РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ

ISSN 1726-1139
e-ISSN 1816-8590
DOI 10.22394/1726-1139

УПРАВЛЕНЧЕСКОЕ КОНСУЛЬТИРОВАНИЕ

2020. №8(140)

Научно-практический журнал

Выходит ежемесячно

Издание входит в Перечень рецензируемых научных изданий Высшей аттестационной комиссии при Минобрнауки России, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим специальностям: 08.00.05 – Экономика и управление народным хозяйством, 08.00.13 – Математические и инструментальные методы экономики, 08.00.14 – Мировая экономика, 23.00.01 – Теория и философия политики, история и методология политической науки, 23.00.02 – Политические институты, процессы и технологии, 23.00.04 – Политические проблемы международных отношений, глобального и регионального развития

С 2005 года статьи включаются в Российский индекс научного цитирования (РИНЦ), доступный по адресу http://elibrary.ru (Научная электронная библиотека). Размещается в открытом доступе в полнотекстовом виде

Сведения, касающиеся издания и публикаций, включены в базу данных ИНИОН РАН и публикуются в международной справочной системе по периодическим и продолжающимся изданиям “Ulrich's Periodicals Directory” и в базе данных EBSCO

Журнал включен в индексацию международной базы данных научных публикаций DOAJ

АДРЕС РЕДАКЦИИ:
199004, Санкт-Петербург, В.О., 8-я линия, д. 61.

Тел.: (812) 335-94-72, 335-42-10. E-mail: antonova-ev@ranepa.ru

Точка зрения редакции может не совпадать с мнением авторов статей

При перепечатке ссылка на журнал «Управленческое консультирование» обязательна

© Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, 2020
© Северо-Западный институт управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, 2020
© Редколлегия журнала «Управленческое консультирование» (составитель), 2020
© Все права защищены

Контент доступен под лицензией Creative Commons Attribution 4.0 License

КОЛОНКА РЕДАКТОРА

ГОСУДАРСТВЕННАЯ И МУНИЦИПАЛЬНАЯ СЛУЖБА

ПОЛИТИКА И ПРАВОВОЕ ГОСУДАРСТВО

ВЛАСТЬ И ЭКОНОМИКА

DOI 10.22394/1726-1139-2020-8-55-66

Проблема классификации объектов применения силы в информационных конфликтах

Коростелёв С. В.

Секретариат Совета Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств, Санкт-Петербург, Российская Федерация; ksv1@iacis.ru

РЕФЕРАТ

Как следствие изменений в технологическом укладе и соответствующей ему организации мировой экономики, в составе участников вооруженных конфликтов произошли серьезные изменения. Во-первых, противоборствующими сторонами являются не только государства. Во-вторых, абсолютное большинство целей, подлежащих поражению для обеспечения победы в конфликте, в настоящее время находятся в частном секторе и вне государственного контроля. Также существенной особенностью информационного противоборства является то, что в абсолютном большинстве ситуаций непосредственный исполнитель информационного нападения не может быть идентифицирован немедленно и в существенной степени из-за того, что «военные» конфликты в киберпространстве в контексте международных отношений могут быть «встроены» в различные формы борьбы за влияние: политические, экономические, информационные, технологические, медийные и идеологические и др. То есть значительное число участников обычной повседневной деятельности во всех сферах жизни из любой точки земного шара могут стать не только косвенными, но и непосредственными участниками инфомационного конфликта.

В цифровую эпоху объекты, выбираемые для поражения, могут иметь совершенно иные и неожиданные свойства, что обусловливает существование значительного числа подходов к классификации объектов информационного воздействия. Сила применяется против физических и виртуальных объектов в физическом, информационном и когнитивных измерениях.

Сложность оценки причиненного государствам и их населению ущерба в когнитивной сфере и, соответственно, сопоставления с практикой присвоения ответственности за использование традиционных средств ведения вооруженного противоборства делает невозможным в ближайшее время формирование какого-либо адекватного универсального международного политико-правового режима противодействия информационным угрозам. Устранение угроз в киберпространстве является общим интересом по обеспечению международной стабильности, но в настоящее время может осуществляться государствами только лишь самостоятельно.

Заявление в федеральном законодательстве перечня недопустимых агрессивных действий, осуществляемых посредством информационных воздействий, будет, по своей сути, превентивной мерой, так как установит пороговые ограничения для осуществления вмешательства во внутренние дела государства извне для других международных акторов.

Ключевые слова: киберпространство, цели информационного противоборства, применение силы, когнитивное измерение, международная ответственность, международное гуманитарное право

Для цитирования: *Коростелев С. В.* Проблема классификации объектов применения силы в информационных конфликтах // Управленческое консультирование. 2020. № 8. С. 55–66.

The Problem of Classification of Targets in Informational Conflicts

Stanislav V. Korostelev

Secretariat of the Council of the Interparliamentary Assembly of the Commonwealth of Independent States, Saint Petersburg, Russian Federation; ksv1@iacis.ru

ABSRACT

As a result of changes in the technological tenor and congruous with it organization of the world economy, serious changes have occurred in the gradation of participants in armed conflicts. Firstly, the warring parties are not only states now. Secondly, the vast majority of the targets to be overpowered to ensure victory in the conflict are currently in the private sector and out of state control. Also, an essential feature of the information confrontation is that in the vast majority of situations, the direct perpetrator of an information attack cannot be identified immediately and to a large extent due to the fact that "military" conflicts in cyberspace in the context of international relations can be "embedded" in various forms of struggle for power: political, economic, informational, technological, media and ideological, etc. That is, a significant number of participants in ordinary everyday life implicit activities in all walks of life from all over the globe can be not only indirect but also direct participants of informational conflict.

In the digital era, targets selected for destruction can have completely different and unexpected properties, which leads to the existence of a significant number of approaches to the classification of targets of informational impact. Force is used against physical and virtual objects in the physical, informational and cognitive dimensions.

The complexity of assessing the physical damage inflicted on states, and their population in the cognitive sphere conformably, and relating it with the practice of assigning international responsibility for the use of traditional means of warfare makes it impossible to form any adequate universal international political and legal regime for countering information threats in the near future. The elimination of threats in cyberspace is a common interest in ensuring international stability, but at present it can be carried out by states only on their own.

A statement of the specified list of unacceptable aggressive actions carried out through information influences in the federal legislation will be, in essence, a preventive measure, since it will establish a threshold restriction for other international actors to interfere in the internal affairs of the state from outside.

Key words: cyberspace; targets in informational confrontation; use of force; cognitive dimension; international responsibility; international humanitarian law

For citing: Korostelev S. V. The Problem of Classification of Targets in Informational Conflicts // Administrative consulting. 2020. No. 8. P. 55–66.

Применение термина «информационная война» ко всему спектру деятельности в сфере получения и распределения информации представляется не совсем удачным. Во-первых, использование термина «война» является по своей сути исторической традицией и может быть применимо только к ситуациям вооруженного насилия прошлого, когда сторонами конфликта являлись государства, которые руководствовались нормами права войны и нейтралитета. Правовой режим войны также предполагал обнародование соответствующей декларации о переходе в состояние войны с избранным конкретным противником (animus belligerendi). С принятием Пакта Бриана — Келлога, Устава ООН, Женевских конвенций 1949 г. войны были поставлены вне закона, и в обиход вошли понятия «применение силы» и «вооруженный конфликт», хотя по факту государства могут находиться в состоянии «войны». Кроме того, в настоящее время переход в состояние войны требует особого юридического оформления в национальном законодательстве, например в случае, если совершаются акты применения вооруженной силы (вооруженное нападение) иностранным государством (группой государств) против суверенитета, политической независимости и территориальной целостности государства или каким-либо иным образом, несовместимым с Уставом ООН, — то есть в случае агрессии, ее непосредственной угрозе или действий, указывающих на ее подготовку, а также в случае необходимости выполнения международных договоров[1].

[1] См. например: Федеральный конституционный закон от 30.01.2002 № 1-ФКЗ «О военном положении» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_35227/

Более того, в современную эпоху для причинения ущерба противнику в связи с изменениями в технологическом укладе исчезла необходимость содержания инфраструктуры, необходимой для ведения масштабных и продолжительных боевых действий в их привычном понимании. Так, например, в случае обращения к информационным средствам противоборства, инженерное оборудование предполагаемых районов ведения боевых действий, накопление ресурсов, различные аспекты мобилизационных мероприятий, ранее служившие признаками непосредственности угрозы агрессии, более не являются существенными фактами, оправдывающими обращение государства-объекта предполагаемого нападения, например, к упреждающим действиям.

Так же, как следствие изменений в технологическом укладе и соответствующей ему организации мировой экономики, в составе участников вооруженных конфликтов произошли серьезные изменения. Во-первых, противоборствующими сторонами являются не только государства. Ими могут быть, например: международные организации, которые осуществляют меры принуждения по отношению к каким-либо государствам; государства, уничтожающие элементы террористической инфраструктуры на территориях других государств; террористические группы и экстремистские движения, оказывающие давление на государства; индивиды, объявляющие войну всем и вся; не связанные с государством частные лица и организации и т. п. А для решения задач формирования и средства вооруженных сил государства не обязательно должны пересекать физические границы государства — объекта принуждения. Во-вторых, абсолютное большинство целей, подлежащих поражению для обеспечения победы в конфликте, в настоящее время находятся в частном секторе и вне государственного контроля. А это уже само по себе затрагивает моральные и правовые основы процессов подготовки и ведения боевых действий государственными вооруженными формированиями, особенно, если последствия применения информационных средств ведения боевых действий, даже исключительно против военных объектов, сказываются в гораздо большей степени на населении и гражданской инфраструктуре. Также существенной особенностью информационного противоборства является то, что в абсолютном большинстве ситуаций непосредственный исполнитель информационного нападения не может быть идентифицирован немедленно и в существенной степени из-за того, что «военные» конфликты в киберпространстве в контексте международных отношений могут быть «встроены» в различные формы борьбы за влияние: политические, экономические, технологические, информационные (в том числе медийные и идеологические) и др. То есть значительное число участников обычной повседневной деятельности во всех сферах жизни из любой точки земного шара могут стать не только косвенными, но и непосредственными участниками инфомационного конфликта.

Таким образом, применение не только термина «война», но и «вооруженный конфликт» к информационному противостоянию вступает в противоречие с традиционными теорией и практикой использования методологического аппарата военных наук, политики и права для политико-правового анализа актов применения силы в межгосударственных отношениях. Можно утверждать, что термины «война», «вооруженный конфликт», «нападение» имеют достаточно «неудобное» фактологическое и нормативное содержание для современных ситуаций применения информационных средств борьбы. Главным образом ввиду того, что еще менее определенным становится содержание термина «законная военная цель», что, в свою очередь, создает проблемы для начальной правовой квалификации актов применения силы.

(дата обращения: 24.05.2020); Федеральный закон «Об обороне» от 31.05.1996 № 61-ФЗ Электронный ресурс]. URL:http://www.consultant.ru/document/cons_doc_LAW_10591/ (дата обращения: 24.05.2020).

Лозунговое определение новой ситуации в сфере применения силы, например, как «гибридные», «информационные» войны, «войны нового поколения», мало что дает для политико-правового обоснования обращения к необходимым и соразмерным ответным мерам.

Как можно определить нормативные рамки для конфликтов, если в них используются информационные технологии? Когда можно сделать заявление, что масштаб, интенсивность и продолжительность информационных действий свидетельствуют о состоянии войны (вооруженного конфликта) и возможности присвоения международной ответственности?

Очевидно, что в цифровую эпоху объекты, выбираемые для поражения, могут иметь совершенно иные и неожиданные свойства, что обусловливает существование значительного числа подходов к классификации объектов информационного воздействия.

Например, иногда в доктрине информационных противоборств предлагается разделение целей на четыре категории: физические, кибернетические, информация, сознание [2, с. 117].

Из определения «информационной войны», данного в Стратегии обеспечения информационной безопасности государств — участников Содружества Независимых Государств[1], можно выделить три категории целей: физические объекты (информационные системы, процессы и ресурсы, критически важные и другие структуры); политическую, экономическую и социальную системы; и население.

Рассматривая Стратегию национальной безопасности[2] и Доктрину информационной безопасности[3] Российской Федерации можно выделить следующие объекты возможного применения силы: конституционные права и свободы человека и гражданина (см. п. 8 (а) Доктрины, п. 22 Стратегии), в том числе культурные, исторические и духовно-нравственные ценности, и общественное сознание (п. 21 Стратегии); информационная инфраструктура (в первую очередь критическая информационная инфраструктура) и единая сеть электросвязи (см. п. 8 (б, в) Доктрины); государственная политика и культура (см. п. 8 (г) Доктрины); международная стратегическая стабильность и суверенитет Российской Федерации (см. п. 8 (д) Доктрины).

Единое руководство по целеуказанию Объединенного комитета начальников штабов Вооруженных сил США[4] (далее — ОКНШ) выделяет две категории целей: физические (географические объекты или объекты инфраструктуры, либо их группы, которые в силу своих свойств обеспечивают функционирование цели; вооружение и технические средства; индивиды; организационные структуры и др.); и виртуальные (объекты в киберпространстве, которые являются носителями функций, определяющими свойства цели).

Единое руководство ОКНШ по ведению информационных действий[5] рассматривает их физическое, информационное и когнитивное измерения.

---

[1] [Электронный ресурс]. URL: http://cis.minsk.by/reestr/ru/index.html reestr/view/text?doc=6162 (дата обращения: 17.01.2020).

[2] Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. URL: https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html (дата обращения: 18.01.2020).

[3] Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 18.01.2020).

[4] Joint Publication 3-60. Joint Targeting. 31 January 2013. Section A. Targets. 2. Target Description (a) [Электронный ресурс]. URL: https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1F4_jp3-60.pdf (дата обращения: 03.02.2020).

[5] Joint Publication 3-13. Information Operations. Ch. I. 2. The Information Environment [Электронный ресурс]. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf (дата обращения: 19.01.2020).

В данном случае физическое измерение включает, прежде всего, системы управления и категорию «лиц, принимающих решения» (далее — ЛПР), а также обеспечивающую их деятельность инфраструктуру. То есть, это физические платформы и соединяющие их коммуникационные сети. Физическое измерение включает в себя, но не ограничивается ими, людей, специальное оборудование, предназначенное для решения военных задач, различные излучающие и вычислительные устройства, в том числе персональные, или любые другие объекты, в том числе печатные издания, — т. е. все, что может быть выявлено наблюдением. Физическое измерение не ограничивается исключительно военными или даже общегосударственными системами и процессами — к нему может быть отнесена, например, распределенная трансграничная сеть, связанная через государственные, экономические и географические границы.

Информационное измерение охватывает процессы сбора, обработки, хранения, распространения и защиты информации и именно в нем осуществляется управление и передаются замыслы. Всякое действие в данном измерении оказывает влияние на содержание, объем и направление движения информации.

Когнитивное измерение информационной среды охватывает мыслительные процессы лиц, участвующих в передаче информации, являющихся ее адресатом, реагирующих или воздействующих на нее. Это может происходить на этапах обработки информации, восприятия, оценки и принятия решений отдельными лицами или их группами. На эти элементы влияют многие факторы, включая личные и групповые культурные убеждения, социальные нормы, уязвимости, мотивации, эмоции, опыт, мораль, образование, психическое здоровье, идентичность, идеологические установки и др. Понимание масштаба и характера влияния таких факторов в конкретной обстановке имеет решающее значение для оказания наиболее эффективного влияния на ЛПР.

Как таковое, когнитивное измерение представляет собой наиболее важный компонент информационной среды, поскольку именно когнитивные характеристики описывают то, как цели информационного воздействия обрабатывают информацию или осуществляют функции управления. В тех случаях, когда объектом, равно как и субъектом, информационного воздействия является индивид, когнитивные характеристики сосредоточены на описании моделей мыслительных процессов, свойственных данному человеку, либо оказания влияния на принятие решений данным лицом[1].

Когнитивные характеристики объекта применения силы особенно важны для правильной оценки критических узлов в системе целей, предназначенных для поражения, поскольку практически каждой системе присуща определяющая ее деятельность управляющая функция, нейтрализация которой может иметь решающее значение для достижения желаемых изменений в поведении цели.

---

[1] Так, например, в разделе IV «Стратегические цели и основные направления обеспечения информационной безопасности» п. 23 Доктрины информационной безопасности Российской Федерации определяется, что: «Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются: а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации; <...> к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей». Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 15.01.2020).

Однако ход информационных конфликтов последнего времени показывает, что противники не стремятся к разрушению, например, социальных сетей, а наоборот, к использованию их в своих информационных операциях по назначению, т. е. для манипулирования ими и, соответственно, распространения дезинформации. Именно этот аспект информационного противоборства ставит международное сообщество перед проблемой согласования стандартов поведения в сетях, поскольку нападать и обороняться в среде, где нормы в настоящее время регламентируют лишь технические аспекты ее функционирования, намного сложнее. Но также является очевидным,что в настоящее время единая регламентация оборота информации в социальных сетях представляется невозможной из-за различий в философии сути контроля объема свободы выражения мнений в противоборствующих государствах.

То есть для снижения вероятности ответного применения силы, основанном на принципе взаимности, *основная задача противоборствующих сторон состоит в противодействии распространению дезинформации без создания препятствий свободе выражения мнений*. Причем в ходе иноформационного противоборства в социальных сетях особенно важное значение приобретают знания в социально-политической сфере, психологии, коммуникации и других гуманитарных науках. Именно эти знания помогают построить доверие к государственным институтам, обучить население медийной грамотности и методике проверки фактов и, тем самым, обеспечить устойчивость государства в новой информационной среде.

А сами инфраструктура и платформы социальных сетей нуждаются в защите всеми сторонами информационного конфликта в такой же степени, как и критически важные объекты физической инфраструктуры государства. Этот аспект является одним из парадоксов стратегии обеспечения иформационной безопасности.

Как и в случае с функциональными, когнитивные характеристики объектов информационного воздействия идентифицируются очень сложно. Для определения свойств цели необходимо определять[1]:

1) как цель обрабатывает информацию;
2) как работает цикл принятия решения целью (если применимо);
3) как обрабатываются входные данные, которые необходимы цели для выполнения своих функций;
4) как обрабатываются результаты, полученные в результате выполнения целью своих функций;
5) какой объем информации может обработать цель;
6) как цель или система целей хранит информацию;
7) если целью является физическое лицо или организация:
   а) как организован мыслительный процесс;
   б) каковы ее мотивы;
   в) какое поведение демонстрирует цель;
   г) каковы правила, нормы и убеждения цели;
   д) каковы ее когнитивные уязвимости;
8) культурные представления (восприятие, взгляды, религиозная и этническая идентичность).

Одной из сложностей нормативной оценки ведения информационного противоборства в когнитивном измерении является то, что еще недавно его основным направлением предполагались оказание физических воздействий на критически важную инфраструктуру и компьютерные сети, взлом компьютерных программ, нарушение конфиденциальности, целостности информации и ее доступности. Именно такая форма вероятного конфликта послужила первоосновой для обоснования путей развития

[1] Joint Publication 3–13, см. выше.

норм киберправа, т. е., по сути, правового обеспечения технологической устойчивости информационно-коммуникационной инфраструктуры (далее — ИКИ). Данный подход по регулированию технических и технологических аспектов защиты ИКИ нашел отражение в докладе Группы правительственных экспертов под эгидой ООН 2015 г. В этом докладе собственно защите информации уделено немного внимания, чему есть очевидное объяснение: следование примату прав человека не допускает какого-либо жесткого контроля потоков информации и нарушения фундаментального права на свободу выражения мнений и неприкосновенность частной жизни. В данном рекомендательном документе как раз демонстрируется неопределенность в определении нормативных порогов для вмешательства извне в ту сферу информационного пространства, которое государство предполагает находящимся в своей юрисдикции. С другой стороны, если предположить, что государство способно установить такие пороги и объявить их для других государств, то физическое лицо может оценить такие действия как нарушение его личных прав и свобод государством национальности.

Очевидным образом выбор объектов для применения силы и способы воздействия на них определяются предметом воздействия и способом формирования проблемы: в процессе обеспечения информационной безопасности необходимо постоянно осуществлять оценку не только возможного характера угроз, происходящих извне, но и состояние собственных объектов вероятного информационного воздействия, находящихся в пределах юрисдикции государства. Определение того, что является угрозой и как мы должны ей противодействовать, и какое состояние информационной безопасности является желаемым результатом, должно осуществляться непрерывно.

Как и в случае ведения боевых действий с использованием «привычных» нам средств поражения, в ходе решения задач принуждения с использованием информационных средств могут происходить события, влекущие гибель и страдания людей, разрушение объектов, необходимых для их выживания. Следовательно, и в процессе присвоения международной ответственности за поведение в такого рода конфликтах необходимо обращаться к императивным принципам международного гуманитарного права (далее — МГП), а именно: непричинения излишних страданий, избирательности поражения, запрещения вероломства, непричинения окружающей среде долговременного и существенного ущерба.

Ранее воюющие государства служили гарантами выполнения норм МГП участниками боевых действий, даже если второй стороной в конфликте являются организованные группы и лица, не связанные с каким-либо государством, как минимум в силу так называемой «оговорки Ф. фон Мартенса»: «В случаях, не предусмотренных международными соглашениями, гражданские лица и комбатанты остаются под защитой и действием принципов международного права, проистекающих из установившихся обычаев, из принципов гуманности и из требований общественного сознания». В современных условиях отправной точкой для установления разграничения между «условно безопасной» информационной деятельностью и деятельностью с применением тех же информационных технологий, но, когда намеренно причиняется ущерб каким-либо государствам и лицам, также может служить данное обычное положение МГП, хотя, как было сказано выше, участниками информационного противоборства могут быть не связанные с государствами акторы. Но правом такой оценки и возможностями присвоения ответственности, по-прежнему, обладают лишь государства.

Каждое государство самостоятельно в своих нормативных актах определяет, является ли для него какое-либо состояние международных отношений вооруженным конфликтом. Например, Федеральный конституционный закон от 30 января 2002 г. № 1-ФКЗ «О военном положении»[1] в ст. 3 определяет действия, которые

[1] Ст. 3. Основания для введения военного положения [Электронный ресурс]. URL: http://ivo.garant.ru//document/184121/paragraph/2678:0 (дата обращения: 15.01.2020).

Российской Федерацией считаются актом агрессии. Закон в то же время определяет, что применение силы должно осуществляться (или непосредственно указывать на подготовку к его совершению) иностранным государством (группой государств) против суверенитета, политической независимости и территориальной целостности. Причем, обычное международное право определяет, что поведение отдельных органов государств, лиц, осуществляющих элементы государственной власти, лиц или группы лиц, действующих по указаниям, либо под руководством или контролем государств, либо в отсутствие или несостоятельности официальных властей, а в некоторых случаях, даже повстанческих движений, органов или агентов международной организации — могут быть расценены как основания для присвоения международной ответственности[1] и осуществления ответных мер для отражения агрессии или пресечения ее подготовки.

Таким образом, информационное воздействие должно осуществляться против «суверенитета, политической независимости и территориальной целостности» с тем, чтобы государство имело возможность использовать правовые механизмы (о которых должно быть предварительно оповещено мировое сообщество) для реагирования на акт агрессии. Возникает вопрос о том, каковы должны быть масштабы такого вмешательства в каждой из сфер кибернетического конфликта — физической, собственно информационной, когнитивной? Какие пороги (качественные / количественные) устанавливает государство для заявления политико-правового обоснования своего обращения к силе как справедливого для отражения акта агрессии?

Очевидно, что в случае наступления определенных государством в законе пороговых событий, начинают действовать нормы МГП, и для России возникнет состояние вооруженного конфликта, либо войны. Поскольку ни международные, ни национальные акты не определяют перечень способов исполнения нападения на территорию государства, то, возможно предположить, что применение для нападения информационных технологий также может порождать для России состояние вооруженного конфликта. Но в каком случае? Здесь очевидно следует исходить из определения того, причиняют ли информационные действия ущерб, сопоставимый с тем, который причиняется привычными и понятными нам средствами ведения вооруженной борьбы, и который подробно исследован в процессе развития норм МГП.

Любая деятельность государства в информационном пространстве регламентируется теми же нормами международного права, что и все иные виды деятельности[2]. Например, применение силы против территории суверена очевидным образом является нарушением международного права, определяется в парадигме ООН как применение силы, запрещенное ст. 2 п. 4 Устава ООН. То есть, всякая деятельность государственных органов, причиняющая вред другому государству в пределах территории последнего, является неправомерным применением силы. Наиболее очевидным примером такого применения силы является нанесение ударов посредством систем оружия через границу государства — данное положение обычного международного права не подлежит оспариванию. Однако применение современных средств

[1] Доклад Комиссии международного права (53-я сессия). Генеральная Ассамблея. Официальные отчеты пятьдесят шестой сессии. Дополнение № 10 (Документ ООН A/56/10 «Тексты проектов статей об ответственности государств за международно-противоправные деяния») [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/pdf/responsibility.pdf (дата обращения: 20.01.2020); Доклад Комиссии международного права (63-я сессия). Генеральная Ассамблея. Официальные отчеты шестьдесят шестой сессии. Дополнение № 10 (Документ ООН A/66/10 «Текст проектов статей об ответственности международных организаций») [Электронный ресурс]. URL: https://digitallibrary.un.org › record › files › A_66_10-RU (дата обращения: 20.01.2020).

[2] Статья 2 п. 3 Устава ООН накладывает на государства обязанность разрешать свои международные споры мирными средствами, таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость.

информационного противодействия по элементам физической критической инфраструктуры государства может иметь эффект сравнимый и, даже более того, превосходящий по своим последствиям результаты огневого поражения.

Случайный ущерб, причиненный государству в пределах его суверенной территории в мирное время, влечет международную ответственность, но не является таким применением силы по смыслу ст. 2 п. 4 Устава ООН, которое порождает право потерпевших государств обращаться к самообороне в соответствии со ст. 51 Устава ООН. Но «умышленность» причинения ущерба субъективно оценивается государствами в конкретном случае с учетом всех доступных им для оценки обстоятельств. Таким образом, только намеренная деятельность в информационном пространстве, причиняющая ущерб государству, его гражданам, объектам в пределах национальной территории, либо вне ее, является незаконным применением силы. Сама по себе такая деятельность не обязательно порождает право государств на самооборону, так как она не всегда может/должна быть оценена государством по масштабу, продолжительности и интенсивности действий, как «вооруженное нападение» вне зависимости от использованных средств вооруженной борьбы. Может ли, например, вызванный посредством информационного вмешательства в когнитивном измерении блэкаут послужить причиной для реторсий и, тем более, репрессалий со стороны потерпевшего государства? Очевидно, что нет. Однако десятки подобных инцидентов уже могут быть расценены как состоявшееся «вооруженное нападение», так как в этом случае свидетельство намеренности действий в информационном пространстве становится очевидным.

Сбор информации с использованием технических средств, несмотря на намеренный характер, также не противоречит существующему международному праву. Однако в определенных условиях такая деятельность может получить оценку как враждебные намерения другого государства и, в итоге, как «угроза силой» по смыслу ст. 39 Устава ООН, особенно если она намеренно ведет к причинению ущерба в пределах территории суверена.

Допустимость разведывательной деятельности является частью обычного неотъемлемого права государств на самооборону. Гаагская (IV) Конвенция о законах и обычаях войны на суше от 18 октября 1907 г.[1] (Положение, ст. 24, 29–31) явным образом признает право государств на разведывательную деятельность в ходе вооруженного конфликта. Аналогичным образом ст. 3 Венской конвенции о дипломатических сношениях 1961 г.[2] также явно признает право государств на разведывательную деятельность в мирное время[3]. Практика государств также демонстрирует, что они относятся к сбору разведывательной информации как неотъемлемой сфере деятельности во внешней политике и международных отношениях. В то же время, шпионаж против себя расценивается внутренним законодательством большинства государств как уголовное преступление, причем как во время мира, так и во время вооруженного конфликта.

Собственно, все МГП построено на принципе сравнения последствий применения различных средств и способов ведения войны (см. [1]). Для объявления какого-либо средства ведения военных действий запрещенным последствия его применения сравнивались с последствиями применения известных видов вооружения и затем делался вывод о «гуманности/негуманности» данного средства или спосо-

[1] [Электронный ресурс]. https://www.icrc.org/ru/doc/resources/documents/misc/hague-convention-iv-181007.htm (дата обращения: 17.01.2020).

[2] [Электронный ресурс]. https://www.un.org/ru/documents/decl_conv/conventions/dip_rel.shtml (дата обращения: 17.01.2020).

[3] Статья 3 Конвенции: «Функции дипломатического представительства состоят, в частности: … d) в выяснении всеми законными средствами условий и событий в государстве пребывания и сообщении о них правительству аккредитующего государства…».

ба его применения. Таким образом, если последствия информационного воздействия могут быть сопоставлены с материальным ущербом, причиненным государству и его гражданам в ходе какого-либо вооруженного конфликта каким-либо средством ведения военных действий, либо способом его применения, то можно сделать вывод о существовании состояния информационной войны (вооруженного конфликта). Приемлемый ущерб, до превышения которого государство не обращается к ответным действиям, определяется этим государством самостоятельно в соответствии с его политической ситуацией, военными, экономическими, географическими и иными возможностями.

Кроме того, существует необходимость учитывать такой аспект акта применения силы, как «соразмерность». В случае превышения порога, который государство-объект информационного воздействия может посчитать для себя неприемлемым вмешательством, оно может осуществить ответные меры. Но в таком случае оно не обязано отвечать симметрично именно в информационной сфере. Как международное право, так и неправовой принцип взаимности, не накладывают таких ограничений. Выбор сферы реализации ответных мер всегда остается на усмотрение государства, и всегда существует большая вероятность того, что при разрушении стабильности в информационном пространстве конфликт будет перенесен в другую сферу, например, специальных экономических и принудительных мер[1].

Следовательно, ответные меры могут выйти, по оценке не только государства, против которого они применяются, но и третьих сторон, за рамки объема предполагаемой справедливой международной ответственности, и причиняя ущерб сверх того, что считается разумным ответом, привести к раскручиванию спирали конфликта[2]. Эта опасность усугубляется риском ненамеренного наказания случайного актора; и, в свою очередь, неправильная атрибуция может привести к нежелательной эскалации напряжения в отношениях с третьими сторонами, в то время как истинный агрессор остается безнаказанным.

Можно сделать ряд выводов в отношении обращения к институту международного права как средству регулирования поведения в киберпространстве.

Во-первых, международное право не может служить средством предотвращения вмешательств с использованием информационных средств именно по причине сложности немедленной аттрибуции: возникает сложность в обращении к гарантированному ст. 51 Устава ООН неотъемлемому праву на самооборону как политико-правовому обоснованию акта применения силы. До настоящего времени не сложилось сколько-либо авторитетной практики Совета Безопасности ООН, и тем более Международного суда ООН в определении временны́х параметров для обращения к самообороне: должно ли ответное применение силы происходить немедленно, или это возможно осуществить какое-либо время спустя? И не будут ли расценены такие действия, если они не проведены немедленно, а значительно позднее, как репрессалии? Что может быть законной целью для применяемой силы и для ответных мер? Какие способы могут использоваться? Ведь как было показано выше, современная практика в сфере МГП регламентирует осуществление «вооруженных» нападений лишь «кинетическим» оружием, а также устанавливает абсолютные запреты на использование химических, бактериологических, биологических и токсинных средств. Специальные же экономические и иные принудительные меры, а именно: экономическое давление, визовые запреты или другие действия

[1] Федеральный закон № 83-ФЗ «О специальных экономических мерах и принудительных мерах» [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102111154 (дата обращения: 29.01.2020).

[2] Всякая сторона конфликта считает свои действия a priori «справедливыми», поэтому лишь третьи стороны, используя механизмы международного права, могут определять их как правомерные/неправомерные.

не запрещаются международным правом, если они не приводят к масштабным страданиям. Чрезмерное же полагание на институт международного права в процессе исполнения государством международных обязательств в сфере международной безопасности и непринятие соразмерных ответных мер, не обязательно симметричных, может, как ни удивительно, свидетельствовать о его недостаточном политическом авторитете, слабой национальной мощи в целом.

Во-вторых, представляется маловероятным возможность заключения сколько-либо действенного соглашения в сфере недопустимости вмешательства с использованием информационных средств опять же ввиду сложности аттрибуции актов применения силы и верификации последствий применения силы третьими сторонами, что является необходимым условием существования международных правовых норм. Так, например, единственным, по сути, соглашением в данной сфере является Конвенция Совета Европы о компьютерных преступлениях 2001 г.[1] Ее положения оказались заведомо неэффективными, поскольку не успевают за развитием технологического уклада. Кроме того, данная конвенция не предусматривает присвоения каких-либо мер международной ответственности государствами, если они сами вовлечены в противоправную деятельность.

Таким образом, в настоящее время невозможно построить стратегию противодействия информационным вмешательствам, дающую представление о разграничении собственно «информационной войны (информационного вооруженного конфликта)» и постоянно присутствующего в нашей жизни информационного противоборства. Сложность оценки причиненного государствам и их населению ущерба в когнитивной сфере и, соответственно, сопоставления с практикой присвоения ответственности за использование традиционных средств ведения вооруженного противоборства, делает невозможным в ближайшее время формирование какого-либо адекватного универсального международного политико-правового режима противодействия информационным угрозам. Устранение угроз в киберпространстве является для государств общим интересом по обеспечению международной стабильности, но в настоящее время оно может осуществляться ими лишь самостоятельно.

Можно предположить, что вышеупомянутый Федеральный конституционный закон «О военном положении» должен также установить более широкий перечень действий (как минимум, отсылая к разъясняющим нормам), которые можно относить к актам агрессии, осуществляемой посредством информационных воздействий. В цифровую эпоху объекты, выбираемые для поражения, могут иметь совершенно иные и неожиданные свойства, что обусловливает существование значительного числа подходов к классификации объектов информационного воздействия. Сила применяется против физических и виртуальных объектов не только в физическом, но и в информационном и когнитивных измерениях. Заявление в федеральном законодательстве перечня недопустимых агрессивных действий, осуществляемых посредством информационных воздействий, будет, по своей сути, превентивной мерой, так как установит пороговые ограничения для осуществления вмешательства во внутренние дела государства извне для других международных акторов.

Для этого представляется необходимым осуществить значительный объем исследований для определения влияния информационных воздействий в когнитивном измерении на суверенитет, политическую независимость и территориальную целостность государства. Но ответ будет найден, очевидно, не в праве, в котором необходимый методологический аппарат отсутствует, а в тех отраслях знаний, которые изучают свойства личности.

[1] [Электронный ресурс]. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (дата обращения: 01.02.2020). Россия в данном соглашении не участвует. Соединенные Штаты Америки, не являясь членом Совета Европы, — участвуют.

Литература

1. *Коростелев С. В.* О некоторых особенностях правового режима «новых» средств и методов ведения вооруженной борьбы // Управленческое консультирование. 2015. № 6. С. 50–57.
2. *Robert D. Steele.* Takedown: Targets. Tools, and Technology in Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated? (ed. Lloyd J. Matthews). U. S. Army War College Strategic Studies Institute. Carlisle Barracks. Pennsylvania. July 1998.

Об авторе:

Коростелёв Станислав Валентинович, Ответственный секретарь Объединенной комиссии при Межпарламентской Ассамблее государств — участников Содружества Независимых Государств по гармонизации законодательства в сфере безопасности и противодействия новым вызовам и угрозам, кандидат юридических наук, доцент; ksv1@iacis.ru

References

1. Korostelev S. V. About Peculiarities of Legal Regime of "New" Means and Methods of Warfare // Administrative consulting [Upravlencheskoe konsul'tirovanie]. 2015. N 6. P. 50–57. (In rus)
2. Robert D. Steele. Takedown: Targets. Tools, and Technology in Challenging the United States Symmetrically and Asymmetrically: Can America be Defeated? (ed. Lloyd J. Matthews). U. S. Army War College Strategic Studies Institute. Carlisle Barracks. Pennsylvania. July 1998.

About the author:

Stanislav V. Korostelev, Executive Secretary of the Joint Commission under the Interparliamentary Assembly of the Commonwealth of Independent States on Harmonization of Legislation in the Sphere of Security and Countering Emerging Threats and Challenges, PhD in Jurisprudence, Associate Professor; ksv1@iacis.ru