О НЕКОТОРЫХ ПРОБЛЕМАХ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА В СВЕТЕ КИБЕРНАПАДЕНИЙ

***Лилит Еремян* ***

Определенные действия в киберпространстве, квалифицируемые как МВК или НМВК, регулируются нормами МГП. В данной статье мы пытаемся ответить на вопрос: отвечают ли существующие регуляции МГП вызовам технического прогресса и стремительного развития кибернападений. В статье рассматриваются проблематичные аспекты соблюдения принципов избирательности, пропорциональности и мер предосторожности в свете военных кибероперациий. На данный момент не существует международных договоров, регулирующих проблемные аспекты защиты гражданского населения при кибервойне. Необходимость разработки такого договора в будущем позволит адекватно реагировать на вызовы современных кибервойн.

Военное применение киберпространства

Быстрый прогресс компьютерных технологий поднимает ряд теоретических и практических вопросов в контексте регуляций международного гуманитарного права ("МГП"). Несмотря на "бескровные возможности" некоторых видов оружия, последствия их применения могут быть устрашающими[1]. Мощное распространение всемирной компьютерной сети, бесспорно, является одной из наиболее значимых технологических революций[2]. Физические лица, юридические лица и военный сектор тесно взаимосвязаны в киберпространстве. Так, Департамент Безопасности ("ДБ") США сильно зависит от частных провайдеров компьютерных технологий. ДБ "управляет 15000 сетями через 4000 установок в 88 странах [,используя] более 7 миллионов компьютеров"[3]. Более 95% военной информации США[4] и 98% государственной информации передаются через сети, которые являются собственностью частных лиц и ими же управляются[5]. В ближайшем будущем все компьютерные устройства могут быть объединены в сетевой структуре между странами. По приблизительным подсчетам к 2015 году число взаимосвязанных между собой компьютерных устройств будет превышать количество людей на земле[6]. Не удивительно, что киберпространство считается удобным для военных операций. Для организации кибератаки достаточно наличие обыкновенного компьютера или даже мобильного телефона с интернет-связью[7]. "Привлекательность" военного использования киберпространства увеличивается еще и потому, что отсутствие установленных границ в киберпространстве очень усложняет преследование кибератакующего[8]. Специальные правовые регламентации для регулирования вопросов, связанных с кибератаками, еще недостаточно разработаны[9]. Вопрос заключается в том, отвечают ли существующие регуляции МГП вызовам кибервойн.

Может ли кибератака квалифицироваться как вооруженный конфликт?

Очень важно провести различие между киберпреступлениями и кибератаками, составляющими вооруженный конфликт. Киберпреступления подпадают под действие

* Еремян Лилит Араевна, эксперт Постоянной Комиссии по государственно-правовым вопросам Национального Собрания РА; LL.M., Эссекский университет (Великобритания);
соискатель кафедры международного права и европейского права Российско-Армянского Университета

уголовного законодательства, тогда как положения МГП будут применимы только в ситуациях, когда кибератака составляет вооруженный конфликт[10].

Одна из особенностей кибератаки заключается в том, что предельно усложняется возможность определения действительного "атакующего"[11]. Принимая во внимание виртуальный характер киберпространства и отсутствие кинетической силы, спорным может показаться вопрос о том, должна ли кибератака считаться применением вооруженной силы[12]. Ответ на этот вопрос утвердительный. Кибератака определяется как акт насилия в отношении противника, в том числе и кибероперации, которые могут повлечь ранения или смерть гражданских лиц либо причинить ущерб гражданским объектам, независимо от того, совершаются ли они при наступлении или при обороне[13]. Между тем общепризнано, что дефиниция понятия "атака" в контексте Первого дополнительного протокола к ЖК ("ДП I") понимается в том числе и как акт насилия в отношении противника, влекущий жестокие последствия, без применения какой-либо кинетической силы[14].

Международный вооруженный конфликт ("МВК") и немеждународный вооруженный конфликт ("НМВК") - это единственные виды вооруженного конфликта в рамках регуляций МГП[15]. "[Все случаи] объявленной войны или всякого другого вооруженного конфликта, возникающего между двумя или несколькими [государствами], даже в том случае, если одно из них не признает состояния войны", составляют МВК[16]. В контексте общего положения Женевской конвенции ("ЖК") ("Статья 2") МВК возникает, "когда одно или несколько государств прибегают к вооруженной силе против другого государства"[17].

Таким образом, кибератака может приравниваться к МВК, если:

а) эта атака происходит между двумя или более государствами

б) государство прибегает к вооруженной силе[18].

Существует мнение, что кибератака, осуществленная каким-либо государством, или вмененная какому-либо государству, должна считаться МВК, если эта атака "спроектирована для причинения вреда другому государству ... непосредственно причиняя смерть, повреждения или разрушения, [а также атака, которая] непосредственно отрицательно сказывается на военных операциях или военном потенциале"[19]. При этом, международная группа экспертов пришла к выводу, что кибероперация приравнивается к МВК также в случае, когда негосударственный субъект под *"общим контролем"* одного государства вступает в военные действия с другим государством. Следует отметить, что на практике очень сложно установить наличие "общего контроля" со стороны государства[20].

Кибернападение может также квалифицироваться как НМВК, который возникает на территории государства, когда военные действия происходят между "правительственными вооруженными силами и негосударственными [организованными вооруженными] группами или только между такими группами"[21].

Для того, чтобы ситуация квалифицировалась как НМВК необходимо, чтобы: а) эта ситуация достигла бы определенного уровня интенсивности и б) соответствующая негосударственная группа имела бы определенный уровень организации[22]. Анализ вышеуказанных критериев в свете кибернападений поднимает ряд вопросов. Например, можно ли квалифицировать как НМВК определенное количество кибернападений, причиняющих существенный ущерб государству, если эти нападения осуществляются небольшой группой лиц с невысоким уровнем "виртуальной" онлайн-организации? Как определить тот порог, при котором кибернападение считается НМВК?[23] Должен ли этот порог "зависеть от степени вреда, причиненного атаками компьютерных сетей: [иными словами] чем больше вред, тем больше вероятность, что ситуация будет квалифицирована в качестве вооруженного конфликта"?[24]

Целесообразно применение индивидуального подхода к оценке случаев кибернападений с учетом особенностей и обстоятельств каждого конкретного случая. Считаем, что акты насилия в отношении противника, в том числе и кибернападения, которые потенциально могут повлечь ранения или смерть гражданских лиц либо причинить ущерб гражданским объектам, должны квалифицироваться в качестве вооруженного конфликта, если атакующей стороной является либо государство, либо, в зависимости от интенсивности атаки, негосударственный субъект. При установлении факта, является ли кибернападение вооруженным конфликтом, также необходимо учесть, было ли нападение "реализовано в контексте вооруженного конфликта"[25]. Если устанавливается, что кибернападение явля-

ется МВК или НМВК, тогда ситуация регулируется положениями МГП[26]. Таким образом, следующей задачей будет определение того, являются ли существующие регуляции МГП эффективными или нет.

Принцип избирательности в свете кибератак

Недопустимость осуществления нападений на гражданских лиц и гражданские объекты рассматривается как краеугольный камень принципа избирательности[27]. В соответствии с принципом избирательности запрещается любая *военная операция, [подчеркнуто мною - Л.Е.],* направленная против гражданского населения и гражданских объектов[28]. Кибернападения, произведенные в контексте вооруженного конфликта и связанные с вооруженным конфликтом, подпадают под формулировку "военная операция." Как было отмечено *supra*, кибернападение считается "нападением" в контексте статьи 49.1 ДП I, если оно непосредственно подвергает опасности гражданские лица, основываясь не на фактически причиненных разрушительных последствиях, а на их возможном наступлении. Возникает вопрос: должен ли применяться принцип избирательности в случае кибернападения, реализованного в контексте вооруженного конфликта и связанного с ним, но потенциально не причиняющего гибель, увечья или разрушения? По мнению большинства международных экспертов, МГП не запрещают такие кибероперации, направленные против гражданского населения, которые причиняют только неудобства, раздражение и сбой систем (например, психологические кибероперации, блокирование электронной связи по всей территории страны и т.п.)[29]. С другой стороны, МГП предоставляет общую защиту гражданским лицам против "опасностей, возникающих в результате военных операций"[30], а кибероперации, составляющие неотъемлемую часть более широкой военной операции, должны подпадать под регулирование МГП[31]. В указанном контексте считаем, что принцип избирательности должен учитываться и быть соблюден в процессе планирования и осуществления кибернападений, если они составляют часть военных действий в целом. Следует отметить также, что, по мнению технических экспертов, представляется очень сложным осуществление кибернападения в соответствии с принципом избирательности, учитывая высокий уровень электронной взаимосвязанности между гражданскими и военными системами, однако теоретически это возможно[32]. Полем боя в случае кибератаки является киберпространство, описанное как сеть, "связывающая всех со всем",[33] а также как "глобальная взаимосвязанность людей через компьютеры и телекоммуникации без учета физической географии"[34]. Любое нападение на конкретный узел системы может рассматриваться как нападение на всю систему в целом[35]. В таком контексте даже кибератаки, спроектированные для нападения на военные объекты, скорее всего распространят негативные последствия на гражданские лица и гражданские объекты, если последние хотя бы в незначительной степени взаимосвязаны с целевыми военными объектами[36]. Основной проблемой при кибернападениях является сложность моделирования возможных последствий этого средства ведения вооруженного конфликта.

Определение неизбирательного характера кибернападений должно осуществляться в индивидуальном порядке в каждом конкретном случае.

Принцип пропорциональности в контексте кибернападений

Избирательные кибернападения должны быть спланированы и осуществлены в соответствии с принципом пропорциональности[37]. Принцип пропорциональности отражен в ДП I в статьях 51.5.b, 57.2.a.iii and 57.2.b. Кибернападение будет считаться незаконным, если возможно, что оно "попутно повлечет за собой потери жизней среди гражданского населения, ранения гражданских лиц и ущерб гражданским объектам или то и другое вместе, которые были бы чрезмерны по отношению к конкретному и непосредственному военному преимуществу, которое предполагается таким образом получить"[38]. Предопределение последствий кибернападений в контексте кибервойны может быть непредсказуемым. Более того, сторона может предпочесть достигнуть военного преимущества путем осуществления кибернападений, которые, предполагается, не создают прямых угроз для жизни гражданских лиц, но которые тем не менее могут иметь негативное воздействие на различные сферы гражданской жизни. Может возникнуть вопрос о том, что является более предпочтительным и законным с точки зрения регуляций МГП: распространенный нефизический ущерб (например, банковской системы), нанесенный миллионам граждан, или физический вред,

причиненный нескольким гражданским лицам. Группа международных экспертов считает, что такие последствия кибероперации как стресс, неудобства, раздражение или страх среди гражданского населения не должны считаться нанесенным ущербом с точки зрения МГП и не должны учитываться при определении пропорциональности операции[39]. С другой же стороны, как было отмечено выше, необходимо соблюдать принцип избирательности в процессе планирования и осуществления кибернападений, составляющих неотъемлемую часть военных действий в целом, в противном случае, думаем, что подобные кибернападения должны считаться неизбирательным и незаконным *per se*.

Меры предосторожности при нападении

Государства обязаны предпринять "все практически возможные" меры предосторожности для обеспечения защиты гражданского населения и гражданских объектов от последствий военных нападений[40]. Данное правило признается нормой обычного международного права[41]. Положения МГП разрабатывались, имея в виду территорию в традиционном понимании этого слова, а не виртуальное пространство. Очевидно, что меры предосторожности акцентируют физическое разграничение комбатантов от гражданских лиц, а также гражданские объекты от военных объектов[42]. В свете кибернападений данное обязательство государств становится практически бессмысленным, учитывая взаимосвязанность и взаимозависимость военных и гражданских виртуальных сетей[43]. В контексте кибернападений единственным способом для государства эффективно реализовать требования мер предосторожности являлось бы установление и эксплуатация собственной дискретной информационной инфраструктуры. На практике может быть "очень сложным, если не невозможным" реализовать указанные требования, но государства должны делать все возможное для этого[44]. Таким образом, при кибернападении для государств практически невозможно экономически и/или технически соблюдать все требования указанных мер предосторожности[45]. С учетом же специфичных характеристик компьютерных коммуникаций употребляемая формулировка "все практически возможное" *de facto* освобождает государства от обязанности строго соблюдать меры предосторожности в случаях кибернападений.

Правовое регулирование кибервойны

Военное применение киберпространства поднимает и много других правовых и практических вопросов. Так, например, проблематично применение принципа различия, ввиду того, что во время кибероперациий часто происходит милитаризация гражданских лиц и гражданских обьектов[46]. Проблематичны также аспекты проведения правовой экспертизы новых средств ведения войны в соответствии со статьей 36 ДП I в контексте кибероперациий.

Правовые аспекты кибервойны не отражаются в каком-либо многостороннем договоре, устанавливающем запрет на определенные виды кибернападений, либо регламентирующем ограничения для планирования и реализации конкретных видов кибернападений. На международном уровне нет консенсуса относительно того, должны ли быть специальные положения, регулирующие кибервойны[47]. Согласно официальной государственной позиции Великобритании и США, существующие положения МГП адекватно регулируют эту сферу и нет необходимости в принятии специальных обязывающих договоров[48]. Многие утверждают, что регуляции МГП не могут адекватно справиться с проблемами, возникающими в результате кибернападений[49]. Обсуждается идея о необходимости разработки международной конвенции, регулирующей использование кибер-пространства для военных целей[50]. Существует мнение, что в связи с быстрым развитием и изменчивостью информационных технологий, недостаточностью опыта в этой сфере, "любые международные договоры относительно интернет-войны [в момент их принятия уже] будут устаревшими..."[51].

Надо отметить, что международное сообщество уже в 2010 году консолидировало силы с целью разработки свода правил, применяемых во время кибервойны. В результате совместной работы в марте 2013 года было опубликовано так называемое "Таллиннское руководство", которое дает интерпретацию международно-правовых норм, применяемых при кибервойне. Считаем, что на данном этапе, с учетом того, что некоторые государства перманентно высказывались против необходимости принятия юридически обязательных регуляций относительно кибервойны, разработка необязывающего свода правил относительно кибервойны является *per se* прогрессивным шагом. Впоследствии же, после проверки эффективности регуляций "мягкого права" на практике,

государства могут смоделировать и разработать юридически обязывающий договор, основанный на существующих правилах, их специальной интерпретации и лучшей практике государств.

ON ISSUES IN INTERNATIONAL HUMANITARIAN LAW IN THE LIGHT OF CYBER ATTACKS

The paper explores the issue whether international humanitarian law meets the challenges of technological progress and the fast growth of cyber attacks. Issues regarding compliance with the principles of selectivity, proportionality and observance of precautionary measures in the light of military cyber operations are analyzed. The need to produce legislation on protection of civilian population against cyber wars is shown.

Lilit Yeremian,
LLM, Postgraduate Researcher, Department of International and European Law, Russian-Armenian University, Advisor, Commission for State-Legal Matters, National Assembly of the Republic of Arminia

Ключевые слова:
международное гуманитарное право, кибернападения, вооруженный конфликт, принцип избирательности, принцип пропорциональности, защита гражданских лиц и гражданских объектов, правовое регулирование

Keywords:
international humanitarian law, cyber attacks, armed conflict, selectivity, proportionality, protection of civilian population and facilities, legal regulation.

Литература:

[1] Blake D., Imburgia J. "Bloodless Weapons?" The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons"// Air Force Law Review. № 66. 2010. P. 161.

[2] Melzer N. Cyber War and International Law // United Nations Institute for Disarmament Research Resources. 2011. P. 3.

[3] Lynn W.J. // Remarks at USAF-Tufts-Institute for Foreign Policy Analysis Conference // http://www.defense.gov.

[4] Solce N. The Battlefield of Cyberspace: The Inevitable New Military Branch — The Cyber Force // Albany Law Journal of Science & Technology. 2008. P. 297.

[5] Jensen E.T. Cyber Warfare and Precautions against the Effects of Attacks // Texas Law Review. № 88. 2009-2010. P. 1533.

[6] A Strong Britain in an Age of Uncertainty: The National Security Strategy // http://www.direct.gov.uk./prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf

[7] Brenner S.W., Goodman M.D. In Defense of Cyber-terrorism: An Argument for Anticipating Cyber-attacks // University of Illinois Journal of Law Technology & Policy. 2002. P. 13; Geiss R. The Legal Regulation of Cyber Attacks in Times of Armed Conflict // Bruges Colloquium. CIRC. 2010. P. 50.

[8] Robbat M.J. Resolving the Legal Issues Concerning the Use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework and a Creation of a New Paradigm // Boston University Journal of Science & Technology Law. 2000. P. 269.

[9] Blake D., Imburgia J. "Bloodless Weapons?" The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons". P. 183.

[10] Melzer N. Cyber War and International Law. P. 3-4.

[11] Lubell N. Cyber Warfare as Armed Conflict // Bruges Colloquium "Technological Challenges for the Humanitarian Legal Framework". CICR. 2010. P. 44.

[12] Melzer N. Cyber Operations and Jus in Bello // Disarmament Forum. 2011. P. 5.

[13] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, (ed.- Schmitt M.) // Tallinn Manual Applicable to International Law Applicable to Cyber Warfare (draft). Cambridge University Press, 2013. P. 92 // http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf

[14] Schmitt M.N. War, Technology and International Humanitarian Law // Harvard University Program on Humanitarian Policy and Conflict Research, Occasional Paper Series. 2005. P. 44.

[15] How is the Term "Armed Conflict" Defined in International Humanitarian Law // International Committee of the Red Cross. 2008. Opinion paper. P. 1.

[16] Женевские Конвенции (1949). Общая статья 2.

[17] How is the Term "Armed Conflict" Defined in International Humanitarian Law. Opinion paper. p. 1.

[18] Статья 1.4 ДП I к Общей статье 2 дополняет ситуации вооруженного конфликта, в которых "народы ведут борьбу против колониального господства и иностранной оккупации и против расистских режимов в осуществление своего права на самоопределение..." Данное положение применимо только к государствам-участникам ДП I. Статья 1.4 не является нормой обычного права (См.: Lubell N. Extraterritorial Use of Force against Non-State Actors. Oxford Scholarship Online. 2010. P. 97).

[19] Melzer N. Cyber Operations and Jus in Bello. P. 5.

[20] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, (ed. -Schmitt M.) // Tallinn Manual Applicable to International Law Applicable to Cyber Warfare (draft). P. 72.

[21] How is the Term "Armed Conflict" Defined in International Humanitarian Law. Opinion paper. P. 3.

[22] Ibid.; International Criminal Tribunal for the former Yugoslavia, Prosecutor v. Fatmir Limaj Judgment (2005). Case № IT-03-66-T. Paras 94-170.

[23] Melzer N. Cyber Operations and Jus in Bello. P. 5.

[24] Dörmann K. Applicability of the Additional Protocols to Computer Network Attacks // International Expert Conference on Computer Network Attacks and the Applicability of IHL, Stockholm, 2004. P. 3.

[25] Melzer N. Cyber Operations and Jus in Bello. P. 4.

[26] Schmitt M.N. International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed // Harvard International Law Journal. 2012. P. 15.

[27] Дополнительный протокол к Женевским конвенциям 1949 года, касающийся защиты жертв международных вооруженных конфликтов (ДП I) (1977) ст. 51.2, 51.4, 51.5, 52.1, 52.2 и др.

[28] Ibid., ст. 48, 51, 52; International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, (ed.- Schmitt M.) // Tallinn Manual Applicable to International Law Applicable to Cyber Warfare. P. 96.

[29] Ibid., P. 92, 94.

[30] ДП I, supra n. 27, ст. 51.1; Дополнительный Протокол II, касающийся защиты жертв вооруженных конфликтов немеждународного характера (1977) ст. 13.

[31] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, (ed.- Schmitt M.) // Tallinn Manual Applicable to International Law Applicable to Cyber Warfare (draft). P. 94.

[32] Geiss R. The Legal Regulation of Cyber Attacks in Times of Armed Conflict. P. 51.

[33] Lubell N. Cyber Warfare as Armed Conflict. P. 43.

[34] Hildreth S.A. Cyber Warfare // Congressional Research Service Report for Congress on Cyberspace. 2001. P. 1.

[35] Shackelford S.J. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law // Berkeley Journal of International Law. Vol. 27. 2009. P. 200-201 // http://scholarship.law.berkeley.edu

[36] Melzer N. Cyber Operations and Jus in Bello. P. 10.

[37] Gardam J. Necessity, Proportionality and the Use of Force by States. New York, 2004. P. 95; см. также: ICTY. Prosecutor v. Kupreskic et. al., Judgment (Jan.2000). Case №. IT-95-16-T. P. 524.

[38] ДП I. Supra n. 27. Ст. 51.5.b, 57.2. a.iii.

[39] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, (ed.- Schmitt M.) // Tallinn Manual Applicable to International Law Applicable to Cyber Warfare (draft). P. 133.

[40] ДП I. supra n. 27. Ст. 57, 58.

[41] Henckaerts J.-M., Doswald-Beck L. Customary International Humanitarian Law. Vol. 1: Rules. New York, 2005. P. 68-71.

[42] ДП I. Supra n. 27. Ст. 58.

[43] Kanuck S. Sovereign Discourse on Cyber Conflict Under International Law // Texas Law Review. Vol. 88. 2009-2010. P. 1595.

[44] Kalshoven F., Zegveld L. Constraints on the Waging of War. International Committee of the Red Cross. Geneva, 2001. P. 110.

[45] Kanuck S. Sovereign Discourse on Cyber Conflict Under International Law. P. 1595.

[46] Jensen E.T. Cyber Warfare and Precautions against the Effects of Attacks. P. 1544.

[47] Kanuck S. Sovereign Discourse on Cyber Conflict Under International Law. P. 1589.

[48] Ibid., P. 1588.

[49] Walker J.K. The Demise of the Nation-State, The Dawn of New Paradigm Warfare, and a Future for the Profession of Arms // Air Force Law Review. Vol. 51. 2001. P. 337.

[50] Brown D. A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict // Harvard International Law Journal. Vol. 47. 2006. P. 179.

[51] Walker G.K. Information Warfare and Neutrality // Vanderbilt Journal of Transnational Law. Vol. 33. 2000. P. 1200.