Александра Куликова
Координатор программы ПИР-Центра
«Глобальное управление интернетом и международная информационная безопасность»

Киберпакт Китая и России: есть ли повод для беспокойства?

Соглашение Китая и России по кибербезопасности может являться предупреждением США, если договор будет расценен как растущая угроза экономическим интересам США и ее интересам безопасности в киберпространстве.

Статья (на англ.яз.) первоначально написана для Russia Direct и опубликована 21 мая 2015 г.

Применимость международного права и законов вооруженного конфликта к киберпространству широко признается, детали этого подхода обсуждаются на международных площадках. Фото: AP

Последний визит президента Китая Си Цзиньпина в Москву был отмечен подписанием ряда соглашений между Россией и Китаем. Одним из них было соглашение в области международной информационной безопасности, которое уже получило название «киберпакта» в СМИ. Это соглашение привлекло массу внимания, поскольку рассматривается как важный и символический шаг России и Китая друг к другу в одной из самых актуальных сфер международных отношений.

Документ определяет основные угрозы глобальной информационной безопасности, с которыми страны намереваются бороться вместе. Эти угрозы включают использование технологий «для осуществления враждебных действий, направленных на нарушение суверенитета, безопасности и территориальной целостности стран», «для вмешательства во внутренние дела государств», для причинения экономического вреда, совершения преступлений, включая утечку данных, для террористических целей или для распространения информации, которая «вредит политическим и социально-экономическим системам или духовному, моральному, культурному укладу других государств».

Что значит новое соглашение по кибербезопасности для России и Китая

Россия и Китай заявили о намерении тесно сотрудничать по совместному реагированию на угрозы посредством усиления взаимодействия и обмена данными между соответствующими правоохранительными органами по киберпреступности и терроризму, посредством обмена опытом в технологиях кибербезопасности и созданием каналов коммуникации, которые позволяли бы быстро реагировать на киберугрозы в мире.

Две стороны договорились по ряду мер укрепления доверия и «совместному продвижению норм международного права для обеспечения государственной и международной информационной безопасности», в частности под эгидой площадок соответствующих международных организаций: ООН, ОБСЕ, МСЭ.

Соглашение выглядит амбициозной попыткой установить правила игры в киберпространстве во время, когда подобный консенсус по нормам поведения кажется маловероятным на глобальном уровне. Как показала Глобальная конференция по киберпространству в Гааге в апреле, государства еще не готовы к подписанию такого договора.

Из-за технологий двойного назначения как основного элемента того, что можно считать кибероружием, в настоящий момент очень сложность создать эффективный механизм надзора, чтобы обеспечить выполнение любого международного договора, запрещающего кибероружие в условиях растущего недоверия в мире.

Несмотря на призывы к обеспечению глобального мира и безопасности, политика некоторых государств видится направленной на усиление гонки кибервооружений, что влияет на усилия по нераспространению и разоружению, так и на глобальную безопасность в целом.

В этих условиях общая близость позиций России и Китая по информационной и кибербезопасности сделала возможным заключение пакта о ненападении и описания в соглашении ключевых элементов стратегического партнерства в информационной безопасности.

Соглашение России и Китая как ответ на стратегию кибероборонs США

Соглашение кажется логичным в свете того, что фокус России смещается к сотрудничеству с ее восточными партнерами в условиях экономической и дипломатической «блокады» у ее западных границ.

Кроме того, в недавно опубликованной киберстратегии Департамента безопасности США, Россия и США признаются одними из главных оппонентов, которые «значительно продвинулись в развитии своих кибервозможностей и стратегий», в то же время упоминается необходимость сохранять диалог с Китаем.

«Российские акторы незаметны в своей кибербразведке и очень часто определить их намерения довольно сложно. Китай присваивает интеллектуальную собственность глобального бизнеса в пользу китайских компаний, чем подрывает конкурентоспособность США», говорится в документе в описании того, как США воспринимают Россию и Китай.

Более того, в апреле США объявили о новой программе санкций, которая «уполномочивает министра финансов США по консультации с генеральным прокурором и Государственным секретарем накладывать санкции на злоумышленников, действия которых угрожают национальной безопасности, проведению внешней политики, здоровью экономики и финансовой стабильности США».

Примечательно, что российско-американское соглашение 2013 года по укреплению мер доверия предполагало подобное сотрудничество и в числе прочего обмен информацией между российскими и американскими группами по реагированию на чрезвычайные ситуации в киберпространстве (CERT), создание рабочей группы по возникающим угрозам и использование существующей ядерной «горячей линии» для прямой связи в случае киберкризиса.

К сожалению, этот процесс не получил должного развития и был заторможен с началом современного геополитического кризиса.

Кибердиалог Китая и США так же зашел в тупик после подписания подобного соглашения по укреплению мер доверия в том же году. Разоблачения Сноудена в 2013 году так же не способствовали реализации договора.

Считается, что третье звено в этом треугольнике наметилось в конце 2014 года и, по ожиданиям, должно было превзойти в масштабе обе попытки. В настоящее время российско-китайское соглашение больше похоже на рамочный документ, во многом основанный на ранее определенных общих ценностях и ожиданиях.

Тем не менее в соглашении получила отражение Секция 10 обновленного предложения правил поведения в киберпространстве от стран ШОС в области выработки практических мер по укреплению доверия, «направленных на повышение предсказуемости и снижение вероятности недопонимания и угрозы конфликта», - наименее спорная тема среди политиков, как и наименее сложная для оценки и надзора.

Пока стороны не были вовлечены в крупные публичные скандалы, связанные со взаимными кибератаками, что придает этому «пакту о ненападении» характер меморандума о понимании, о которому дается максимальное международное освещение.

Некоторые эксперты приписывают это желанию России ограничить влияние США и создать объединенный фронт по борьбе с возможными кибервторжениями, которые кажутся более чем вероятными в контексте текущего противостояния. В то же время, то, что китайско-американский диалог по киберсотрудничеству застопорился, придает Китаю дополнительный стимул объединить усилия с Россией.

На Западе есть опасения, что в результате взаимного обмена технологиями двух стран пострадает западный бизнес. Фото: AP

Кибер-соглашение России и Китая как стратегический ход

Тем не менее, сводить соглашение просто к попытке уязвить США было бы слишком упрощенным подходом к вопросу. Иначе говоря, то, что мы наблюдаем, может быть только верхушкой айсберга.

Даже если пакт обладает символический смыслом, он укрепляет линию сотрудничества России и Китая и является дальнейшим шагом в политике России на востоке, что придает соглашению приоритетный характер в контексте текущей сложной дипломатической обстановки.

Выгода Китая не очевидна, но, возможно, следует брать в расчет более широкий ряд соглашений, подписанных в начале мая 2015 года в Москве между двумя странами. Кроме того, соглашение может помочь в процессе легитимизации внутренней киберполитики обеих странах и способствовать укреплению действующих режимов. Соглашение сочетается с положениями правила поведения ШОС и подкрепляет эту попытку выработки норм на многих уровнях.

По-прежнему сохраняется возможность будущих поправок к соглашению и его расширение с более подробным описанием того, как будут регулироваться действия в области технологии, инфраструктуры, политики на уровне национальных сегментов интернета. Возможно, это то, чего Россия хотела изначально, и то, к чему китайская сторона была не готова до настоящего момента, но дверь остается открытой.

В этой связи, подводная часть айсберга может существовать, но оставаться скрытой от глаз еще долгое время. Тем не менее, до сих пор неясно, насколько вероятным и желаемым для двух сторон на практике является международное киберсдерживание и соблюдение достигнутых договоренностей. Только будущая реализация упомянутых в соглашении мер по укреплению доверия выявит реальную приверженность прозрачности и взаимное доверие.

Продвижение глобального управления киберпространством

В более широком масштабе, соглашение демонстрирует текущие попытки России продвигать подход, ориентированный на выработку норм, к управлению киберпространством. Применимость международного права и законов вооруженного конфликта к киберпространству широко признается, детали этого подхода обсуждаются на международных площадках, включая формат Группы правительственных экспертов ООН, в котором Россия исторически была двигателем повестки ответственного поведения в киберпространстве.

Инициатива ШОС пока является единственной международной попыткой применить подход с позиции саморегулирования к ненападению в киберпространстве, к которому могут присоединиться все заинтересованные стороны. Тем не менее, из-за разницы в подходах к определению угроз в киберпространстве, которую усугубляет крайне низкий уровень дипломатических контактов между Россией и Западом, она пока не встретила широкой поддержки вне ШОС.

В этом смысле, очевидно, что двустороннее соглашение основано на взаимоприемлемых вопросах и укрепляет лидерство России в формировании норм, которое поддерживает ее важный восточный партнер.

Все упомянутое выше подпадает под понятие «секьюритизации» повестки информационного пространства, которому Россия долгое время придавала большое значение. В некоторых дискуссиях можно почувствовать, что продолжающаяся радикализация публичной онлайн сферы из-за экстремистских и террористических движений помогает заполнить существующий пробел в понимании угроз и рисков в киберпространстве.

Дипломатическая напряженность может препятствовать заметному сближению на международной арене в этой области, но шаги на региональном и двустороннем уровне уже принимаются.

Тонкая грани между нападением и защитой в киберпространстве

По-прежнему остается открытым вопрос, насколько серьезным является обещание не совершать хакерские атаки за рамками российско-китайского соглашения. В киберстратегии США сказано, что «для вооруженных сил США приемлемо проводить кибероперации для подрыва сетей, связанных с военной деятельностью, или инфраструктуры для того, чтобы вооруженные силы США могли защищать интересы США в районе операций».

Такой подход проистекает из предположения, что «сдерживание частично является вопросом восприятия», что «оно не может быть достигнуто только через выработку политики, но через совокупность всех действий США», включая возможности по предотвращению и реагированию, оборонительную позицию и общую отказоустойчивость сетей США.

Такой подход демонстрирует довольно широкую трактовку возможных угроз для США и дает правительству страны карт-бланш в оценке и ответе на то, что воспринимается как агрессия, что еще больше размывает грань между защитой и нападением в киберпространстве.

С учетом этого, соглашение России и Китая, которое строится на идее о верховенстве суверенитета в управлении киберпространством и борьбе с действиями извне, направленных против внутренней стабильности и целостности государств, в случае реализации может рассматриваться как растущая угроза интересам США.

Следовательно, если будущая реализация соглашения выглядит угрожающей, нет гарантии того, что ответная реакция будет симметричной. Что является «симметричным» в киберпространстве пока не было четко определено.

Пока рано говорить о практических последствиях российско-китайского соглашения до того, как будут предприняты конкретные меры по его реализации. Тем не менее, определенно будет интересно посмотреть, будет ли придаваться большое значение этим положениям на саммите БРИКС в июле 2015 года в Уфе.

В частности, будет ли двустороннее соглашение России и Китая стимулировать другие стороны следовать этому примеру (по крайней мере, на двустороннем уровне внутри группы БРИКС) в отсутствие четко сформулированного общего подхода к информационной и кибербезопасности.

В то время, как на Западе есть опасения, что в результате взаимного обмена технологиями двух стран пострадает западный бизнес, ключевые опасения все же касаются вопросов мира и безопасности: лучшей демонстрацией рекомендованного подхода к кибербезопасности будет более безопасное глобальное общество.