Сургуладзе Вахтанг Шотович*, кандидат философских наук, ведущий методолог Компании "Р.О.С.Т.У." по стратегическому планированию.

Союз государства и бизнеса в кибервойнах США[1]

В условиях возрастающей эскалации информационной войны и нарастающего противостояния между ведущими центрами силы современного мира особую актуальность приобретают работы, посвящённые анализу современных тенденций развития указанных процессов[2]. Одной из таких работ является книга известного американского журналиста, специализирующегося на освещении деятельности спецслужб Шейна Харриса[3] "Кибервойн@: Пятый театр военных действий".

Это исследование посвящено проблематике ведения современными развитыми государствами войн в киберпространстве — пятом театре военных действий, наряду с воздушным, сухопутным, водным и космическим пространствами.

Автору удалось чрезвычайно интересно описать механику взаимоотношений между специальными и силовыми ведомствами США и их подрядчиками — Lockheed Martin, Raytheon, General Dynamics, Boeing, Northrop Grumman, Harris Corporation, Booz Allen Hamilton и др. В частности, он называет компании, которые разрабатывают программное обеспечение для американских спецслужб — Computer Associates, Net Witness и др[4]. Шейн Харрис описывает деятельность частных компаний, занимающихся как обеспечением кибербезопасности, так и ведением кибервойн. Многие из этих компаний являются активными игроками чёрного рынка уязвимостей программного обеспечения и могут как оказывать помощь в сохранении и защите данных, так и взламывать базы данных и запускать в них сетевых червей[5].

* bafing@mail.ru

[1] Рецензия на книгу: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий / Пер. с англ. М.: Альпина нон-фикшн, 2016. 390 с.

[2] См., например: *Николайчук И.А.* Политическая медиаметрия. Зарубежные СМИ и безопасность России. М.: РИСИ, 2015. 230 с.; *Николайчук И.А.* О сущности гибридной войны в контексте современной военно-политической ситуации // Проблемы национальной стратегии. № 3 (36). 2016. С. 85–104. URL: http://riss.ru/images/pdf/journal/2016/3/08.pdf (дата обращения: 24.10.2016); Кризис на Украине и крымские события 2014: практика информационной войны. 2-е изд., испр. и доп. М.: РИСИ, 2015. 628 с.; *Сургуладзе В.Ш.* Скрытые методы борьбы за идентичность. "Твёрдая", "мягкая", "умная" — будущее власти в трёх лицах силы // Проблемы национальной стратегии. № 4 (31). 2015. С. 233–240. URL: http://riss.ru/images/pdf/journal/2015/4/14_.pdf (дата обращения: 24.10.2016); *Най С.Д.* Будущее власти: Как стратегия умной силы меняет XXI век / Пер. с англ. В.Н. Верченко. М.: АСТ, 2014. 448 с.

[3] Среди других его работ см., например: *Harris, S.* The Watchers: The Rise of America's Surveillance State. New York: Penguin Press, 2010. 432 p.

[4] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 55.

[5] Сетевые черви — вредоносные программы, обладающие способностью к самостоятельному распространению через компьютерные сети. — *Прим. авт.*

Одним из ключевых, пользующихся спросом со стороны государственных спецслужб и профильных подразделений крупных корпораций продуктов этого рынка являются "уязвимости нулевого дня" — слабые места системы, не известные разработчикам программного обеспечения, при обнаружении которых в случае атаки у разработчика не останется времени для их устранения[6].

Агентство национальной безопасности США[7] скупает сведения об этих уязвимостях у обнаруживших их хакеров, а также сотрудничает с компаниями — разработчиками программного обеспечения с тем, чтобы они не раскрывали информацию о наличии таких уязвимых мест при их обнаружении, а также не сообщали пользователям о наличии в их программном обеспечении бэкдоров — специально созданных в программном продукте точек доступа[8].

По мнению автора, всплеск глобальной активности в киберпространстве привёл к тому, что в настоящее время существует обширный рынок по продаже результатов трудов хакеров, работающих в нише выявления подобных угроз. При этом на теневом рынке уязвимостей нулевого дня никто не даёт гарантий эксклюзивности получаемой информации, в связи с чем можно говорить о значительном потенциале для злоупотреблений со стороны спецслужб, которые тратят миллиарды долларов на приобретение таких данных и способствуют возникновению мыльного пузыря на рынке кибербезопасности[9].

Как доказывает автор книги, АНБ скупает уязвимости, чтобы воспользоваться ими в случае войны, когда потребуется дестабилизировать общество, материально-технические средства и инфраструктуру потенциального противника. Частные корпорации приобретают эти же уязвимости для того, чтобы ликвидировать их и улучшить свой продукт. Более того, не имея возможности отвечать на кибератаки конкурентов в легальном правовом русле, корпорации вынуждены принимать собственные меры и вести свою кибервойну, используя в ней все методы, которыми пользуются в данной сфере государственные спецслужбы, а временами предпринимать совместные с государственными органами усилия в данной сфере[10].

Киберсреда — серая зона, где сталкиваются интересы не только соперничающих государств и конкурирующих корпораций, но и государственных органов, которые, казалось бы, должны добиваться одинаковых целей. Так, вызывает интерес рассматриваемое Шейном Харрисом столкновение подходов к обеспечению анонимности информационной

---

[6] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 123–124, 156–165, 325, 359 и др.

[7] См.: National Security Agency. The National Security Agency: Missions, Authorities, Oversight and Partners. 7 p. 9 August 2013. URL: http://cryptome.org/2013/08/nsa-13-0809.pdf (дата обращения: 24.10.2016); National Security Agency. 60 Years of Defending Our Nation. 62 p. URL: https://assets.documentcloud.org/documents/726599/nsa-60th-anniversary.pdf (дата обращения: 24.10.2016).

[8] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 146–153, 275, 372 и др. См. также: *Greenberg A.* Cisco's Backdoor For Hackers. Forbes. February 3, 2010. URL: http://www.forbes.com/2010/02/03/hackers-networking-equipment-technology-security-cisco.html (дата обращения: 24.10.2016).

[9] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 196.

[10] Там же. С. 261–281.

киберсреды между Государственным департаментом США и АНБ. Внешнеполитическое ведомство Соединённых Штатов вкладывает значительные средства для обеспечения программными продуктами шифрования групп повстанцев в разных дестабилизируемых США государствах[11], в то время как АНБ тратит ресурсы на то, чтобы ослабить эффективность этого программного обеспечения и иметь доступ к любым шифруемым данным[12].

Шейн Харрис анализирует подходы к кибербезопасности, характерные для бизнеса и государственных структур, сопоставляет кибернавыки АНБ с разработками крупных корпораций и приходит к заключению, что "бóльшая часть информации АНБ устаревала к тому моменту, когда она поступала получателям"[13]. В частности, отставание АНБ выявилось при сопоставлении с системами кибербезопасности, разрабатываемыми финансовыми структурами и крупнейшими банками[14]. В этой связи в книге делается важный вывод: "Государство само никогда не справится с обеспечением… всестороннего режима безопасности"[15]. Только тесное сотрудничество с бизнесом позволяет эффективно обновлять арсенал киберсредств нападения и защиты. В отсутствие такого сотрудничества работа государственных спецслужб становится неэффективной, а зачастую выливается в прямое введение в заблуждение принимающих политические решения лиц[16].

Шейн Харрис много места уделяет описанию карьерного пути офицеров американских кибернетических подразделений. В связи с чем обращает на себя внимание часто встречающийся (или широко распространённый) в США феномен реализации принципа вращающейся двери[17] — когда сотрудники осуществляют переход с государственной службы в бизнес и обратно[18].

Автору удалось показать на конкретных примерах, как работают и взаимодействуют между собой АНБ, ЦРУ, ФБР, подразделения спецназа, элитных воинских подразделений и операторы беспилотных летательных аппаратов (БПЛА)[19]. Благодаря обилию фактов, книга Шейна Харриса является своеобразным путеводителем по спецслужбам США, хотя больше всего внимания он закономерно уделяет АНБ.

---

[11] См, например: *Клинтон Х.Р.* Тяжёлые времена / Пер. с англ. К.А. Мовчан. М.: Эксмо, 2016. 736 с.

[12] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 145–146.

[13] Там же. С. 253.

[14] Там же. С. 255–258, 286, 303–304 и др.

[15] Там же. С. 281. Ср. С. 306, 330.

[16] Там же. С. 249–250, 253 и др. См. также: *Timberg C., Rein L.* Senate cybersecurity report finds agencies often fail to take basic preventive measures // Washington Post. February 4, 2014. URL: https://www.washingtonpost.com/business/technology/senate-cybersecurity-report-finds-agencies-often-fail-to-take-basic-preventive-measures/2014/02/03/493390c2-8ab6-11e3-833c-33098f9e5267_story.html (дата обращения: 24.10.2016).

[17] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 92, 117, 127, 139, 157, 165–167, 175, 178–179, 303–304, 327, 332–333 и др. О принципе вращающейся двери см., например: *Оболенский А.В.* Бюрократия для XXI века? Модели государственной службы: Россия, США, Англия, Австралия. М.: Дело, 2002. 168 с.

[18] О вопросах подбора сотрудников См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 118–120 и др.

[19] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 51.

Шейн Харрис последовательно и достаточно подробно описывает опыт кибернетической войны США в Ираке, направленной на борьбу с компьютерными сетями иракских повстанцев, джихадистов и террористов[20], который затем ещё в большем масштабе применялся в Афганистане[21]. Автор останавливается на описании работы в полевых условиях в рамках мобильных механизированных соединений, созданных для быстрого развёртывания и вступления в бой[22], даёт интересные зарисовки будней американской армии и в то же время прослеживает динамику развития кибервойны и принятия политических решений на уровне Белого дома и руководителей ключевых государственных ведомств. Такая широта охвата рассматриваемой темы позволяет составить представление о проводимой США политике в киберпространстве в целом — от принятия решений в кабинете президента и заканчивая действиями низового разведывательного подразделения в ближневосточной пустыне. Разностороннее осмысление феномена кибервойны, показанной как с точки зрения офицеров кибернетических подразделений, так и с позиций эволюции государственных институтов и бизнеса читается на одном дыхании.

Шейн Харрис описывает увенчавшиеся успехом методы информационной борьбы на поле контрпропаганды и подрывной деятельности на форумах членов "Аль-Каиды". "За первые шесть месяцев 2008 г., — пишет автор, — было зафиксировано 28 взрывов и других нападений, организованных Аль-Каидой в Ираке, тогда как годом ранее подобных атак было около 300. Кроме того, число жертв террористов среди гражданского населения резко сократилось — от 1500 человек в 2007 г. до 125 в первой половине 2008 г."[23]

Освещены в книге и операции кибервойск США против Ирана, в частности рассматривается разрушение тысячи иранских центрифуг, которое принято связывать с результатом действия вируса Stuxnet[24].

---

[20] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 349. См. также: *Peterson D.E.* Surveillance Slips Into Cyberspace // Signal. February 2005. URL: http://www.afcea.org/content/?q=surveillance-slips-cyberspace (дата обращения: 24.10.2016); *Warrick J., Wright R.* U.S. Teams Weaken Insurgency In Iraq // The Washington Post. September 6, 2008. URL: http://www.washingtonpost.com/wp-dyn/content/article/2008/09/05/AR2008090503933.html (дата обращения: 24.10.2016); *Petraeus D.H.* How We Won in Iraq // Foreign Policy. October 29, 2013. URL: http://foreignpolicy.com/2013/10/29/how-we-won-in-iraq/ (дата обращения: 24.10.2016).

[21] См., например: *McChristal S.A.* It Takes a Network // Foreign Policy. February 22, 2011. URL: http://foreignpolicy.com/2011/02/21/it-takes-a-network/ (дата обращения: 24.10.2016); *Schmitt E., Shanker T.* Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda. New York: Times Books, 2011. 336 p.

[22] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 32, 34.

[23] Там же. С. 58–59.

[24] Там же. С. 90–91, 319, 349. См. также: *Langner R.* Stuxnet's Secret Twin. The real program to sabotage Iran's nuclear facilities was far more sophisticated than anyone realized // Foreign Policy. November 19, 2013. URL: http://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/ (дата обращения: 24.10.2016); S*anger D.E.* Obama Order Sped Up Wave of Cyberattacks Against Iran // The New York Times. June 1, 2012. URL: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 (дата обращения: 24.10.2016); *Finkle J.* Researchers say Stuxnet was deployed against Iran in 2007 // Reuters. February 26, 2013. URL: http://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226 (дата обращения: 24.10.2016).

Интерес представляют сделанные автором зарисовки характеров и анализ деятельности ключевых фигур кибернетических спецслужб США. В качестве примера можно привести усилия Джона Майкла Макконнелла по созданию киберармии[25] АНБ. Именно Макконнелл объяснял американским законодателям, что "большая часть мирового телекоммуникационного трафика проходит через кабели, маршрутизаторы и коммуникаторы, расположенные на территории страны"[26], убеждая их в том, что АНБ не должно получать разрешение на использование этого оборудования в целях шпионажа за гражданами других государств. Не менее интересной является и представленная в книге характеристика директора АНБ и главы Кибернетического командованием США[27] Кита Александера[28].

В книге явно присутствует элемент пропаганды, стиль повествования живой, восторженный, победный, не ведающий сомнений, голливудски яркий и увлекательный, скорее описательный, нежели аналитический. Однако несмотря на эти особенности, книга даёт хороший срез организационных особенностей работы американских спецслужб, высвечивает проблемы координации их работы и межведомственного взаимодействия.

Описание взаимодействия государственных структур США с частными корпорациями[29] — наиболее важная часть работы. Прежде всего здесь важно отметить систему сбора данных PRISM, благодаря которой АНБ получало от американских компаний массив электронных писем и другой информации о пользователях сети Интернет. Шейн Харрис пишет: "Первой компанией, вошедшей в программу PRISM, стала Microsoft. Это произошло 11 сентября 2007 г. Yahoo присоединилась в марте следующего года. За последующие четыре года в список программы PRISM вошли крупнейшие игроки американского бизнеса, в том числе Google, Facebook, YouTube и Apple. В октябре 2012 г. программа PRISM охватывала девять компаний. Сегодня эти компании отвечают за огромную часть трафика Интернета в Соединённых Штатах. Одна только Google генерирует четверть всего трафика, проходящего через оборудование провайдеров в Северной Америке. YouTube — это почти 20 % всего входящего трафика в Соединённых Штатах. ...Представляемый компанией сервис электронной почты также привлекает миллиарды людей по всему миру. Через три года, после того как Google вошла в программу PRISM, компания заявила, что её продукт Gmail используют 425 млн человек. В декабре 2012 г. Yahoo рассказала о 281 млн пользователей своего почтового сервиса. А в феврале 2013 г. Microsoft сообщила о 420 млн пользователей её почтовой системы Outlook. Наконец, Apple, которая

---

[25] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 81–120.

[26] Там же. С. 86. О подключении АНБ к морским кабелям, обеспечивающим телекоммуникационную связь между континентами см. там же с. 89.

[27] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 93, 108 и др.

[28] См. также: *Bamford J.* NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar // Wired. December 6, 2013. URL: https://www.wired.com/2013/06/general-keith-alexander-cyberwar/ (дата обращения: 24.10.2016).

[29] Ср.: *Сургуладзе В.Ш.* Глобальные бренды как проводники и носители "мягкой" силы // Проблемы национальной стратегии. № 3 (30). 2015. С. 163–188. URL: http://riss.ru/images/pdf/journal/2015/3/12_.pdf (дата обращения: 24.10.2016).

подключилась к программе PRISM последней в 2012 г., рассказала, что в том году она продала 250 млн своих смартфонов iPhone"[30].

Нашли в работе Шейна Харриса отражение и проблемы юридического оформления тотальной слежки АНБ. В частности, проблемы правового обеспечения взаимодействия спецслужб с частными корпорациями[31]. Так, например: "Qwest Communications категорически отказалась выполнять запросы агентства по передаче телефонных метаданных, поскольку на это не было судебного решения"[32].

Бросается в глаза, насколько большое место уделяется в книге кибернетическим угрозам США со стороны Китая[33]. Шейн Харрис пишет: "…Если американским кибервойскам когда-нибудь и придётся участвовать в войне, то они столкнутся с противником, настолько же хорошо подготовленным и имеющим численное превосходство. В течение более десяти лет действовало несколько групп хакеров из Китая. Кое-что из их первой работы можно было увидеть в 1999 г., когда американские войска непреднамеренно разбомбили китайское посольство в Югославии во время войны в Косово. Негодующие „патриотические хакеры“ взломали сайты Министерства энергетики, Министерства внутренних дел и службы национальных парков США. Хакеры убрали обычное содержимое сайтов и заменили его антиамериканским посланием: „Протестуйте против фашистских действий США! Протестуйте против зверств НАТО!“ Белый дом также подвергся массированной… атаке"[34]. Отдельно автор рассматривает инициированный, по его мнению, Государственным департаментом доклад компании Mandiant о выявленных группах китайских хакеров[35].

Столь пристальное внимание киберугрозам со стороны КНР может вызвать удивление российских читателей, привыкших к тому, что часто именно российские хакеры подвергаются преследованиям властей США,

---

[30] *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 88. См. также: *Bamford J.* URL: Connecting the Dots on PRISM, Phone Surveillance, and the NSA's Massive Spy Center // Wired. December 6, 2013. URL: https://www.wired.com/2013/06/nsa-prism-verizon-surveillance/ (дата обращения: 24.10.2016); *Greenwald G., Ackerman S.* NSA collected US email records in bulk for more than two years under Obama // The Guardian. June 27, 2013. URL: https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama (дата обращения: 24.10.2016); *Greenwald G., MacAskill E., Poitras L., Ackerman S., Rushe D.* Microsoft handed the NSA access to encrypted messages // The Guardian. July 12, 2013. URL: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (дата обращения: 24.10.2016).

[31] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. О юридических проблемах, связанных с новыми реалиями эпохи кибернетических угроз см.: С. 131, 162, 168, 185, 192–193, 202, 234, 275, 334–335 и др.

[32] *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 69.

[33] Там же. С. 99, 105–106, 112–116, 124–126, 165, 167, 173, 176, 194–195, 207, 224, 238–240, 263–266, 269–271, 288–290, 298, 302, 306–314, 354–356, 366, 370, 373–374.

[34] Там же. С. 112.

[35] Там же. С. 116, 306–314. См. также: *Gellman B., Nakashima E.* U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show // The Washington Post. August 30, 2013. URL: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html (дата обращения: 24.10.2016).

а киберугроза со стороны нашей страны стала одной из заметных тем американской президентской гонки 2016 г. Между тем России в книге Шейна Харриса уделено мало места[36]. Судя по всему, это связано с объективными причинами — как бы не была агрессивна антироссийская риторика представителей политического истеблишмента Соединённых Штатов, в реальности в качестве основной стратегической угрозы США, по-видимому, рассматривается в первую очередь Китай.

Многое из написанного Шейном Харрисом известно благодаря разоблачениям Эдварда Сноудена[37] и утечкам WikiLeaks, однако, как и следовало ожидать от книги, посвящённой теме работы спецслужб, сама постановка некоторых вопросов напоминает бой с тенью, а описание отдельных операций настолько непрозрачно и подозрительно, что вызывает мысли о том, не устраивают ли сами спецслужбы США кибернетические провокации с целью нагнетания угрозы и выбивания у Конгресса бо́льших бюджетных средств на борьбу с невидимым врагом[38].

Книга Шейна Харриса вполне может служить основой для создания справочника по хакерским группам, госструктурам и компаниям США и некоторых других стран Запада, связанным с обеспечением кибербезопасности и генерацией киберугроз[39]. Однако наиболее важным итогом его работы является сделанный автором вывод о том, что "*информационное доминирование включает в себя пропаганду, дезинформацию и компьютерные операции*"[40].

Военно-сетевой комплекс — гибридный инструмент, результат срастания государственных структур США и частного бизнеса, приведший к тому, что рыночная стоимость ведущих оборонных предприятий превышает ВВП многих стран мира, а создание оружия, транспортировка солдат и даже их питание в зоне боевых действий доверено частным подрядчикам[41]. "*Союз государства и бизнеса,* — пишет Шейн Харрис, *— сердце военно-сетевого комплекса. Именно этот союз будет определять характер киберпространства и то, как все мы будем в нём работать и жить в XXI веке*"[42].

Тесная спайка государственных структур и бизнеса — характерная особенность военно-сетевого комплекса США, которую важно учитывать, прорабатывая возможные контрмеры, направленные на предотвращение доминирования Соединённых Штатов в информационном и киберпространстве.

Ключевые слова: *информационная безопасность — кибернетическая война — АНБ — США — военно-сетевой комплекс.*

Keywords: *information security — cyberwar — NSA — USA — military network complex.*

---

[36] См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 114, 179, 258, 292.

[37] Там же. С. 123, 145, 151–152, 315–317, 320–321, 325, 352–354, 356, 358, 375.

[38] Там же. С. 231–235.

[39] Оборонному бизнесу посвящена отдельная глава. См.: *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 297–321.

[40] *Харрис, Шейн.* Кибервойн@. Пятый театр военных действий. С. 111.

[41] Там же. С. 327.

[42] Там же. С. 214.