Информационная война

Уильям Черч*

Слухи о новом виде войны волнуют воображение военных стратегов вот уже почти десять лет. Косовский кризис обнаружил, что слухи эти стали реальностью. Некоторые из технологий и тактических приемов, являвшиеся предметом таких разговоров, превратились в военную доктрину, и теперь одна из мировых держав просит ООН исследовать этот сдвиг в способах ведения военных действий.

К переменам, о которых здесь идет речь, обычно применяется популярный термин «информационная война» (ИВ), но в понимании военных это часть более широкого стратегического нововведения, называемого «информационными операциями» и «революцией в военном деле». Но, как это явление ни назови, суть одна: использование во враждебных целях высокотехнологичных компьютерных и телефонных систем противника как в военной, так и в гражданской инфраструктуре.

Поскольку определение информационной войны находится все еще в стадии разработки и разные страны формулируют его по-разному, лучше всего понять такой вид войны можно, рассмотрев, как он уже использовался и как его можно использовать. В настоящей статье анализируется применение двух категорий ИВ:

- ИВ, не сопровождающаяся применением физической силы, — в мирное время;
- ИВ с применением физической силы — во время вооруженного конфликта.

* **Уильям Черч —** главный редактор Центра исследований инфраструктурной войны (CIWARS) и «РМА Уотч» (Глазго, Великобритания). В настоящее время работает над докторской диссертацией на тему «Международное гуманитарное право и информационная война» в университете Глазго. Настоящая статья подготовлена на основе ряда источников, главный из которых — CIWARS Intelligence Report, выпуски 1997 и 1998 г. См.: www.iwar.org/ciwars.html. Обзор политики США в отношении информационных операций (информационной войны) см. www.iwar.org/USJointIO.html. По другим странам — www.iwar.org/country.html. (Сведения об авторе указаны на момент представления рукописи в редакцию Журнала. — *Прим. ред.*)

Статья написана на английском языке.

Информационная война, не сопровождающаяся применением физической силы

Прежде чем начать этот раздел, важно поставить один серьезный вопрос: допустимо ли вообще пользоваться термином «информационная война», если войны нет? Ответ можно найти в определении войны, сформулированном в начале XIX столетия известным немецким военным теоретиком Карлом фон Клаузевицем, — он понимал войну как «продолжение политики иными средствами». В свете ИВ «иные средства» могут рассматриваться как нечто весьма похожее на практикуемый в морской войне предупредительный выстрел поверх носа корабля, с той только разницей, что это делается при помощи компьютеров — беззвучно, но не менее эффективно.

Около двух лет назад метод информационной войны был применен для того, чтобы помешать переводу средств между подразделениями одной из ближневосточных террористических группировок. Банковский счет тех, кто финансировал террористов, был тайно вскрыт и средства с него были сняты. Подобным образом в начале косовского конфликта обсуждались и были одобрены методы оказания давления на президента Милошевича. Среди них — манипуляции с его банковскими счетами или их взлом, вывод из строя его личной электронной почты.

В первом случае взлом банковской системы прошел успешно. О попытках взломать счета сербского президента или вывести из строя его электронную почту ничего неизвестно. Однако здесь необходимо заострить внимание на вопросах, возникающих в связи с применением этих методов и их результатами. Например, взлом банковского счета является нарушением законов того государства, в котором счет домицилирован, и если такая операция удалась, значит, она включала в себя перехват и взлом кода защиты международной банковской системы. Но взлом банковских систем связан в большей степени с вопросами уголовного, чем международного гуманитарного права, хотя в нашем случае он был осуществлен как враждебное действие в ситуации конфликта. Этот пример дает также пищу для дальнейших размышлений о возможностях такой стратегии. Большинство операций на фондовом рынке сейчас осуществляются в электронной форме, и уже происходили сбои, которые можно преднамеренно вызывать с помощью ИВ. Например, в 1998 г. стажер, проходивший подготовку на фондовой бирже, нажал не на ту кнопку компьютера и спровоцировал панику на рынке, в результате чего за один день котировки акций снизились на несколько сот миллионов долларов.

Дело не просто в том, что такую ситуацию можно воспроизвести, взломав или испортив компьютер фондового рынка: именно такой порядок действий используется в наши дни как в наступательной, так и в оборонительной стратегии вооруженными силами ряда стран. Цель при этом состоит в том, чтобы вызвать финансовый крах экономики какой-либо страны и тем самым лишить ее возможности закупать оружие в больших количествах.

Чем вероятнее применение физической силы в вооруженном конфликте, тем агрессивнее становится тактика ИВ. Комиссия при президенте США по защите жизненно важной инфраструктуры указала в 1998 г. на необходимость подготовки к отражению воздействия ряда методов ИВ, которые, по ее мнению, могут быть использованы против Соединенных Штатов. К ним относятся выведение из строя электросетей и (или) телекоммуникационных систем с целью воспрепятствовать военной мобилизации или заставить гражданское население задуматься над тем, во что обойдется надвигающаяся война.

По мере нарастания напряженности в месяцы, непосредственно предшествовавшие вооруженной интервенции в Косово, американская военная компьютерная инфраструктура подвергалась зондированию в постоянно возраставших масштабах, и в некоторых случаях ее работа была затруднена. Эта операция получила кодовое название «Восход солнца», и, хотя впоследствии выяснилось, что она проводилась не Федеративной Республикой Югославия и не кем-либо из ее союзников, это явилось серьезным предупреждением для вооруженных сил США.

Аналогичная возможность рассматривалась в 1999 г. на конференции «Будущее войны» в Санкт-Петербурге. Однако на этот раз в качестве примера была взята фолклендская война. Аргентина могла бы использовать методы ИВ для нарушения электроснабжения, телефонной связи и работы транспорта в Лондоне, создавая тем самым помехи для мобилизации; это позволило бы отсрочить отплытие флота и дать Аргентине больше времени для пополнения запасов ракет «воздух—воздух» и «воздух—земля» или вызвать политические затруднения для британского премьер-министра. Можно было бы не принимать всерьез все эти воображаемые сценарии, но ведь они взяты непосредственно из ныне действующей военной доктрины.

Высказывались предположения о том, что ИВ станет следующим новым наиболее эффективным оружием, которое будет использоваться в качестве средства принуждения террористами и повстанческими арми-

ями. Колумбийские повстанческие силы уже сегодня подвергают нападению гражданские системы электроснабжения: так, в прошлом году было взорвано более 30 опор ЛЭП. Учитывая, что приемы ИВ уже применяются на поле боя для нарушения коммуникаций колумбийской армии, идея использования ИВ против гражданской инфраструктуры не представляется такой уж невероятной. Следовательно, у нас есть достаточно оснований обратиться к международному гуманитарному праву.

Информационная война, сопровождающаяся применением физической силы

В этом разделе содержится скорее краткий обзор, чем исчерпывающее описание ИВ; здесь выделены шесть областей ее использования. Для удобства они рассматриваются с позиций первоочередного и второстепенного применения. Это разграничение сделано на основе известной доктрины и существующих возможностей. Соображения относительно первоочередного применения основаны на том, что известно и вероятно, в то время как второстепенное применение все еще носит предположительный характер.

Первоочередное применение

К ИВ можно обращаться для создания помех при использовании бомб высокой точности. Чем чаще их будут применять, тем большее развитие получит использование ИВ в оборонительных целях. Этот вид бомб — их часто называют «умными» — был впервые использован почти десять лет назад во время войны 1991 г. в Персидском заливе между странами коалиции и Ираком. С тех пор применение такого оружия увеличилось с 8% в упомянутой войне до 35% в ходе косовского конфликта. Считается, что высокоточные бомбардировки позволяют нацеливаться на военные объекты, окруженные зданиями гражданского назначения, — по таким целям неоднократно наносились удары как во время войны в Персидском заливе, так и в ходе косовского кризиса — и именно в этом и состоит проблема. Бомбы наводятся с помощью либо ответчиков, тайно установленных на объекте, либо координации сигналов глобальной навигационной спутниковой системы (ГНСС), которые могут определить точное местоположение на земле и направить бомбу в это место. ИВ может быть применена с целью создания помех для сигналов, направляющих бомбы, или для их искажения.

Однако ручной передатчик преднамеренных помех для ГНСС, способный изменить курс бомбы высокой точности, можно сейчас купить менее чем за 10 тысяч долларов. Ввиду того, что некоторые военные объекты расположены в непосредственной близости от мест нахождения гражданского населения, возникает вопрос ответственности:

- Кто несет ответственность за последствия нарушения курса и за случайный ущерб?
- Если известно, что противник имеет такую возможность, следует ли воздержаться от применения бомб высокой точности в дальнейшем, поскольку они могут стать неизбирательным оружием?

К сожалению, передатчики помех для ГНСС — не единственная угроза для бомб высокой точности. В современных вооруженных силах разработано оружие, поражающее силой электромагнитного импульса (ЭМИ). Оно выводит из строя компьютерные операционные системы и средства телекоммуникации. Принцип действия этого оружия легче всего объяснить, сравнив его с магнитом, который кладется рядом с компьютерным диском и начисто стирает с него всю информацию. Оружие ЭМИ — его используют как в качестве наступательного оружия, так и в качестве контрмеры — также создает целый ряд проблем: оно обычно неизбирательно и поражает не только свою цель. От него могут пострадать в больницах гражданские пациенты, чья жизнь поддерживается с помощью компьютеризованной аппаратуры, оно может причинить ущерб жизненно важным системам электроснабжения и транспорта. Это снова поднимает вопрос о случайном ущербе и ответственности за применение оружия ИВ.

Как во время войны в Персидском заливе, так и во время косовского конфликта, вся инфраструктура превратилась в мишень, и специалисты по международному гуманитарному праву тщательно изучили эту тактику. Однако цель настоящей работы состоит в том, чтобы рассмотреть применение ИВ вместо физической силы. Иными словами, речь идет о взломе компьютерных систем соответствующей страны и порче их путем внедрения туда вируса или каким-либо другим способом. Такая мера, естественно, воспрепятствовала бы их использованию в течение какого-то времени, а впоследствии не пришлось бы нести расходы по финансированию восстановления инфраструктуры, как это сейчас имеет место в Косово.

Каким бы маловероятным ни казался подобный сценарий, факты свидетельствуют о том, что он рассматривался и был отвергнут при планировании интервенции в Косово. Таким образом, можно только предпо-

лагать, что необходимые для этого основные средства уже были в наличии и что в следующей войне их можно будет уверенно применить. Основная концепция ограниченного ущерба была проверена 5 мая 1999 г. путем использования устройства под названием «мягкая бомба»: на электрические провода были сброшены куски графита, что вызвало временное короткое замыкание в системе. Проверка прошла успешно: подача электричества прекратилась на 5 часов, так что, разумеется, поиск «мягких» средств будет продолжен.

Еще одной областью ИВ является возможное использование таких «мягких» средств для взлома компьютерных систем, контролирующих инфраструктуру страны, в результате чего гражданская инфраструктура государства окажется в положении «заложника». Опять-таки эта тактика рассматривалась и была отвергнута в отношении Косово, однако тем не менее возникает вопрос о ее применении в будущем. Подобным же образом была отброшена мысль о том, чтобы с помощью электронных средств отрезать Югославию от Интернета, поскольку это повлияло бы и на военнослужащих, и на гражданское население и могло бы иметь катастрофические последствия для отраслей, использующих Интернет для контроля за своими жизненно важными функциями, например, для современных систем электро- и водоснабжения. Больницы во многих странах используют Интернет для доступа к медицинским архивам и даже для консультаций со специалистами при выполнении медицинских процедур.

Кроме того, такая акция может нарушить выполнение каких-либо транснациональных соглашений о поставках энергии — они становятся все более популярными в нашем глобализованном и приватизированном мире. Превращение гражданской структуры в объект нападения поднимает интересный вопрос, касающийся процесса определения целей и его общего воздействия, которое, по мнению отдельных специалистов, может приобрести неизбирательный характер в связи с взаимозависимостью глобальной и национальной инфраструктур. Например, энергосистемы Лаоса и Таиланда, Венесуэлы и Бразилии, Канады и США, Индонезии и Сингапура связаны между собой. А особенно яркий пример — Сингапур, который получает половину поставляемой ему воды из Малайзии.

Эта проблема касается и средств связи. Она отчетливо видна на примере Восточной и Юго-Восточной Азии, так как там все наземные и подводные телефонные кабели представляют собой единую систему

и повреждение в любой точке нарушит всю ее работу. Поэтому удар, направленный против одной из стран этого региона, прервет передачу значительной части телекоммуникационных сообщений в Азии и заставит осуществлять их исключительно с помощью спутниковой связи, возможности которой ограничены. Это поднимает вопрос об ущербе, наносимом нейтральным или третьим странам.

Третья область первоочередного применения ИВ при одновременном применении физической силы — удары хакеров по военным системам, что, как сообщалось, имело место в ходе косовского конфликта. Было подтверждено, что происходило манипулирование системой противоракетной обороны югославских ВВС; возможный пример — помещение на компьютерный экран ложных целей или простое нарушение системы. Такая деятельность в большой степени входит в категорию военных хитростей, но ее потенциал значительно мощнее.

Один из самых очевидных примеров — хакерский удар по системам ядерных ракет, вызывающий незапланированный запуск, или искажение базы данных для целеуказания при применении обычных ракет или бомб с тем, чтобы нанести намеренный ущерб гражданским объектам и тем самым изменить общественное мнение. Это не так нереально, как кажется. Многие из этих функций контролируются базой данных по целеуказанию, которая постоянно обновляется, даже в мирное время. Это особенно верно, поскольку в современном военном мышлении утверждается концепция ведения огня прямой наводкой, когда оценка причиненных в бою повреждений происходит с помощью дистанционных средств, анализ — с помощью моделирования и последующее повторное целеуказание — посредством подачи информации в огневые комплексы на местах, которые затем снова ведут огонь при весьма ограниченном участии человека. Возможно, следовало бы рассмотреть с точки зрения международного гуманитарного права ответственность за неправильно нацеленный удар, осуществленный на основе приемов ИВ, или ответственность за контролирование комплекса огня прямой наводкой (что, очевидно, снизило бы эффективность этого комплекса в случае боя).

Второстепенное применение

В этой части рассматриваются вопросы, которые имеют более прямое отношение к боевым действиям с применением обычного оружия и касаются прежде всего вероломных действий и превращения больных и раненых солдат в объект нападения. В отличие от большинства случаев,

кратко описанных выше, нет убедительных доказательств того, что такая тактика уже применялась, но она рассматривалась на военных семинарах и в дискуссионных группах.

Вероломные действия могут включать в себя использование флага или формы противника, либо имитацию ранения или смерти с целью обмануть доверие противника и напасть на него. Именно это намерение — заманить противника обманом и убить его — отличает вероломство от военной хитрости. Понятие вероломства сравнительно легко определить в материальном мире. Однако, как мы уже видели, в наше время поле боя не всегда бывает непосредственно наблюдаемым. В современных армиях используются комбинации электронных датчиков — их носят на себе военнослужащие или они устанавливаются на боевой технике. Приборы обнаружения, реагирующие на движение, или инфракрасные лучи используются для того, чтобы определить перемещения противника, которые могут быть скрыты темнотой или препятствиями. Это электронное поле боя отображается на дисплее портативных полевых компьютеров, так что можно следить за всем, что происходит на поле боя. Такие условия весьма благоприятны для ИВ.

Одной из возможных мер противодействия может быть использование или ношение ответчиков неприятельских вооруженных сил для того, чтобы заставить противника поверить, что перед ним его собственные войска. Такие действия можно приравнять к ношению военной формы противника. Это возможно осуществить, проникнув в систему, изменив изображение и обойдя процесс проверки кодирования, либо просто физически завладев ответчиком.

Противник может также замаскировать инфракрасный сигнал, используя технологию, которая применяется на бомбардировщиках «Стеле». Это создаст впечатление, что он мертв или неподвижен и испускает очень слабое тепловое излучение. Дозор, используя инфракрасные боевые системы опознавания, отметит такой объект и низкий уровень выделяемого тепла. Не видя никакого движения и думая, что имеет дело с безжизненным объектом, патруль может приблизиться к нему без должной осторожности. Однако подобная маскировка сигналов предполагает применение технологий, находящихся пока на опытной стадии разработки. Примеров их применения пока что не зафиксировано.

Наконец, нападению могут быть подвергнуты медицинские базы данных противника с целью отсрочить лечение или вызвать смерть находящегося на излечении военнослужащего. В этом случае компьютерная

система противника будет взломана и отдельные поля данных, например группа крови, будут изменены. Такие действия повлекут за собой повышение смертности. Когда проблема будет обнаружена, возникнут неразбериха и дополнительные задержки при лечении. Считается, что подобное вмешательство пока возможно только теоретически. Но оно относится к той категории вероятных событий, которые необходимо исследовать, чтобы предотвратить, особенно если объектом таких действий может стать гражданское население.

Выше обсуждались наиболее очевидные способы применения ИВ, однако есть еще одна область, требующая изучения. Речь идет об использовании методов ИВ в психологической войне и разведывательной деятельности. Хотя психологическая война не представляет собой нового явления, некоторые из ее приемов могут породить новые проблемы. Цель психологической войны состоит в воздействии на взгляды военнослужащих противника и гражданских лиц, которые их поддерживают. Примером тому могут послужить операции «Tokyo Rose» и «Axis Sally», осуществленные во время Второй мировой войны. Еще один пример — сбрасывание листовок, призывающих солдат сдаться ввиду предстоящего вторжения или внушающих гражданскому населению невыгодное представление о войне в надежде, что оно перестанет ее поддерживать. На вопрос о том, противоречат ли современные методы ведения психологической войны уголовному или международному гуманитарному праву, нет однозначного ответа, однако здесь вполне могут быть основания для обсуждения нравственных проблем, поскольку Интернет все шире используется в целях осуществления психологической войны и разведки.

На другом уровне Интернет используют группировки в Восточном Тиморе и Мексике, с тем чтобы добиться международной поддержки и обличить случаи нарушения прав человека, имеющие место по их утверждению. Однако, если рассуждать подобным же образом, такие действия можно рассматривать как террористические акты, если они ведут к повреждению сайтов или посылке «почтовых бомб» — забрасыванию электронного адреса огромным количеством писем.

Нравственные вопросы возникают в тех случаях, когда в Интернете преднамеренно помещают дезинформацию для создания напряженности внутри страны. В прошлом году в Малайзии арестовали двух человек, которые предположительно распространяли в Интернете слухи о расовой вражде между малайцами и проживающими в стране китайцами.

Поскольку в соседней Индонезии уже происходили межнациональные столкновения, могли быть реальные основания опасаться их распространения на Малайзию. Во время азиатского финансового кризиса 1997 г. в Интернете распространялись слухи о разорении банков — несомненно, с целью подлить масла в огонь. Причастность какого-либо государства к этим событиям не была установлена, однако сам факт, что они имели место, заставляет задуматься об их возможном повторении.

Перспективы

В ноябре 1998 г. Россия обратилась в ООН с просьбой рассмотреть применение ИВ и выработать заключение относительно необходимости изменения международного гуманитарного права, чтобы оно могло регулировать ведение ИВ, или о мерах в поддержку принятия в какой-либо форме соглашения о контроле над вооружениями. В своей резолюции A/RES/53/70 от 4 января 1999 г. под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» Генеральная Ассамблея согласилась рассмотреть эти вопросы.

Одной из первых проблем, заслуживающих рассмотрения, может быть соотношение актов ИВ и запрета на применение силы, содержащегося в Уставе ООН. Вопрос состоит в следующем: является ли использование ИВ без применения силы в качестве стратегии принуждения применением силы по смыслу Устава? На тот же вопрос, поставленный в отношении экономического давления, ответ был дан отрицательный.

Найти ответы на вопросы, возникающие в связи с ИВ, не так просто, как может показаться. Как оценивать ситуации, в которых применение ИВ приводит к тем же конечным результатам, что и применение физической силы? Например, нарушение работы телекоммуникационных систем с помощью компьютерного вируса можно сравнить с бомбовым ударом по телефонному коммутатору. В обоих случаях ущерб впоследствии устраним, в обоих случаях отсутствует намерение вызвать людские потери. Если бы разрушение системы добычи и распределения нефтепродуктов в Косово было осуществлено с помощью компьютеров или если бы югославские системы управления и контроля были подавлены средствами ИВ, которые бы вывели из строя телефонную сеть, спутниковые установки, радиовещание и телевидение всей страны, считалось бы такое действие запрещенным применением силы? Далее, может быть, еще более

важно ответить на вопрос: как могла бы Югославия ответить на такие действия и на каких правовых основаниях? Последний вопрос обращен в большей степени к державам с ядерным потенциалом, поскольку некоторые страны уже классифицируют ИВ как возможное оружие массового поражения.

Обдумывая эти проблемы, можно начать с попытки осмыслить ИВ в категориях современных представлений о применении силы. Поскольку ИВ направлена в значительной мере против инфраструктуры, используемой как гражданским населением, так и военными, целесообразно было бы рассмотреть данный вопрос в рамках международного гуманитарного права.

Весьма важно было бы рассмотреть вопрос об использовании высокоточных бомб и о возможности их порчи. Применимы ли здесь положения Протокола I? Этот же вопрос необходимо поставить и в отношении выведения из строя базы данных по целеуказанию, а также в отношении оружия с использованием ЭМИ. По моему мнению, основанному на опыте военных действий, а не на правовых познаниях, проблема вероломного использования и порчи медицинских карт со временем решится сама собой, после того как на практике станет ясно, насколько пагубны такие действия для обеих сторон. Комбатанты могут прийти к молчаливому соглашению о том, чтобы воздерживаться от них ввиду возможных осложнений в ведении войны.

Эта ситуация заставляет вспомнить об относительной легкости, с которой был заключен Протокол 1995 г. об ослепляющем лазерном оружии. Всем участникам было ясно, что такое оружие не подходит для ведения войны, некоторые даже сомневались в возможности его практического применения. Данный Протокол — один из немногих на сегодняшний день примеров запрещения оружия до того, как оно было использовано.

Проблемы контроля над вооружениями, возникающие в рамках ИВ, разрешить непросто. Для эффективного ведения ИВ достаточно персонального компьютера, телефонной линии и хакерских программ, которые легко скачиваются из Интернета. Это не значит, что мир полон потенциальных «киберсолдат» — от обладания одной машиной, позволяющей осуществить отдельный взлом компьютерной системы, далеко до выработки способности наносить координированные удары с использованием современной системы управления и контроля, необходимой для ведения военной кампании.

Заключение

Надеюсь, мне удалось дать представление о потенциальных проблемах, связанных с применением ИВ, и указать ряд возможных решений. ИВ стоит на повестке дня ООН, которая проработает различные вопросы. Эта дискуссия во многом бы выиграла, если бы специалисты по международному гуманитарному праву также рассмотрели проблемы, поднятые в настоящей статье. Найти правильный путь возможно.