УДК 14:355.1+351.73

Романюк С. Н.

ИНФОРМАЦИОННОЕ ОБЩЕСТВО И ЕГО ВОЙНЫ

У статті розглянуто філософські аспекти концепції інформаційних війн, яка є найвідомішою моделлю техніко-технологічного детермінізму збройної боротьби та методологічно базується на концепції інформаційного суспільства. Виявлено, що поле дії інформаційних війн охоплює всі сфери життєдіяльності суспільства; виділено ключові особливості стратегічного інформаційного протиборства. Подано рекомендації щодо процесу військового реформування, який повинен будуватися на основі врахування сучасних тенденцій розвитку інформаційного суспільства.

Ключові слова: *інформаційне суспільство, інформаційна війна, простір інформаційного протиборства, техніко-технологічний детермінізм.*

The article presents consideration of philosophical aspects of the conception of information wars, which is one of the best-known war insights of technical and technological determinism and which methodological basis is the conception of information society. It is concluded that the information battlefield embraces all vital activity spheres of society determining the key features of strategic information confrontation. It is suggested that under reforming the Military Forces in Ukraine the latest tendencies discussed should be taken into consideration.

Keywords: *information society, information warfare, technical and technological determinism, battlefield.*

Постановка проблемы**.** Стремительное развитие информационных технологий, расширение производства технических средств и сфер использования компьютерной техники, а самое главное – наличие человеческого фактора в виде удовлетворения властолюбивых собственнических амбиций таят в себе неимоверный потенциал как для созидания, так и для разрушения. Перед человечеством встала угроза качественно новых войн третьего тысячелетия – информационных войн.

Анализ основных исследований и публикаций**.** Западная социально-философская парадигма войны и мира наиболее проявляется в различных милитаристских концепциях XX века. Одна из таких концепций – технологический детерминизм. Методологически она базируется на концепции информационного общества, которое достаточно хорошо разработано Д. Беллом, З. Бжезинским, Э. Тоффлером и др. [1–5]; саму концепцию информационных войн обосновали Д. Адаме, Р. Акерман, Д. Александер, К. Блаунт, О. Дженсен, Э. Короалес, Р. Моландер, Р. Дженсен, А. Д. Кэмпен, Р. Моландер, Г. Саммерз и др. Однако комплексного исследования западной социально-философской парадигмы войны и мира, в которых был бы сделан акцент на информационной сфере как мощном оружии в руках тех, кто хочет нарушить мир, проведено не было, не осуществлялся и анализ ее трансформации в условиях перехода от противостояния двух социально-политических систем к однополярному миру.

Постановка задания**.** Основная цель данного исследования – продолжить

комплексный анализ современной западной парадигмы войны и мира посредством анализа концепции информационных войн и ее роли в трансформации парадигмы в условиях перехода от двуполярного к однополярному мироустройству. Более того, согласно технико-технологическому детерминизму изменение технико-технологического порядка является причиной изменения структуры вооруженных сил, организации их боевой подготовки, военной тактики и стратегии, что в свою очередь делает необходимым формирование методологической платформы для усовершенствования Вооруженных сил Украины.

Не нужно быть пророком, для того чтобы предсказать, что рост уровня зависимости жизнедеятельности любой национальной инфраструктуры от информационных технологий, чему неоднозначно способствует глобализация, – процесс необратимый, который привел к революции в военной сфере. В Китае была опубликована книга, где два военных офицера излагают алгоритм разрушения военной мощи США посредством применения компьютерных технологий. Последствия такого кибернападения можно сравнить с разрушительной силой средств массового поражения. Террористические организации (Хизболла, ХАМАС, Абу Нидал и др.) используют продвинутые информационные технологии и Интернет для пропаганды, передачи секретной информации, незаконного пополнения денежных ресурсов и совершения террористических операций. Не для кого не секрет, что 11 сентября 2001 года террористы использовали для связи электронную почту и средства компьютерной стенографии.

Концепции информационных войн методологически базируется на концепции информационного общества. По мнению известного американского футуролога Э. Тоффлера, развитие науки и техники осуществляется рывками, «волнами» [3–5]. «Первая волна – сельскохозяйственная цивилизация» – прокатилась 10 000 лет назад, сломала первобытнообщинные формы самоорганизации, привела к разделению труда и созданию иерархических структур. «Вторая волна – промышленная цивилизация» – началась 300 лет назад, создала самую могучую, сплоченную и экспансионистскую социальную систему, равной которой мир еще не знал. «Третья волна – технологической цивилизации», начавшаяся в середине 1950-х годов, связана с так называемым «информационным взрывом», то есть лавинообразным ростом информации, в результате которого человек оказался не в состоянии справиться с ее объемом без помощи новых информационных технологий. Каждая из волн имела свою экономику, свои социальные и политические институты, культуру, свои средства коммуникации, а также свой способ и характер ведения войны. Подробно эти вопросы были рассмотрены супругами Элвином и Хейди Тоффлер в книге «Война и анти-война» [6]. Войны «первой волны» велись за землю, войны «второй волны» – за способность физической продуктивности; возникающие войны третьей волны будут вестись за доступ к знаниям и контроль над ними. Поскольку формы боевых действий любого общества следуют за формами создания благосостояния этого общества, то войны будущего будут в основном, но не только, информационными войнами.

В конце XX века концепцию информационных войн стали разрабатывать такие

западные специалисты, как Д. Адаме, Р. Акерман, К. Блаунт и др. [7–9]. Большое внимание разработке концепции информационных войн уделяла корпорация RAND. Основные результаты исследований RAND были изложены в отчетах MR-661-OSD «Strategic Information Warfare. A new Face of War» (1996), MR-963-OSD «The Day After… in the American Strategic Infrastructure» (1998), MR-964-OSD «Strategic Information Warfare Rising» (1998).

Под *информационными войнами,* по взглядам американских аналитиков (Р. Дженсен, А. Д. Кэмпен, Р. Моландер и др. [10, P. 2; 11, P. 32; 12, P. 3–4]), следует понимать целостную всеобъемлющую стратегию, обусловленную все возрастающей значимостью и ценностью информации в вопросах командования, управления и политики. Поле действия информационных войн в этом случае охватывает следующие области: 1) инфраструктуру систем жизнеобеспечения государства – телекоммуникации, транспортные сети, электростанции, банковские системы и т. д.; 2) промышленный шпионаж – хищение патентованной информации, искажение или уничтожение особо важных данных, услуг, сбор информации разведывательного характера о конкурентах и т. п.; 3) взлом и использование личных паролей VIP-персон, идентификационных номеров, банковских счетов, данных конфиденциального плана, производство дезинформации;4) электронное вмешательство в процессы командования и управления военными объектами и системами, «штабную войну», вывод из строя сетей военных коммуникаций; 5) всемирную компьютерную сеть Интернет, в которой, по некоторым оценкам, действуют 150 000 военных компьютеров и 95 % военных линий связи проходят по открытым телефонным линиям [13, P. 37–39]. Выделены ключевые особенности стратегического информационного противоборства: низкая стоимость реализации средств информационного противоборства; крушение статуса традиционных государственных границ при подготовке и проведении информационных операций; усиление роли управления восприятием ситуации путем манипулирования информацией по ее описанию; изменение приоритетов в деятельности стратегической разведки, которые смещаются в область завоевания и удержания информационного превосходства; усложнение проблем обнаружения начала информационной операции; сложность создания коалиции против агрессора, развязавшего информационную войну и др. [14, P. 25–41]. В программах Университета национальной обороны США выделены следующие формы информационной войны: радиоэлектронная борьба; психологическая война; война с использованием средств разведки; война с хакерами; кибернетическая война [15, P. 8–9].

Цели информационной войны совершенно иные, нежели войны в общепринятом понятии: не физическое уничтожение противника и ликвидация его вооруженных сил, не уничтожение важных стратегических и экономических объектов, а широкомасштабное нарушение работы финансовых, транспортных, коммуникационных сетей и систем, частичное разрушение экономической инфраструктуры и подчинение населения атакуемой страны воле страны-победителя. Более того, в эпоху информационных войн планы боевых операций разрабатываются военными вместе с гражданскими специалистами, причем нередко последние играют

ведущую роль в этом. Впервые вооруженные силы оказались вынуждены вначале овладевать новыми информационными технологиями, а уже потом изыскивать пути их использования.

В настоящее время многими государствами осуществляется обширный комплекс мероприятий по подготовке к информационной войне. Так, в США эта подготовка ведется по трем направлениям: в вооруженных силах, в спецслужбах и в национальном масштабе. В вооруженных силах подготовка включает теоретические, организационные и материально-технические мероприятия. В армии введены должности офицеров, занимающихся проблемами информационной войны (Info war Officers). Ежегодно проводятся десятки штабных игр по ведению информационной войны [16]. Вооруженные силы США оснащаются различными видами информационного оружия. В спецслужбах также развернута всесторонняя подготовка к ведению информационных войн: разрабатываются способы внедрения легко инициируемых в нужное время логических бомб и вирусов в информационные системы военно-промышленного комплекса противника; разрабатываются способы воздействия на программистов, работающих на оборонных предприятиях, с целью привлечения их для внедрения вирусов и логических бомб в обслуживаемые ими информационные системы и т. п. [16]. В национальном масштабе подготовка к информационной войне заключается в совершенствовании национальной информационной инфраструктуры, включающей все электронные СМИ, банковские системы, системы связи, транспорта, энергетики, промышленности и сферы услуг. Кроме того, эта инфраструктура фактически дополняется непрерывно разрастающейся сетью Интернет, клиентура которой исчисляется сотнями миллионов пользователей, разбросанных по всему миру [17, P. 62–65].

Таким образом, можно сделать вывод, что в западной социально-философской мысли 90-х годов XX столетия сформировалась четкая тенденция нового видения войны в условиях глобализации и информационного прогресса, которые привели к очередному витку развития военного дела. Технико-технологический прогресс является детерминантом этой концепции. Поэтому, чтобы отвести какую бы то ни было угрозу войны, будет ли она вестись обычными средствами или через Интернет, Вооруженные силы Украины должны отвечать тем требованиям, которые предъявляет современный уровень развития технологий. Для этого, прежде всего, необходимо создание целостной системы научных исследований, обучения, подготовки и переподготовки военных специалистов.

Литература:

1. *Белл, Д.* Грядущее постиндустриальное общество. Опыт социального прогнозирования [Текст] / Д. Белл ; пер. с англ. – М., 1999.
2. *Бжезинский, З.* Великая шахматная доска. Господство Америки и его геостратегические императивы [Текст] / З. Бжезинский. – М., 2000.
3. *Тоффлер, Э.* Шок будущего [Текст] / Э. Тоффлер ; пер. с англ. – М., 2002.
4. *Тоффлер, Э.* Третья волна [Текст] / Э. Тоффлер ; пер. с англ. – М., 2002.
5. *Тоффлер, Э.* Метаморфозы власти [Текст] / Э. Тоффлер ; пер. с англ. – М., 2002.

6. *Toffler, Alvin.* War and Anti-War: Survival at the Dawn of the 21st Century [Text] / Alvin Toffler and Heidi Toffler. – N.Y., 1993.
7. *Adams, J.* The Next World War: Computers are the Weapons and the Front Line is Everywhere [Text] / J. Adams. – N.Y., 1998.
8. *Acherman, R. K.* Military Planners Gird for Information Revolution [Text] / R. K. Acherman // Signal. – 1995. – May.
9. *Blount, K. A.* A Two-component Strategy for Winning the Information War [Text] / K. A. Blount // ARMY. – 1995. – January.
10. *Jensen, R. M.* Information War Power: Lessons from Air Power [Text] / R. M. Jensen. – Cambridge, 1997.
11. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War [Text] / Alan D. Campen, contributing editor. – Fairfax, 1992.
12. Strategic Information Warfare Rising [Text] / Roger C Molander [et al.]. – Santa Monica, 1998.
13. *Houghtaling, P. A.* New Information Warfare System Advances Army into Next Century [Text] / P. A. Houghtaling // Signal. – 1996. – March.
14. *Hill, M. R.* It is Time to Get on with Information Warfare [Text] / M. R. Hill // Defense Intelligence Journal. – 1996. – Spring.
15. *Burnette, G.* Information: Battlefield of the Future [Text] / G. Burnette // Surface Warfare. – 1995. – July-August.
16. *Molander, R. C.* Strategic Information Warfare: A New Face of War [Text] / R. C. Molander, A. S. Riddile, P. A. Wilson. – Washington, 1996.
17. *Libicki, M. C.* Silicon and Security in the Twenty-First Century [Text] / M. C. Libicki // Strategic Review. – 1992. – Summer.