МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОБЩАЯ ХАРАКТЕРИСТИКА И РОССИЙСКИЙ ПОДХОД К ИЗУЧЕНИЮ

Аннотация

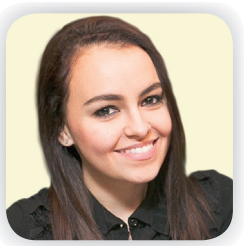
XXI век ознаменовал качественно новый этап развития, ключевой характеристикой которого является активное использование информационно-коммуникационных технологий (далее — ИКТ). В эпоху глобальной информатизации присутствие государства во всемирной паутине формирует его положительный образ за рубежом, влияет на климат отношений с другими акторами, а также рассматривается как важный инструмент популяризации и защиты национальных интересов. Уязвимость цифровой сферы вкупе с уникальными возможностями передовых ИКТ способствовали появлению нового вида оружия — информационного, а обеспечение информационной безопасности стало одним из главных вопросов мировой повестки дня. Россия предпринимает серьезные шаги по обеспечению информационной безопасности не только в рамках государственной политики, но и на международной арене. Однако существующие противоречия в подходах России и Запада обусловили отсутствие общепринятого понятийного аппарата и международных правил поведения в информационном пространстве.

Ключевые слова: международная информационная безопасность, информационное пространство, информационное оружие, кибервойна.

Автор

Ющенко Виктория Александровна

Магистр международных отношений
МГИМО (У) МИД РФ (Москва, Россия)



Информационное пространство как новая сфера международных отношений

Научно-технический прогресс (далее — НТП) является безусловным благом человечества, одним из ключевых условий прогресса и безграничного продвижения процессов демократизации. Вместе с тем его продукты стали источником новых угроз и вызовов, связанных с использованием потенциала ИКТ в целях, несовместимых с поддержанием международного мира, стабильности и безопасности. Среди них — появление информационного оружия, активизация информационной преступности, развязывание и ведение информационных войн. Важным шагом в развитии ИКТ стало появление информационного пространства, которое существенным образом отличается от традиционных сфер международных отношений, таких как воздушное и морское пространство, земля и ее недра.

Сложность феномена международной информационной безопасности (далее — МИБ) в том, что для его наиболее полного осмысления необходимо рассмотрение смежных с изучаемой проблематикой терминов, таких как информационное пространство и информационное общество. Ряд экспертов особо подчеркивают принципиальное различие между контекстуально близкими информационным

пространством и информационным обществом, которые нередко употребляются в качестве синонимов. Информационное пространство представляет собой совокупность информационных ресурсов, систем и технологий, функционирующих на основе общих принципов и формирующих структуру, которая обеспечивает информационное взаимодействие между людьми. Составляющими элементами такого пространства выступают неодушевленные объекты, результаты человеческого труда. В свою очередь, информационное общество (также нередко именуемое умным обществом) — это новая фаза развития цивилизации, в которой главными продуктами являются информация и знания, а главным элементом — человек [10].

В эпоху беспрецедентно быстрого развития науки, активного внедрения в повседневную жизнь высоких технологий и, как следствие, всеобщей компьютеризации интегрированность в информационное пространство становится фактором, определяющим основные направления прогресса, а сама информация — важным стратегическим ресурсом современного государства. Информационное пространство отражает существующую политическую карту мира и все ее значимые тенденции, а процесс информатизации охватывает всех субъектов мировой политики — от гражданского сектора и частных лиц до ведущих международных организаций и непосредственно государств. Таким образом, обеспечение устойчивого развития государства, защита национальных интересов, поддержание стабильности и ориентация на идею безопасности мирового сообщества неразрывно связаны с понятием «информационная безопасность».

Информационная безопасность или кибербезопасность?

Проблематика МИБ — феномен не новый, а уже достаточно изученный. Тем не менее по-прежнему не существует единства мнений относительно терминологии в рассматриваемой сфере. В начале 1990-х гг., когда информационная безопасность стала объектом политологических работ, под ней понимали сферу отношений, противопоставленную информационной войне. Принципиальное отличие сущности современного понятия «информационная безопасность» и вкладываемого в него формального наполнения объясняется спецификой подхода к изучению МИБ, сложившегося почти два десятилетия назад.

Впервые в научно-аналитической литературе вопрос информационной безопасности (кибербезопасности) был затронут американским ученым Дж. Наем, автором концепции «мягкой силы» государства, в рамках работы «Будущее силы в XXI веке». Най освещает беспрецедентное формирование новой концепции в международных отношениях — концепции киберсилы. Ее смысл в следующем: иметь способность оказывать влияние на политическую, социальную и экономическую сферы международного сообщества через интернет-пространство. Сегодня, когда вызовы глобальной информатизации становятся одной из главных проблем международной повестки дня, а информационное пространство и его террористическое осмысление — предметом ряда исследований, интерес российской общественности, политического истэблишмента и представителей экспертного сообщества к проблематике МИБ неизменно растет.

Как объект приложения интересов всех мировых акторов МИБ способствовала формированию новой сферы, ставшей не только широким полем сотрудничества, но и источником новых противоречий. Страны Запада, прежде всего США, придерживаются узкого подхода к определению информационной безопасности, используя в научной и дипломатической риторике термин «кибербезопасность» и ограничиваясь

лишь техническим регулированием вопросов, связанных с защитой информации. В свою очередь, представители российского экспертного сообщества смотрят на эту проблему гораздо шире. Они исходят не только из обеспечения технической стороны вопроса, которая, безусловно, важна, но и включают в понятие «информационная безопасность» совокупность политических, социальных, экономических и правовых аспектов, анализируют этот феномен как явление в большей мере социальное, нежели техническое, а также подчеркивают необходимость усиления контроля над «национальным сегментом» глобального информационного пространства [9]. Несмотря на тесное переплетение в ряде вопросов, кибербезопасность и информационную безопасность ошибочно рассматривать в качестве синонимов в силу разных предметных полей.

Разработка самостоятельного всеобъемлющего подхода к изучению МИБ отечественными исследователями и формирование собственного научного дискурса разрушает монополию западных стран в сфере изучения данной проблематики. Это отражается на эффективности российской внешней политики в данном направлении: в вопросах обеспечения МИБ Россия исходит из необходимости усиления контроля над Интернетом, демилитаризации информационного пространства, а также разработки определенных правил поведения в цифровой среде. Однако в то же время отсутствие согласованной позиции между Россией и Западом отдаляет перспективы введения единых принципов поведения и формирование общего подхода к регулированию складывающихся в цифровой сфере отношений.

Война нового поколения и информационное оружие

Неугасающий интерес к проблеме МИБ объясняется тем, что в условиях глобализации все участники мировой политики настолько технологически и информационно связаны друг с другом, что вывод из строя одной части глобальной информационно-коммуникационной сети в результате кибердара может иметь серьезные последствия для каждого из них. Действительно, глобализация сделала мир доступнее и меньше, процессы в нем теперь протекают быстрее, а передовые технологии расширяют охват участников, создавая для каждого ситуацию сопричастности к любому событию. Новые технологии призваны выступать как механизм продвижения сотрудничества и укрепления доверия, однако, как и любое достижение науки и техники, ИКТ используются не только в общественно-полезных целях, но и для выполнения противоправных задач. Будучи ключевой инфраструктурой, вокруг которой строится информационное пространство, Интернет оказывает существенное влияние на систему международных отношений и мировую политику.

Взаимосвязь между достижениями в области ИКТ и силой государства, его «умной» внешней политикой очевидна: чем более развито государство в технологическом плане, тем существеннее его рычаги воздействия, шире диапазон возможностей, тем эффективнее обеспечивается его национальная безопасность. Обладание информационным оружием дает преимущество над теми, кто его не имеет. В этой связи необходимо отметить существующую проблему «цифрового разрыва», или неравенства между «инфобогатыми» и «инфобедными» в распределении научно-технологических ресурсов, доступе к ИКТ. Политический вес, роль и возможности государства во многом определяются уровнем развития технологий, однако не все участники мировой политики имеют возможность продемонстрировать всю мощь информационного потенциала, что приводит к неравным шансам в развитии и, как следствие, новым формам протекания

конфликтов. К слову сказать, ориентация на сохранение такого неравенства была наглядно продемонстрирована странами Запада во главе с США, которые в ходе последнего голосования по вопросу принятия российской резолюции по противодействию информационной преступности заявили о своем нежелании выносить на обсуждение проблему борьбы с преступностью в информационном пространстве в рамках ООН [4; 7].

Речь идет о влиянии продуктов НТП на становление современной революции в военном деле. Так, небольшой коллектив способен нанести удар, который раньше был под силу только государствам; стало возможным ведение бесконтактных войн и применение высокоточных оружий; современные конфликты находят широкое освещение в СМИ, привлекая таким образом внимание многочисленной аудитории по всему миру; манипулирование, пропаганда и прочие возможности социально-психологического воздействия становятся одной из форм информационных войн; остро встает вопрос защиты частной жизни и конфиденциальности личных данных. Под влиянием передовых технологий традиционные способы межгосударственных противостояний становятся все более опасным оружием, поскольку происходит «информатизация» и «интеллектуализация» вооруженных сил. Если в войне прошлого столетия недостатки тактической информации могли быть компенсированы привлечением дополнительных сил, то в век информационный исход вооруженного конфликта во многом определяет информационное превосходство [4].

Явные изменения в понимании природы новой войны и актуальность осмысления нового облика терроризма стали происходить после событий 11 сентября 2001 г. Стратегия войны нового типа, ориентированная не на физическое уничтожение противника, а его подрыв изнутри — результат осознания неприемлемой цены человеческих потерь в ходе традиционных боевых действий. В этом ключевая особенность войны нового поколения. Однако это не умаляет катастрофических последствий в результате возможного кибердара. Информационный терроризм и преступность, использование информации и технологий в военных целях, вмешательство в частную жизнь, незаконный оборот объектов интеллектуальной собственности, неправомерный доступ к ресурсам и услугам информационных сетей, информационная безопасность бизнеса — все это является отражением реальной эксплуатации продуктов НТП, которые способны привести к «кибернетическому Перл-Харбору» [11]. Сегодня национальная безопасность государства во многом зависит от его способности адекватно обеспечивать должный уровень безопасности в цифровой среде. Представляется, что в информационную эпоху эта зависимость будет возрастать по экспоненте параллельно с развитием информационных возможностей и технической стороной прогресса.

Российские инициативы по вопросам МИБ в рамках ООН

Транснациональный характер информационного пространства определяет природу появляющихся в цифровой среде вызовов и угроз. В связи с этим проблема обеспечения режима МИБ и противодействия информационной преступности подчеркивает важность организации международного сотрудничества, учитывающего особенности информационного пространства и опирающегося на нормы международного права. Как известно, Россия в течение многих лет указывала на необходимость взаимодействия и на сегодняшний день остается главным инициатором открытого диалога и продвижения норм и правил кибербезопасности, используя все существу-

ющие механизмы — от двусторонних переговоров с другими государствами и рассмотрения на полях различных форумов, таких как G20 и БРИКС, и до региональных интеграционных объединений и международных организаций [1; 2; 9].

Начиная с 1998 г., когда Россия впервые внесла на рассмотрение ГА ООН проект резолюции «Достижения в сфере информатизации и телекоммуникаций в контексте международной информационной безопасности», стало очевидно стремление российской стороны создать всеобъемлющие условия для формирования системы МИБ, а впоследствии — доказать всем участникам мирового сообщества, что угрозы в информационном пространстве сопоставимы по масштабу и последствиям с угрозами применения ядерного оружия. Не случайно многие журналисты со всего мира нередко сравнивают проблему кибербезопасности с третьей мировой войной. Действительно, взаимодействие и равноправное стратегическое партнерство — это ключевое условие поддержания порядка и стабильности в цифровой среде. Информационная политика России и ее позиция по МИБ преследуют целью не развитие аналогичной противостоянию времен холодной войны системы международных отношений, а создание объединяющей площадки для практического сотрудничества и конструктивного открытого диалога [6].

Так, например, благодаря многолетним усилиям и активному участию России в вопросе обеспечения МИБ и мирного развития информационной среды, в ООН создается важный с дипломатической и политической точки зрения переговорный механизм — рабочая группа открытого состава (РГОС), пришедшая на смену ранее действовавшей Группы правительственных экспертов, которая прекратила свою работу ввиду ряда противоречий между участниками (США и их союзниками с одной стороны, и Россией, БРИКС и развивающимися странами — с другой)[3; 5; 8]. Несмотря на по-прежнему существующие разногласия, формирование РГОС — большой успех для российской стороны, которая остается главным идеологом продвижения вопросов МИБ.

Россия неоднократно обращалась к государствам — членам ООН с вопросом о целесообразности создания международно-правового режима противодействия преступности с использованием ИКТ. С момента официальной постановки вопроса перед ООН российская резолюция по МИБ ежегодно принимается ГА ООН (в период с 1971 г. по сегодняшний день их было принято более сорока, в частности последние «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» и «Противодействие использованию информационно-коммуникационных технологий в преступных целях»), а положения документа постоянно развиваются и дополняются идеями, отвечающими безопасности мирового сообщества. Не стал исключением текст резолюции «Противодействие использованию информационно-коммуникационных технологий в преступных целях», закрепивший принципиально важные положения об исключительно мирном использовании ИКТ, действие общепризнанных принципов международного права в информационном пространстве, обладание государственным суверенитетом над ИКТ-инфраструктурой на своей территории, запрет на ничем не подкрепленные обвинения в кибернападении и ряд других [5; 6].

В этой связи стоит отметить и тот вклад, который Россия внесла в развитие терминологии ООН по МИБ. В ответ на революционные действия в ходе «арабской весны», когда социальные сети выступали инструментом обеспечения интересов и координации

деятельности протестных режимов, Россия дополнила уже существующую так называемую «триаду угроз» новыми элементами, а именно: опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушение общественной стабильности и разжигание межэтнической, межнациональной розни. Тем не менее миротворческая киберконцепция России не соответствует позиции ряда государств во главе с США, которые опасаются потерять контроль и влияние в ИКТ-сфере и ограничить свои возможности, что в результате приводит к торможению процесса принятия и реализации российских инициатив по данному вопросу.

Выводы

Глобализация сделала информацию ключевым двигателем развития и одновременно ахиллесовой пятой современного государства. Роль информации в жизнедеятельности современного общества постоянно возрастает — это объективный процесс, начавшийся задолго до появления информационного пространства. Однако беспрецедентные успехи в науке и технике привели к тому, что информация превратилась в новый источник проблем. Сегодня, когда мир вступил в эпоху войн нового поколения, основной ареной военных действий становится не земное пространство, а информационное, использование ИКТ в целях, противоречащих нормам мирового общежития, все больше становится перспективным направлением научно-теоретического осмысления, о чем свидетельствует значительный пласт работ российских исследователей по данной проблематике, целый ряд официальных документов Российской Федерации и авторитетных международных организаций.

Серьезные перемены в системе международных отношений ознаменовали становление нового качества мировой политики, повлекшее за собой переосмысление стратегии обеспечения безопасности. Значимость информационной безопасности в политическом процессе, а также в архитектуре построения безопасности современного мира очевидна. Российский подход к определению и изучению МИБ характеризуется подробным анализом основных понятий, инициативными предложениями на национальном, региональном и международном уровне. Несмотря на конфликт интересов между Россией и Западом, Россия с большой вероятностью сохранит свою инициативную роль в рассмотрении вопросов МИБ в стенах ведущей организации на международной арене, что подчеркивает ее активная позиция на данном направлении.

Литература

1. *Бойко С.* Формирование системы международной информационной безопасности: российские подходы и инициативы [Электронный ресурс] // Международная жизнь. — 2018. — Режим доступа: https://interaffairs.ru/jauthor/material/2021.
2. *Забродин Алесей.* Москва поднимет вопрос кибербезопасности на Генассамблее ООН [Электронный ресурс] // Известия. — 2017. — 28 августа. Режим доступа: https://iz.ru/636710/aleksei-zabrodin/rossiia-podnimet-vopros-o-kiberbezopasnosti-na-ga-oon.
3. *Зиновьева Е.С.* Дипломатическое наступление России в области информационной безопасности [Электронный ресурс] // Говорят эксперты МГИМО. — 2018. — 22 ноября. — Режим доступа: https://mgimo.ru/about/news/experts/diplomaticheskoe-nastuplenie-rossii-v-oblasti-informatsionnoy-bezopasnosti/.
4. *Крутских А.В., Зиновьева Е.С.* Информатизация и макротехнологии: новое лицо мировой политики / А.В. Крутских, Е.С. Зиновьева // Международные процессы. — 2014. — Т. 12, № 1–2 (36/37): январь-июнь. — С. 20–32.

5. Международная информационная безопасность: успехи России в ООН [Электронный ресурс] // РСМД. — 2019. — 12 февраля. — Режим доступа: http://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-uspekhi-rossii-v-oon/.
6. О принятии Генассамблеей ООН российской резолюции по противодействию информационной преступности [Электронный ресурс] // Официальный сайт МИД РФ. — 2018. — 7 декабря. — Режим доступа: http://www.mid.ru/ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3437775.
7. О принятии Генассамблеей ООН российской резолюции по противодействию информационной преступности [Электронный ресурс] // Официальный сайт МИД РФ. — 2018. — 18 декабря. — Режим доступа: http://www.mid.ru/ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3449030.
8. Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере [Электронный ресурс] // Официальный сайт МИД РФ. — 2017. — 29 июня. — Режим доступа: http://www.mid.ru/ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/2804288.
9. Россия и США перетягивают всемирную паутину [Электронный ресурс] // Коммерсантъ. — 2018. — 12 ноября. — Режим доступа: https://www.kommersant.ru/doc/3797617.
10. *Фененко А.В.* Информационная борьба и глобальное информационное пространство / А.В. Фененко // Международные отношения России в «новых политических пространствах» / Отв. ред. А.В. Фененко. — М.: Ленанд, 2011. — С. 169–170.
11. *Черненко Е.* Холодная война 2.0? [Электронный ресурс] // Россия в глобальной политике. — 2013. — 3 марта. — Режим доступа: http://www.globalaffairs.ru/number/Kholodnaya-voina-20-15874.