УДК 004.056.5(73+510)
ББК 32.973.202(7Сое+5Кит)

Дубов Дмитрий Владимирович*, заведующий отделом исследований информационного общества и информационных стратегий Национального института стратегических исследований, кандидат политических наук (Украина).

Американо-китайское соперничество в киберпространстве: новая "холодная война"

В последние 5–10 лет наблюдается настоящий бум внимания к тематике киберпространства и возможностям его использования в целях далеко не мирных.

В 90-е гг. XX столетия в отношении к глобальному киберпространству и оценкам его возможностей господствовал сугубо неопозитивистский подход, который был характерен для научной и технической мысли в целом. Интернет предлагалось воспринимать "вне ценностей и оценок" как некую научно-технологическую данность. Ныне такой сугубо технологический, политически безоценочный подход стремительно уступает место более жёстким оценкам в духе классической теории реализма и неореализма, согласно которым киберпространство рассматривается как пространство нового мирового политического соперничества.

В политическом лексиконе всё чаще появляются слова с приставками "кибер-", говорят они не столько о мирном развитии, сколько о "войне", "терроризме", "агрессии" и "атаках". И это отнюдь не случайно. Более того, становится очевидным, что возможности ведения агрессивных действий в киберпространстве осваивают всё новые государства и аффилированные с ними структуры. В частности, в 2011–2013 гг. в общественном мнении утвердилась мысль о том, что масштабные акции кибершпионажа и даже кибердиверсий из мрачных прогнозов фантастов превращаются в ту жёсткую реальность, с которой вынуждены считаться все крупные игроки на мировой политической арене.

Говоря о "киберпространстве", нельзя не отметить и сложившуюся вокруг этого термина (а также целого ряда иных) неопределённость, и в частности – в точной формулировке понятия. На сегодняшний день учёными и практиками наработано несколько подходов к проблеме "киберпространства"[1]. Задача определения того, что же такое "киберпространство", в последнее время всё чаще становится самостоятельным вопросом на международной повестке дня. В данной статье под этим термином мы будем понимать среду, созданную организованной совокупностью

* dubov@niss.gov.ua.

[1] См., например: *Дубов Д.* Підходи до формування тезаурусу у сфері кібербезпеки / Д. Дубов // Політичний менеджмент. 2010. № 4. С. 19–30.

информационных процессов на основе объединённых общими принципами и правилами информационных, телекоммуникационных и информационно-телекоммуникационных систем[2] (вне зависимости от форм собственности). Соответственно, под "кибервойной" следует понимать применение государством или группой государств специальных средств (кибервооружений) против страны (группы стран) в киберпространстве, которое направлено на нарушение стабильной работы информационных, телекоммуникационных и информационно-телекоммуникационных систем и сетей объектов критической инфраструктуры. Частью таких действий могут быть "кибердиверсии" – классические по целям диверсионные акции, однако совершаемые посредством использования киберпространства.

Серьёзная дискуссия идёт и о термине "кибервооружения". Проблема во многом заключается в том, что практически любой программный комплекс (как ядро возможных "кибервооружений") является технологией двойного назначения. В связи с этим существует объективная проблема того, как отделить обычные программные комплексы от "кибервооружений". Как варианты решения подобного вопроса – уделять большее внимание целям конкретного программного комплекса, а также разработать систему показателей их оценки. В статье предлагается понимать термин "кибервооружения" как специально созданные для противоправных целей программные комплексы, направленные на несанкционированное получение информации из информационно-телекоммуникационных сетей, а также использование таких сетей для контроля над объектами, в которых они используются, и/или нанесение вреда таким объектам.

Примечательно, что с признанием киберпространства в качестве "пятого" (после земли, воды, воздуха и космоса) пространства политического соперничества оно перешло из категорий сугубо технических (а в лучшем случае экономических) в сферу категорий геополитики, ибо противостояние в нём является либо самостоятельной частью борьбы больших государств за влияние, либо опосредованно эту борьбу отражают.

Образно говоря, современное киберпространство в политическом и геополитическом смысле становится всё больше похожим на аллегорию Платона о "пещере" и "тенях" на стене, противоположной входу. В нашем случае в киберпространстве, как на стене "пещеры", отражаются "тени" реальной геополитической борьбы государств (в отдельных случаях – и негосударственных субъектов). В то же время уникальность ситуации состоит в том, что нынешние "тени" (виртуалии) имеют возможность вполне конкретным образом взаимодействовать с реальностью, не оставаясь исключительно эфемерными конструкциями.

Говоря о связи кибербезопасности и геополитики, сложно не заметить взаимопроникновение этих тем, а также то, что в этой проблематике всё сильнее обнаруживается, с одной стороны, глобальное соперничество между США и Китаем, а с другой – формирование новой постбиполярной (с высокой долей вероятности – многополярной) модели мироустройства.

---

[2] Проект Закону про кібернетичну безпеку України // Верховна Рада України : офиц. интернет-сайт. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=47240 (дата обращения: 12.07.2013).

Вписывая тематику кибербезопасности в более широкий контекст глобальных политических процессов, сложно игнорировать тот факт, что довольно короткий период тотального американского унилатерализма, возникшего на руинах биполярной системы, был существенно скорректирован несколькими факторами.

Во-первых, ЕС при отсутствии реально сформированной и согласованной политики в отношении своего будущего стремится, тем не менее, играть более значительную роль на международной арене.

Во-вторых, восстановившись в начале нового века, Россия стала выступать в роли сначала полноценного регионального лидера, а на нынешнем этапе и как важный мировой игрок.

В-третьих, усилили своё геополитическое влияние страны, входящие в группу БРИКС. Количественный и качественный рост экономики Китая породил закономерные ожидания относительно того, что эта страна постепенно со временем станет реальным противовесом США как единственному сверхгосударству. На этом фоне КНР не просто демонстрирует стабильный рост, но и строит действительно развитое государство, которое успешно конвертирует собственные достижения в то, что в геополитической теории называют либо просто "силой", либо "национальной силой".

В-четвёртых, стремясь к мировому переустройству в своих интересах, США сделали серию неоднозначных внешнеполитических шагов (прежде всего, на Ближнем Востоке и Севере Африки).

Особое напряжение в это двустороннее соперничество вносит то обстоятельство, что Китай строит свою модель не просто вопреки так называемым "универсальным ценностям" и неолиберальным парадигмам экономического и политического развития, а осторожно продвигает собственную систему ценностей, во многом "авторскую" политическую модель. При сохранении весьма жёсткого контроля за внутренней политической жизнью страны китайское руководство демонстрирует удивительную гибкость и адаптивность, но при этом – прогнозируемость и стабильность во внешней политике. В этом контексте российский исследователь А. Ломанов отмечает: "Коллективное руководство китайского Политбюро намного более гибкое, чем режимы Ближнего Востока, которые десятилетиями возглавляются единоличными руководителями… Срок же пребывания на китайском политическом Олимпе ограничивается десятью годами… и передача власти новой команде проходит мирно и спокойно"[3].

При этом вовне не до конца ясны планы самого Китая относительно ви́дения своего геополитического будущего, своего места в нём и, соответственно, избранных им геостратегий. Если бóльшая часть 90-х гг. прошла для Китая под лозунгами Дэн Сяопина "Скрывать в темноте свои возможности" и "Не становиться лидером", то уже в начале нового века была сформулирована концепция "мягкого возвышения", ставшая основной внешнеполитической концепцией на весь период правления Ху Цзиньтао.

[3] *Ломанов А.* Флаги китайских отцов / Александр Ломанов // Россия в глобальной политике : интернет-сайт. 2011. 19 апреля. URL: http://www.globalaffairs.ru/number/Flagi-kitaiskikh-ottcov-15183 (дата обращения: 02.06.2013).

В своей основе эта концепция (сформулированная в книге Ся Липина и Цзян Сиюаня "Мирное возвышение Китая"[4]) была направлена на адаптирование идей Дэн Сяопина к текущим на тот момент геополитическим реалиям. В рамках новой концепции Китай описывается как "ответственное большое государство", которое заинтересовано в мирных внешних условиях для своего развития и способно, в свою очередь, содействовать миру в Азиатском регионе. Отсюда и ключевые тезисы: опора на собственные силы, на внутренний рынок, на трудовые и финансовые ресурсы, осуществление взаимовыгодного сотрудничества с внешним миром. Приоритет в рамках данной системы отдавался построению эффективных двусторонних отношений с США по самому широкому кругу вопросов, а с другой стороны – в рамках многосторонних отношений: Китай – Япония – США, Китай – Европа – США, Китай – "большая восьмёрка" – НАТО и Китай – РФ – США.

В первое десятилетие нового века эта концепция удачно совпадала с ви́дением руководства США того, каким образом с Китаем можно и нужно работать. Практически и поныне политика Б. Обамы базируется на представлениях, которые сложились ещё при Дж. Буше-мл., – сделать Китай "ответственным держателем акций" либерального миропорядка, объединив это с хеджированием рисков, связанных с растущим могуществом Китая[5].

Важно учесть, что всё это происходит на фоне определённой нерешительности Вашингтона в отношении Китая, поскольку там тоже идёт своеобразное переосмысление того, каким образом следует воспринимать обновлённый и постоянно меняющийся Китай. В частности, по мнению американского исследователя Р. Беттса, "Вашингтон должен определиться, считать ли Пекин угрозой, которую нужно сдерживать, или государством, с которым необходимо уживаться". И хотя, по его мнению, на сегодняшний день "малопонятный компромисс – это широко известная и иногда разумная дипломатическая стратегия, в отношении Азии это означает недооценку рисков, вызванных колебаниями и нерешительностью в тот момент, когда мощь Китая растёт, а его сдержанность – уменьшается"[6]. Об этом же говорит и украинский аналитик А. Шевчук, который отмечает, что "американская внешнеполитическая стратегия относительно КНР имеет противоречивый характер и является скорее реакцией на конкретные обстоятельства, чем составной частью общей стратегии, направленной на продвижение интересов США"[7].

---

[4] *Ся Липин, Цзян Сиюань*. Чжунго хэпин цзюэци (Мирное возвышение Китая) / Ся Липин, Цзян Сиюань // Россия в глобальной политике : интернет-сайт. 2005. 10 января. URL: http://www.globalaffairs.ru/book/n_4246 (дата обращения: 01.06.2013).

[5] *Зевелёв И.* Реализм в XXI веке / Игорь Зевелёв // Россия в глобальной политике : интернет-сайт. 2012. 23 декабря. URL: http://www.globalaffairs.ru/number/Realizm-v-XXI-veke-15792 (дата обращения: 13.05.2013).

[6] *Беттс Р.* Утраченная логика сдерживания / Ричард Беттс // Россия в глобальной политике : интернет-сайт. 2013. 1 мая. URL: http://www.globalaffairs.ru/number/Utrachennaya-logika-sderzhivaniya-15954 (дата обращения: 02.06.2013).

[7] *Шевчук О. В.* Зовнішньополітична стратегія США та РФ щодо КНР : автореф. дис. … д-ра політ. наук : 23.00.04 / О. В. Шевчук ; Ін-т світ. економіки і міжнар. відносин НАН України. Київ, 2009. 33 с.

Сам Китай сегодня точно так же находится в процессе поиска удобной для него формы этих сложных отношений с США, поскольку, с одной стороны, в своём нынешнем состоянии Китай – это уже явно нечто большее, чем региональный лидер, а с другой – официальный Пекин не хочет брать на себя те обязательства, которые, как представляется, очень хотели бы "перепоручить" ему США как второй "сверхдержаве".

В научной среде есть значительное число сторонников идеи того, что стратегическая цель Китая состоит именно в получении статуса "сверхгосударства" и закреплении биполярного мира (это, в частности, утверждает украинская исследовательница М. Грымская[8]), однако в данном случае гораздо больше смысла прислушаться к внутренним политическим и медийным дискуссиям в самом Китае. В этом плане кажется справедливым вывод Я. Ерёмина, полагающего, что тотальный вызов США не отвечает планам Китая. Часто подчёркивается, что "не нужно вести с Америкой борьбу за мировую гегемонию. Долгосрочным государственным курсом является то, что Китай не станет сверхгосударством. Однако в то же время не стоит и соглашаться с американской гегемонией, подстраиваться под неё"[9].

По нашему мнению, наиболее рациональным объяснением сегодняшнего состояния геополитических отношений между США и КНР является точка зрения китайских экспертов: "Хотя между Пекином и Вашингтоном существуют серьёзные противоречия, они не превратились в соперников, могут и должны наращивать сотрудничество. Расширение западных военных союзов не означает их нацеленность на развязывание агрессивных войн. Вместе с тем сложно не признать, что к происходящим процессам не следует относиться слишком спокойно, рассчитывая на нестабильность НАТО и американо-японского союза, на то, что они сами по себе станут слабыми"[10]. Схожее мнение высказывают и другие эксперты: "В своей стратегии Пекин старается всемерно уйти от лобового противостояния с США. Тут он следует методам классической китайской дипломатии – уступать стратегическую инициативу в обмен на привлекательное промежуточное положение, которое предусматривает балансирование между основными носителями противоречий"[11].

Своеобразное резюме вышеприведённых подходов к американо-китайским отношениям даёт бывший руководитель Госдепартамента США

---

[8] *Гримська М. І.* Еволюція зовнішньої політики КНР в умовах реалізації стратегії "чотирьох модернізацій" : автореф. дис. … канд. політ. наук : 23.00.04 / М. І. Гримська ; Київ. нац. ун-т ім. Т. Шевченка, Ін-т міжнар. відносин. Київ, 2009. 16 с.

[9] *Ерёмин Я. И.* Роль и место США во внешнеполитической стратегии Китая: политологический анализ / Ерёмин Ярослав Игоревич // DisserCat – электронная библиотека диссертаций : интернет-сайт. URL: http://www.dissercat.com/content/rol-i-mesto-ssha-vo-vneshnepoliticheskoi-strategii-kitaya-politologicheskii-analiz (дата обращения: 21.03.2013).

[10] Цит. по: *Ерёмин Я. И.* Указ. соч.

[11] *Жданова Н. А.* Стратегия расширения геополитического влияния КНР на рубеже XX–XXI веков / Жданова Наталья Александровна // DisserCat – электронная библиотека диссертаций : интернет-сайт. URL: http://www.dissercat.com/content/strategiya-rasshireniya-geopoliticheskogo-vliyaniya-knr-na-rubezhe-xx-xxi-vekov (дата обращения: 23.01.2013).

Г. Киссинджер: "Обе стороны должны быть готовы воспринимать деятельность друг друга как естественную часть международной жизни, а не повод для беспокойства. ***Китаю и США не обязательно удастся выйти за границы обычного процесса соперничества великих государств*** **[Выд. авт.]**. Однако ради самих себя и мира они должны по крайней мере попробовать это сделать"[12].

Следует заметить, что поведение обоих государств в киберпространстве выразительно указывает на то, что стратегии "соперничества" и "противостояния" США и КНР пребывают ныне на весьма тонкой грани, когда первое ("соперничество") легко может превратится во второе ("противостояние"). Однако в условиях объективной невозможности (вследствие как глобализационных процессов, так и текущей международной ситуации) разрешить это противоречие лобовым столкновением в духе войн традиционного типа стороны медленно, но верно движутся к состоянию, которое можно обозначить как "холодная война 2.0". Причём "2.0" означает не только своеобразный порядковый номер, но отсылает к её ключевой характеристике – пространству, где эта война будет разворачиваться, – киберпространству.

И действительно, многое в характеристиках современного противостояния в киберпространстве США – КНР и классической "холодной войны" между США и СССР роднит их. Прежде всего речь идёт о латентных обострениях на международной арене и непрямых методах борьбы: об активизации с обеих сторон разведывательно-подрывной деятельности, вынесении конфликтов на территории третьих стран (в нашем случае – в киберпространство) и, конечно, гонке кибервооружений.

То, что складывающаяся ситуация похожа на "холодную войну" "первого типа", подметили многие политологи и аналитики. В частности, президент Eurasia Group Я. Бремор констатирует: "Ситуация всё больше похожа на новую "холодную войну"[13]. При этом киберпространство вносит в логику противостояния США – КНР существенные коррективы, позволяя реализовывать элементы "холодной войны" в несколько иных нетрадиционных формах, а также войны "не по правилам" (*unconventional warfare & irregular warfare*). Так, кибершпионаж в условиях максимального насыщения общества информационными технологиями становится едва ли не более эффективным, чем традиционный. И действительно, с ростом числа систем, которые оперируют всё бóльшим количеством чувствительной информации, растёт число разведывательных групп и разведсетей в разных странах мира, нацеленных на сбор информации именно этого типа. При этом кибершпионаж оказывается для обеих сторон в таких условиях едва ли не самой оптимальной альтернативой, позволяя поддерживать глобальное геополитическое *статус-кво* при сохранении жёсткого противостояния в отдельно взятом "пространстве".

---

[12] *Киссинджер Г.* Будущее американо-китайских отношений / Генри Киссинджер // Россия в глобальной политике : интернет-сайт. 2012. 3 мая. URL: http://www.globalaffairs.ru/number/Buduschee-amerikano-kitaiskikh-otnoshenii-15533 (дата обращения: 12.06.2013).

[13] What if there was a Cold War between the U.S. and China? // Time : website. 2012. November 28. URL: http://world.time.com/2012/11/28/what-if-there-was-a-cold-war-between-the-u-s-and-china/ (дата обращения: 06.03.2013).

Именно то, что можно назвать кибершпионажем (т.е. передача или сбор с целью передачи посредством киберпространства иностранному государству, иностранной организации или их представителям информации с ограниченным доступом), всё чаще становится предметом взаимных обвинений США и Китая. Достаточно условно начало активной фазы взаимных конфликтов можно отнести к 2009–2010 гг. В то же время первые серьёзные разведывательные акции в киберпространстве, приписываемые китайским военным, относятся ещё к 2006–2007 гг., когда им как минимум несколько раз удавалось проникать в компьютерные сети Пентагона[14], взламывать электронную почту его сотрудников и похищать чертежи новейших разработок. В 2008 г. три американские нефтедобывающие компании стали жертвой продуманной атаки, в результате которой атакующим удалось завладеть важной коммерческой информацией (в том числе результатами разведки территорий, стратегиями развития компаний и иной информацией)[15]. Из последних заметных акций, приписываемых китайским специалистам, можно назвать взлом "Национального реестра дамб" в 2013 г.[16] – базы данных, содержащей информацию о 79 тыс. дамб на территории США, которую ведёт Инженерный корпус армии США. Особенность этой базы данных в том, что в ней указаны слабые места сооружений, дана прогнозная оценка числа жертв в случае прорыва и многое другое.

Несмотря на активную критику и обвинения в адрес китайских специалистов со стороны Вашингтона за акты шпионских кибератак, сами США тоже используют подобные инструменты против компьютерных сетей Китая. По данным разоблачительных заявлений бывшего сотрудника ЦРУ Э. Сноудена[17], Агентство национальной безопасности США ежедневно осуществляет достаточно массированные атаки на компьютеры и серверы, расположенные в Китае.

Надо сказать, что преступления в киберпространстве в высшей степени латентны по двум основным причинам: во-первых, сами жертвы атак далеко не всегда быстро узнают про нападения (например, про взлом упомянутого "Национального реестра дамб" стало известно только через 3 месяца), а во-вторых, даже когда про атаку известно, далеко не всегда предприятия и ведомства хотят раскрывать этот факт. Можно предположить, что значительная часть атак регистрируется, но не публикуется. В том числе и чтобы не демонстрировать степень уязвимости своих систем перед подобными атаками.

---

[14] Китайцы взломали Пентагон // Information Security. Информационная безопасность : интернет-сайт. 2007. 4 сентября. URL: http://www.itsec.ru/newstext.php?news_id=34060 (дата обращения: 09.05.2013).

[15] *Clayton M.* US oil industry hit by cyberattacks: Was China involved? / Mark Clayton // The Christian Science Monitor : website. 2010. January 25. URL: http://www.csmonitor.com/USA/2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved (дата обращения: 08.05.2013).

[16] Взломан Национальный реестр плотин США // SecurityLab : интернет-сайт. 2013. 6 мая. URL: http://www.securitylab.ru/news/440120.php (дата обращения: 02.06.2013).

[17] *Te-Ping Chen.* Snowden alleges U.S. hacking in China / Te-Ping Chen // The Wall Street Journal : website. 2013. June 23. URL: http://online.wsj.com/article/SB10001424127887324577904578562483284884530.html (дата обращения: 02.07.2013).

Другой важной особенностью киберпространства является возможность влиять с его помощью на вполне конкретные реальные объекты на территории других стран, включая проведение там всевозможных диверсий. И хотя призывы "обеспечить безопасность критически важных объектов от кибератак" становятся всё более громкими, в действительности все субъекты переговорного процесса (как политические, так и экономические) не готовы решать эту проблему на международно-правовом уровне. Что, кстати, показали и те дискуссии, которые начались в 2011 г. и продолжаются по сей день вокруг нескольких важных инициатив относительно будущего киберпространства. Речь идёт прежде всего о "Международной стратегии для киберпространства" США, проекте конвенции "О международной информационной безопасности" РФ, а также проекте "Правил поведения в области обеспечения международной информационной безопасности" – совместного документа РФ, Китая, Таджикистана и Узбекистана.

Между тем угроза применения настоящих кибервооружений становится всё более реальной, что показала сначала активность боевых вирусов "Stuxnet", а затем "Wiper". И именно отсутствие международного правового регулирования (особенно в части использования кибервооружений) делает возможным дальнейшее применение боевых вирусов и других типов кибервооружений.

Однако здесь следует уточнить, что на сегодняшний день термин "кибервойна" в международном дискурсе используется всё же по большей части в публицистическом ключе, причём как обозревателями, так и политиками. И обусловлено это, в первую очередь, тем, что сам термин по-прежнему официально не закреплён в международном праве, а во-вторых – существуют определённые сугубо технические сложности доказательства того, что та или иная атака была организована именно "государством", т.е. однозначно структурами государственными: вооружёнными силами, специальными подразделениями и т.п. В целом следует понимать, что современные разговоры о кибервойнах чаще всего имеют в виду систематическое использование киберпространства и соответствующего инструментария (прежде всего, программного) для достижения целей, которые могут быть сравнимы по своим последствиям с действиями, направленными против объектов той или иной страны в ходе войны.

Конечно, этот нюанс делает любые дискуссии о "кибервойнах" достаточно расплывчатыми, однако вероятность того, что в обозримом будущем более точное определение для этого понятия будет найдено, довольно высока, что подтверждают и исследования зарубежных специалистов, например под руководством М. Шмидта – соавтора книги "Таллиннское руководство по международному законодательству относительно кибервойны"[18].

Несмотря на вышеприведённые уточнения, можно с уверенностью предполагать, что новая "холодная война", которая уже во многом является реальностью, будет не менее жёсткой, чем предыдущая. Причём если во время противостояния США – СССР были хотя бы попытки взаимного сдерживания или разоружения, то латентный характер создания

[18] The Tallinn Manual // NATO Cooperative Cyber Defence Centre of Excellence : website. URL: http://www.ccdcoe.org/249.html (дата обращения: 01.07.2013).

кибервооружений делает этот механизм либо абсолютно невозможным, либо весьма затруднительным.

Похожие мысли относительно новой "холодной войны" в контексте роста роли киберпространства высказывают многие исследователи сферы международных отношений. Так, Д. Роткопф, главный редактор "The Foreign Policy" называет новый тип противостояния между США и КНР "прохладной войной" (*Cool War*) и прежде всего из-за технологий, которые используются. "Технологии "холодной войны" делали противостояние почти невозможным, технологии "прохладной войны" делают его неотразимым (*irresistible*)", ведь если "цель "холодной войны" была в том, чтобы получить преимущество, которое станет полезным в случае перехода в стадию "горячей" или полностью предотвратит её, эту стадию, то цель "прохладной войны" в ином – в получении возможности нанести удар, не вызывая состояния "горячей" войны"[19].

Следует отметить, что Д. Роткопф не случайно использует именно слово *cool* для обозначения новой войны, поскольку в английском языке оно несёт двойную нагрузку – может означать как "прохладу", так и "крутость". Объясняя такую двойную природу нового типа войны, исследователь называет две причины. С одной стороны, новое противостояние действительно "прохладное", поскольку явно "теплее", нежели классическая "холодная война". Однако при этом стороны едва ли не всё время втянуты в наступательные действия, которые, хотя далеки от того, что можно назвать войной, тем не менее направлены на то, чтобы нанести урон или ослабить конкурента путём нарушения его суверенитета. С другой стороны, эта война действительно "крутая", поскольку втянутые в неё передовые технологии и её медиасопровождение создают ощущение захватывающего действа, доступного не простым смертным, а избранным. И эти же технологии меняют саму парадигму конфликта сильнее, чем любой из тех, кто принимал участие в "холодной войне", которая была, что бы там ни говорили, "старомодной геополитической борьбой за ожидаемые преимущества в случае ведения такой же старомодной потенциальной тотальной войны".

Более того, особенностью новой войны является то, что, несмотря на в принципе похожие методы противостояния, к которым относится прежде всего разведывательная и контрразведывательная деятельность, становится маловероятным разрыв двусторонних отношений даже в случае выявления кибершпионов, что было постоянной угрозой во время "холодной войны". И все взаимные "последние предупреждения" здесь не более, чем игра на публику.

Как резюмирует Д. Роткопф: "Это лишь начало. Это новая игра. Безусловно, она будет включать в себе новые неожиданные повороты, которые будут вынуждать игроков из Китая и США переосмыслить то, что игра становится всё более опасной, но мы должны понимать, что находимся посередине дороги переосмысления природы силы наций"[20].

Про киберпротивостояние как про новый тип "холодной войны" говорит и профессор университета в г. Буффало Р. Диперт: "Сегодня

[19] *Rothkopf D*. The Cool War / David Rothkopf // The Foreign Policy : website. URL: http://www.foreignpolicy.com/articles/2013/02/20/the_cool_war_china_cyberwar (дата обращения: 08.05.2013).

[20] Ibid.

мы стоим перед лицом длинной "киберхолодной войны" (*Cyber Cold War*), которая характеризуется хоть и ограниченными, но частыми повреждениями информационных систем"[21]. "Киберхолодной войной" называет растущее число киберинцидентов и Д. Редклиф[22]. Е. Черненко, говоря о "холодной войне 2.0", акцентирует внимание на более широких фронтах противостояний: США – РФ – КНР или США+НАТО против ОДКБ+Китай[23].

На проблему новой "холодной войны" обращает внимание и редакционный материал "The Observer"[24]. В частности, в нём указывается, что нарастание напряжённости между ключевыми мировыми игроками объективно усложняется не только "кибервойной", но и гонкой кибервооружений.

Между тем упоминание в контексте "холодной войны 2.0" понятия "гонка кибервооружений" также отсылает нас к характеристике, присущей классической "холодной войне". Израильский специалист по кибербезопасности Д. Рафф отмечает: "Мы являемся свидетелями настоящей гонки вооружений, однако использовать это оружие смогут не только государства, но и любые люди или компании, которые имеют для этого достаточные ресурсы"[25].

Аналогично про возможность наращивания гонки кибервооружений говорят специалисты известных антивирусных компаний. Например, начальник исследовательского отдела компании F-Secure М. Хиппонен отмечает, что вирусы, которые появились в последнее время, существенно "меняют игру" на поле развития опасных программ, и констатирует: "Мне кажется, что мы наблюдаем первые шаги гонки вооружений"[26].

Для специалистов в сфере международной безопасности очевидной является связь между гонкой вооружений и классической "дилеммой безопасности", которая, по сути, состоит в следующем: наращивание сил для повышения собственной безопасности влечёт за собой гипертрофированный ответ со стороны остальных игроков, что приведёт, в свою очередь, к наращиванию вооружённых сил.

В интересном исследовании Э. Джелленс[27], посвящённом проблеме гонки кибервооружений, проводятся прямые аналогии между гонкой

---

[21] Cyber Cold War looming for U.S. // Questia : website. URL: http://www.questia.com/library/1G1-245805413/cyber-cold-war-looming-for-u-s (дата обращения: 06.01.2013).

[22] *Radcliff D*. Cyber Cold War / Deb Radcliff // SC Magazine. 2012. September. P. 24–26.

[23] *Черненко Е*. Холодная война 2.0? / Елена Черненко // Россия в глобальной политике : интернет-сайт. URL: http://www.globalaffairs.ru/number/Kholodnaya-voina-20-15874 (дата обращения: 11.06.2013).

[24] The Cold War is history. Now it's the Cool War // Guardian : website. 2013. February 24. URL: http://www.guardian.co.uk/commentisfree/2013/feb/24/cool-war-cyber-conflict (дата обращения: 22.05.2013).

[25] Кибершпион вирус – Красный октябрь – Red October // YouTube : интернет-сайт. 2013. 20 января. URL: http://www.youtube.com/watch?v=C2i7ENSgkXw (дата обращения: 23.04.2013).

[26] F-Secure: Человечество стоит на пороге развития гонки кибервооружения // SecurityLab : интернет-сайт. 2012. 22 августа. URL: http://www.securitylab.ru/news/428659.php (дата обращения: 07.03.2013).

[27] *Jellenc E*. Explaining politico-strategic cyber security: The feasibility of applying arms race theory / Eli Jellenc // 11th European Conference on Information Warfare and

кибервооружений и гонкой вооружений времён "холодной войны" и отмечается, что если в 2005 г. только 5 стран, как считалось, имели стратегические интересы в киберпространстве и были способны их отстаивать, то в 2012 г. таких стран было уже 25. По его мнению, начальное развёртывание гонки кибервооружений происходило по следующей логике: сначала США, Китай и Россия, первыми поняв потенциал кибершпионажа, разработали свои киберарсеналы, а вслед за ними в эту гонку тоже включились те страны, которые внимательно "наблюдали за ними" (Франция, Великобритания и Австралия, копируя США, а Тайвань и обе Кореи – следуя за Китаем). Если в 2007 г. общие расходы на кибервооружения достигли 10 млрд дол., то в 2012 г. эта цифра перешагнула отметку в 50 млрд, из которых до 15 млрд затратили США.

Э. Джелленс считает, что по состоянию на 2012 г. геополитическая конкуренция между основными игроками в киберпространстве сосредоточилась на двух линиях противостояния.

Первая. США против России, КНР, Ирана и Северной Кореи.

Вторая. КНР против Южной Кореи, России, Японии и Индии.

Кроме того, сформировалось несколько дополнительных "осей" противоборства:

– Южная Корея против Северной Кореи;
– Индия против Пакистана;
– Россия против Грузии;
– Иран против Израиля;
– Сирия против Израиля.

Логика увеличения кибервооружений и сфер их возможного применения обусловлена в первую очередь наступательной сутью доктрин противостояния в киберпространстве. Более того, именно подобная логика поддерживается многими экспертами как наиболее адекватная. "Поскольку вы не знаете, как построить гарантированно хорошую защиту, вы не сможете противодействовать масштабному наступлению. И вы не можете обеспечить эту защиту потому, что эффективное сдерживание вообще сложная вещь. Таким образом, если вы хотите воспользоваться киберпространством, вы будете делать ставку на наступательные операции ради собственной обороны", – утверждает В. Линн[28].

Э. Джелленс делает вывод, что гонка кибервооружений, судя по её динамике, имеет высокие шансы закончиться значительным конфликтом, который, возможно, сможет сдвинуть с мёртвой точки диалог по данной проблеме на международном уровне.

Несмотря на сугубо непубличный характер разработки кибервооружений (хотя надо понимать, что, говоря о "кибервооружениях", мы говорим о неопределённом в международно-правовом поле понятии), некоторые страны уже открыто признают, что либо разрабатывают подобные вооружения, либо даже имеют опыт их использования. Например,

Security / The Institute Ecole Supérieure en Informatique, Electronique et Automatique, Laval, France, 5–6 July 2012 ; ed. by Eric Filiol, Robert Erra. Laval, 2012. P. 151–162.

[28] *Lynn W. J.* Defending A New Domain: The Pentagon's Cyberstrategy / William J. Lynn // Foreign Affairs : website. URL: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (дата обращения: 03.04.2013).

США, через заявление экс-директора АНБ, признали, что имеют опыт использования новейших технологий, которые нарушают работу компьютерных систем потенциального противника[29]. Другим примером является Великобритания, которая заявила о начале реализации программы разработки наступательных кибервооружений[30].

Интересно, что, несмотря на столь, казалось бы, деструктивный характер таких технологий, немало экспертов (в основном западных) выступают против необходимости разработки международных договоров об ограничении кибервооружений, исходя из того, что такой договор был бы абсолютно неэффективным из-за правовой неопределённости в данной сфере и недоказуемости преступлений (Л. Мюир – профессор права Университета Вашингтона[31]), изначального "двойного назначения" всех информационных технологий (Ш. Лоусон – Университет штата Юта[32] и Дж. Линдсей[33]), невозможности реального контроля за созданием кибервооружений (М. Либицки[34]), бессмысленности реализации подобных договоров в нынешних условиях развития ИТ (Дж. Льюис – директор программ по технологиям и государственной политике Центра стратегических и международных исследований[35]).

В США, однако, некоторые исследователи всё же считают необходимым упорядочить международное правовое поле в сфере кибербезопасности. Например, бывший сотрудник Агентства США по защите информационной инфраструктуры Д. Браун ещё в 2006 г. предложил[36] своё ви́дение международного регулирования кибервойны и даже представил

---

[29] США признались в применении кибероружия // Nur.kz. Казахстанский портал : интернет-сайт. 2012. 24 января. URL: http://news.nur.kz/207185.html (дата обращения: 12.04.2013).

[30] Британцы занялись разработкой кибероружия // Актуальные комментарии : интернет-сайт. 2011. 31 мая. URL: http://actualcomment.ru/news/25317/ (дата обращения: 26.05.2013).

[31] *Muir L. L., Jr.* Cyberwarfare a viable nonviolent alternative to military strikes / Lawrence L. Muir, Jr. // News : website. 2012. June 8. URL: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-a-viable-nonviolent-alternative-to-military-strikes (дата обращения: 11.02.2013).

[32] *Lawson S.* Cyberwarfare treaty would be premature, unnecessary, and ineffective / Sean Lawson // News : website. 2012. June 8. URL: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-treaty-would-be-premature-unnecessary-and-ineffective (дата обращения: 11.02.2013).

[33] *Lindsay J.* International cyberwar treaty would quickly be hacked to bits / Jon Lindsay // News : website. 2012. June 8. URL: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/international-cyberwar-treaty-would-quickly-be-hacked-to-bits (дата обращения: 12.02.2013).

[34] *Libicki M.* Setting international norms on cyberwar might beat a treaty / Martin Libicki // News : website. 2012. June 8. URL: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/setting-international-norms-on-cyberwar-might-beat-a-treaty (дата обращения: 10.02.2013).

[35] *Lewis J.* A Cybersecurity treaty is a bad idea / James Lewis // News : website. 2012. June 8. URL: http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/a-cybersecurity-treaty-is-a-bad-idea (дата обращения: 10.02.2013).

[36] *Brown D.* A Proposal for an international convention to regulate the use of information systems in armed conflict / Davis Brown // The Harvard International Law Journal : website. P. 184. URL: http://www.harvardilj.org/wp-content/uploads/2010/10/HILJ_47-1_Brown.pdf (дата обращения: 07.03.2013).

структуру проекта Международной конвенции по регулированию использования информационных систем в военных конфликтах. Среди прочего он обращает внимание на то, что бóльшая часть войн и конфликтов приводили к появлению международных рестриктивных конвенций. Например, Женевский протокол, Конвенция о биологическом и химическом оружии и др. Аргументом в пользу этого становилось то, что активность в киберпространстве неизбежно порождает ответную правовую реакцию. При этом Д. Браун предлагает весьма интересную логику определения "информационного оружия", проводя аналогии с обычным, кинетическим (огнестрельным). Сам по себе пистолет, винтовка или другой вид стрелкового оружия не может убить человека (разве что случайно выстрелит или взорвётся). Таким образом, собственно оружием является только *заряженное устройство, из которого был сделан выстрел для достижения определённой цели* – нанести урон противнику[37]. В отношении "информационного оружия" он предлагает пользоваться схожей логикой[38].

Что касается темы наращивания противостояния США и Китая в киберпространстве как основного среди ключевых пунктов современной международной ситуации, то приходится констатировать, что продолжающееся приблизительно с 2010 г. активное противостояние в киберпространстве между США и Китаем уже в ближайшие годы грозит стать значительно более "горячим", нежели того хотелось бы обоим участникам конфронтации. То, что начиналось с осторожных обвинений США в адрес Китая во взломе электронных ящиков правозащитников в 2010 г., к 2013 г. эволюционировало до весьма жёстких официальных взаимных обвинений и решений.

Например, в марте 2013 г. появилось специальное распоряжение Б. Обамы относительно процедур государственных закупок высокотехнологических решений. Согласно новым правилам Госдепартамент США запретил сотрудничество с Китаем в сфере поставок ИТ-оборудования организациям государственного сектора (в частности, Минторговли и юстиции, НАСА и Национальному научному фонду)[39]. Это решение вызвало недовольство как внутри страны, так и вне её. В первом случае в убытке оказались производители, зависевшие от китайских производственных мощностей, такие ИТ-гиганты, как Apple, Dell, HP. Во втором случае ущерб был нанесён прежде всего Китаю, который через своего министра иностранных дел заявил протест против подобных действий руководства США, отмечая, что любые подозрения в отношении китайских компаний ничем не подкреплены, а значит, такая политика больше напоминает нерыночные методы протекционизма.

В мае 2013 г. Минобороны США официально через доклад для конгресса США "Военный и безопасностный потенциал КНР в 2013 г."[40] прямо обвинило правительство Китая и Народно-освободительную армию

[37] С юридической точки зрения дефиниция "оружие" исходит из иного подхода. – *Прим. ред.*

[38] *Brown D.* Op. cit. P. 185.

[39] Америка не будет закупать китайское IT-оборудование // CY-PR.com : интернет-сайт. 2013. 1 апреля. URL: http://www.cy-pr.com/news/other/6843/ (дата обращения: 21.05.2013).

[40] Military and security developments involving the people's republic of China 2013 : Annual Report to Congress // Office of the Secretary of Defense : website. 83 p.

Китая (НОАК) во враждебных кибератаках против Минобороны США и других американских учреждений[41]: "Китай использует возможности компьютерных сетей для поддержки разведдеятельности, направленной против дипломатических организаций США, экономики и индустриального сектора обороны, в том числе тех, которые участвуют в национальных оборонных программах США". Кстати, в этом же докладе содержатся обвинения в адрес не только Китая, но и РФ, якобы обе страны пытаются на международном уровне "установить контроль за интернет-пространством", подразумевая под этим совместные китайско-российские инициативы, направленные на решение проблем обеспечения "цифрового суверенитета".

В этом же контексте показательна перепалка, которая стихийно возникла в мае 2013 г. во время Азиатского саммита по безопасности в Сингапуре, где министр обороны США Ч. Хейгл неоднократно высказывал обеспокоенность ростом числа кибератак, часть из которых имеет непосредственное отношение к китайскому правительству и военным структурам. На это директор Центра китайско-американских отношений в сфере обороны при Академии военных наук НОАК генерал-майор Яо Юньчжу ответил вопросом: "Как, по мнению Вашингтона, увеличение военного присутствия США в Азиатско-Тихоокеанском регионе будет способствовать усилению доверия в американо-китайских отношениях?"[42] Данная полемика указывает на то, что обе стороны уже открыто признают вопросы кибервойны и классических форм военного присутствия сопоставимыми по важности в системе региональной и глобальной безопасности.

Проблема кибербезопасности в этих непростых двусторонних отношениях США – КНР занимает всё большее место, о чём говорит и то, что она стала предметом полуофициальных переговоров лидеров обеих стран во время встречи 7–9 июня 2013 г. в рамках американо-китайского саммита в Калифорнии. Особую остроту этому разговору придал скандал, который начался как раз в день начала переговоров, когда стало известно о функционировании в США системы PRISM – договора между специальными органами США и ключевыми коммерческими компаниями ИТ-сектора (Microsoft, Google, Apple, Skype и др.) относительно мониторинга контента, проходящего через серверы этих компаний.

* *
*

Таким образом, уже сегодня можно с уверенностью говорить о нескольких важных для дальнейшего будущего киберпространства тенденциях.

Прежде всего становится очевидно, что в ближайшее время киберпространство перестанет быть преимущественно мирной площадкой. Мало

URL: http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf (дата обращения: 27.06.2013).

[41] Ibid. P. 36.

[42] *Кирьянов О.* Китайский генерал поспорила с главой Пентагона / Олег Кирьянов // Российская газета : интернет-сайт. URL: http://www.rg.ru/2013/06/02/general-site-anons.html (дата обращения: 23.06.2013).

того, большая часть инициатив, выдвигаемых для того, чтобы она таковой и оставалась, будет тормозиться ключевыми геополитическими игроками. Но этот вопрос всё же стоит поднимать на самом высоком уровне, поскольку не исключено, что результатом длительной дискуссии может стать принятие какого-либо компромиссного решения.

Важно учитывать, что продолжающееся весьма жёсткое соперничество США и Китая – стран, которые имеют самые крупные экономики и больше других тратят на вооружения, будет серьёзно отражаться на киберпространстве и направлениях его развития. В условиях глобализации и порождённой ею взаимозависимости, когда любое "лобовое" столкновение стран становится невозможным, а напряжение в отношениях накапливается, противостояние в киберпространстве может стать той "отдушиной", куда будет сбрасываться конфронтационное напряжение. Уже в ближайшем будущем это приведёт к формированию принципиально нового формата отношений в духе "холодной войны 2.0", когда усилия определённых стран направлены на то, чтобы как можно жёстче обозначить своё присутствие в киберпространстве. Это неизбежно будет сопровождаться повышенной кибершпионской активностью и кибердиверсиями.

Следует также учитывать, что, как и в классической "холодной войне" второй половины XX столетия, новая "холодная война" охватит в той или иной степени все страны мира. При этом чем более экономически и информационно будет развита страна, тем более жёстко она будет вовлечена в это противостояние.

В то же время реальные механизмы защиты национального киберпространства, базирующиеся на существенных ограничениях или контроле за контентом Интернета, хотя и дают ситуативные позитивные эффекты (как, например, в Китае), однако не решают проблемы в целом, о чём свидетельствует и рост атак на правительственные сети того же Китая. Однако и "калифорнийская идеология" абсолютной открытости национального киберпространства тоже весьма далека от реального ви́дения того будущего, которое ожидает эту сферу и деятельность в ней в ближайшей перспективе. Тотальная открытость, несмотря на апелляцию её защитников к неотъемлемым правам и свободам человека и целесообразности для инновационного развития, вряд ли способна оправдать те риски для общества в целом, которые сопряжены с такого рода открытостью. Соответственно, в ближайшем будущем следует ожидать постепенного взаимопроникновения двух моделей развития киберпространства. Сугубо рестриктивные и "свободные" имеют все перспективы к объединению в некую новую синтетическую, в значительной степени либеральную по своей сути модель.

Ключевые слова: "*холодная война*" – *Китай* – *США* – *киберпространство* – *гонка кибервооружений* – *эскалация напряжённости.*

Keywords: *Cold War* – *China* – *USA* – *cyberspace* – *cyber arms race* – *escalation of tension.*