

ДЕМИЛИТАРИЗАЦИЯ КИБЕРПРОСТРАНСТВА И ПРОБЛЕМЫ «КИБЕРСДЕРЖИВАНИЯ»: ВОЗМОЖНЫЕ РЕШЕНИЯ

Последние 2-3 года принципиальным стал вопрос о будущем киберпространства: останется ли он источником экономического, инновационного и социального развития или превратится в новое пространство военного противостояния. Деятельность целой группы вирусов класса «кибероружие» (например, Stuxnet), наращивание государствами своих киберпотенцилов и кибермогущества (в том числе – через увеличение кибервозможностей разведывательных и военных структур) – все это говорит о том, что киберпространство уже сейчас активно милитаризируется и используется силовыми структурами ключевых стран для осуществления влияния на другие международные субъекты.



Соответственно, ключевые геополитические игроки должны серьезно подойти к проблеме не просто констатации факта увеличения силовых возможностей киберпространства, но принять меры относительно его демилитаризации, а превентивно – не допустить его дальнейшей милитаризации.

Говоря о вопросах киберпространства в контексте проблемы его милитаризации и заинтересованности в этом великих государства, геополитик Ф.Макдональд обращает внимание на очевидную схожесть проблемы милитаризации киберпространства с аналогичной проблемой милитаризации космоса: «Несмотря на то, что еще в 1967 году был принят Договор ООН относительно космоса, в котором прямо запрещается его милитаризация, ведущие мировые игроки и тогда и сейчас, раздумывая про дальнейшее исследование космоса, прежде всего думают про его военный потенциал... это справедливо и для киберпространства» [1, с. 600].

Причины непреодолимого желания государств превратить киберпространство в поле военного противостояния обусловлено его специфическими признаками. Американский политолог Дж.Най говорит об этом следующим образом: «Киберпространство включает в себя не только подсоединенные к Интернету компьютеры, но и интранет, мобильные технологии, оптико-волоконные кабели и базированные в космосе коммуникации. Киберпространство имеет физический уровень инфраструктуры который следует экономическим законам соперничества за ресурсы и политическим законам суверенной юрисдикции и контроля. Этот аспект Интернета не является «общим» в традиционном понимании. В тоже время он имеет виртуальный или информационный уровень который увеличивает экономические прибыли и особую политиче-

скую практику, которая делает контроль за ним сложным. Атаки из информационной реальности стоят чрезвычайно мало, однако могут быть направлены против физического пространства, где ресурсы ограничены и не дешевы. С другой стороны, контроль над физическим уровнем может иметь территориальные и экстерриториальные эффекты на информационном уровне. Кибермогущество может продуцировать результаты, как в киберпространстве, так и за его пределами. По аналогии, морская сила направлена на использование ресурсов в морском пространстве ради победы в морских битвах в океанах, однако океаны точно так же могут быть использованы для осуществления мероприятий влияния на торговлю и точек зрения на суше. Схожую аналогию можно применить и для воздушного пространства» [2, с.19].

Еще более точно про особенности киберпространства с точки зрения заинтересованности в нем военных структур говорит британский дипломат Дж.Шелдон: «Основным стратегическим признаком кибермогущества, который и делает его настолько уникальным в современном мире является возможность как в военное, так и мирное время манипулировать стратегической обстановкой одновременно не давая противнику возможности сориентироваться в той же обстановке» [3, с. 104].

Государства явным образом чувствуют «дефицит безопасности» когда имеют дело с киберпространством и сетью Интернет. В то время, когда все проявления межгосударственной агрессии на физическом уровне более чем формализованы и нормированы на всех уровнях (национальном, международном), киберпространство с его возможностями влиять на физическое пространство вызывает у них естественное желание исправить существующую неопределенность.

Вынуждены признать, что идеи стремительной милитаризации киберпространства исходят из объективной неспособности государств выработать такие международные правила игры, которые бы хотя бы на общем уровне обеспечили им уверенность в сохранении баланса сил. Г.Раттрей по этому поводу отмечает: «Киберпространство становится основным источником для политического и военного соперничества. Новые угрозы исходят от акторов, которые не были соперниками в иных пространствах (realms)... Новые военные возможности и интересы частного сектора требуют сбалансирования возможностей и рисков; это требует пристального анализа, что так и не сделано. США должны изучить как защитить свое присутствие в киберпространстве экономически-целесообразным способом. Это может привести к созданию масштабных атакующих сил для защиты коммерческих интересов в Сети; управления международными усилиями и нормами, которые должны быть направлены на ограничение разрушительной активности одних государств против других и наказания негосударственных акторов; возможно новый «кибер Манхэттенский проект» может восстановить более безопасную технологическую основу киберпространства» [6, с. 265].

При этом, сейчас на экспертно-научном уровне происходит серьезная дискуссия относительно того, действительно ли угрозы милитаризации киберпространства настолько серьезны, что им стоит уделять повышенное внимание на международном уровне, в том числе – что бы осуществлять действия по предупреждению этого процесса.

Интересно, но значительная часть американских ученых и экспертов, особенно среди тех, кто приближен к американскому военному сектору, достаточно скептически подходят к определению военных возможностей киберпространства.

Один из известных исследователей вопросов кибербезопасности М.Либицки, говоря про потенциал киберпространства как источника угроз и разрушений, отмечает, что: «уничтожение или отсоединение киберсистем способно вернуть экономику в 1990-е годы. Однако мы должны помнить, что ядерный удар вполне может вернуть нас в Каменный век» [4, с.136]. М.Либицки последовательно отстаивает скептическую позицию относительно «алармистских» настроений в отношении киберугроз. В частности он отмечает, что большинство организаций (независимо от их величины – будь то государство или частная компания) зависимы от киберпространства ровно настолько, насколько хотят быть зависимы [5, с. xiv]. Кроме того, по его мнению «операции, которые могут трактоваться как «кибервойна» наносят вред, прежде всего, индивидуальный, не уничтожая оборудование (за редким исключением). В лучшем случае эти операции могут смутить или дезориентировать оператора военных систем и то лишь временно. Поэтому кибервойна может выполнять функцию поддержки для других элементов военных действий, в том числе – для обезоруживания противников» [5, с. xiv-xv].

Существенные «кибероперации» в рамках такого курса рассматриваются как часть мероприятий поддержки основных сил, поскольку самостоятельные «принуждаю-



щие» возможности киберпространства весьма ограничены. Интересно, что для иллюстрации этих «ограничений» исследователи пользуются теми же примерами, которые обычно используют, дабы показать опасность кибератак – события в Эстонии и Грузии.

Уже упомянутый Дж.Шелдон в этом контексте замечает: «Эстония, в первую очередь, реагировала на более традиционные угрозы со стороны России – прежде всего дипломатические, в то время как киберсоставляющая стала лишь дополнительным неприятным фактором. Аналогично в Грузии. Российские кибератаки вызвали нарушения предоставления Интернет-услуг, однако сложно представить, что российская военная компания была бы менее эффективной или вообще бы не удалась, если бы киберсоставляющая была не эффективна или не удалась» [3, с. 99].

При этом, несмотря на подобные «успокаивающие» и «примеряющие» подходы именно США остается лидером по созданию технологий, которые могут быть использованы во время противостояния в киберпространстве.

В тоже время не можем хотя бы частично не согласиться с подобными скептическими настроениями в связи с тем, что все более доминирующим дискурсом обсуждения киберугроз становится идея «цифрового Перл-Харбора», как некоего обобщенного образа тотального поражения государства вследствие его неготовности ответить на мгновенный и неожиданный киберудар. Львиная доля сегодняшних научных исследований и еще большая часть полупублицистических работы посвященных противостоянию в киберпространстве, апеллируют как раз к этому образу, пытаясь запугать читателя поражающими воображение масштабами катастрофы.

По нашему мнению даже на сегодняшний день подобные сценарии тотальных повреждений и возвращения экономик целых стран чуть ли не до «до индустриальных» времен является больше вымыслами, чем реальностью. Однако и чрезмерно оптимистичные и самоуспокаивающие размышления про абсолютную периферичность киберпространства также выглядят неадекватными современному уровню проникновения ИКТ во все сферы жизни общества.

Наиболее вероятностным и похожим на реальное развитие событий представляется описание потенциального масштабного конфликта Дж.Бренером – одной из важных фигур в структуре американской разведки, который почти 20 лет посвятил разведсообществу. В своей книге «Уязвимая Америка» он целую главу посвящает гипотетическому дипломатическому кризису между США и Китаем, который, не перерастая в жесткое противостояние, находит свое отображение в киберпространстве. Вследствие действий китайских хакеров не происходят взрывы на химических предприятиях, на падают авиалайнеры, не сходят с рельс поезда – нет, им просто удается стереть значительный массив данных в военных сетях

Пентагона, внести «шумы» в системы управления ракетами и навигационное оборудование военных самолетов, а также целый ряд иных действий. Их основная цель не остановить атаку, но принудить руководство страны и разведывательные органы понять то, что в действительности они не владеют ситуацией и не могут с уверенностью предвидеть где именно будет нанесен следующий удар [приводиться по 15].

На международно-правовом уровне проблема недопущения милитаризации киберпространства, использования его в целях военных противостояний сталкивается сразу с несколькими существенными сложностями, каждая из которых будет требовать своего решения. Среди ключевых проблемных точек: выработка согласованной позиции относительно того, можно ли считать кибератаку «актом войны» и формулирование адекватной нормативно-правовой базы относительно контроля над кибервооружениями.

При этом вынуждены отметить, что позиции ключевых геополитических игроков по каждому из этих вопросов существенно отличается, что не способствует поиску действительно согласованного решения. Частично это объясняется и неточностью базовых нормативно-правовых актов, которые на международном уровне регулируют «силовые» вопросы.

Например, по сути «акт войны» является достаточно условным термином, который является скорее политической конструкцией, чем юридическим понятием. Как отмечает Д.Чарльз [8] ООН сделало все, что бы выбросить из международного юридического лексикона слово «война». В ключевых статьях Устава ООН, которые относят к «военным» (то есть статьи 2(4) и 51), понятие «войны» не встречается – вместо этого там упоминается значительное количество других эвфемизмов вроде «угроза силой», «применение силы против территориальной целостности», «вооруженное нападение» и «право на самооборону».

В тоже время юристы-международники находят возможности применения действующего международного законодательства и для кибератак. Например, для этого предлагается использовать отдельные положения Протокола 1 Женевской Конвенции. Однако все это скорее временные решения, которые все еще имеют сомнительные с точки зрения политиков обоснования.

Вся эта ситуация является частью иное, более широкой по масштабам проблемы, связанной с тем, что вообще можно считать «актом войны» и что может трактоваться как события, отвечающие статье 51 Устава ООН. В отдельных случаях Международный Суд ООН признавал случаи предоставления военной помощи повстанцам недостаточными для применения силы в ответ. Таким образом, вопрос возникает и относительно традиционного понимания «акта войны».

В случае же с киберпространством это усложняется еще одним обстоятельством – уже упомянутая статья

51 регулирует отношения между государствами, то есть живет реалиями вестфальского мироустройства, в той время как проблемы киберпространства это, очевидно, проблемы поствестфальской модели международных отношений, которая все еще пребывает в процессе своей институализации. И в контексте проблемы определения «акта войны» этот вопрос становится особо острым, поскольку атака на государственные структуры может осуществляться и негосударственным актором, который в тоже время находится на территории определенного государства. На это обстоятельство обращает внимание юрист-международник М.Шмидт: «Кибернасилие любого уровня насыщенности, если оно осуществляется отдельными лицами или даже неорганизованными преступниками, даже если оно осуществляется против правительства, не создает «вооруженного конфликта» в том смысле, как его понимает Женевская конвенция» [12]. Однако возникает вопрос относительно ответственности как атакующего, так и того, с чьей территории была осуществлена атака. Принимая во внимание возможности злоумышленников удачно маскировать свою деятельность и даже представлять, что агрессивные действия были осуществлены с территории другого государства, этот вопрос звучит особенно остро.

Среди возможных путей решения подобных проблем предлагается обращаться к правительствам (или уполномоченных национальных силовых/правоохранительных структур) стран с целью прекратить деятельность злоумышленников и лишь тогда, когда правительства не захотят/не смогут повлиять на ситуацию, считать возможным осуществлять мероприятия по самообороне. Это решение является достаточно условным по целому ряду причин. И даже если отбросить сомнительный с точки зрения международного права базовый посыл остается другая проблема: во многих случаях реагирование на кибератаки должно осуществляться в режиме реального времени, если не параллельно самой атаке. В предлагаемой же схеме предусматриваются длительные переговоры, на которые просто нет времени.

Должны отметить, что речь в большей части описанных выше случаев идет о более-менее «физических» атаках, то есть влиянии на конкретные автоматизированные системы и оборудование. Если же мы добавим к этому и «информационно-психологическую» составляющую (на чем настаивают Россия и Китай, но против чего выступает США), то проблема станет значительно более точной, но при этом и значительно более сложной.

Интересно, что несмотря на якобы жесткую позицию руководства США относительно не смешивания кибервопросов и того, что можно назвать «информационно-психологической» составляющей, есть достаточно масштабный набор примеров, согласно которым органы безопасности США (прежде всего Минобороны и ЦРУ) уделяют особое внимание деятельности в блогосфере с целью улучшения

своего имиджа, сбора развединформации и влияния на общественное мнение по актуальным вопросам безопасности (например, относительно компаний в Ираке и Афганистане) [8, с. 96].

Подводя промежуточный итог можно с уверенностью сказать, что пока не будет дан четкий ответ на то, что в киберпространстве можно считать актом войны, государства будут чувствовать очевидную неопределенность в том, какие конкретно инструменты могут быть использованы против них в киберпространстве. Одновременно с этим те же информационно-развитые государства, понимая нерешенность данного вопроса, будут не в состоянии устоять перед непреодолимым желанием и самим воспользоваться такими инструментами, пока они могут быть уверены в отсутствии обратного ответа от потенциальной жертвы.

Это подводит нас к второму аспекту проблемы – внедрения механизмов международного контроля за кибервооружениями (точного определения которого на сегодняшний день так же нет). И это при том, что по мнению экспертов, времени на создание адекватного киберсоглашения все меньше и это приводит к тому, что использование кибервооружений так и остается юридически не урегулированным вопросом, хотя вероятность киберконфликтов и возрастает [9].

Впрочем, даже наиболее оптимистические юристы-международники сомневаются в том, что в ближайшее время будет принят подобный международный документ. И обусловлено это прежде всего его весьма условной потенциальной эффективностью. Известный американский политолог и публицист Ч.Краутхаммер формулирует проблему режимов сдерживания и нераспространения следующим образом: «Начиная с морского соглашения 1920 года и до сегодняшних дней контроль над вооружениями всегда балансировал между двумя полюсами, одним из которых (и это в лучшем случае) был сугубо символизм этого режима и до (в худшем случае) абсолютной бессодержательности, которая могла даже нанести вред безопасности во всем мире. Проблема никогда не была в оружии как таковом, это проблема самого режима контроля над оружием» [10].

И действительно, сам режим контроля редко был эффективным и адекватно воспринимался большими странами, которые часто считали его элементом их сдерживания. Например, замминистра обороны У.Линн заявил, что традиционные соглашения по контролю над вооружениями, скорее всего, не способны предупредить кибератаки и прежде всего потому, что провести соответствующую проверку невозможно [11]. Несмотря на это те же США в целом демонстрируют готовность принять участие в разработке новых норм поведения в киберпространстве, однако, очевидно, не на базе тех идей и подходов, которые сейчас предлагаются Россией и Китаем [приводиться по 8].

Преимущественно негативная позиция относительно



перспектив международных договоров, которые направлены на «киберсдерживание» и «контроль за кибервооружениями» характерна и для экспертного сообщества. Специалисты обращают внимание на то, что «такой договор был бы абсолютно не эффективным и прежде всего из-за правовой неопределенности большинства из «кибер» понятий» [16], «практически все технологии, которые связаны с киберпространством являются технологиями «двойного назначения», а те, которые называются «кибероружием» оружием вообще не являются» [17] и [18], «такой договор был бы просто неэффективным из-за сложности контроля того, ради чего он и был бы принят: при производстве кибервооружений ничего, собственно, не производится, что можно было бы контролировать и отслеживать» [19].

Подобная критичность позиций по поводу перспектив киберсдерживания характерна не только для американских специалистов. Исследователь Тенг Лан отмечает, что концепция киберсдерживания, видимо, не является тем ответом, который может дать мир на рост киберугроз в том числе – из-за интерконнективности Всемирной Сети, множества акторов и наличия потенциального эффекта от «киберответа» (например, дестабилизация работы банковской системы оппонента может привести к потерям и собственной экономики). Адекватным ответом может быть лишь усиление международного сотрудничества, в том числе – относительно выработки согласованных международных подходов об основных принципах функционирования киберпространства, усовершенствования международной правовой базы и более интенсивного межгосударственного диалога [22].

В тоже время есть и иные мнения на этот счет. М. Макконел (экс-руководитель Национальной разведки

США) считает, что киберсдерживание вполне может стать основой для построения действительно безопасного киберпространства. Он обращается к идее, что наличие могучих кибернаступательных потенциалов будет выступать сдерживающим фактором относительно возможности применения масштабных кибератак против США [27].

Иные эксперты, которые так же считают, что разработка подобных документов не только возможна, но и необходима, апеллируют к истории принятия иных аналогичных документов: Женевского протокола 1928 года, конвенции про биологическое оружие 1972 или Конвенцию про химическое оружие 1992 года [21].

Еще один вариант решения данной проблемы предложили специалисты East-West Institute. Речь идет о специальной «цифровой маркировке» сугубо гражданских объектов, против которых не должны применяться кибервооружения. Однако даже в этом случае мы должны понимать всю ограниченность подобных договоров, как с точки зрения попыток положиться на моральность участников кибервойны, так и самой технологии, которая применяется для кибервооружений.

Несмотря на подобную пессимистическую перспективу относительно возможности принятия эффективных международных договоров, в целом дискуссия об этой проблеме все чаще возвращается к временам Холодной войны, идее политики «сдерживания», «гарантированного уничтожения», а в целом – проблемы появления ядерного оружия и того, как мировые государства пришли к пониманию необходимости создания механизма, дабы не допустить самоуничтожения человечества. Уже упомянутый Тенг Лан отмечает, что «киберпространство сегодня такое же небезопасное, как и мир в 1950-х годах, когда сложился ужасный баланс ядерного террора» [22, с. 44].

Дж.Най, который обращается к этой проблеме более подробно в своей статье «Ядерный урок для кибербезопасности?» [2] отмечает, что сама возможность заимствования опыта событий 70-летней старины для описания сегодняшней ситуации хотя и выглядит на первый взгляд малоцелесообразно (прежде всего через существенное отличие в технологиях), однако вопрос истории и динамики решения ядерной проблемы, на которую все более схожа проблема кибербезопасности, актуализирует этот вопрос.

Важной особенностью ядерного сдерживания был его экзистенциальный характер – все понимали, что в случае массовых ядерных ударов вопрос будет стоять не про победителей или проигравших, а про само выживание человечества. Особо остро этот вопрос стал после изобретения водородной бомбы. И хотя глобальная киберугроза не может соперничать с ядерной, однако чем больше человечество зависит от киберпространства, тем более близкими становятся аналогии.

В ядерном противостоянии проблема дополнительно обострялась значительным взаимным недоверием, которое существовало между ключевыми геополитическими игроками на протяжении всей Холодной войны. Это недоверие не стало принципиально меньше в наше время, хотя глобализационные процессы (в первую очередь – в экономике) внесли в это недоверие определенные коррективы.

Несмотря на это недоверие, геополитические субъекты понимают необходимость сотрудничества ради обеспечения глобальной кибербезопасности. С каждым годом становится все понятнее, что как и в случае с ядерным сдерживанием, попытки самостоятельно решить проблемы кибербезопасности будут ограниченно эффективными и сотрудничество становится необходимым. Это и выступает в качестве сильного источника для стратегической идеи демилитаризации киберпространства или создания хотя бы механизмов взаимного сдерживания в нем. Однако для закрепления подобного понимания, по мнению исследователей, потребуется нечто большее, чем рациональное мышление – и скорее всего это будет цифровой аналог «Кубинского кризиса».

Уже упомянутый Дж.Най считает, что исходя из истории взаимоотношений больших стран на протяжении последних 70 лет сложно представить, что бы они действительно смогли создать такие международные правила игры, которые будут реально ограничивать их в обеспечении своих национальных интересов. В тоже время вполне вероятно, что часть действий, которые на сегодняшний день наносят вред всем игрокам (например - кибершпионаж) могут получить некие неформальные ограничения, которые будут взяты на себя странами добровольно.

И это снова может отослать нас к реалиям Холодной войны и формированию того, что З.Бжезински назвал «кодексом правил взаимного поведения, направленных на поведение, которое уменьшает опасность, которая в

ином случае может стать смертельной» [25, с.244]. Во многом именно эти правила, в свое время, привели к взаимному уважению сфер влияния и решению «Кубинского кризиса», а в дальнейшем стали основой для ядерного разоружения. Скорее всего и для киберпространства ситуация будет складываться аналогичным образом – будет приходиться постепенное и непростое понимание всеми заинтересованными сторонами необходимости наработать общие подходы.

Правда на пути этого могут стать некие принципиальные отличия между ядерным и кибер сдерживаниями. Показательным тут является аспект усиления доверия и прозрачности подготовительных мероприятий к агрессивным действиям. В то время, как для обычных вооружений есть целый комплекс общепризнанных мероприятий контроля за прозрачностью действий (например, согласованный порядок проведения военно-морских суден, предупреждения соседних стран про перемещения крупных групп войск, отчеты перед международными структурами относительно масштабов закупок военной техники и т.д.), то для киберпространства, с его неопределенными границами и зонами ответственности, все это выглядит достаточно условно. Особенно принимая во внимание то, что генерирование необходимых для кибератаки сил может происходить абсолютно тайно. Более того, сам успех кибератак во многом зависит от тайности действий и, соответственно, отсутствия любой прозрачности для других.

Проблема киберсдерживания сталкивается и с проблемой, которая не была характерна для периода ядерного сдерживания – существует целая группа факторов, которые влияют на возможность определить, кто, собственно, нанес удар и, соответственно, против кого должен быть нанесен удар в ответ. М.Либицки по этому поводу выделяет группу вопросов, которые описывают проблемы у в целом:

- далеко не всегда можно определить, кто вас атакует;
- даже если вам удастся ответить на масштабную кибератаку не факт, что вам удастся это сделать аналогичным образом хотя бы дважды;
- даже если вы сможете нанести обратный удар это не гарантирует того, что цель действительно будет выведена из строя;
- нет никаких гарантий относительно того, что в это противостояние не втянутся третьи стороны и прежде всего – негосударственный сектор;
- киберсдерживание может нести не верный сигнал для внутренних игроков (например, если будет четко заявлено, что кибератака на объекты критической инфраструктуры, которые часто принадлежат частному сектору, будут пониматься как акт, для обратного удара со стороны государства, то это уменьшит желания собственников этой инфраструктуры вкладывать деньги в их безопасность);
- государствам будет крайне сложно установить пороговые значения за которыми будет идти обратный ответ,

поскольку это может вынудить государство отвечать даже на наиболее незначительные атаки или недооценивать другие;

- киберпротивостояние, скорее всего, не сможет иметь ограниченную (сугубо киберпространством) сферу функционирования и в случае обострения может перекинуться в реальный мир.

Еще одна (хотя и не последняя) проблема подобных конфликтов – отсутствие четких механизмов их прекращения или уменьшения эскалации на высшем уровне. В то время, как в обычных конфликтах есть тысячелетиями наработанные механизмы взаимных гарантий и обязательств, сама природа киберпространства делает их достаточно условными и не надежными.

На этом фоне показательной стала последняя конференция Международного Союза Электросвязи в Дубаи, когда группе стран так и не удалось поставить на обсуждение вопрос относительно баланса между наднациональностью и суверенными правами государств в сети Интернет. В тоже время, несмотря на эту, очевидно, неудачную попытку на фоне общего роста обеспокоенности ведущих стран масштабными мониторинговыми возможностями спецслужб США, эта дискуссия вполне может вернуться на повестку дня. В том числе – по инициативе тех стран, которые в Дубаи выступили против подобных обсуждений.

Однако даже этот случай демонстрирует заметную проблемность выработки действительно согласованного международного документа, который бы положил начало процессу киберразоружений и демилитаризации киберпространства,

Между тем создание подобного соглашения является объективным требованием времени. Более того – похоже, что решение этого противоречия станет одним из доминирующих мотивов международных дискуссий по кибербезопасности в ближайшие годы.

И тут опыт Холодной войны и решения «ядерной проблемы» может стать тем указателем, который окажется актуальным и для киберпространства. В частности речь идет про то, каким именно образом разворачивалась политика взаимного ядерного сдерживания и контроля над ядерными вооружениями. Ведь первые соглашения касались не столько взаимного разоружения или ограничений, сколько третьих стран (например – не передача ядерных технологий третьим сторонам). Аналогично и в случае демилитаризации киберпространства целесообразно начать с договоров по вопросам, которые не вызывают жестких противоречий. Например, среди таких могли бы стать договора про противодействие террористическим кибератакам, которые осуществляются при помощи ИКТ. Возможно со времени количество найденных общих позиций станет основой для более масштабного взаимопонимания [2].

На сегодняшний день ведущие государства де-факто

уже пытаются идти таким путем, выделяя отдельные конфликтные позиции и пытаются их решить не захватывая более сложных вопросов. К примеру, проблема кибершпионажа становится настолько масштабной, что, видимо, вынудит информационно развитые государства выработать определенные правила в этой сфере (хотя бы ради более прогнозируемого экономического роста). В 2013 году Китай официально заявил, что будет разрабатывать и вводить новые правила борьбы с международным кибершпионажем [28]. Другой пример: по результатам Саммита ЕС 24-25 октября 2013 года канцлер Германии А.Меркель и Президент Франции Ф.Олланд (на фоне информации о фактах прослушки телефонов европейских руководителей со стороны АНБ США) выступили с идеей заключения «антишпионского пакта».

К аналогичным, по сути, попыткам поиска точек соприкосновения можно отнести идею, с которой выступили Президент РФ В.Путин и премьер-министр Индии М.Сингх относительно необходимости «принять [международные] нормы и правила, которые исключили бы возможность использования информационных технологий в преступных или террористических целях» [29].

При поиске подобных механизмов обеспечения глобальной кибербезопасности следует помнить, что в отличие от классических силовых угроз, которые исходят преимущественно со стороны крупных стран (поскольку лишь они владеют достаточным экономическим и военным потенциалом), новые угрозы включают в процесс глобальных дискуссий значительно более широкий круг стран. В том числе тех, которые не являются игроками глобального уровня, однако имеют достаточные интеллектуальные и технические ресурсы, которые являются доминирующим фактором в киберпротивостояниях. Соответственно вопросы выработки глобальных подходов к вопросам кибербезопасности будет невозможно решить в случае не включения этих стран в общий диалог.

В целом же можем констатировать, что путь к поиску компромиссных, но при этом общих для всех решений не будет ни быстрым, ни простым, а его конечный результат, видимо, будет существенно отличаться от того, каким мы его видим сейчас. Это объясняется как тем, что уровень прогресса (инновационности и изменчивости) в данной сфере остается глобальной доминантой, так и тем, что сама концепция «кибербезопасности» и всех ее составляющих (в том числе – кибермогущества, цифрового суверенитета и т.д.) пребывает на начальных этапах своего становления.

Дубов Дмитрий Владимирович,

Кандидат политических наук, Национальный институт стратегических исследований (Киев, Украина),
Заведующий отделом исследований информационного общества и информационных стратегий

СПИСОК ЛИТЕРАТУРЫ

1. MacDonald F. Anti-Astropolitik – outer space and the orbit of geography / Fraser MacDonald // Progress in Human Geography.- 2007.- №31(5).- P.592–615
2. Nye J. Nuclear lessons for cyber security? / Joseph S. Nye // Strategic Studies Quarterly.- 2011.- №5(4).- P.18-38
3. Sheldon J.B. Deciphering cyberpower strategic purpose in peace and war / J.Sheldon // Strategic Studies Quarterly.- 2011.- №5(2).- P.95-112.
4. Libicki M. Cyberwar as a Confidence Game / Martin C. Libicki // Strategic Studies Quarterly.- 2011.- №5(1).- P.132-146
5. Libicki M. Cyberdeterrence and Cyberwar / Martin C. Libicki.- RAND Corporation, 2009.- 238 p.
6. Kramer F., Starr S., Wentz L. Cyberpower and National Security / Franklin D. Kramer, Stuart H. Starr, Larry Wentz.- Washington, D.C: Potomac Books, 2009.- 642 p.
7. Addico J. Cyberterrorism: Legal Policy Issues / Jeffrey F. Addico // Legal Issues in the Struggle against Terrorism / John N. Moore, Robert F. Turner.- Durham, NC: Carolina Academic Press, 2010.- P.592
8. Charles, J. D., Jr. Perspectives for cyber strategists on law for cyberwar/ J.Charles // Strategic Studies Quarterly.- 2011.- №5(1).- P.81-99.
9. It will soon be too late to stop the cyberwars [Электронный ресурс] / Bruce Schneier // Financial Times, 2 December 2010, - Режим доступа: <http://www.ft.com/cms/s/0/f863fb4c-fe53-11df-abac-00144feab49a.html#axzzl9cNCeszp>
10. The irrelevance of START [Электронный ресурс] / Charles Krauthammer // The Washington Post.- Режим доступа: <http://www.washingtonpost.com/wp-dyn/content/article/2010/11/25/AR2010112502232.html>
11. Defending a New Domain: The Pentagons Cybers strategy [Электронный ресурс] / William J. Lynn // Foreign Affairs.- 2010.- №89 (5).- Режим доступа: <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>
12. Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict [Электронный ресурс] / Michael N. Schmitt // Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US. Policy.- Washington: National Academies Press, 2010.- Режим доступа: http://books.nap.edu/openbook.php?precord_id=12997&page=R1
13. Clarke R., Knake R. Cyber War: The Next Threat to National Security and What to Do About It / Richard A. Clarke, Robert K. Knake.- Harper Collins, 2010.- 320 p.
14. Creveland van M. Command in War / Martin van Creveld.- Cambridge: Harvard University Press, 1985.- 352 p.
15. Joel Brenner. America the Vulnerable. Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. N. Y.: The Penguin Press. 2011. 320 p / О. Демидов // Индекс безопасности.- №1(104).-Том 19.- С. 257-260
16. Cyberwarfare a Viable Nonviolent Alternative to Military Strikes [Электронный ресурс] / L.Lawrence, Jr.Muir // U.S.News.- Режим доступа: <http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-a-viable-nonviolent-alternative-to-military-strikes>
17. Cyberwarfare Treaty Would Be Premature, Unnecessary, and Ineffective [Электронный ресурс] / Sean Lawson // U.S.News.- Режим доступа: <http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-treaty-would-be-premature-unnecessary-and-ineffective>
18. International Cyberwar Treaty Would Quickly Be Hacked to Bits [Электронный ресурс] / Jon Lindsay // U.S.News.- Режим доступа: <http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/international-cyberwar-treaty-would-quickly-be-hacked-to-bits>
19. Setting International Norms on Cyberwar Might Beat a Treaty [Электронный ресурс] / Martin Libicki // U.S.News.- Режим доступа: <http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/setting-international-norms-on-cyberwar-might-beat-a-treaty>
20. A Cybersecurity Treaty Is a Bad Idea [Электронный ресурс] / James Lewis // U.S.News.- Режим доступа: <http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/a-cybersecurity-treaty-is-a-bad-idea>
21. A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict [Электронный ресурс] / Davis Brown // The Harvard International Law Journal Online.- Режим доступа: http://www.harvardilj.org/wp-content/uploads/2010/10/HILJ_47-1_Brown.pdf
22. Tang L. New Approaches to Information Security / Lan Tang // Contemporary International Relations.- 2010.- Vol.20 №3.- P.41-49
23. Carnesale A. Living with Nuclear Weapons / A.Carnesale.- Harvard University Press; 5th Edition edition, 1983.- 288 p.
24. В Gartner борьбу с киберугрозами считают финансовой пирамидой [Электронный ресурс] // SecurityLab.ru.- Режим доступа: <http://www.securitylab.ru/news/443716.php>
25. Brzezinski Z. Game Plan: A Geostrategic Framework for the Conduct of the U.S.-Soviet Contest / Zbigniew Brzezinski.- Boston: Atheneum, 1986.- 288 p.
26. Lin, H. Escalation dynamics and conflict termination in cyberspace / H.Lin // Strategic Studies Quarterly.- 2012.- №6(3).- 46-70.
27. McConnell M. How to Win the Cyber-war. We're Loosing [Электронный ресурс] / Mike McConnell // The Washington Post.- 2010.- Режим доступа: <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html>
28. Китай собирается вводить новые правила борьбы с международным кибершпионажем [Электронный ресурс] // SecurityLab.ru.- Режим доступа: <http://www.securitylab.ru/news/438546.php>
29. Путин обсудил с премьером Индии тему международного терроризма, затронув вопрос использования инфотехнологий в преступных целях [Электронный ресурс] // NEWSru.com.- Режим доступа: http://www.newsru.com/arch/russia/21oct2013/put_ter.html