УДК 327.821

КИТАЙСКИЕ КИБЕРУГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ США

© 2013 г. **П.А. Шариков***

Институт США и Канады РАН, Москва

Статья посвящена анализу китайских киберугроз национальной безопасности США. Автор приводит доказательства того, что в последнее время КНР проявляет наибольшую активность в киберпространстве. Эта активность носит не только экономический, но и военный характер. Такое развитие ситуации требует пересмотра ряда положений национальной стратегии Соединённых Штатов.

Ключевые слова: *информационные войны, глобализация, национальная безопасности США, китайские киберугрозы.*

В XXI веке всё большее влияние на политику США в области обеспечения национальной безопасности оказывает фактор киберугроз. С целью противодействия угрозам информационной безопасности американское политическое руководство вынуждено кардинально корректировать стратегию обеспечения национальной безопасности.

Как представляется, изменение американской стратегии в данной области происходит под влиянием двух ключевых факторов: научно-технического прогресса и трансформации системы международных отношений.

Стремительное распространение в глобальных масштабах информационной сети и внедрение информационных технологий (ИТ) во все сферы общественной жизни, с одной стороны, предоставляют значительные преимущества, но с другой – создают колоссальную уязвимость, связанную с тем, что развитие и стабильное функционирование национальной экономики напрямую зависят от работы информационной инфраструктуры. Широкое участие частного сектора в сфере ИТ не позволяет органам государственного управления обеспечить адекватный уровень информационной безопасности. Американское политическое руководство давно признало проблему информационной безопасности и призвало представителей частного сектора и гражданского общества активнее участвовать в обеспечении информационной безопасности на основе тесного взаимодействия.

Информационные технологии одновременно являются средством нападения, фактором развития и средой для взаимодействия. По мере их развития в XXI веке изменялись и инструменты нанесения урона. Так, в конце 1990-х – начале 2000-х годов основную проблему в области информационной безопасности создавали хакеры, создатели вирусов и т.д. По этой причине вопросами инфор-

* **ШАРИКОВ Павел Александрович – кандидат политических наук, руководитель Центра прикладных исследований ИСКРАН.** E-mail: pasha.sharikov@gmail.com

Работа выполнена при поддержке гранта Администрации Президента № МК-189.2013.6.

мационной безопасности на государственном уровне занимались Федеральное бюро расследований, генеральный прокурор и Министерство юстиции США. В 2000 г. генеральный прокурор США Дж. Рино в своём выступлении отмечала, что «телекоммуникации и банковские системы, станции энерго- и водоснабжения, национальная оборона и многие другие объекты инфраструктуры зависят от информационных сетей. Интернет проник в жизнь граждан как в офисе, так и дома, и, возможно, он станет самым удивительным изобретением человечества. Если правоохранительные органы не могут наказать преступников, безопасность общества и сохранность информации оказывается под угрозой. Нельзя жертвовать информационной безопасностью ради сохранности частной информации. Необходимо разработать всеобъемлющую стратегию обеспечения информационной безопасности, используя ресурсы промышленности, местных и федеральных законодательных органов, членов исполнительной власти» [9]. Таким образом, угроза информационной безопасности осознана на самом высоком государственном уровне.

Серьёзную угрозу безопасности США представляет проблема промышленного шпионажа и коммерческой разведки. Данная проблема выходит за рамки обеспечения индивидуальных пользователей, вместе с тем она создаёт угрозу конкурентоспособности американских компаний на мировом рынке.

В конце первого десятилетия XXI века киберугрозы всё в большей степени обретают стратегическое значение для национальной безопасности. Особую роль в данном случае играет использование ИТ в вооружённых силах. Если в начале века информационные технологии рассматривались в основном как фактор значительного тактического преимущества на поле боя, то к началу второго десятилетия XXI века они стали явным фактором глобальной американской военной стратегии.

Интересно проследить изменение подходов американского руководства к восприятию киберугроз на основе выступлений руководителей американского разведывательного сообщества на ежегодных слушаниях по вопросам угроз национальной безопасности в Объединённом комитете по разведке Сената США.

В 2007 г. на слушаниях вопрос кибербезопасности поднимался только в выступлении директора ФБР Р. Мюллера [21]. Вопросы кибербезопасности обсуждались в последнюю очередь, при этом основная опасность в киберпространстве, по его словам, исходила от террористов, криминальных группировок и отдельных преступников. Угрозы, которые могли представлять государственные лица даже не обсуждались.

Начиная с 2008 г. угрозы кибербезопасности уже ставились в повестку дня и освещались в выступлениях директоров национальной разведки. Основной проблемой была признана угроза американской экономической конкурентоспособности, исходящая от государств и криминальных группировок [5].

В 2009 г. новый директор разведки Д. Блэр [6] особо отметил угрозу финансовому сектору американской экономике, исходящую от террористов. Впервые была озвучена оценка разведывательного сообщества, в которой говорилось, что Россия и Китай обладают технической возможностью нанесения критического ущерба американской информационной инфраструктуре и могут собирать разведданные.

В 2010 г. Д. Блэр [7] обратил внимание на значительный рост угроз в киберпространстве, причём впервые заявил, что для противодействия угрозам необходимо международное сотрудничество.

В 2011 г. вновь назначенный директор разведки Дж. Клэппер впервые отметил военную угрозу в сфере кибербезопасности, исходящую от ряда государств. Особое внимание он уделил проблемам сбора разведданных и угрозе американской экономической конкурентоспособности [22].

В 2012 г. директор национальной разведки заявил [27], что противодействие угрозам кибербезопасности является «стратегическим интересом» американского политического руководства [27]. Российские и китайские действующие лица упоминались как ключевые источники компьютерных атак на американские компьютерные сети и похитители объектов американской интеллектуальной собственности.

На слушаниях в 2013 г. вопросы кибербезопасности были поставлены уже на первое место. Дж. Клэппер утверждал [23], что государства и негосударственные акторы используют различные инструменты кибератак для достижения своих стратегических целей. Впервые в контексте обсуждения угроз кибербезопасности поднимался вопрос управления Интернетом и глобального регулирования информационного пространства.

Киберугрозы в настоящее время воспринимаются политическим руководством Соединённых Штатов в качестве стратегической угрозы национальной безопасности. Её основным источником признана уязвимость информационно-технической инфраструктуры, которая в настоящее время используется практически всеми элементами национального хозяйства США. Под влиянием необходимости обеспечения безопасности гражданских инфраструктур пересматривается вся стратегия действий государства.

Другой фактор, под влиянием которого меняются подходы к обеспечению национальной безопасности США, – трансформация системы международных отношений. С приходом новых лиц на руководящие посты в различных странах можно говорить о завершении периода «после "холодной войны"». Большинство исследователей мировой ситуации солидарны в том, что современное поколение становится свидетелем формирования полицентричного (или многополярного) мира.

Впервые идею формирования многополярного мира сформулировал академик РАН Е.М. Примаков. В своей книге «Мир без России» он отметил: «Реальную картину сегодняшнего мира создаёт диалектика между складывающейся многополярностью и взаимозависимостью образующихся центров мировой системы» [3, с. 24].

Даже ястреб американской политики Зб. Бжезинский согласен, что однополярный мир не состоялся. Развивая теорию глобального политического пробуждения, он пишет: «В своём развитии оно (глобальное пробуждение. – *П.Ш.*) вызывает смещение центра глобального притяжения. А это, в свою очередь, в глобальном масштабе меняет расположенность центров власти оказывать серьёзное влияние на роль Америки в мире» [1, с. 177].

Биполярная система, в которой все политические решения в мире так или иначе были связаны с ключевой «осью» СССР – США, перестала существовать

с распадом Советского Союза. Вместе с тем, можно с уверенностью констатировать, что однополярный мир во главе с Соединёнными Штатами не состоялся и что нет оснований полагать, что это произойдёт в ближайшее время.

Среди ключевых тенденций развития современной системы международных отношений, авторы американского доклада «Глобальные перспективы 2030» отмечают «распространение мощи» (*power dissemination*). Иными словами, если в биполярной системе международных отношений значительная часть мощи (власти, влияния) была сосредоточена «в руках» США и СССР, то в современном мире происходит формирование новых центров силы, оказывающих всё большее относительное влияние на международную обстановку.

Одним из таких центров силы является Китайская Народная Республика. Именно КНР становится не только мощной региональной державой, но и демонстрирует беспрецедентные темпы роста по сравнению с такими традиционными мировыми лидерами международных отношений, как, например, США и Европейский Союз.

В первой половине 1990-х годов информационно-технический потенциал играл едва ли не определяющую роль в экономическом росте американской экономики. В начале XXI века можно сказать, что Китай перехватил инициативу у Соединённых Штатов и по многим показателям догнал и перегнал традиционных лидеров в области технического развития (прежде всего Японию, Германию, Великобританию и Францию).

Эта тенденция во многом определяет изменение подходов американского руководства к стратегии обеспечения национальной безопасности. Так, представители разведывательного сообщества Соединённых Штатов отмечают, в частности, что угрозы кибербезопасности, исходящие с территории КНР, представляют особую угрозу национальной безопасности Соединённых Штатов.

Китайская киберугроза

Одним из ключевых факторов экономического роста КНР в начале XXI века является динамичное развитие информационно-технического комплекса.

В табл. 1 представлен такой традиционно распространённый показатель информационного потенциала, как количество пользователей Интернетом. В таблице показана динамика развития количества китайских пользователей всемирной сети: Китай менее чем за 20 лет почти в 2 раза опередил количество американцев, пользующихся Интернетом.

На фоне общей тенденции увеличения числа пользователей Интернетом во всех странах, сегодня США уже уступают Китаю по их количеству в общемировом масштабе, которое превышает треть населения страны, что больше численности всего населения Соединённых Штатов, хотя относительное количество американцев – пользователей сети превышает две трети населения страны.

Одним из важнейших показателей информационного потенциала является количество сайтов в национальном домене. С самого начала существования Интернета, все сайты разделялись на различные категории. В начале 1990-х, когда технология Интернета только-только перестала быть одним из научно-

Таблица 1

Количество пользователей Интернета

Год	Китай, %	Россия, %	США, %	Всего пользователей в мире, млн.
1993	0,01	0,14	41,94	9,9
1995	0,13	0,49	54,95	39,3
2000	5,45	0,70	29,42	386,0
2005	10,87	2,14	19,67	1 018,3
2006	11,99	2,24	17,90	1 138,8
2007	15,43	2,58	16,55	1 353,2
2008	19,22	2,46	14,45	1 580,3
2009	21,99	2,36	12,45	1 809,5
2010	22,61	3,02	11,29	н.д.
2011	22,58	3,06	10,67	н.д.

World Bank. World Development Indicators 2012 (www.worldbank.org).

исследовательских проектов Министерства обороны США, основное количество сайтов в Интернете находилось в домене *.edu* (от *educational* – образовательный), данная тенденция хорошо видна в табл. 2. В 2005 г. их доля составляла около 20%, такое же количество сайтов находилось и в домене .com. Созданный домен «дотком» (от *commercial* – коммерческий) для коммерческих предприятий продолжает оставаться одним из наиболее популярных среди американских пользователей, даже не имеющих отношения к коммерции. Национальный американских домен .us не популярен.

Домены .com появились в начале 1990-х годов, что было связано с коммерциализацией Интернета. В то же время был создан институт управления доменными именами, который впоследствии получил название Интернет-корпорации по распределению доменных имён и адресов – ИКАНН.

Глобальное развитие Интернета в тот период было основано на том, что все страны приняли распространённый в США стандарт протокола связи и появление каждого нового домена зависело от корпорации ИКАНН.

В то же время Китай активно экспериментировал с собственными доменными именами и в 2005–2006 гг. создал собственные доменные имена: .中国 (*.china)*, .公司 (*.company)* и .网络 (*.network)* [10]. Подобные действия со стороны китайских властей представляли угрозу монополии ИКАНН на всемирное управление Интернетом. Именно этим, как представляется, была спровоцирована реформа ИКАНН в 2009 г., результатом которой стало создание механизма национальных доменов, не связанных с латиницей. В России, в частности, появился домен *.рф*, не получивший пока широкого распространения.

С определённой степенью уверенности можно говорить о «доткоме» как об американском домене. Сравнивая его с другими популярными доменами, необходимо отметить, что большой популярностью пользуются не связанные с государствами домены в зоне *.net* (*networks* – сети): они составляют почти 35% всех интернет-сайтов. Большое количество сайтов находится в японской доменной зоне *.jp* (почти 7,5%), что свидетельствует о высокой активности Японии в информационном пространстве. Важно отметить, что в абсолютных показателях количество доменов возросло. Согласно Консорциуму интернет-

систем [28], если в 1995 г. общее количество сайтов составляло менее 5 млн. единиц, то к концу 2011 г. их число выросло до 850 миллионов.

По данному показателю Китай также демонстрирует достаточно уверенные темпы роста. Важно отметить, что даже учитывая эксперименты с «китайским Интернетом», не связанным с всемирной информационной сетью, позиции Китая по этому показателю очень внушительные.

Высокая доля «доткомов», а также других сайтов, не привязанных к государственным информационным ресурсам, как представляется, является одним из подтверждений ключевой особенности современной системы международных отношений – высокой активности негосударственных участников в условиях полицентричности, а также роли информационного потенциала для повышения конкурентоспособности и обеспечения безопасности государства.

Опыт формирующихся центров силы в полицентричном мире доказывает, что развитие информационного потенциала становится приоритетом. Особенно интересным представляется опыт Соединённых Штатов, показывающий, что, даже учитывая проблемы сохранения государственного суверенитета в условиях глобализации, развития информационного пространства и полицентричности, взаимозависимость и взаимовыгодные интересы заставляют государство, бизнес и общество консолидироваться с целью развития информационного потенциала, оказывающегося в таком случае неким «общим благом».

Важно отметить, что информационно-технический комплекс включает не только показатели технического развития, но и показатели производства знаний. Необходимо обратить внимание на такой важный показатель производства знаний, как патентные заявки. Всемирный банк представляет данные по патентным заявкам, поданным резидентами и нерезидентами, работающими на территории страны. Судя по количеству поданных патентных заявок, в 1990 г. ситуация практически полностью повторяла производство высокотехнологичных товаров. Совокупная доля заявок в США, ЕС и Японии составляла почти 85% мирового уровня. Однако стоит отметить, что в Японии крайне низка доля патентных заявок, подаваемых нерезидентами. Это свидетельствует о том, что там созданы благоприятные условия для научно-исследовательской деятельности японцев, но при этом иностранные граждане сталкиваются с рядом проблем.

А в Канаде, например, доля иностранных патентозаявителей за 20 лет почти ни разу не опустилась ниже 90%, что свидетельствует, с одной стороны, о низкой патентной активности канадских граждан и, с другой – о благоприятных условиях работы в Канаде для иностранцев. При этом доля Канады в общемировом числе патентных заявок на протяжении 20 лет составляет 2–3%.

Нельзя не отметить динамику развития китайских патентных заявок. В 1990 г. доля Китая по количеству заявок в мире составляла менее 1,5%. До середины 1990-х годов даже Россия обгоняла Китай по данному показателю производства знаний, однако к концу первого десятилетия XXI века Китай занял уверенное место среди мировых лидеров по количеству патентных заявок, значительно обогнав Европейский Союз, а отставание Китая от Японии составляет менее 2%. Важно отметить, что в Китае, как и в Японии, большее количество заявок подаётся резидентами. Количество китайцев, подавших патентные заявки в 2010 г. уже в 2 раза превосходило совокупное количество заявок, поданных на территории Европейского Союза.

Таблица 2

Доля сайтов в Интернете (%)

Год / Расширение:	.net	.com	.jp	.de	.cn	.ru	.edu	.uk	.in	.mil	.gov	.us	.org	.eu
1995	4,52	26,25	2,41	5,28	0,02	0,09	21,25	4,39	0,01	3,38	4,12	1,70	3,04	0,00
2000	25,18	35,14	3,67	2,06	0,09	0,28	7,18	2,24	0,04	2,06	0,89	2,42	1,17	0,00
2004	44,66	18,72	5,77	1,65	0,06	0,30	2,86	1,46	0,05	0,56	0,28	0,82	0,53	0,00
2005	44,28	17,89	6,03	2,17	0,05	0,37	2,56	1,33	0,22	0,52	0,21	0,67	0,41	0,00
2006	42,32	17,46	6,45	2,70	0,05	0,45	2,33	1,38	0,35	0,44	0,17	0,56	0,38	0,00
2007	36,87	17,48	6,81	3,37	2,17	0,58	2,06	1,47	0,47	0,40	0,17	0,40	0,28	0,00
2008	34,50	17,76	6,99	3,96	2,51	0,84	1,90	1,45	0,47	0,39	0,18	0,32	0,22	0,01
2009	33,10	20,19	6,94	3,49	2,08	1,13	1,77	1,37	0,53	0,39	0,22	0,32	0,29	0,02
2010	35,08	19,18	7,13	2,83	1,98	1,35	1,60	0,91	0,59	0,33	0,31	0,28	0,28	0,02
2011	34,94	18,26	7,44	2,37	2,05	1,48	1,47	0,98	0,80	0,35	0,29	0,25	0,25	0,02

Расширение в названии сайта: *net* – сеть; *com* – коммерческий; *mil* – военный; *gov* – правительственный; *org* – некоммерческая организация; *edu* – образовательный. Страновая принадлежность: jp – Япония; de – ФРГ; cn – КНР; ru – РФ; eu – ЕС; uk – Великобритания; in– Индия; us – США.

Подсчитано по: http://ftp.isc.org

Данные табл. 3 дают некоторое представление об информационно-техническом потенциале современных центров силы в системе международных отношений. Более того, на основе этих данных можно судить, что в значительной степени экономический рост современных центров силы был обусловлен информационно-техническим сектором экономики. Однако следует отметить, что важнейшую роль в формировании информационного потенциала государств играет собственно общество, население, которое является основным источником спроса на информационные ресурсы, а также их основным потребителем.

Несмотря на достигнутые успехи, американское руководство обеспокоено состоянием занятости в сфере НИОКР. В 2012 г. Торговая палата США совместно с рядом коммерческих предприятий подготовила доклад [11], в котором, в частности, говорится о том, что за последние 10 лет количество занятых в сфере *STEM*, включающей науку, технологии, инженерию и математику (*STEM: Science, Technology, Engineering and Mathematics*), утроилось. Средний уровень безработицы в стране составляет 8%, а уровень безработицы в областях *STEM* составляет 3,15% для лиц с дипломами докторов наук и 3,4% с дипломами магистров. Учитывая, что, согласно официальным документам, «отсутствие безработицы» составляет 4%, можно констатировать нехватку квалифицированных кадров в областях *STEM*. А по многим специальностям в сфере *STEM* нехватка кадров наблюдается фактически.

Авторы доклада обращают внимание на то, что значительное количество занятых в *STEM*-сфере не являются американскими гражданами (26,1% докторов и 17,7% магистров – иммигранты). Для сравнения, в областях, не связанных со *STEM*-специальностями данные показатели равны соответственно 6,4% и 5,2%.

В этой связи, помощник президента объявил о реформе образования в области *STEM*-специальностей. Предложено потратить из федерального бюджета 3,1 млрд. долл. на различные федеральные программы, направленные на развитие образования в *STEM*-области. Особое беспокойство американского политического руководства вызывает тот факт, что образование по этим специальностям в американских университетах получает много китайцев, которые впоследствии не реализуют эти знания в США, а возвращаются в Китай. Данные по количеству выданных патентов китайским резидентам, представленные в табл. 3, является тому доказательством.

В феврале 2011 г., на встрече президента США с американскими лидерами в области Интернет-технологий, основатель компании «Эппл» (*Apple*) Стив Джобс отметил, что был вынужден перенести производство товаров корпорации в Китай и создать там 700 тыс. рабочих мест по той причине, что не было возможности нанять 300 тыс. инженеров в США [12].

Развитие информационно-технического комплекса КНР идёт не только за счёт закупки иностранных техники и технологий. Китайская информационная техника пользуется колоссальным спросом на мировом рынке. В табл. 4 показаны объёмы двусторонней торговли информационной техникой в 2011 году.

Китай занимает уверенную позицию лидера в экспорте информационной техники вместе с Соединёнными Штатами и Европейским Союзом. На них в совокупости приходится больше половины мировой торговли информационной техникой.

Бурный рост китайского информационного потенциала и его распрстранение в мире воспринимаются как угрозы национальной безопасности Соединённых Штатов Америки.

Одним из первых заметных сигналов грядущего противостояния США и КНР в информационном пространстве стал конфликт американской корпорации «Гугл» (*Google*) и китайского правительства в январе 2010 г. Под влиянием заметно участившихся кибератак на серверы «Гугл» в Китае, а также постоянного введения новых технических требований к работе на внутреннем китайском рынке, руководство компании «Гугл» было вынуждено заявить, что уходит с китайского рынка.

Вскоре после этого заявления «Гугл» в скандал вмешалась государственный секретарь США Хиллари Клинтон. Она выступила с жёсткой критикой в отношении китайских властей, заявив: «Американские компании, принимая деловые решения, всё чаще учитывают такой фактор, как свобода Интернета и свобода информации. Надеюсь, что на эту тенденцию обратят внимание их конкуренты и иностранные правительства. Значительный интерес в последнее время вызвала ситуация, связанная с компанией «Гугл», и мы рассчитываем, что власти КНР проведут серьёзное расследование случаев кибератак, побудивших «Гугл» выступить со своим заявлением. Мы также надеемся, что расследование и его результаты будут прозрачными» [20].

Вскоре после этого газета «Вашингтон пост» (*Washington Post*) написала, что на помощь «Гугл» в борьбе с кибератаками призывается Агентство национальной безопасности США. «В соглашении, которое должно было быть подписано, говорится, что Агентство национальной безопасности США будет помогать «Гугл» анализировать основные коммерческие атаки и попытки шпионажа, источниками которых, согласно показаниям сотрудников корпорации, были граждане Китая. Цель заключаемого соглашения – защитить «Гугл» и её пользователей от будущих атак» [18]. Официально эта информация пока не подтверждена, однако моментально последовала реакция американских правозащитников. Директор американского союза по гражданским правам (*ACLU*) Энтони Ромеро призвал всех написать письма руководству «Гугл» с просьбой «не вступать в заговор с АНБ» [26].

Не удивительно, что американское политическое руководство использует элементы «протекционизма» в отношении собственных корпораций. Однако обращает на себя внимание тот факт, что защиту компаний в сфере ИТ обеспечивают американские спецслужбы и вооружённые силы.

Ещё большее беспокойство Соединённых Штатов вызывает развитие информационно-технического потенциала китайских вооружённых сил. Очевидно, что тот ущерб американским компаниям или национальной американской инфраструктуре, который может быть нанесён хакерами-хулиганами или даже организованной группой технических специалистов, не сопоставим с тем, что может сделать специально обученное и натренированное подразделение китайской армии.

Таблица 3

Численность патентозаявителей в Китае, Японии, России, США и ЕС, 1990–2009 гг.

Год		Китай, %	Япония, %	Россия, %	США, %	ЕС, %	Весь мир, %	Весь мир, тысяч	
								резиденты	нерезиденты
1990	Резиденты	0,74	42,41	н.д.	11,55	11,02	68,97		
1990	Нерезиденты	0,55	3,54	н.д.	10,26	5,66	31,03		
1990	**Всего**	**1,29**	**45,95**	**н.д.**	**21,80**	**16,67**	**100**	**541,4**	**243,6**
1995	Резиденты	1,03	34,26	1,80	12,73	9,41	68,28		
1995	Нерезиденты	0,89	3,60	0,71	10,69	3,50	31,72		
1995	**Всего**	**1,92**	**37,86**	**2,51**	**23,42**	**12,91**	**100**	**665,1**	**309,0**
2000	Резиденты	1,99	30,21	1,84	12,96	9,35	64,79		
2000	Нерезиденты	2,09	2,78	0,70	10,31	3,66	35,21		
2000	**Всего**	**4,08**	**32,99**	**2,54**	**23,27**	**13,01**	**100**	**824,0**	**447,8**
2005	Резиденты	6,01	23,66	1,52	13,36	6,51	62,03		
2005	Нерезиденты	5,13	3,80	0,55	11,76	2,12	37,97		
2005	**Всего**	**11,14**	**27,46**	**2,07**	**25,12**	**8,63**	**100**	**964,8**	**590,7**
2009	Резиденты	13,62	17,56	1,52	13,38	6,56	63,06		
2009	Нерезиденты	5,09	3,17	0,77	13,75	1,37	36,94		
2009	**Всего**	**18,71**	**20,73**	**2,29**	**27,12**	**7,93**	**100**	**1 060,3**	**621,2**

World Bank. World Development Indicators 2012.

Таблица 4

Объёмы двустороннего экспорта информационных технологий в 2011 г., млн. долл.

	Китай	Япония	Россия	США	АСЕАН	ЕС	Весь мир
Китай	..	19 375,4	103,1	9 212,7	36 231,4	6 563,1	244 615,4
Япония	29 906,0	..	1,8	4 706,8	17 921,4	2 203,3	73 400,7
Россия	4 852,7	363,7	..	318,3	315,3	9 454,5	18 153,9
США	105 455,5	9 507,0	23,1	..	24 617,8	12 514,3	254 376,2
АСЕАН	31 354,0	13 808,3	65,5	16 865,0	50 656,0	11 038,6	169 754,4
ЕС	106 397,9	8 491,2	204,3	17 532,2	28 048,5	227 427,4	435 950,2
Весь мир	508 012,2	75 966,1	1 226,8	140 567,6	239 625,2	334 393,7	1 803 017,0

UNCTAD, UNCTADstat http://unctadstat.unctad.org

Проблема милитаризации информационного пространства давно является приоритетным направлением международного права. Различные американские источники регулярно публикуют разведданные о военном китайском потенциале в области информационных войн.

Основная дискуссия международных экспертов разворачивается вокруг вопроса о том, в какой степени можно считать информационные ресурсы частью государственного суверенитета и в какой степени можно применить международное военное право в отношении использования информационного оружия.

По этой причине киберугрозы, исходящие именно от вооружённых сил государств, воспринимаются Соединёнными Штатами как наиболее серьёзные. Согласно многочисленным оценкам американской разведки, именно китайские и российские киберугрозы являются наиболее серьёзными для национальной безопасности США.

В докладе корпорации «Нортроп Грумман» (*Northrop Grumman*), выполненном по заказу Американо-китайской комиссии по экономике и безопасности (*US-China Economic and Security Review Commission*) отмечается, в частности, что в доктринальном документе «Военно-стратегические рекомендации» для китайских вооружённых сил по долгосрочному развитию и модернизации китайской армии хотя и нет прямого указания о разработке техники и технологий информационных войн, однако ряд формулировок даёт основания полагать, что «информатизация вооружённых сил» [16] является стратегическим направлением развития китайской военной машины.

Учитывая, что экономика Китая всё в большей степени становится зависимой от информационной инфраструктуры, нет ничего удивительного в том, что китайские вооружённые силы стремятся обеспечить безопасность в киберпространстве. Но беспокойство Соединённых Штатов вызывает разработка наступательных информационных средств.

В 2010 г. в вооружённых силах КНР была создана База информационной безопасности – подразделение, отвечающее за координацию и контроль за проведением компьютерных сетевых операций.

Согласно оценке военной разведки Соединённых Штатов, возможности кибероружия могут быть востребованы китайскими вооружёнными силами в трёх

случаях: во-первых, для сбора разведданных в целях проведения компьютерных атак; во-вторых, для сдерживания действий или для нарушения процесса принятия решения посредством поражения информационно-телекоммуникационной инфраструктуры противника. В третьих, для использования кибероружия в качестве инструмента, дополняющего традиционные военные возможности КНР [4, p. 36].

Вместе с тем, все американские источники, предоставляющие информацию о китайском информационном военном потенциале, отмечают, что данная информация носит секретный характер, а детали развития китайского информационного наступательного потенциала не отражены даже в стратегических доктринальных документах.

Большой интерес представляют материалы компании «Мандиант», которая по заказу Министерства обороны США расследовала многочисленные инциденты проникновения в военные информационные сети. В докладах «Мандиант» утверждается, что компания при помощи специальных инструментов определила источник многочисленных информационных атак на сети Министерства обороны и что именно этот источник является секретным подразделением китайской армии, сотрудники которого атакуют Соединённые Штаты в киберпространстве.

Авторы доклада называют его «подразделение 61398». По оценке «Мандиант», это подразделение располагается в 12-этажном здании в Шанхае общей площадью 130663 кв. фута (более 1200 кв. м), построенном в начале 2007 г. Численность подразделения составляет от нескольких сот до нескольких тысяч человек. Компания «Чайна телеком» (*China Telecom*) предоставляет специальное оптоволоконное соединение с Интернетом. Каждый сотрудник должен быть экспертом по информационной безопасности, а также владеть английским языком [8]. Авторы доклада утверждают, что «подразделение 61398» является аналогом американского киберкомандования, созданного в 2010 году.

Учитывая вышесказанное, более чем логичными представляются появляющиеся данные о различных актах промышленного шпионажа и кражах конфиденциальной, коммерческой информации, а порой даже и государственных тайн.

В мае 2013 г. американское общество было потрясено публикацией в «Вашингтон пост», где говорилось об утечке критической информации о новейших разработках в области вооружений из десятков различных американских компаний ВПК. Среди украденных секретов оказались военные разработки региональной противоракетной обороны в Азии, Европе и Персидском заливе, система *THAAD*, системы ПРО «Патриот» и «Иджис». Кроме того, украденными оказались секреты таких критически важных технологий, как *F/A-18 Fighter Jet, the V-22 Osprey, the Black Hawk Helicopter and the Navy's new Littoral Combat Ship, the F-35 Joint Strike Fighter* [14]. «Неназванный сотрудник Министерства обороны США оценил кражу в миллиарды долларов преимущества китайской армии, заявив, что в результате произошедшей утечки КНР сэкономила 25 лет НИОКР» [14].

Противодействие китайским киберугрозам

В определённой степени деятельность в киберпространстве может осуществляться анонимно. Определить источник атаки не всегда представляется возможным. В случае с китайской киберугрозой принципиальное значение для Соединённых Штатов имеет определение источника угрозы: была ли атака инициирована негосударственными акторами или органами государственного управления.

Как представляется, в течение долгого времени Соединённые Штаты воспринимали китайские киберугрозы как негосударственные. Об этом свидетельствует тот факт, что на разных дипломатических уровнях американское руководство призывало китайские власти принять меры по обеспечению кибербезопасности и наказать виновных в атаках на США.

Однако, как представляется, в конце 2012 – начале 2013 г. риторика изменилась, американское руководство стало воспринимать китайские кибератаки как действия, выполняемые по приказу китайского военного командования.

В настоящее время ещё не понятно, какие ответные действия планируют Соединённые Штаты на китайские киберугрозы. Согласно американской информационной доктрине, США для противодействия кибератакам оставляют за собой право применять любые средства (военные, экономические, дипломатические, политические).

Так, в частности, помощник президента США по национальной безопасности Т. Донилон в марте 2013 г. в своём выступлении в Азиатском обществе Нью-Йорка заявил, что «проблема кибербезопасности стала серьёзной проблемой в двусторонних американо-китайских отношениях. США сделают всё возможное для защиты национальных сетей, критических инфраструктур и частной собственности, представляющей большую ценность. США ожидают от КНР действий в трёх направлениях: во-первых, признания приоритетности решения проблем кибербезопаности и рисков, которые возникают в результате промышленного шпионажа и экономической разведки; во-вторых, Пекин должен провести расследование кибератак на американские сети, чтобы положить конец непрекращающимся кибератакам; и, в-третьих, США рассчитывают на конструктивный диалог с китайскими властями, направленный на установление взаимовыгодных норм поведения в киберпространстве» [19].

Кроме того, как представляется, Соединённые Штаты будут максимально использовать свой информационный оборонный потенциал. В подобных случаях как раз и призвано действовать созданное в 2010 г. киберкомандование.

В целях предотвращения китайских кибератак на информационные сети органов государственного управления Соединённых Штатов в 2013 г. был принят закон, запрещающий федеральным ведомствам Соединённых Штатов приобретать информационные технику и технологии китайского производства.

В этой связи, особо следует отметить, что президент Обама в послании «О состоянии в государстве» в 2013 г. с гордостью заявил, что корпорация «Эппл» переводит производство из Китая обратно в Соединённые Штаты. Важно подчеркнуть, что смартфоны *iPhone* и планшетные компьютеры *iPad* фирмы «Эппл» широко востребованы в американских вооружённых силах.

Соединённые Штаты ведут достаточно активную внешнеполитическую деятельность, направленную на укрепление сотрудничества по вопросам кибербезопасности со своими ключевыми военно-политическими союзниками. Вопросы кибербезопасности были включены в ряд международно-правовых договоров, посвящённых коллективной безопасности, в частности, в договор АНЗЮС. В официальном совместном заявлении, подписанном 15 сентября 2011 г. министрами обороны и иностранных дел США и Австралии, говорится, что «в случае кибератак, угрожающих территориальной целостности, политической независимости или безопасности любого из государств, Австралия и Соединённые Штаты проведут совместные консультации и выработают адекватные меры по противодействию угрозе» [17].

Особый интерес в данном контексте вызывает активизация усилий в области кибербезопасности в рамках Организации Североатлантического договора. Доктринально стратегия НАТО в области кибербезопасности была закреплена в Стратегической концепции обороны и безопасности членов Североатлантического договора [24], а также в декларации, подписанной по итогам лиссабонского саммита в ноябре 2010 г. [13]. В июне 2011 г. в НАТО была принята доктрина кибербезопасности, которая широкой публике на данный момент недоступна. Кроме того, в рамках НАТО создаются административные и организационные структуры, в функции которых входит обеспечение коллективной кибербезопасности.

В середине июня 2010 г. в Таллине прошла первая международная конференция «Киберконфликт-2010», организованная НАТО. Примечательно, что именно Эстония настаивала на создании в рамках НАТО института противодействия киберугрозам после скандала, в ходе которого Россия была обвинена в организации массированных кибератак против эстонских государственных информационных систем.

Особого внимания заслуживает появившийся в марте 2013 г. документ «Таллинское пособие по международно-правовому регулированию кибервойны» [25]. Документ затрагивает самые сложные вопросы относительно использования киберинструментов в вооружённых действиях. Авторами пособия была проделана колоссальная работа по изучению норм международного права, регламентирующих использование информационной техники вооружёнными силами. Особый интерес представляет попытка интерпретировать транснациональные информационные атаки как нарушение государственного суверенитета, т.е. фактически как условие для применения пятой статьи Североатлантического договора.

Так, авторы пособия утверждают, что суверенитет государства распространяется на киберинфраструктуру, находящуюся на его территории. «Киберинфраструктура является субъектом государственного правового регулирования, и, соответственно, на все её элементы распространяется государственный суверенитет, независимо от того, находится она в частной или государственной собственности. Кибератака одного государства, направленная на поражение информационной инфраструктуры другого, определённо является нарушением суверенитета последнего» [25]. Публикация пособия спровоцировала острую дискуссию в экспертном сообществе. Можно предположить, что в военных кругах некоторых

стран активно лоббируется идея создания военно-политических коалиций для сотрудничества в области кибербезопасности.

В настоящее время пока неясным остаётся вопрос о том, насколько совпадают взгляды американского и натовского руководства относительно стратегии кибербезопасности. Очевидно, что проблемы военной политики приобретают всё большее значение среди вопросов международного регулирования информационного пространства.

В случае если мировые лидеры согласятся с тем, что кибератаки являются актом войны, в отношении Китая может быть применена пятая статья Североатлантического договора.

Заключение

В формирующемся полицентричном мире, в условиях появления в системе международных отношений различных акторов, назревает противостояние США и Китая, в том числе в такой «новой» области, как киберпространство.

Это противостояние имеет стратегическое значение и в значительной степени непредсказуемо. В отличие от сценария гонки вооружений времён «холодной войны», развитие кибервооружений предсказать труднее. Из всех существующих государственных участников международных отношений, судя по всему, именно Китай и США станут основными лидерами кибервооружений. Последствия эскалации киберконфликта также непредсказуемы.

В своей последней книге «О Китае» Генри Киссинджер отметил, что «если Соединённые Штаты будут рассматривать каждый шаг в развитии китайской военной мощи как враждебный, они быстро окажутся втянутыми в бесконечную серию споров по поводу неких тайных замыслов. Но Китай, исходя из собственной истории, должен осознавать невидимую грань между наступательными и оборонительными возможностями и видеть последствия ничем не ограниченной гонки вооружений» [2, с. 572–573]. Как представляется, классик американской дипломатии говорил, в том числе, и о перспективах гонки кибервооружений между Соединёнными Штатами и Китаем.

Конфликт США и Китая в данной области также нашёл выражение на конференции Международного союза электросвязи в Дубае в декабре 2012 г., Китай принял сторону России и подписал новый регламент по управлению Интернетом. Это вызвало серьёзную озабоченность американских властей.

И США, и Китай имеют немало союзников в киберпространстве. В этой связи особое место занимает Россия и многочисленные инициативы российских дипломатов. В частности, Россия и Китай являются участниками предложенной Российской Федерацией Конвенции по международной информационной безопасности.

Проблема отражения китайских киберугроз национальной безопасности Соединённых Штатов осложняется также и тем, что у США и Китая практически нет общих дипломатических площадок для обсуждения этих вопросов.

Фактически первая американо-китайская встреча на высшем уровне, на которой поднимались вопросы кибербезопасности, состоялась в начале июня 2013 г. в США. Президент Б. Обама начал встречу с Си Цзиньпинем с обсуж-

дения вопросов кибербезопасности в рамках американо-китайского «Стратегического диалога по экономике и безопасности». На пресс-конференции Б. Обамы, состоявшейся после встречи с китайским руководством, американский президент заявил, что была достигнута договорённость с Китаем о необходимости выработки общих подходов по вопросам кибербезопасности [18]. Президент Китая также заявил, что китайские власти обеспокоены проблемами кибербезопасности.

Список литературы

1. *Бжезинский Зб.* Ещё один шанс: три президента и кризис американской сверхдержавы. М.: Международные отношения, 2010. С. 177.
2. *Киссинджер Г.* О Китае. М.: Астрель, 2013. С. 572–573.
3. *Примаков Е.* Мир без России. К чему ведёт политическая близорукость. М.: Российская газета, 2009. С. 24.
4. Annual Report to Congress on Military and Security Developments Involving the People's Republic of China 2013. Office of the Secretary of Defense 2013. P. 36.
5. Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence 5 February 2008 J. Michael McConnell, Director of National Intelligence (http://www.intelligence.senate.gov/080205/mcconnell.pdf).
6. Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence Dennis C. Blair, Director of National Intelligence. 12.02.2009 (http://www.intelligence.senate.gov/090212/blair.pdf).
7. Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence Dennis C. Blair, Director of National Intelligence. 2.02.2010 (http://www.intelligence.senate.gov/100202/blair.pdf).
8. APT1 (Advanced Persistent Threat 1) Exposing One of China's Cyber Espionage Units. Mandiant. Report. August 2013 (www.mandiant.com).
9. Attorney General Janet Reno Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation. Stanford University Law School, California. 5.04.2000.
10. China's New Domain Names: Lost in Translation. 28.02.2006. Rebecca MacKinnon CircleID (http://www.circleid.com/posts/chinas_new_domain_names_lost_in_translation/).
11. Help Wanted: The Role of Foreign Workers in the Innovation Economy. New American Economy, Information Technology Industry Council and U.S. Chamber of Commerce. November 2012.
12. *Isaacson W.* Steve Jobs. Simon and Schuster, 2011.
13. Lisbon Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council. Lisbon. 20.11.2010.
14. *Nakashima E.* Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies // The Washington Post. 29.05.2013.
15. *Nakashima E.* Google to Enlist NSA to Help It Ward off Cyberattacks // The Washington Post. 4.02.2010 (http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057_pf.html).
16. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage Prepared for the U.S.-China Economic and Security Review

Commission by Northrop Grumman Corp. Bryan Krekel, Patton Adams, George Bakos. 7.04.2012. P. 14.

17. Panetta: Regional Defense, Cyber Highlight AUSMIN Talks by Cheryl Pellerin American Forces Press Service (http://www.defense.gov/news/newsarticle.aspx?id=65337).

18. Remarks by President Obama and President Xi Jinping of the People's Republic of China after Bilateral Meeting Sunnylands Retreat Rancho Mirage. California 8.06.2013 (http://www.whitehouse.gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-).

19. Remarks by Tom Donilon, National Security Advisor to the President: The United States and the Asia-Pacific in 2013. The Asia Society. New York, New York. 11.03.2013 (http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a).

20. Remarks on Internet Freedom; Secretary of State Hillary Rodham Clinton. The Newseum. Washington, DC. 21.01.2010 (http://www.state.gov/documents/organization/135878.pdf).

21. Robert S. Mueller, III Director Federal Bureau of Investigation before the Select Committee on Intelligence of the United States Senate. 11.01.2007 (http://www.intelligence.senate.gov/070111/mueller.pdf).

22. Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee in Intelligence. James R. Clapper, Director of National Intelligence. 19.02.2011 (http://www.intelligence.senate.gov/110216/dni.pdf).

23. Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence James R. Clapper, Director of National Intelligence. 12.03.2013 (http://www.intelligence.senate.gov/130312/clapper.pdf). 23

24. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government. Lisbon. 19.11.2010.

25. Tallinn Manual on the International Law Applicable to Cyber Warfare / Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. General Editor Michael N. Schmitt. Cambridge University Press, 2013. P. 25.

26. Tell Google not to Enter into Agreement with NSA (http://www.aclu.org/blog/national-security-technology-and-liberty/tell-google-not-enter-agreement-nsa).

27. Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee in Intelligence. James R. Clapper, Director of National Intelligence. 31.01.2012 (http://www.intelligence.senate.gov/120131/clapper.pdf).

28. http://ftp.isc.org