 г., третья – с началом войны в Ираке (март 2003 г.). С тех пор все события, дестабилизирующие обстановку в регионе, неизменно сопровождаются кибернападениями на интернет-ресурсы участников очередного общерегионального, внутри- или межгосударственного конфликта[4]. Первоначально кибератаки приводили к нарушению работы и дефейсменту (размещению логотипов, пропагандистских лозунгов и политических протестных заявлений) сайтов противоборствующих сторон. Однако со временем хакеры стали наносить удары по объектам военной, промышленной, финансовой и транспортной инфраструктуры региона. В связи с этим власти Израиля, Турции, Ирана, Саудовской Аравии и ряда других ближневосточных стран приступили к созданию национальных киберподразделений, которые вскоре трансформировались в важный инструмент борьбы с внутренней оппозицией и проведения внешней региональной политики[5] [2]. К исходу первого десятилетия XXI в. нарастающее киберпротивостояние на Ближнем Востоке оставалось скорее угрозой региональной, нежели глобальной безопасности, а предположения о причастности глобальных игроков к боевым действиям в цифровом пространстве региона не имели доказательной базы.

Ситуация кардинально изменилась летом 2010 г., когда в ходе кибератаки на научно-исследовательский ядерный центр Ирана в Натанзе были уничтожены центрифуги по обогащению урана, что отбросило иранскую ядерную программу на годы назад. Инструментом кибернападения стал вирус нового поколения Stuxnet: после внедрения в компьютерные сети завода он действовал как шпион, собирая информацию о работе систем, а затем трансформировался в боевую программу и нанес удар – перехватил управление оборудованием и уничтожил его. По результатам многочисленных исследований инцидента эксперты сошлись во мнении о причастности к разработке Stuxnet США и Израиля, а сам вирус был отнесен к разряду нового, ранее не применявшегося, вида вооружений – кибероружия. Деструктивные возможности подобных вредоносных компьютерных программ соотносимы с оружием массового уничтожения и стратегическими наступательными вооружениями. Угроза повторения «цифровой Хиросимы» в любой точке мира стала для мирового сообще-

[4] Жертвами кибернападений неоднократно становились правительства ближневосточных стран и их внерегиональные союзники; ООН и другие международные организации, связанные с урегулированием очередного кризиса; транснациональные медиакорпорации; оппозиционные, в том числе антисистемные, группировки («Аль-Каида», ИГИЛ, «Хизбалла», ХАМАС, Рабочая партия Курдистана и т.п.).

[5] Эффективность подобных спецгрупп была продемонстрирована в сентябре 2007 г. в ходе нанесения Израилем точечного бомбового удара по военной базе в Сирии, где предположительно находился практически готовый к запуску ядерный реактор. Троянские программы, внедренные израильскими военными в сирийские компьютерные сети, позволили не только получить информацию об этом объекте, но и управлять системой противовоздушной обороны противника в ходе налета.

ISSN 2618-9569

ства первым серьезным стимулом к поиску путей создания коллективной системы международной кибербезопасности[6] [3; 4].

Предположения экспертов о том, что на Ближнем Востоке проводится масштабное тестирование цифровых вооружений, подтвердили события 2011–2012 гг. Новые образцы кибероружия были обнаружены преимущественно в компьютерных системах Ирана (вирусы Stars, Duqu, Wiper, Narilam), Саудовской Аравии и Катара (вирус Shamoon[7]); серьезный ущерб они также нанесли экономике Ливана, Израиля, Палестины, Сирии и ОАЭ; в относительно меньшей степени пострадали Турция, Египет, Ирак, Иордания, Кувейт и Бахрейн. Кроме того, в регионе были выявлены высокоточные системы кибершпионажа, явно разработанные при государственной поддержке, – Flame, Gauss, Mahdi, miniFlame и др. Примечательным был и тот факт, что новые виды вредоносного программного обеспечения (ПО) внедрялись не только в компьютерные системы правительств и корпораций: для сбора данных были задействованы такие общедоступные интернет-сервисы и приложения, как Gmail, Hotmail, Yahoo! Mail, ICQ, Skype, Google+ и Facebook. Указанный период был переломным не только по количеству инцидентов и расширению географии применения цифровых вооружений на весь Ближневосточный регион. Проблематика цифровых войн вышла за пределы конспирологических теорий и стала предметом обсуждения на международном уровне, начался процесс научного осмысления роли киберфактора в мировых политических и экономических процессах[8].

Громкие разоблачения кибершпионажа 2013 г. свидетельствовали о давней причастности ведущих держав мира к ведению цифровых войн, в которые, вслед за Ближним Востоком, постепенно были втянуты другие регионы[9].

[6] *Kaspersky Security Bulletin 2013: Развитие угроз в 2013 году*. Режим доступа: https://securelist.ru/analysis/ksb/19140/kaspersky-security-bulletin-2013-razvitie-ugroz-v-2013-godu/ [Дата обращения: 21.10.2018].

[7] Некая группировка «Cutting Sword of Justice» анонсировала атаку на нефтегазовую корпорацию «Saudi Aramco» непосредственно в день проведения (15 августа 2012 г.), мотивируя ее протестом против Саудовской монархии и возможной причастности Эр-Рияда к организации беспорядков в Сирии, на Бахрейне, в Йемене, Ливане, Египте и других арабских странах. См.: *Untitled guest*. Pastebin.com. August 15, 2012. Available at: https://pastebin.com/HqAgaQRj [Accessed 28.10.2018]. Тем не менее эксперты убеждены, что за данными операциями стояли государства, предположительно Иран или США.

[8] *Kaspersky Security Bulletin 2012: Развитие угроз в 2012 году*. Режим доступа: https://securelist.ru/analysis/ksb/167/kaspersky-security-bulletin-2012-razvitie-ugroz-v-2012-godu/ [Дата обращения: 21.10.2018].

[9] Показателен пример шпионской программы «Red October», которая с 2007 г. собирала данные и секретную информацию с сетевого оборудования, компьютеров и мобильных устройств практически во всех странах Ближнего Востока (за исключением Израиля, Египта, Сирии и Йемена), а затем была внедрена в США, России, Японии, Австралии, странах Западной Европы, Южной и Юго-Восточной Азии, Латинской Америки, Восточной и Западной Африки. Ее жертвами стали правительственные структуры и дипломатические представительства; научно-исследовательские институты, в первую очередь связанные с ядерной проблематикой; торговые и коммерческие корпорации, преимущественно энергетического профиля; аэрокосмическая отрасль; военные ведомства и компании, связанные с вооружениями.

Проступили ключевые линии киберпротивостояния на глобальном и региональных уровнях: США – Китай, США – Россия, США – Иран, Иран – Саудовская Аравия, КНДР – Республика Корея, Индия – Пакистан и т.д.[10] В 2014–2016 гг. усовершенствованные боевые вирусы, прошедшие тестирование на Ближнем Востоке, стали главным инструментом противоборства в глобальном интернет-пространстве. О стремительном «расползании» кибервооружений свидетельствовал и тот факт, что, например, вредоносные коды вирусов Stuxnet и Flame также стали применяться интернет-мошенниками для хищения платежных данных обычных пользователей[11].

Тенденция постепенного стирания рамок и размывания традиционных границ между различными типами киберугроз и видами вредоносной деятельности в цифровом пространстве четко обозначилась в 2017 г., который вошел в историю развития компьютерных программ как «год размытых границ». «Многие угрозы на поверку оказались не тем, чем представлялись поначалу: вымогатель оказался программой-вайпером, легитимное бизнес-ПО – вредоносным оружием, продвинутые кибергруппировки стали использовать простые методы, а в руки мелких злоумышленников попали высокотехнологичные инструменты, возможно, разработанные АНБ, – отмечается в отчете Лаборатории Касперского за 2017 г. – С точки зрения ландшафта киберугроз этот год принес перемены, которые поставили перед специалистами по кибербезопасности новые непростые задачи»[12].

Сегодня средства ведения цифровых войн варьируются от относительно несложных хакерских программ до вредоносного ПО, которое можно причислить к стратегическим наступательным вооружениям. Доступные вирусные программы, созданные не с разрушительными целями, могут использоваться в качестве примитивного инструмента ведения кибервойны, а вооруженные подобными средствами слабо подготовленные группы (например, онлайн-активисты) вполне способны одержать победу за счет своей массовости. Очевидно, что проблема парирования угроз, порождаемых ИКТ, выходит далеко за рамки цифровых технологий. Первым шагом к ее правильному пониманию и разработке эффективных ответов является определение четкой линии между кибернетическим оружием и неоружием. Эта тема пока остается предметом острых дискуссий [5].

Стремительное внедрение прорывных ИКТ в военно-политическую сферу привело к формированию нового, цифрового фронта противостояния между

[10] *Kaspersky Security Bulletin 2013: Развитие угроз в 2013 году*. Режим доступа: https://securelist.ru/analysis/ksb/19140/kaspersky-security-bulletin-2013-razvitie-ugroz-v-2013-godu/ [Дата обращения: 21.10.2018].

[11] *Kaspersky Security Bulletin 2015*. Режим доступа: https://securelist.ru/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_RUS.pdf [Дата обращения: 21.10.2018].

[12] *Kaspersky Security Bulletin: обзор 2017 года*. Режим доступа: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09043350/KSB_Review-of-2017_final_RU.pdf [Дата обращения: 21.10.2018].

ISSN 2618-9569

государствами. Противоречивые последствия втягивания мира в цифровые войны наглядно иллюстрирует опыт мусульманских стран и сообществ.

Гонка цифровых вооружений и мусульманские государства

В отличие от обычных вооружений, военный киберпотенциал современных государств не поддается точной качественной или количественной оценке. Согласно данным «Wall Street Journal» за 2015 г., разработкой высокоточных систем кибершпионажа и хакерских программ занимаются не менее 60 стран. Наличие киберподразделений в национальных военных и разведывательных структурах признали 29 государств, в том числе США, КНР и Иран. 63 страны используют инструменты сплошного наблюдения внутри страны (преимущественно в отношении внутренней оппозиции и повстанческих групп) и на глобальном уровне. 49 государств закупают специализированное хакерское ПО[13], причем в качестве поставщиков могут выступать частные компании. Наиболее известной в этом сегменте является итальянская компания «Hacking Team», которая продает спецслужбам различных стран свой «хакерский набор для правительственной слежки». В июле 2015 г. «Hacking Team» сама стала жертвой взлома. В результате последовавшей утечки данных стало известно, что, помимо США, Великобритании и ряда европейских государств, компания поставляла свою продукцию правительствам стран Восточной Азии, Латинской Америки и Африки. Но наиболее внушительно в клиентском списке «Hacking Team» представлен мусульманский мир: Саудовская Аравия, Турция, Египет, ОАЭ, Бахрейн, Оман, Ливан, Марокко, Судан, Нигерия, Малайзия, Азербайджан, Узбекистан, Казахстан[14].

Бесспорным лидером глобальной гонки цифровых вооружений остаются США, которые своими главными соперниками на этом поле считают КНР, Россию, Иран и КНДР[15]. Исламская Республика Иран является пока единственной мусульманской страной в составе главных участников глобальных цифровых войн. Опыт Ирана весьма поучителен. С одной стороны, это развивающееся государство в беспрецедентно короткие сроки сумело выстроить четко отлаженную систему национальной кибербезопасности, которая стала

[13] Cyberwar Ignites a New Arms Race. *The Wall Street Journal.* October 11, 2015. Available at: https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128 [Accessed 28.10.2018].

[14] Cyberwar Ignites a New Arms Race. *The Wall Street Journal.* October 11, 2015. Available at: https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128 [Accessed 28.10.2018]; Неизвестные взломали сеть поставщика шпионского ПО для правительственных спецслужб. *SecureLab*. 2015. 6 июля. Режим доступа: http://www.securitylab.ru/news/473587.php [Дата обращения: 28.10.2018].

[15] Cyberwar Ignites a New Arms Race. *The Wall Street Journal.* October 11, 2015. Available at: https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128 [Accessed 28.10.2018]; *Informational Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* Washington: The White House; May 2011. Available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf [Accessed 28.10.2018].

эффективным инструментом внутренней и внешней политики. Вместе с тем появление в цифровом пространстве нового сильного игрока способствовало усилению конфликтного потенциала и Ближнего Востока, и глобальной мировой системы в целом.

На Иран возлагается ответственность за проведение сотен громких кибератак, в том числе с использованием вредоносных программ класса цифровых вооружений. Наиболее показательными свидетельствами реальной кибермощи и намерений страны считаются нападения на «Saudi Aramco»[16] и «RasGas», а также шпионские киберкампании «Saffron Rose», «Newscaster», «Cleaver», «NewsBeef» и др. Географический и целевой размах приписываемых Ирану кибероперациий[17], а также уровень их исполнения вывели страну на четвертое место в мире по оснащенности цифровыми вооружениями[18] [6, p. 83–84]. По данным Агентства национальной безопасности США, прогресс в международных переговорах по иранской ядерной программе привел к заметному снижению боевой активности Ирана в глобальном цифровом пространстве. Тем не менее Вашингтон убежден в том, что Тегеран и в дальнейшем будет использовать кибервооружение в качестве важного элемента государственной стратегии[19].

Особую озабоченность в США вызывает расширение научно-технического сотрудничества Ирана с «оппонентами» Вашингтона и так называемыми странами-изгоями. В первую очередь речь идет о возможном усилении за счет иранских разработок военного киберпотенциала КНДР[20]. Обоснованность подобных опасений довольно сложно подтвердить или опровергнуть в силу специфики феномена ИКТ. Результаты исследований представителей различных отраслей научного знания, связанных с изучением проблем кибербезопасности (IT-аналитики, военные эксперты, политологи и т.д.), скорее в очередной раз подчеркивают разрушительные последствия «горизонтального»

[16] В ходе атаки на «Saudi Aramco» данные, хранившиеся на 75 % (порядка 35 тыс.) компьютеров компании, были стерты, а обои на рабочих столах были заменены изображением горящего флага США. Нападение не затронуло производство нефти, но потрясло компанию и представителей спецслужб, продемонстрировав широту возможностей Ирана в сфере кибертехнологий, поскольку, по сути, речь шла об использовании вредоносного ПО для физического уничтожения объектов (компьютеров).

[17] В число мишеней попали правительства, госучреждения, дипмиссии, объекты критической инфраструктуры, военная, медицинская и образовательная сферы США, Израиля и стран Ближнего Востока, а также России, ряда европейских государств, Китая, Японии, Индии и других стран Восточной и Южной Азии.

[18] *Cylance Operation Cleaver Report.* 2014. December. Available at: http://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf [Accessed 28.10.2018].

[19] Cyberwar Ignites a New Arms Race. *The Wall Street Journal.* October 11, 2015. Available at: https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128 [Accessed 28.10.2018].

[20] *Cylance Operation Cleaver Report.* 2014. December. Available at: http://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf [Accessed 28.10.2018].

ISSN 2618-9569

распространения цифровых вооружений, взаимозависимость и уязвимость современного мира.

Так, например, Лаборатория Касперского обнаружила связь между кибератаками, приписываемыми Ирану (нападение на «Saudi Aramco», 2012 г.) и КНДР (операция «Dark Seoul», Южная Корея, 2013 г. и атака на «Sony Pictures», США, 2014 г.). Во всех трех случаях использовались модификации вредоносного Shamoon, базовой платформой которого является троянская программа Wiper, предположительно разработанная в США на основе Stuxnet и Duqu[21]. В 2015–2016 гг. жертвой «мистического» троянца стала критическая инфраструктура Украины (операция «Black Energy»), а затем он вернулся на Ближний Восток в составе модифицированного зловредного Shamoon 2.0 и нового вредоносного ПО StoneDrill. В период с ноября 2016 г. по январь 2017 г. они атаковали организации, работающие в критически важных экономических секторах Саудовской Аравии и ряда других стран региона. За Shamoon и StoneDrill могут стоять как одна, так и две разные группы с совпадающими интересами и географией жертв. С точки зрения атрибуции Shamoon включает ресурсы на йеменском диалекте арабского языка, тогда как StoneDrill преимущественно базируется на персоязычных кодах[22]; эксперты также не исключают возможность установки в указанных вредоносных программах ложных лингвистических флажков[23]. В любом случае, очевидно, что в прокси-конфликте между Ираном и Саудовской Аравией используются цифровые вооружения.

Помимо Ирана и Саудовской Аравии заявка на региональное лидерство втянула в глобальную гонку кибервооружений и третьего ближневосточного «тяжеловеса» – Турцию. Активными участниками цифровых войн также являются Пакистан и Индонезия. После событий «арабской весны» нефтедобывающие монархии Персидского залива форсированными темпами стали разрабатывать системы обеспечения национальной кибербезопасности, ориентированные преимущественно на подавление интернет-активности, направленной на разжигание протестных настроений [7].

---

[21] Данный факт, однако, отнюдь не является ни безапелляционным доказательством утечки секретных военных кибертехнологий по цепочке США – Иран – Пхеньян, ни в целом причастности КНДР, Ирана и даже США к кибернападениям на Южную Корею и «Sony Pictures». Подр. см.: Асмолов К. *Северокорейские хакеры: нестрашная правда*. 2018. 3 августа. Режим доступа: http://russiancouncil.ru/analytics-and-comments/analytics/severokoreyskie-khakery-nestrashnaya-pravda/?sphrase_id=20541863 [Дата обращения: 10.10.2018].

[22] В пользу версии о том, что действуют две группировки, свидетельствует и тот факт, что StoneDrill связан с активностью обнаруженного в 2016 г. вируса NewsBeef, который предположительно разработан Ираном и продолжает атаковать организации в Саудовской Аравии. С этой точки зрения NewsBeef и StoneDrill, возможно, предназначены для длительного использования в атаках на организации в Саудовской Аравии, тогда как Shamoon является высокоэффективным инструментом кратковременного применения.

[23] От Shamoon к StoneDrill. Wiper-подобные программы атакуют компании в Саудовской Аравии и не только. *SecureList*. 2018. 6 марта. Режим доступа: https://securelist.ru/from-shamoon-to-stonedrill/30350/ [Дата обращения: 21.10.2018].

Несмотря на то что отдельные мусульманские государства активно наращивают свой киберпотенциал, в целом исламский мир демонстрирует высокую уязвимость перед лицом цифровых угроз. Так, в первой десятке Глобального индекса кибербезопасности 2017 г. представлены всего две мусульманские страны – Малайзия и Оман. Топ-10 самых защищенных стран исламского мира формируют Малайзия (3-е место в мировом рейтинге и 2-е место в рейтинге стран Азиатско-Тихоокеанского региона) и Оман (4-е место в мировом рейтинге, 1-е место в рейтингах арабского мира и Ближнего Востока), далее следуют Египет, Катар, Тунис, Турция, Саудовская Аравия, Нигерия, ОАЭ и Азербайджан (с 14 по 48 строчку мирового рейтинга). Иран, Пакистан и Индонезия, самые продвинутые среди мусульманских стран участники цифровых войн, занимают средние строки (60-е, 67-е и 70-е места соответственно), а Йемен (еще один весьма активный игрок региональных кибервойн) является практически самой незащищенной страной планеты (164-е место в Глобальном индексе кибербезопасности)[24].

Это обусловлено тем, что устойчивость государства к цифровым угрозам обеспечивается не только способностью противостоять кибератакам и наличием развитого военного и / или полицейского киберсектора. Развитие национальной критической цифровой инфраструктуры является необходимым условием функционирования продуктивной и безопасной экономики. Это предусматривает наличие таких взаимосвязанных компонентов, как отлаженная система нормативно-правового регулирования киберпространства, технологическая инфраструктура и ее применение в ключевых отраслях, широкое использование ИКТ в экономической и социальной сферах.

В целом приведенные показатели свидетельствуют о серьезных диспропорциях в развитии цифровой отрасли мусульманских стран. По сути, реалии цифровой эпохи не только подчеркивают, но и значительно усиливают разнородность и противоречивость современного исламского мира. Соответственно, киберфактор в целом и гонка кибервооружений в частности формируют качественно новые угрозы и вызовы безопасности как для мусульманских сообществ, так и на глобальном уровне. Сложность решения данной проблемы усугубляется тем, что носителями цифровых угроз все чаще выступают не только государства, но также вне- и антисистемные акторы мировой и региональной политики.

Негосударственные участники цифрового противостояния

Имеется целый комплекс факторов, сдерживающих использование национальными государствами наступательных кибервооружений, чего нельзя сказать о негосударственных игроках, довольно широко представленных в современном цифровом пространстве. Речь идет о киберкомандах, декларирующих свою независимость, но предположительно спонсируемых государством, а также хактиви-

[24] *Global Cybersecurity Index 2017*. Geneva: ITU; 2018. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [Accessed 28.10.2018].

ISSN 2618-9569

стах и хакерах-одиночках. Все они способны нанести значительный ущерб в рамках кибератак, проводимых ими по тем или иным политическим мотивам.

Наибольшее внимание экспертов привлекает деятельность «Электронной армии Ирана» (*Iranian Cyber Army*), объединяющей более 20 хакерских группировок[25] и созданной по инициативе и при финансовой поддержке Корпуса Стражей Исламской Революции (КСИР). Первоначально иранская «кибердружина» проводила показательные акции по дефейсменту недружественных Ирану сайтов зарубежных массмедиа, но затем стала стремительно наращивать свой деструктивный потенциал. Иранским хакерам приписывают такие нашумевшие инциденты, как похищение в воздушном пространстве Ирана американского беспилотника (2011), взлом сервера МАГАТЭ (2012), кибернападения на банковскую систему США (2012)[26] и ряд других[27] [6].

С ухудшением военно-политической обстановки на Ближнем Востоке связывают и появление двух других, предположительно поддерживаемых правительствами Сирии и Йемена, высокопрофессиональных хакерских групп, деятельность которых претендует на глобальный охват, – «Сирийской электронной армии» (*Syrian Electronic Army*) и «Киберармии Йемена» (*Yemen Cyber Army*). Используя такие относительно несложные методы, как атаки спама, дефейсмент, внедрение вирусов, фишинг и отказ в обслуживании, группировки нацелены на веб-ресурсы политических оппозиционных групп, западных медиа и правозащитных организаций, которые критикуют соответственно сирийский и йеменский режимы. В государственной поддержке со стороны Ирана подозреваются киберподразделения «Хизбаллы» (*Hezbollah Cyber Group*), которые базируются на территории Ливана и Палестины и используют передовые образцы вредоносного ПО для осуществления атак на объекты критической инфраструктуры Израиля[28].

В 2014 г. Лабораторией Касперского была выявлена первая арабоязычная хакерская группа «Соколы пустыни» (*Desert Falcons*), которая проводит полноценные кибершпионские операции по всей планете. На ее счету уже более 3 тыс.

---

[25] Некоторые из них сегодня уже известны: «Ashiyane», «Tarh Andishan», «Islamic Cyber Resistance Group», «Cyber Fighters of Izz ad-Din al-Qassam», «Sword of Justice», «Ajax Security Team», «Parastoo», «Shabgard», «Iran Black Hats», «Cocaine Warriors from Persia», «Cadelle», «Chafer» и др.

[26] Эти атаки оказались весьма чувствительными для высокоразвитого интернет-банкинга США. В число жертв попали ведущие банки страны – Wells Fargo, J.P. Morgan Chase, Bank of America, Citigroup и др. Хакеры на время перегружали сайты банков, прибегнув к раздражающему, но сравнительно несложному методу DoS-атак (отказ в обслуживании). Предположительно, нападение было совершено в ответ на публикацию на YouTube видео с пророком Мухаммедом. В Вашингтоне допускают, что это была месть в ответ на санкции и Stuxnet.

[27] *Cylance Operation Cleaver Report.* 2014. December. Available at: http://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf [Accessed 28.10.2018].

[28] *Cyber Terrorism: Assessment of the Threat to Insurance.* Cambridge Centre for Risk Studies, University of Cambridge Judge Business School, UK, November 2017. P. 18. Available at: https://www.poolre.co.uk/wp-content/uploads/2017/11/Pool-Re-Cyber-Terrorism-Insurance-Futures-Print-Version-19112017-1.pdf [Accessed 28.10.2018].

атак и похищение более 1 млн файлов, содержащих секретную информацию, которую можно использовать в политических целях. В состав группировки предположительно входят около 30 хакеров, которые действуют с территории Палестины, Египта и Турции. Географический охват (более 50 стран), целевые установки, высокая квалификация и используемый инструментарий свидетельствуют о наличии у «Соколов пустыни» правительственной поддержки со стороны одного из ведущих региональных игроков Ближнего Востока[29].

Спонсируемые государством кибергруппировки демонстрируют все более продвинутый уровень владения новейшими ИКТ, усиливая тем самым свою роль в асимметричных конфликтах современности. Формально независимый статус подобных групп существенно сокращает и без того невысокие шансы привлечь поддерживающие их правительства к ответственности в рамках действующей международно-правовой системы.

Хактивисты – свободно организованные кадры активистов, способных и желающих проводить хакерские атаки по политическим мотивам, – также являются участниками современных цифровых войн, развернувшихся в интернет-пространстве мусульманского мира. Как правило, подобные группы имеют сетевую структуру, ее ячейки не связаны между собой и могут формироваться для конкретной цели, выполнив которую, распадаются; они географически разбросаны, а их участники могут придерживаться диаметрально противоположных политических взглядов и идеологий. Наглядным примером подобных гетерогенных сообществ может служить международная группа анонимных активистов-хакеров «Anonymous», прославившаяся серией успешных, но противоречивых кибератак. Так, одни ее участники с происламскими убеждениями организуют масштабные DDoS-атаки на правительственные и частные сайты Израиля в рамках ежегодной киберкампании #OpIsrael. Другие активисты аналогичными методами стремятся ограничить возможности присутствия в Глобальной сети представителей радикально-экстремистских группировок исламистского толка[30].

---

[29] *Kaspersky Security Bulletin: обзор 2017 года*. Режим доступа: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09043350/KSB_Review-of-2017_final_RU.pdf [Дата обращения: 21.10.2018]; *Desert Falcons Targeted Attacks*. Kaspersky Lab Report, February 2015. Available at: http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf [Accessed 28.10.2018].

[30] Так, в ответ на серию терактов в Париже 2015 г. группа «Anonymous» в рамках объявленной ею киберкампании #OpIsis выявила 149 сайтов и 5900 пропагандистских видео, связанных с ИГИЛ, а также 101 тыс. Twitter-аккаунтов членов и сторонников этой террористической группировки. Кроме того, хакеры обнародовали список конкретных мест и учреждений во Франции, США, Индонезии, Италии и Ливане, где, согласно добытым ими данным, планировались следующие теракты ИГ. Подр. см.: Хакеры обещают киберджихад за Париж: Anonymous объявили войну «Исламскому государству». *Коммерсант.ru*. 16 ноября 2015 г. Режим доступа: http://kommersant.ru/doc/2855376 [Дата обращения: 28.10.2018]; *Cyber Terrorism: Assessment of the Threat to Insurance*. Cambridge Centre for Risk Studies, University of Cambridge Judge Business School, UK, November 2017. Available at: https://www.poolre.co.uk/wp-content/uploads/2017/11/Pool-Re-Cyber-Terrorism-Insurance-Futures-Print-Version-19112017-1.pdf [Accessed 28.10.2018].

ISSN 2618-9569

Талантливая молодежь из среды хактивистов является предметом особого внимания структур, специализирующихся на вербовке и рекрутинге боевиков для террористических организаций. Наиболее показательным является пример британского хактивиста Джунаида Хусейна, который присоединился к джихадистам и после переезда в Сирию в 2013 г., несмотря на свой юный возраст (19 лет), стал главным экспертом по кибербезопасности ИГИЛ. Он сформировал и возглавил первые киберподразделения этой террористической группировки, значительно усилил защиту ее интернет-платформ и разработал хакерские программы[31]. Под прицел исламистов попадают хакеры, дислоцирующиеся не только в странах Европы, но и в других регионах мира. Высокая хакерская активность характерна для мусульманских стран Юго-Восточной Азии, особенно Индонезии, цифровое пространство которой активно используется для сбора финансовых средств для террористической деятельности и оказания поддержки арестованным экстремистам[32].

Киберпотенциал хактивистов весьма неоднозначно оценивается экспертами по кибербезопасности. С одной стороны, имеющийся сегодня в распоряжении хакер-активистов набор технических средств и методов не представляет стратегической угрозы для объектов критической инфраструктуры. С другой стороны, коммерциализация новейших технологий будет расширять возможности проведения хактивистами более сложных атак[33]. С учетом роста полити-

[31] Джунаид Хусейн проживал в Бирмингеме и состоял в хактивистской группе «Team Poison». Он «прославился» в 2012 г. взломом личной страницы Марка Цукербергера на Facebook и почтового аккаунта действовавшего на тот момент премьер-министра Великобритании Тони Блэра (после чего сменил имя в Сети на Абу Хусейн аль-Британи). На Дж. Хусейна и созданные им кибергруппы ИГИЛ возлагается ответственность за взлом Twitter-аккаунтов Центрального командования Вооруженных сил США, что стало одной из самых громких кибероперациий исламистов. В «послужном списке» молодого хакера-джихадиста также числятся взлом официального канала YouTube, а также атаки на сайты Newsweek, International Business Times, TV5 Monde и других влиятельных американских и европейских медиаресурсов. 24 августа 2015 г. Дж. Хусейн был убит близ г. Ракка в результате целевого точечного удара американского беспилотника. Подробнее см.: Cyberwar Ignites a New Arms Race. *The Wall Street Journal*. October 11, 2015. Available at: https://www.wsj.com/articles/cyberwar-ignites-a-new-arms-race-1444611128 [Accessed 28.10.2018]; *Cyber Terrorism: Assessment of the Threat to Insurance*. Cambridge Centre for Risk Studies, University of Cambridge Judge Business School, UK, November 2017. Available at: https://www.poolre.co.uk/wp-content/uploads/2017/11/Pool-Re-Cyber-Terrorism-Insurance-Futures-Print-Version-19112017-1.pdf [Accessed 28.10.2018].

[32] *Cyber Terrorism: Assessment of the Threat to Insurance*. Cambridge Centre for Risk Studies, University of Cambridge Judge Business School, UK, November 2017. Available at: https://www.poolre.co.uk/wp-content/uploads/2017/11/Pool-Re-Cyber-Terrorism-Insurance-Futures-Print-Version-19112017-1.pdf [Accessed 28.10.2018].

[33] *Cyber Terrorism: Assessment of the Threat to Insurance*. Cambridge Centre for Risk Studies, University of Cambridge Judge Business School, UK, November 2017. Available at: https://www.poolre.co.uk/wp-content/uploads/2017/11/Pool-Re-Cyber-Terrorism-Insurance-Futures-Print-Version-19112017-1.pdf [Accessed 28.10.2018]; *Europol TE-SAT Report 2018: EUnion Terrorism Situation & Trends*. Hague, 2018. Available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 [Accessed 28.10.2018].

чески мотивированного хакинга в условиях «осыпающегося» мира можно предположить, что хактивисты будут увеличивать степень своего участия в кибервойнах, усиливая тем самым конфликтный потенциал киберфактора, его деструктивное влияние и на мировую политику, и на исламский мир.

С точки зрения оценки стратегических угроз национальной и международной кибербезопасности серьезные опасения экспертов вызывает деструктивный потенциал хакеров-одиночек, которые могут иметь передовые кибернавыки и средства проведения цифровых атак, а также желание действовать. «Одинокие волки» могут действовать индивидуально или оказывать помощь заинтересованным акторам в подготовке кибероперации; наибольшую угрозу для критической инфраструктуры представляют хакеры-инсайдеры, чьи конкретные знания и доступ к объекту нападения могут значительно усилить разрушительный эффект атаки[34]. Ответ на вопрос о причинах сотрудничества продвинутых хакеров с террористами может быть найден в рамках продолжающихся дискуссий о причинах политизации и радикализации современного ислама.

Предметом отдельного исследования является проблема конвергенции угроз международной безопасности, исходящих от ИКТ и терроризма. В контексте определения глобальной радикально-исламистской угрозы данная проблематика представлена опасениями мирового сообщества по поводу возможности приобретения экстремистами кибервооружений и их последующего применения.

Заключение

Беспрецедентное усиление уязвимости современного мира перед лицом угроз, порождаемых ИКТ, актуализирует задачу объединения усилий всех участников мирового сообщества по формированию функционального мирового порядка. Речь идет как о фундаментальном долгосрочном осмыслении проблем, связанных с милитаризацией и радикализацией интернет-пространства, так и о незамедлительных действиях по их урегулированию. Сегодня при ООН создана Рабочая группа по информационной безопасности, эксперты уже готовят основу международных соглашений по контролю за применением кибертехнологий, которые априори имеют двойное назначение и способны трансформироваться в оружие массового поражения. В этих условиях исключительную значимость приобретает политическая воля ведущих мировых держав и их готовность к многостороннему сотрудничеству. Однако пока глобальные игроки сохраняют приверженность политике двойных стандартов, призывая к прекращению эскалации насилия в цифровом пространстве, но продолжая разра-

[34] *Cyber Terrorism: Assessment of the Threat to Insurance*. Cambridge Centre for Risk Studies, University of Cambridge Judge Business School, UK, November 2017. Available at: https://www.poolre.co.uk/wp-content/uploads/2017/11/Pool-Re-Cyber-Terrorism-Insurance-Futures-Print-Version-19112017-1.pdf [Accessed 28.10.2018].

ISSN 2618-9569

батывать и применять новые виды кибервооружений. Подобная практика вовлекает в глобальные кибервойны новых системных и внесистемных акторов мировой политики, делая неизбежным дальнейшее погружение в конфликты не только мусульманских сообществ, но и всего мира.

Литература

1. Libicki M. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND; 2009. Available at: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf [Accessed 28.10.2018].

2. Clarke R. A., Knake R. *Cyber War. The Next Threat to National Security and What to Do About It*. New York: Harper Collins e-books; 2010. Available at: https://www.harpercollins.com/9780061962233/cyber-war [Accessed 28.10.2018].

3. Futter A. Nuclear Weapons in the Cyber Age: New Challenges for Security, Strategy and Stability. *Valdai Club. Valdai Paper 56*. September 2016. Available at: http://valdaiclub.com/a/valdai-papers/valdai-paper-56-nuclear-weapons-in-the-cyber-age-n/ [Accessed 28.10.2018].

4. Симоненко М. Stuxnet и ядерное обогащение режима международной информационной безопасности. *Индекс безопасности*. 2013;19(1):233–248.

5. Каберник В. В. Проблемы классификации кибероружия. *Вестник МГИМО Университета*. 2013;(2):72–78.

6. Siboni G., Kronenfeld S. Developments in Iranian Cyber Warfare 2013–2014. *Military and Strategic Affairs*. August 2014;6(2):83–104. Available at: http://www.inss.org.il/uploadImages/systemFiles/SiboniKronenfeld.pdf [Accessed 28.10.2018].

7. Хайрутдинов А. Киберполицейское государство уже реальность. *Islam Today*. 2018. 18 марта. Режим доступа: https://islam-today.ru/blogi/ajdar_xajrutdinov/kiber-policejskoe-gosudarstvo-uze-realnost/ [Дата обращения: 18.10.2018].

References

1. Libicki M. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND; 2009. Available at: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf [Accessed 28.10.2018].

2. Clarke R. A., Knake R. *Cyber War. The Next Threat to National Security and What to Do About It*. New York: Harper Collins e-books; 2010. Available at: https://www.harpercollins.com/9780061962233/cyber-war [Accessed 28.10.2018].

3. Futter A. Nuclear Weapons in the Cyber Age: New Challenges for Security, Strategy and Stability. *Valdai Club. Valdai Paper 56*. September 2016. Available at: http://valdaiclub.com/a/valdai-papers/valdai-paper-56-nuclear-weapons-in-the-cyber-age-n/ [Accessed 28.10.2018].

4. Simonenko M. Stuxnet and Nuclear Enrichment of International Information Security Regime. *Security Index*. 2013;19(1):233–248. (In Russ.)

5. Kabernik V. V. Approaches to Cyber Weapons Classification Problem. *Bulletin of MGIMO University*. 2013;(2):72–78. (In Russ.)

6. Siboni G., Kronenfeld S. Developments in Iranian Cyber Warfare 2013–2014. *Military and Strategic Affairs*. August 2014;6(2):83–104. Available at: http://www.inss.org.il/uploadImages/systemFiles/SiboniKronenfeld.pdf [Accessed 28.10.2018].

7. Khairutdinov A. The cyber-police state is already a reality. *Islam Today*. March 18, 2018. Available at: https://islam-today.ru/blogi/ajdar_xajrutdinov/kiber-policejskoe-gosudarstvo-uze-realnost/ [Accessed 18.10.2018]. (In Russ.)

Информация об авторе

Валиахметова Гульнара Ниловна, доктор исторических наук, профессор, Уральский федеральный университет им. первого Президента России Б. Н. Ельцина, г. Екатеринбург, Российская Федерация.

Information about the author

Gulnara N. Valiakhmetova, Ph. D (Hist.), Professor, Ural Federal University named after the first President of Russia B. N. Yeltsin, Yekaterinburg, Russian Federation.

Раскрытие информации о конфликте интересов

Автор заявляет об отсутствии конфликта интересов.

Conflicts of Interest Disclosure

The author declares that there is no conflict of interest.

Информация о статье

Поступила в редакцию: 25 декабря 2018 г.
Одобрена рецензентами: 30 января 2019 г.
Принята к публикации: 27 февраля 2019 г.

Article info

Received: December 25, 2018
Reviewed: January 30, 2019
Accepted: February 27, 2019

ISSN 2618-9569