УДК 101.1:316

Кибервойна и проблема безопасности в информационном обществе

И. Н. Сидоренко, кандидат философских наук, доцент*

В статье показана важность осмысления такой проблемы современного общества, как тотальность информационного насилия, радикальной формой которого стала кибервойна, порождающая новый мировой порядок, базирующийся не на прямом насилии, а на страхе. Решающее значение в кибервойне имеет не физическая, а информационная сфера, поэтому киберпространство современного общества предстает как конфликтная территория. В такой ситуации современные государства переживают трансформацию своей среды безопасности.

Ключевые слова: война, кибервойна, информационное насилие, безопасность, риск, информационное общество, глобализация, сеть, постнациональная война.

Cyber-War and the Problem of Security in the Information Society

I. N. Sidorenko, PhD Philosophy, Associate Professor

The author shows the importance of understanding such problems of modern society as a totality of information violence, a radical form of which has become the cyber-war. This cyber-war is generating a new world order, which is based not on direct violence but on the fear. Instead of physical sphere, the information sphere is of great importance to cyber-war, therefore the cyberspace of modern society is presented as a conflict area. In such situation the modern state is experiencing a transformation of its security environment.

Key words: war, cyber-war, information violence, safety, risk, information society, globalization, network, post-national war.

Становление информационного общества и происходящие сегодня глобализационные процессы размывают традиционное разграничение «полномочий» государства и бизнеса в вопросах обеспечения национальной безопасности, с одной стороны, и частной — с другой, что приводит к формированию своеобразной «идеологии насилия», оправдывающей ослабление власти национальных государств и усиление глобальных институтов, договоров международной торговли. В такой ситуации государства переживают трансформацию своей среды безопасности. И если К. Клаузевиц определил войну как продолжение политики другими средствами, то естественно предположить, что в настоящее время информационная политика обусловливает, с одной стороны, возможность информационной войны или кибервойны, а с другой стороны, необходимость появления новой доктрины безопасности. Так, современное информационное общество способствует не только рационализации жизни, но и сталкивается с новыми проблемами: тотальностью насилия, порождающего новые технологии контроля и социальные практики, прежде всего в пространстве социальных коммуникаций.

Аккумуляция рисков в информационном обществе отождествляется главным образом с дефицитом информации, ее неполнотой или неэффективностью ее использования. Возникновение рисков, порожденных неполнотой информации, связано не только со спецификой принятия решения, но также и с распространением информационного насилия, под которым понимается бессознательное подчинение власти посредством информационных технологий и иерархии ценностей, приобретающих само собой разумеющийся характер, а также использование Интернета как площадки для политики скандалов и кибератак хакеров противника. Власть информационного насилия навязывает значения, заставляя признать их легитимными и одновременно скрывая силовые отношения, лежащие в ее основе. Невозможность обладать полнотой информации приводит к доминированию в современном обществе именно такой скрытой силы, под властью которой индивид на веру принимает любую информацию, если она подается под «соусом научности», будь то реклама, или информация, созданная

* Докторант кафедры философии культуры ФФСН БГУ.

пиар- и полит технологиями. Информационное насилие было всегда, однако в век информационных технологий оно приобретает глобальные масштабы по своему воздействию на сознание людей, а будучи воспроизведенным через систему социальных коммуникаций, масс медиа и т. п., увеличивает склонность индивидов к конформизму.

В информационном обществе Интернет не только превращается в главный инструмент деятельности, информирования и образования, но также становится одним из главных средств вербовки, манипулирования и доминирования. Отсюда киберпространство современного общества предстает как конфликтная территория. С одной стороны, Интернет способствует появлению нового глобального гражданского общества, строящегося посредством объединения в сеть общественных компьютерных сетей и гражданских объединений, с другой стороны, ожидания того, что Интернет превратится в идеальный инструмент будущей демократии, пока не оправдываются. В силу этого с распространением информационных технологий и с постепенным ослаблением национальных государств становится жизненно необходимо для государственной власти сохранить за собой легитимное право на тотальный контроль как средство информационного насилия под эгидой защиты национальной безопасности. Отсюда одним из основных способов осуществления власти становится производство и распространение информации, культурных кодов, а также создание новых технологий контроля и раскрытия анонимности, ограничения приватности. Как отмечает М. Кастельс: «В условиях новой глобальной среды наблюдения и контроля возникает более серьезная угроза свободе: структурирование повседневного поведения через доминирующие нормы социального поведения» [1, с. 211]. Так, информационное насилие, распространяемое посредством информационных технологий, превращает наше существование в «электронный паноптикум», т. е. в жизнь в условиях постоянного информационного контроля.

Вместе с тем оборотной стороной глобализационных процессов становится фрагментаризация социального пространства, которая наглядно проявляется в таких новых формах общественной коммуникации, как информационные сети. Новые сетевые структуры современного общества имеют качественно иной способ организации, в отличие от традиционных обществ. Развитие телекоммуникационных технологий привело к тому, что в XXI в. доминировать стали не локальные информационные обмены, а удаленные и опосредованные контакты, которые осуществляются в распределенной коммуникационной среде. Отсюда новой архитектурой социального пространства становится фрагментарное сетевое поле, а базовым основанием информационного общества является сетевое пространство, в котором информация порождает изменения самой системы.

Информационное насилие в сетевой коммуникации накладывает отпечаток как на наше мировоззрение, так и на изменение социальных практик, в частности на трансформацию ведения войн современного типа, таких как кибервойны, которые проводятся по принципу «роения». Так, кибервойна является радикальной формой информационного насилия, представляющей собой как компьютерное противостояние в пространстве Интернета, направленное на дестабилизацию компьютерных систем и доступа к Интернету государственных учреждений, финансовых центров и создание беспорядка и хаоса в жизни стран, так и манипулирование сознанием и поведением индивидов посредством информации. Такие новые формы противостояния в сетевом фрагментарном обществе, как кибервойна, ведутся путем осуществления главным образом бесконтактных действий посредством использования мощного информационно-технического и информационно-консциентального потенциала, сведенного в одном пространстве — сети. Таким образом, в единое коммуникационное пространство, функционирующее в реальном масштабе времени, сводятся разнородные компьютерно-информационные сети, что позволяет более точно предугадывать действия противника, опережать его на всех этапах подготовки и ведения боевых действий и концентрировать удар, достигая превосходства. Решающее значение в кибервойне имеет, следовательно, не физическая, а информационная сфера. Главным действующим лицом на поле боя в кибервойне может стать оператор компьютера, дистанционно управляющий «умными» машинами. При этом самым привлекательным оружием кибератак в ходе кибервойны выступает зашифрованная информация, передаваемая по открытым каналам связи (например, в социальных сетях Интернета). Так, кибервойна существенно меняет тактику вооруженного противоборства, способствуя превращению противников в скрытые друг от друга, децентрализованные высокоманевренные системы, действующие по принципу «стаи». В силу этого во главу военной мощи в современном фрагментарном обществе становится информация в различных ее формах и проявлениях.

Кибервойна предполагает активное использование принципиально нового вида оружия нелетального действия, чьи возможности наиболее полно иллюстрируются информационным оружием, т. е. средством искажения или хищения информационных массивов, преодоление систем защиты информации, а также само использование информации и связанных с ней технологий контроля и воздействия, как на военные, так и на гражданские системы противника. Информационное оружие можно разделить на два типа. К первому типу относится оружие, воздействующее на информационно-технические средства, ко второму — оружие, оказывающее воздействие на сознание и психику людей. Если информационное оружие первого типа призвано блокировать электронные средства противника и разрушать его компьютерное оборудование и телекоммуникации, то оружие второго типа направлено на подавление воли человека. Таким образом, информационное насилие становится одним из главных средств ведения войн в эпоху глобализации. Так, например, информационное насилие стало действующей силой и средством реализации «бархатных» революций; распространенным стало и такое понятие, как «информационный терроризм». В силу этого суть стратегии информационного противоборства, реализуемого в современных войнах, заключается в том, что цели войны во многом достигаются не за счет захвата и удержания чужих территорий, а за счет подрыва еще в мирное время оборонного и экономического потенциала государства-противника. Поэтому в глобализирующемся мире информационное насилие, приобретая беспрецедентные масштабы и интенсивность, предстает как источник международной напряженности и нестабильности. Как показывают военные конфликты последних лет, целью информационно-психологического воздействия становится изменение системы ценностей и сложившихся норм поведения людей, т. е. осуществление культурно-идеологической экспансии посредством привнесения извне инородных культурных ценностей. Информационное насилие трудно, практически невозможно отслеживать и контролировать, в силу чего многие современные военные конфликты, порожденные и осуществляемые посредством этого насилия, оказываются за пределами норм международного права, регулирующего ведение войн. В силу этого возникает проблема определения конкретного, обозримого и прогнозируемого источника угрозы национальной безопасности.

Кибервойна руководствуется специфически новой логикой массовой информации. Так, уже типичной стала ситуация, когда средства массовой информации регулярно предоставляют микрофоны противникам, в то время как цель любой политики военного времени до недавних пор сводилась к пресечению вражеской пропаганды. Как верно отметил У. Эко по поводу такой новой войны, как война в Персидском заливе: «...Информация не только подрывает веру населения в цель войны, но и вызывает сострадание к гибнувшему неприятелю. Смерть врагов из далекого неявного события превращается в непереносимо наглядное зрелище» [2, с. 23]. Более того, информация допускает врага в чужие тылы, в наш дом. Таким образом, информационный поток выполняет ту же функцию, которую при прежних традиционных войнах выполняли секретные службы, а именно: нейтрализует расчет на упреждение. Такая война, в которой противника невозможно упредить, не предполагает наличия четкой линии фронта и разграничения на своих и врагов.

Можно выделить два основных правила современной войны, к которой относится кибервойна: во-первых, недопустима гибель своего, во-вторых, жертвы в принципе нежелательны. Более того, «враги», сдавшиеся в плен, получают поощрение масс-медиа за то, что сумели найти способ сохранить себе жизнь. Так, кибервойна как современный тип войны преобразуется в шедевр масс-медийности, что, в принципе отвечает заявлению Ж. Бодрийяра о том, что войн вовсе не было наяву, они были только в телевизоре. Приведем слова сербского мыслителя С. Жижека об информационном прикрытии современной войны: «С одной стороны, новый образ войны как события, которое разворачивается исключительно в сфере технологий, на экранах радаров и компьютеров, [...] а с другой — крайняя физическая жестокость, которую было бы невыносимо видеть в средствах массовой информации [...] Когда Бодрийяр заявил, что войны в Заливе не было, это означало, что картину, которая отвечает ее реальному облику, запретили полностью» [3, с. 57].

Следуя логике масс-медиа, кибервойна должна быть короткой, т. е. соответствовать если не принципу максимальной развлекательности и счастливости, то хотя бы принципу минимальной несчастности. Однако, несмотря на то что современные войны в большинстве своем являются короткими, они оказываются бесполезными, так как современную войну в принципе никто не может выиграть. Более того, власть информации и тотальность символического информационного насилия порождает такой феномен как «всеобщая

война». В современную глобализационную эпоху война превратилась из аномалии в естественное, нормальное состояние, из конфликта между государствами в некое подобие «войны всех против всех», описанное Т. Гоббсом, из средства политики в саму политику. Современная всеобщая война происходит в период «межвременья», в ходе которого устанавливаются новые глобальные правила и наблюдается избыток новых властных структур. В силу этого взаимоотношения между политикой и войной в современном информационном обществе превратились в свою противоположность. Этот период «межвременья» характеризуется тем, что в современных условиях война с внешним противником ничем не отличается от борьбы с внутренним врагом. В силу этого возможности ограничения свобод расширяются, а современная война обретает черты, ранее присущие гражданской войне. Различить врага в этой всеобщей войне весьма сложно, он становится невидимым.

Приватизация информационного насилия сделала возможным нивелировку национальных границ. Поэтому кибервойну можно определить как «постнациональную войну», характеризующуюся размыванием базовых различий, которые были определяющими в войнах между государствами. Как справедливо отметил У. Бек, раскрывая сущность постнациональной войны, «на смену принципу „или-или“ приходит принцип „и одно, и другое“: одновременно имеют место и война, и мир; действует как полиция, так и военные; происходят как преступления, так и боевые действия; страдают как гражданские лица, так и солдаты» [4, с. 202]. В современном информационном обществе наблюдается переход в политике от «обороны» к «безопасности», что в итоге приводит к стиранию различий между внешней и внутренней сферами, между армией и полицией. Так, под лозунгом «безопасности» оправдывается постоянная военная активность, как на собственной территории, так и на территории других государств. Постнациональная война проявляется через два феномена: защита прав человека на зарубежной территории и попытка свести к минимуму глобальный риск терроризма за счет военных средств государств. Таким образом, постнациональная война не ведется в национальных интересах, напротив, она снимает ограничение ответственности государств национальной территорией, превращаясь в своеобразные «мировые полицейские войны». Так, постнациональная война стала продолжением постнациональной политики военизированного гуманизма. В силу этого постнациональная война служит средством камуфлирования незаконной войны, оправданием агрессии. Более того, в современных условиях власть, стремящаяся к безопасности, во главу угла ставит не легитимность и лояльность граждан к ней, а порядок, установленный силой. Однако достигнутая так называемая «стабильность» должна быть опять нарушена, иначе возникает вопрос о необходимости самой силы, обеспечивающей этот порядок. В силу этого состояние многих современных обществ можно сравнить с функционированием ядерного реактора, т. е. система действует до тех пор, пока воспроизводится угроза.

Современные войны в общем и кибервойна в частности предполагают переосмысление понятия «мир»: мир перестает восприниматься как тотальное и исконно данное состояние. Речь теперь может идти лишь об островках мира как исключениях из общего правила войны, как результате завоевания. При этом нестабильность является прерогативой уже не только периферии, но и центра. Вот как об этом пишет У. Эко: «Центры становятся территорией ежедневного беспокойства, ареной постоянных террористических атак. Эта нестабильность будет сдерживаться перманентным кровопусканием на периферии и большим количеством Пра-пра-войн, среди которых Афганистан — только первый пример из многих» [2, с. 51—52].

Так, порождаемое кибервойной как информационное, так и физическое насилие будет считаться оправданным до тех пор, пока приводит к воспроизводству существующего порядка, но как только принуждение перестанет обеспечивать порядок, основа его легитимности исчезнет. Таким образом, кибервойна как один из видов современной всеобщей войны порождает новый мировой порядок, базирующийся не на прямом насилии, как это делалось в эпоху традиционных и индустриальных обществ, а посредством страха, вызываемого угрозой насилия и порождаемого информационным террором.

Список цитированных источников

1. *Кастельс, М.* Галактика Интернет. Размышления об Интернете, бизнесе и обществе / М. Кастельс. — Екатеринбург, 2004.

2. *Эко, У.* Полный назад! «Горячие войны» и популизм в СМИ / У. Эко. — М., 2007.

3. *Жижек, С.* Хрупкий Абсолют, или почему стоит бороться за христианское наследие / С. Жижек. — М., 2003.

4. *Бек, У.* Космополитическое мировоззрение / У. Бек. — М., 2008.

Дата поступления в редакцию: 21.05.2014 г.