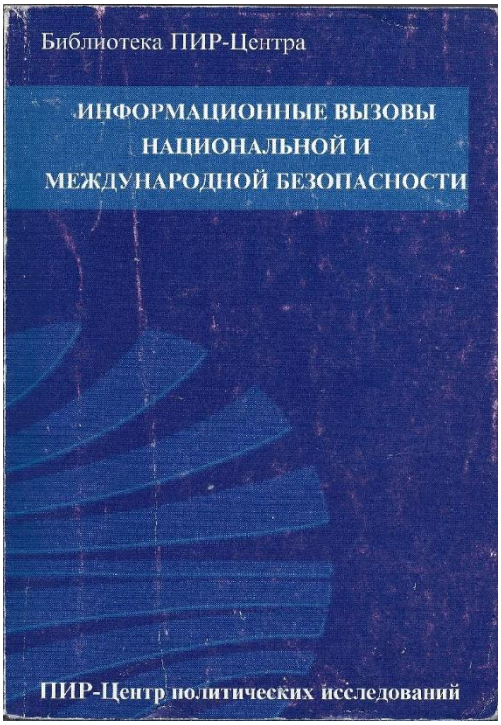
«Все позволено» и новая уязвимость

Владимир Орлов

Автор - Профессор МГИМО МИД РФ; Заведующий Центром глобальных проблем и международных организаций Дипломатической академии МИД РФ; основатель ПИР-Центра



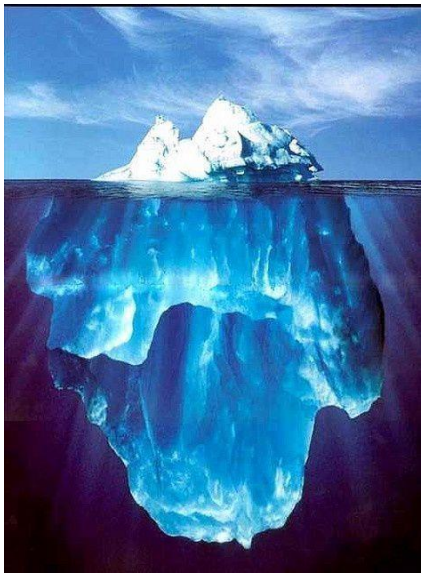
Дело было без малого два десятилетия назад. Мне принесли рукопись книги. Называлась она «Информационные вызовы национальной и международной безопасности». Это сейчас проблематика международной информационной безопасности (МИБ) – или «кибербезопасности», как ее, сильно упрощая, еще называют – у всех на слуху и находится в топе глобальных угроз. А тогда о МИБ не то чтобы никто не говорил: говорили, конечно, особенно в узких экспертных кругах, но как-то «через запятую», и эта проблема оказывалась на заднем плане. А вскоре случилось 11 сентября, и угроза международного терроризма на время затмила все остальные.

Листая старые страницы

Но достаточно мне было пролистать принесенную мне рукопись, как я понял: речь идет об аналитическом труде неординарного калибра. И о глобальной угрозе калибра гораздо большего, чем мне самому казалось до той поры.

Особенное внимание в работе уделялось сценариям кибервойн… хотел сказать «кибервойн будущего», однако авторы справедливо обращали внимание, что это уже «войны настоящего». Авторы книги предупреждали о возможности перерастания киберконфликта в ракетно-ядерный. Они были убеждены, что при двустороннем вооруженном конфликте совершенно непредсказуемой является реакция стороны, подвергшейся воздействию информационного оружия:

«Может сложиться ситуация, когда выявление факта применения информационного оружия даже в очень ограниченном масштабе может привести к «испугу» и предположению, что вскрыта только «вершина айсберга» информационной атаки. Вслед за таким выводом может последовать ограниченное или массированное применение ядерного оружия»[1].



«Запретить разработку и использование информационного оружия на нынешнем этапе вряд ли удастся, как это сделано, например, для химического или бактериологического оружия, – делали авторы неутешительный вывод. – Понятно также, что ограничить усилия многих стран по формированию единого глобального информационного пространства невозможно. Поэтому развязки возможны только на пути заключения разумных соглашений, опирающихся на международное право и минимизирующих угрозы применения информационного оружия»[2].

Рукопись я тогда без промедления опубликовал, и вышедшая книга не прошла незамеченной.

Голые и напуганные

За годы, прошедшие с тех пор, беспрецедентно шагнули вперед информационные технологии. Интернет стал сродни кислороду: отключи – и люди задохнутся; зависимость от интернета сделалась тотальной. Об информационных войнах теперь не пишет только ленивый, а в студенческой среде будущих международников про «кибер» хотят писать свои выпускные работы гораздо больше студентов, чем про «ядерку». В ООН не один год заседала Группа

[1] Информационные вызовы национальной и международной безопасности. Под ред. А.В. Федорова и В.Н. Цыгичко. М.: ПИР-Центр, 2001. С. 94-95.
[2] Информационные вызовы национальной и международной безопасности. Под ред. А.В. Федорова и В.Н. Цыгичко. М.: ПИР-Центр, 2001. С. 198-199.

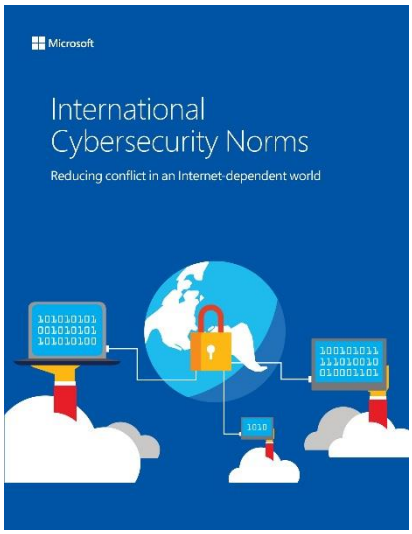
правительственных экспертов (ГПЭ), обеспокоенных проблематикой МИБ [3]. Простые люди чувствуют себя перед угрозами, исходящими из информационного пространства, используя название известного телешоу, будто «голые и напуганные». «Голые» – потому что ничем не защищены. «Напуганные» – потому что знают, что ничем не защищены. Страх и растерянность, граничащие с паникой и паранойей, то и дело окутывают, будто смог, целые страны.

И несмотря на все это, – воз и ныне там. Международное сообщество за все эти годы ни на йоту не приблизилось к выработке того, что могло бы стать «киберДНЯО» - юридически обязывающим договором о нераспространении кибероружия, который поставил бы заслон перед информационными войнами. «Это невозможно. В отличие от ядерного оружия, в случае с кибероружием мы далеко не всегда сможем идентифицировать источник атаки. Больше того, мы почти никогда не сможем отделить государственные субъекты от негосударственных», – разводят руками маститые эксперты. Правда, не менее маститые эксперты не видят тут ничего невозможного:

«Я бы предложила создать (…) международную конвенцию по нераспространению кибероружия и признанию невозможности для всех стран распространения кибероружия, - заявила Наталья Касперская, президент группы компаний InfoWatch. – Необходимо об этом говорить и стремиться к этому, чтобы все страны, особенно ведущие, такую конвенцию подписали»[4].

[3] Полное ее название: Группа правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. О судьбе ее мандата см.: Демидов Олег. Многостороннее регулирование киберпространства: «лебедь, рак и щука». ПИР-Центр, 14 ноября 2018. http://www.pircenter.org/blog/view/id/355

[4] Московская конференция по международной безопасности (MCIS), 2017. М.: Материалы конференции. С. 107



В качестве компромисса (либо первого шага по преодолению «кибербеспредела») выдвигаются идеи по выработке международных «кодексов поведения» в киберпространстве, например, «Парижский призыв к обеспечению доверия и безопасности в киберпространстве» [5], оглашенный в ноябре 2018 г. президентом Франции, или документ по международным нормам кибербезопасности, представленный в 2014 г. корпорацией Майкрософт на саммите Global Cyberspace Cooperation в Берлине[6].

Действительно, первый шаг делать надо, и он не обязательно должен быть юридически обязывающим и всеобъемлющим – хотя и важно, чтобы уже на первом этапе были представлены интересы различных регионов мира. Однако общая слабость «мер по укреплению доверия» и «кодексов поведения» – аморфность, неверифицируемость и необязательность для исполнения. ДНЯО – крупнейший международный договор XX века, ставший краеугольным камнем глобальной безопасности – тем и силен, что близок к всеохватности: в его юрисдикции –192 государства планеты. Глобальный характер информационных угроз требует и глобального ответа: договора, столь же авторитетного и универсального, каким в ядерной области является ДНЯО.

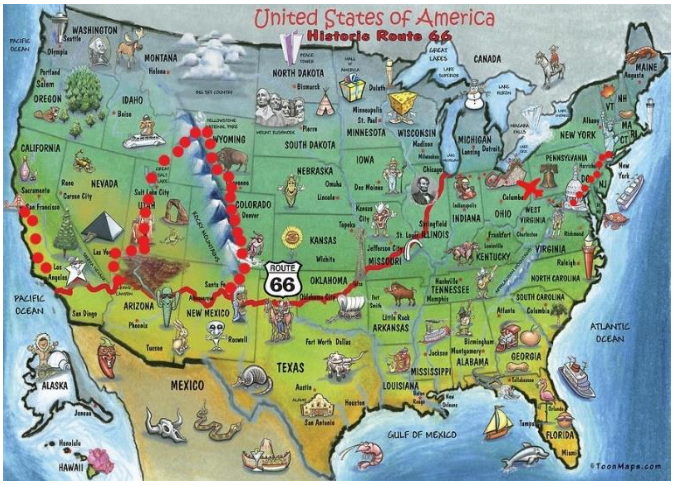
В этих условиях, не окончательным решением, но весомым шагом на пути к нему могли бы стать двусторонние соглашения между ключевыми субъектами информационного пространства. Однако кризис, который мы сегодня наблюдаем – и который на наших глазах усугубляется – в системе договоров по контролю над вооружениями – не позволяет говорить о реалистичности таких двусторонних юридически обязывающих соглашений в информационной сфере (или, если угодно, в области киберoружия) – по крайней мере, на ближайшую перспективу.

Значит, все позволено? Соблазнительный вывод. Потому что как раз вот это чувство вседозволенности, – оно пьянит. Оно развращает. О масштабах американских операций в киберпространстве мы догадывались и раньше. Но благодаря разоблачениям Эдварда Сноудена, сделанным в июне 2013 г., кое-что

[5] О том, почему этот «призыв» не имеет шансов на реализацию, см.: Демидов Олег. Многостороннее регулирование киберпространства: «лебедь, рак и щука». ПИР-Центр, 14 ноября 2018. http://www.pircenter.org/blog/view/id/355
[6] http://aka.ms/cybernorms

из тайного стало явным. Степень американского (и британского [7]) кибервмешательства по всему миру является беспрецедентной. Основной мишенью информационных атак со стороны американского государства оказалась горстка еще не только де-юре, но и де-факто суверенных государств, проводящих независимую внешнюю политику. Так, США неоднократно – и в основном успешно – применяли кибероружие против Ирана, в том числе и против его мирной ядерной инфраструктуры[8].

Но все-таки центральным объектом для американских информационно-кибернетических операций была и остается Россия. Согласно оценке, озвученной в феврале с.г. из Кремля, «территория США постоянно используется для организации огромного количества кибератак против различных российских структур. Это – реальность, в которой мы живем»[9]. Характерен заголовок статьи в свежем номере авторитетного Бюллетеня атомных ученых, выходящего в США: «Кибератаки против России – государства с самым большим ядерным арсеналом – представляют глобальную угрозу»[10] .



Новая уязвимость

Летом 2018 г. я пересек девятнадцать Соединенных Штатов. Говорил с простыми людьми где-нибудь в Оклахоме или в Вайоминге. Пытался разобраться, что тревожит «одноэтажную Америку» сегодня. И как простые американцы относятся к России. А относятся они к России в основном или хорошо, или никак. Никакой «русофобии», которой страдают вашингтонские элиты, я в американской глубинке не заметил… правда, если при наших разговорах был выключен телевизор. Но вот если телевизор был как на зло включен – и если он был включен не на спортивных каналах, а на новостных, – тогда в наши разговоры начинали вклиниваться совершенно сюрреалистичные мотивы: «российской угрозы»…

---

[7] По сообщениям СМИ, Сноуден получил доступ к данным электронной разведки не только США, но и Великобритании; в его распоряжении могли находиться до 58 тыс. британских секретных документов. – См.: ТАСС. 15 ноября 2013 г.

[8] См.: Oleg Demidov. Global Internet Governance and International Security in the Field of ICT Use. Moscow - Geneva, 2015

[9] Kremlin says cyber attacks on Russia often launched from U.S. territory. February 27, 2019. https://www.reuters.com/article/us-usa-trump-russia-kremlin/kremlin-says-cyber-attacks-on-russia-often-launched-from-u-s-territory-idUSKCN1QG183?il=0

[10] Ramana M. V. & Mariia Kurando (2019). Cyberattacks on Russia - the nation with the most nuclear weapons - pose a global threat. Bulletin of the Atomic Scientists, 75:1, pp.44-50.

«вмешательства России в американские выборы»… «косвенного контроля со стороны России за многими местными американскими СМИ», «коварства Кремля»… и т.п. Но если русофобии в американской глубинке я не встретил, зато вот что встретил: ощущение уязвимости. И здесь глубинка вполне совпадает с Вашингтоном, хотя в столице это ощущение уязвимости еще острее. С чего бы это?

16 июля 1945 г. Соединенные Штаты обрели монополию над ядерным оружием, когда испытали атомную бомбу в Аламогордо под кодовым названием «Троица». Но чувство монополии и безнаказанности не прошло у Соединенных Штатов и 29 августа 1949 г., когда атомную бомбу испытал Советский Союз. Вроде бы исключительность США в ядерных вооружениях была подорвана… однако еще несколько лет разрыв в ядерных арсеналах наших двух стран был столь велик – и настолько он был в пользу Соединенных Штатов, – что те продолжали чувствовать себя комфортно и неуязвимо. И даже когда СССР стал сокращать разрыв в ядерных вооружениях, совершенствовать точность и дальность ракетных носителей, даже когда он 30 октября 1961 г. испытал на Новой Земле водородную «царь-бомбу», – и тогда Вашингтон не воспринимал Москву в ядерном соревновании на равных, ощущая себя уверенно-защищенно.

Понадобился Карибский кризис октября 1962 г., появление советских ракет и ядерного оружия на Кубе, в «подбрюшье» Соединенных Штатов, чтобы до американского руководства дошло: мир изменился. Ядерной неуязвимости Соединенных Штатов больше нет и не будет. Надо отдать должное президенту Джону Кеннеди. Когда читаешь расшифровки его совещаний в Белом доме в дни Карибского кризиса[11], видишь, день за днем, как он мужает, тщательно вникает в ситуацию, вникнув, удерживает своих министров и советников от сползания к ядерной войне, как находит в себе силы к компромиссу. И это несмотря на огромное внутриполитическое давление, на призывы «показать себя с русскими пожестче», «ответить со свой мощью», ведь Карибский кризис разворачивался за считанные дни до промежуточных выборов в Конгресс.

Уроки были извлечены. Через каких-то девять месяцев СССР и США ставят свои подписи под Договором о запрещении ядерных испытаний в трех средах (атмосфере, космосе и под водой), вокруг которого несколько лет топтались переговорщики и находили многочисленные предлоги, почему «нельзя подписывать»: а все потому, что не было политической воли лидеров, что не получали «сигнал сверху». Вскоре начинается работа над Договором о нераспространении ядерного оружия, чему не препятствует смена хозяина Белого дома после убийства Кеннеди. Понимание, что нельзя ставить судьбы своих

[11] См.: The Kennedy tapes: inside the White House during the Cuban missile crisis. Harvard University Press, 1998.

стран, судьбы всего мира на грань ядерной катастрофы, пришло как раз в разгар Карибского кризиса. Совместные советско-американские усилия по предотвращению распространения ядерного оружия в мире вкупе с двусторонне выстроенной системой ядерного сдерживания и архитектурой контроля над вооружениями позволили избежать сползания к бездне.

Конечно, нельзя игнорировать тот факт, что между ядерным и кибероружием имеются колоссальные различия. Как справедливо замечает Игорь Иванов, «ядерное оружие создавалось и развертывалось не в целях последующего применения, а для сдерживания потенциальных противников. Страх глобальной ядерной войны предполагал максимальную осторожность и высокую ответственность ядерных держав. С кибероружием дело обстоит иначе – мало кто сейчас считает, что его применение создает непосредственную угрозу всему человечеству. А потому соблазн применить может оказаться слишком большим. При этом кибероружие в значительной степени анонимно, кибератака может быть произведена практически из любой точки планеты, и реальный киберагрессор останется неопознанным, а следовательно – и ненаказанным»[12].

Страх перед кибероружием не синонимичен страху перед оружием ядерным. Но он тоже велик, и нарастает, и особенно мучителен как раз оттого, что нет того «золотого петушка», который позволил бы легко определить, с какой стороны – с запада ли, с востока, или еще откуда – «лезет рать».

Ощущение новой уязвимости, что по «невидимым сетям» вероятный противник (будь то негосударственный субъект или, с большей вероятностью, государство) может добраться и до систем управления ядерным оружием, и до личных электронных почтовых ящиков влиятельных лиц, и до систем подсчета голосования, и до объектов критической инфраструктуры[13], кого-то вводит в ступор, кого-то доводит до паранойи, а кого-

[12] Иванов И.С. Как трава сквозь асфальт. Россия в Глобальной Политике, № 4, 2018.

[13] О киберугрозах для гражданской ядерной инфраструктуры я подробно писал в работе, подготовленной для Всемирного экономического форума. См.: Vladimir Orlov. Our nuclear facilities are increasingly vulnerable to cyber threats. This is what policy makers need to know. October 5, 2016. https://www.weforum.org/agenda/2016/10/our-nuclear-facilities-are-increasingly-vulnerable-to-cyber-threats-this-is-what-policy-makers-need-to-know. См. также: Ramana M. V. & Mariia Kurando (2019) Cyberattacks on Russia - the nation with the most nuclear weapons - pose a global threat. Bulletin of the Atomic Scientists, 75:1, 44-50.

то подталкивает к планированию зеркальных или асимметричных ответных действий «на поражение». Око за око, зуб за зуб. Даже если и око, и зуб – виртуальные. Хотя грань-то между виртуальным и реальным как раз и размывается, и так недалеко до того, чтобы остаться слепым да беззубым. Именно ощущение вот этой новой уязвимости – сродни ощущению времен Карибского кризиса, что на США направлены с Кубы советские ракеты – я все больше замечаю и в Вашингтоне, и за его пределами.

Я не хотел бы сейчас гадать по поводу того, что произошло или не произошло в 2016 году в отношении подготовки к американским президентским выборам. Для меня очевидно, что американские избиратели свой выбор сделали не под «внешним» влиянием, а исходя из своих собственных убеждений. Те, кто думают иначе, по-моему, не уважают свой собственный народ, считая, что он настолько подвержен внешней манипуляции. Вообще, «российская угроза», «российский след» для многих в Вашингтоне сегодня не более чем удобный повод «поквитаться» со своими внутриполитическими оппонентами. Поляризация американских элит зашла так далеко, что для драки здесь любые средства хороши. А Россия просто удобно попалась под руку, вот «российским следом» и швыряются друг в дружку.

Но, в то же время, настороженность в отношении кибервозможностей России – это реальный фактор американской внутренней и внешней политики. Он присутствует не только в стане демократов, но и в стане республиканцев, которых сегодня кто-то наивно причисляет к «русофилам». Ее причина – куда глубже, чем попытка докопаться до ответа на вопрос, вмешивалась ли Россия в американские выборы. Ее причина – как раз в этом ощущении новой уязвимости. Россия не вмешивалась… но ведь могла вмешаться… и еще может.

Ощущение новой уязвимости требует ответа. Инстинктивная реакция – введение санкций. Однако санкциями кибервойны не остановить. Зато ими можно подлить масла в огонь.

На войне как на войне

Кибервойна уже идет. Кто-то не заметил? Впрочем, неудивительно, что не заметили. Потому что это преимущественно невидимая война. Именно такая, которой и положено быть кибервойне[14].

Российские специалисты уже довольно давно определили характеристики таких кибервойн. Они, в частности, обратили внимание на необычайную сложность

[14] См.: Дылевский И.Н., Комов С.А., Петрунин А.Н.. Об информационных аспектах международно-правового понятия «агрессия». Военная мысль, №10, 2013, с. 3-12.

задач тактического предупреждения и оценки ущерба: «Существует реальная возможность того, что представленные национальному военно-политическому руководству оценки правоохранительных органов и разведывательных служб по конкретным случаям воздействия или ситуациям будут довольно противоречивы. Нападающая сторона, используя информационное оружие, способна с беспрецедентной оперативностью проводить стратегические операции и после выполнения задач мгновенно возвращаться в установленные пределы киберпространства»[15].

Для проведения операций, целью которых является дестабилизация внутреннего положения государства-противника, по мнению российских специалистов, в качестве наиболее эффективного канала выступают СМИ. При этом «могут применяться различные способы оказания воздействия через СМИ, в том числе и связанные с воздействием на инфраструктуру самих СМИ; оказание воздействия через национальные СМИ противника; в случае, если это невозможно, а также в целях достижения большего эффекта – формирование альтернативных каналов информационно-психологического воздействия (альтернативные СМИ, иновещание, (…) интернет); оказание внешнего давления на политическое руководство и общественное мнение государства-противника, создание международного климата, препятствующего реализации планов противника»[16].

При этом, подавление существующих систем национального вещания, например уничтожение ретрансляционных спутников, телевизионных и радиовещательных станций специалисты относят к наименее эффективным методам в сравнении с вышеперечисленными.

Диалог по кибервопросам становится в условиях кровожадной внутриполитической борьбы в США проблематичным. В этой связи, неудивительно, что ряд экспертов в Соединенных Штатах ожидает применения Россией кибероружия как неизбежности: око за око… Не как превентивного, но как ответного удара. Тем более там видят, что Россия способна все более эффективно и многопланово, к тому же асимметрично, действовать в информационном поле. Только, в отличие от войны ядерной, здесь могут быть

[15] Информационные вызовы национальной и международной безопасности. Под ред. А.В. Федорова и В.Н. Цыгичко. М.: ПИР-Центр, 2001. С. 93.

[16] Информационные вызовы национальной и международной безопасности. Под ред. А.В. Федорова и В.Н. Цыгичко. М.: ПИР-Центр, 2001. С. 122-123.

сотни тысяч незримых обменов такими ударами; правда, лишь немногие из них будут направлены для использования уязвимости сугубо военной; остальные – для использования уязвимости политической или психологической.

Раз война, значит крупнейшие американские IT-корпорации реагируют. В частности, создают «оперативные штабы», или war rooms. Первенство здесь принадлежит Facebook, при участии принадлежащих этой компании Instagram и WhatsApp. В war room компании Facebook нет окон (в прямом смысле этого слова), и есть двадцать «борцов с фейковым проникновением», число которых со временем предполагается довести до двадцати тысяч. Как сказал Марк Цукерберг, выступая перед Конгрессом, «мы слишком поздно заметили [российское] вмешательство, и теперь всеми силами стремимся предотвратить злоумышленников». По словам главы отдела кибербезопасности Facebook, «наша работа - засечь любого, кто попытается манипулировать общественным мнением. Найти и обезвредить»[17].

О «борьбе» в киберпространстве объявил и ключевой союзник Соединенных Штатов – Великобритания. Причем сделал это устами обычно неразговорчивого руководителя МИ-6 Алекса Янгера, известного также как «С». В своем программном выступлении по кибервопросам глава 3 декабря 2018 г. в шотландском университете Сент-Эндрюс глава МИ-6 заявил, что «борьба за киберпорядок» объявлена, и она ведется против «опытного оппонента, не связанного понятиями закона и морали»[18]. Хотя сначала имя этого «опытного оппонента» (или оппонентов) прямо названо не было, затем в выступлении прямо была названа Россия.

Карибский киберкризис?

Время для диалога уходит. Американское «все позволено» уже наталкивается на серьезное противодействие, причем не только России, но и ее ключевого стратегического партнера в глобальных делах – Китая[19]. Но даже это пока не приводит американцев к понимаю не просто важности, но необходимости договариваться.

---

[17] См.: https://techcrunch.com/2018/10/18/facebook-election-war-room/

[18] In rare speech, MI6 chief says cyber brings ‘potentially existential challenge’. Fifth Domain. December 4, 2018. https://www.fifthdomain.com/international/2018/12/04/in-rare-speech-mi6-chief-says-cyber-brings-potentially-existential-challenge/

[19] При том, что и Россия, и Китай, координируя свои международные подходы в области МИБ, на деле пока, в основном, играют каждый сам за себя, стараясь хотя бы «не стрелять по своим».

Напротив, принятая в 2018 г. Национальная стратегия для киберпространства США предполагает не только оборону, но и наступательные действия в отношении военной и киберинфраструктуры Китая и России. Ведущие американские специалисты с опытом работы на ключевых «киберпостах» в Пентагоне в эти дни высказывают вот такие рекомендации: «Соединенным Штатам следует дистанционно поражать инфраструктуру системы управления российскими вооруженными силами через заражение вирусами или посредством внедрения вредоносных объектов в эту систему через завербованных лиц. Потенциально, США могли бы вырубить электроснабжение вокруг российских военных баз, с которых ведется российская кибердеятельность. Также можно было бы, в партнерстве с частными компаниями, выдавить русских из негосударственных интернет-сетей и закрыть элементы российского сегмента интернета»[20].

Россия не может позволить себе закрыть глаза на такой сценарий. Как заметил недавно Сергей Нарышкин,

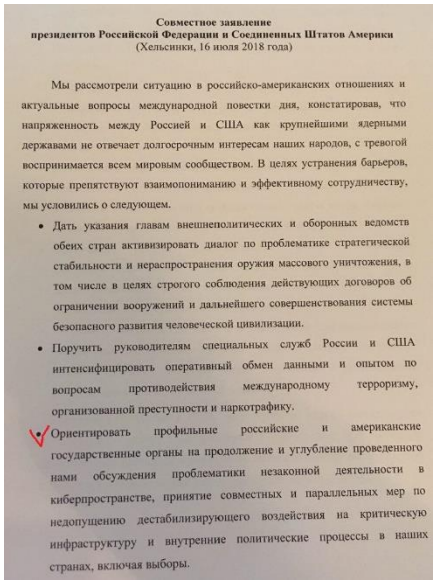
«движимые химерами прошлого, Соединенные Штаты начинают все больше походить на самонадеянного библейского силача Голиафа, который, как известно, был повержен юным Давидом.(…) Важно прекратить безответственную игру на повышение ставок и отказаться от проецирования силы в межгосударственных отношениях. Не доводить дело до нового Карибского кризиса»[21].

Готовясь к саммиту в Хельсинки в июле 2018 г., российская сторона подготовила проект Совместного заявления президентов России и США, где на первой же

[20] Jonathan Reiber. What Happens When the US Starts to 'Defend Forward' in Cyberspace? Defense One. November 5, 2018. https://www.defenseone.com/ideas/2018/11/what-happens-when-us-starts-defend-forward-cyberspace/152580/. По вопросу о Национальной стратегии для киберпространства США, см. глубокий анализ, проведанный Олегом Демидовым и Маргаритой Ангмар в вышедшем в январе 2019 г. докладе: «Киберстратегия США 2018. Значение для глобального диалога о поведении в сфере использования ИКТ и российско-американских отношений». М.: ПИР-Центр; «Триалог» (Серия «Индекс Безопасности»), 2019. – 30 с.

[21] Выступление Директора Службы внешней разведки Российской Федерации Сергея Нарышкина на конференции MCIS-2018. 4 апреля 2018. http://mil.ru/mcis/news/more.htm?id=12170190@cmsArticle

странице, третьим пунктом (следом за вопросами стратстабильности и нераспространения, а также терроризма) было предложено ориентировать профильные российские и американские государственные органы на продолжение и углубление проведенного нами обсуждения проблематики незаконной деятельности в киберпространстве, принятие совместных и параллельных мер по недопущению дестабилизирующего воздействия на критическую инфраструктуру и внутренние политические процессы в наших странах, включая выборы[22].



Совместное заявление
президентов Российской Федерации и Соединенных Штатов Америки
(Хельсинки, 16 июля 2018 года)

Мы рассмотрели ситуацию в российско-американских отношениях и актуальные вопросы международной повестки дня, констатировав, что напряженность между Россией и США как крупнейшими ядерными державами не отвечает долгосрочным интересам наших народов, с тревогой воспринимается всем мировым сообществом. В целях устранения барьеров, которые препятствуют взаимопониманию и эффективному сотрудничеству, мы условились о следующем.

- Дать указания главам внешнеполитических и оборонных ведомств обеих стран активизировать диалог по проблематике стратегической стабильности и нераспространения оружия массового уничтожения, в том числе в целях строгого соблюдения действующих договоров об ограничении вооружений и дальнейшего совершенствования системы безопасного развития человеческой цивилизации.
- Поручить руководителям специальных служб России и США интенсифицировать оперативный обмен данными и опытом по вопросам противодействия международному терроризму, организованной преступности и наркотрафику.
- Ориентировать профильные российские и американские государственные органы на продолжение и углубление проведенного нами обсуждения проблематики незаконной деятельности в киберпространстве, принятие совместных и параллельных мер по недопущению дестабилизирующего воздействия на критическую инфраструктуру и внутренние политические процессы в наших странах, включая выборы.

Как известно, Совместного заявления в Хельсинки принято не было. Больше того, не было ни нового российско-американского саммита, ни даже содержательного разговора между двумя президентами, когда многосторонние встречи в верхах сталкивали их в Париже и Буэнос-Айресе, так как по возвращении из Хельсинки Трамп столкнулся с угрозой обвинений в государственной измене.

> «После изобретения и создания ядерного оружия человечество находится в состоянии относительного покоя, относительного, конечно, за исключением региональных конфликтов, состоянии относительного глобального покоя почти 75 лет. Давайте вспомним Черчилля, который сначала ненавидел Советский Союз, потом называл Сталина великим революционером, когда нужно было бороться с нацизмом, а после того, как американцы получили ядерное оружие, призывал немедленно фактически уничтожить Советский Союз. Помните, его речь в Фултоне была стартом к «холодной войне». Но как только у Советского Союза появилось ядерное оружие, Черчилль стал инициатором сосуществования двух систем. И не потому, что, я думаю, он не был таким приспособленцем, а он исходил из реалий. Из реалий исходил. Умный человек был, практический политик. Здесь мало что поменялось с этого времени. (…)

[22] См.: Елена Черненко и Екатерина Мареева в статье «Кибертрофированное сознание. США боятся кибератак, но отказываются бороться с ними вместе с Россией». Коммерсант, 9 августа 2018.

Мы же много раз говорили: давайте примем какие-то общие правила [в области информационно-коммуникационных технологий], давайте об этом договоримся. Мы много раз предлагали в последние месяцы президентства господина Обамы даже выработать правила и закрепить их в каких-то межправсоглашениях по поводу использования современных коммуникационных ресурсов. Я уже говорил об этом неоднократно. В последние месяцы пребывания у власти администрация господина Обамы вдруг согласилась, но уже просто не успела ничего реализовать. После этого мы предлагали и администрации господина Трампа. Вроде сначала сказали: да, это интересно. Потом тоже опять всё зависло.

Давайте мы договоримся об этом, об общих правилах. Во всех странах эти ресурсы есть, у нас тоже есть. Есть ресурсы, которые не подчинены государству. Государство может начать на них влиять, если сошлётся на какие-то обязательства нашего государства, но они должны быть взаимными – это же абсолютно понятная вещь.

Вот не было ядерного оружия ни у кого, кроме США, и что, США договаривались с кем-то об ограничении в сфере ядерных вооружений? Нет. Но как только у Советского Союза появилось – я же вспомнил Черчилля, – Соединённые Штаты сочли возможным начать в какой-то момент переговоры об ограничении – с целью самосохранения».[23]

В.В. Путин
Встреча с главами мировых информагентств
6 июня 2018 г.

Да, идут отдельные, порой не афишируемые, российско-американские встречи на экспертном уровне, в формате «второй» или «полуторной» дорожек. Последнее более продуктивно. Как со-организатор и участник одного из таких форматов, могу сказать, что российско-американская дискуссия по кибербезопасности, прошедшая в декабре прошлого года в Вене[24], при участии представителей

[23] Встреча с главами мировых информагентств. Санкт-Петербург. 6 июня 2019 г. http://kremlin.ru/events/president/news/60675

[24] "Укрепление стратегической стабильности в российско-американских отношениях: повестка дня на 2018-2020 гг.". Вторая встреча рабочей группы. Вена. 8 декабря 2018 г. http://www.pircenter.org/pages/1049-7919183

нескольких международных организаций, и помещенная в более широкий контекст стратегической стабильности, была, безусловно, полезной и интеллектуально стимулирующей. Однако без иллюзий: вырабатываемые такими форматами и площадками идеи могут быть востребованы лишь когда общий климат в двусторонних отношениях потеплеет. Мы же наблюдаем дальнейшее падение температуры.

Риск перерастания нынешней ситуации в глобально-хаотичную кибервойну все больше тревожит международное сообщество. По словам генерального секретаря ООН Антониу Гутерриша, «злонамеренные действия в киберпространстве приводят к снижению доверия между государствами». В своей Повестке дня по разоружению генсек ООН призывает «безотлагательно выстроить международные меры доверия и повышенной ответственности в киберпространстве»[25].

Неужели, чтобы дойти до осознания важности «договариваться» по киберделам, шире – по всей повестке МИБ[26] – придется пережить некий «Карибский киберкризис»? Или все это не более чем очередные модные «страшилки»?

Не хотелось бы впадать в фатализм. Но еще меньше хотелось бы принимать позу страуса, игнорируя тот очевидный факт, что - хотят того крупнейшие мировые игроки или нет, - но они к такому «Карибскому кризису» скатываются. Потому что кибервойна идет. Без правил. С высокой долей неопределенности. С раскручиваемой спиралью напряженности. С гонкой кибервооружений. И, конечно, нет никаких гарантий, что новый кризис будет контролируемым и что он приведет к «катарсису» в вопросах регулирования МИБ. Ведь только выпусти киберджинна из бутылки…

Поэтому усиливается тревожное ощущение, что новые – настоящие, а не «фейковые» – драматические события в киберпространстве еще только предстоят.

Россия в глобальной политике

Том 17, № 2, март-апрель 2019 г., стр. 46-56

[25] António Guterres, United Nations Secretary-General. “Securing our common future”. An Agenda for Disarmament. May 24, 2018

[26] Термины имеют значение. Два десятилетия назад Россия предложила повестку дня по вопросам «международной информационной безопасности». Термин тогда многим в мире пришелся не по вкусу, и в экспертном сообществе быстро привилось упрощенческое и хлесткое: «кибербезопасность». Тем не менее, с позиций сегодняшнего дня и сегодняшних угроз куда лучше понимаешь, что именно комплексный подход к международной информационной безопасности должен быть взять за основу при поиске глобальных «развязок».