

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт экономики и управления	Кафедра «Экономическая теория и международные отношения»
Направление подготовки	41.03.05 «Международные отношения»
Профиль	Мировая политика и международный бизнес

БАКАЛАВРСКАЯ РАБОТА

на тему

Влияние цифровых технологий на международные конфликты

Студент	_____	Макаров Михаил Сергеевич
	подпись, дата	
Руководитель	_____	Скворцов А. О.
	подпись, дата	
Нормоконтролер	_____	Влазнева С. А.
	подпись, дата	

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой	_____	Рожкова Л. В.
	подпись, дата	

Работа защищена с отметкой _____ (протокол ГЭК от _____ № _____)

Секретарь ГЭК	_____	Рассказова Н. В.
	подпись, дата	

Пенза 2022

ФГБОУ ВО «Пензенский государственный университет»
Институт экономики и управления
Кафедра «Экономическая теория и международные отношения»
Направление подготовки 41.03.05 «Международные отношения», профиль
Мировая политика и международный бизнес

«УТВЕРЖДАЮ»:
Зав. кафедрой
д.с.н., доцент Рожкова Л.В.

«_____» _____ 20__ г.

ЗАДАНИЕ
НА БАКАЛАВРСКУЮ РАБОТУ

студенту Макарову М. С., группа 18ЭА2, обучение очное

1 Тема бакалаврской работы: Влияние цифровых технологий на международные конфликты

утверждена приказом по университету

от «___» _____ 20__ г. № _____

2 Срок сдачи студентом законченной бакалаврской работы: 14.06.2022

3 Исходные данные к бакалаврской работе: научная и справочная литература, данные сети Интернет.

4 Перечень подлежащих разработке вопросов: влияние цифровой революции на мир; международные конфликты в условиях цифровизации.

5 Перечень графического материала: таблицы, рисунки.

6 Дата выдачи задания: 30.12.2021

График подготовки бакалаврской работы

№ п/п	Содержание работы	Срок выполнения	Дата выполнения, подпись руководителя
1	Составление плана ВКР	30.12.2021 – 10.01.2022	
2	Изучение исходных данных к бакалаврской работе	11.01.2022 – 23.01.2022	
3	Написание Главы 1	24.01.2022 – 20.03.2022	
4	Написание Главы 2	21.03.2022 – 1.05.2022	
5	Написание введения и заключения	2.05.2022 – 15.05.2022	
6	Оформление ВКР	16.05.2022 – 29.05.2022	
7	Сдача ВКР нормоконтролю, проверка в системе «антиплагиат.вуз»	30.05.2022 – 12.06.2022	
8	Ознакомление с отзывом руководителя	13.06.2022	
9	Представление законченной бакалаврской работы, передача в ГЭК	14.06.2022	

Руководитель _____ / А. О. Скворцов /
(подпись) (инициалы, фамилия)

Задание принял к исполнению студент _____ / М. С. Макаров /
(подпись) (инициалы, фамилия)

Реферат

Бакалаврская работа 53 с., 2 ч., 16 рис., 10 табл., 42 источника.

ЦИФРОВИЗАЦИЯ, МЕЖДУНАРОДНЫЕ КОНФЛИКТЫ, МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ, ЦИФРОВЫЕ ТЕХНОЛОГИИ, ЦИФРОВОЕ РАЗВИТИЕ, ЦИФРОВЫЕ КОНФЛИКТЫ, ЦИФРОВАЯ РЕВОЛЮЦИЯ, КОНВЕНЦИОНАЛЬНЫЕ КОНФЛИКТЫ, НЕКОНВЕНЦИОНАЛЬНЫЕ КОНФЛИКТЫ

Объект исследования – цифровые технологии.

Цель работы состоит в анализе влияния цифровых технологий на международные конфликты.

Методологическую основу работы составили структурно-функциональный, правовой подходы, историко-описательный, сравнительно-политологический методы.

Результаты работы: рассмотрена история возникновения цифровых технологий; охарактеризована цифровизация международных отношений; проанализирована цифровизация международных конфликтов; исследована гибридная война в эпоху цифровизации; проведен анализ крупнейших войн с использованием цифровых технологий; установлена оценка и последствия международных конфликтов в цифровую эпоху.

Рекомендации по внедрению. Анализ факторов, влияющих на цифровизацию конфликтов, может быть использован органами государственной власти и научным сообществом для более грамотного использования цифровых технологий и расширения теоретической базы проводимых исследований.

Теоретическая и практическая значимость работы состоит в комплексном анализе теоретических основ влияния цифровой революции на мир и выявление тенденций международных конфликтов в условиях цифровизации.

Прогнозные предположения о развитии объекта исследования. Использование и применение цифровых технологий в качестве макиавеллизма и мягкой силы будут иметь важное значение для выживания государства.

Aufsatz

Bachelorarbeit 53 Seiten, 2 Stunden, 16 Zeichnungen, 10 Tabellen, 42 Quellen.

DIGITALISIERUNG, INTERNATIONALE KONFLIKTE, INTERNATIONALE BEZIEHUNGEN, DIGITALE TECHNOLOGIEN, DIGITALE ENTWICKLUNG, DIGITALE KONFLIKTE, DIGITALE REVOLUTION

Gegenstand der Forschung sind digitale Technologien.

Ziel der Arbeit ist es, die Auswirkungen digitaler Technologien auf internationale Konflikte zu analysieren.

Die methodische Grundlage der Arbeit bildeten strukturell-funktionale, rechtliche Ansätze, historisch-beschreibende, vergleichend-politische Methoden.

Ergebnisse der Arbeit: Die Entstehungsgeschichte digitaler Technologien wird betrachtet; die Digitalisierung der internationalen Beziehungen wird geprägt; analysierte die Digitalisierung internationaler Konflikte; erforschte hybride Kriegsführung im Zeitalter der Digitalisierung; die Analyse der größten Kriege mit Hilfe digitaler Technologien wurde durchgeführt; die Einschätzung und Folgen internationaler Konflikte im digitalen Zeitalter werden ermittelt.

Empfehlungen zur Umsetzung. Eine Analyse der Einflussfaktoren auf die Digitalisierung von Konflikten kann von Behörden und Wissenschaft genutzt werden, um digitale Technologien besser zu nutzen und die theoretische Basis laufender Forschung zu erweitern.

Die theoretische und praktische Bedeutung der Arbeit liegt in einer umfassenden Analyse der theoretischen Grundlagen der Auswirkungen der digitalen Revolution auf die Welt und der Identifizierung von Trends in internationalen Konflikten im Kontext der Digitalisierung.

Prognoseannahmen über die Entwicklung des Untersuchungsgegenstandes. Der Einsatz und die Anwendung digitaler Technologien wie Machiavellismus und Soft Power werden für den Staat überlebenswichtig sein.

Отзыв

Оглавление

Введение.....	3
Глава 1 Влияние цифровой революции на мир.....	5
1.1 История возникновения цифровых технологий.....	5
1.2 Цифровизация международных отношений.....	8
1.3 Цифровизация международных конфликтов.....	13
Глава 2 Международные конфликты в условиях цифровизации.....	20
2.1 Гибридная война в эпоху цифровизации.....	20
2.2 Анализ крупнейших войн с использованием цифровых технологий...	29
2.3 Оценка и последствия международных конфликтов в цифровую эпоху.....	38
Заключение.....	48
Список использованных источников.....	50

Введение

Конец XX в. ознаменовался вступлением человечества в новую эпоху своего развития, которую по праву можно назвать цифровой. Цифровизация стала проникать во все сферы жизнедеятельности людей, превратившись в главный ресурс научно-технического и социально-экономического развития мирового сообщества. Наряду с привычным физическим пространством или средой обитания человечества уже сформировалось и развивается новое – виртуальное – цифровое пространство.

Цифровизация, которая вслед за собой принесла сеть Интернет – все более явно и осязаемо становится новой электронной средой обитания человеческой цивилизации. Человечество все более и более становится зависимым от виртуального информационного пространства, и эта тенденция принимает универсальный и необратимый характер.

Цифровое пространство дает огромные возможности развитию науки и бизнеса, дипломатии и войн, культуры и образования, экономики и социальной сферы государства, равно как и творческим способностям индивидуума. Понятия географических границ, физического пространства от части теряют свое былое значение. Стираются языковые и культурные барьеры, рушится традиционная иерархическая структура обществ, взамен которой создается новая структура. Все это коренным образом ломает привычные представления человека о себе, своем месте в этом мире и о самом мире. Однако единое цифровое пространство несет с собой не только огромные возможности и преимущества, но и создает потенциальные угрозы.

Анализ научной литературы по теме исследования позволяет констатировать, что факторы влияния цифровой революции на мир широко освещены как отечественными, так и зарубежными учеными. Так, влияние цифровой революции на мир представлено в монографических трудах таких авторов как: М. Шпитцер, К. Скиннер, А. Мелуа, О. Слоботчиков, Н. Дэвис, К. Швабьи, М. Васильева, Ю. Жеглова, В. Мехонцев и др. Международные конфликты в условиях цифровизации явились предметом изучения таких авторов как; А. Сафонов,

М. Сафонова, В. Овчинский, Е. Ларина, А. Бедрицкий, И. Панарин, А. Белоус, В. Солодуха, С. Туронок, Г. Почепцов и др.

Цель работы состоит в анализе влияния цифровых технологий на международные конфликты.

Для достижения поставленных целей предполагается решение следующих задач:

- рассмотреть историю возникновения цифровых технологий;
- охарактеризовать цифровизацию международных отношений;
- проанализировать цифровизацию международных конфликтов;
- исследовать гибридную войну в эпоху цифровизации;
- провести анализ крупнейших войн с использованием цифровых технологий;
- установить оценку и последствия международных конфликтов в цифровую эпоху.

Объект исследования – цифровые технологии. Предмет исследования – влияние цифровых технологий на международные конфликты.

Теоретическая и практическая значимость работы состоит в комплексном анализе теоретических основ влияния цифровой революции на мир и выявление тенденций международных конфликтов в условиях цифровизации.

Глава 1 Влияние цифровой революции на мир

1.1 История возникновения цифровых технологий

Цифровые технологии «*Digital technology*» основаны на представлении сигналов дискретными полосами аналоговых уровней, а не в виде непрерывного спектра. Все уровни в пределах полосы представляют собой одинаковое состояние сигнала.

Термин цифровые технологии связан с так называемой цифровой революцией или же третьей промышленной революцией, которая ознаменовала переход от механических и аналоговых электронных технологий к цифровой электронике. Сам процесс цифровизации начался во второй половине XX в. с принятием и распространением цифровых компьютеров и цифрового учета, который продолжается и по сей день [33].

Всю историю цифровых технологий можно разделить на несколько этапов, которые связаны между собой неразрывно, но протекающих отчасти независимо друг от друга.

Первый этап заключался в наборе и систематизации научной и практической базы для цифровизации. Началом всех цифровых технологий послужила двоичная система исчисления, которую немецкий философ-математик Готфрид Вильгельм Лейбниц систематизировал из знаний, полученных другими исследователями ранее, и опубликовал в 1705 г. Её математический смысл описан в его трудах и заключается в сведении логики к бинарной системе счисления. В ней единицы и нули формально представляют истинное и ложное значения или включённое и выключенное состояние некоторого элемента, который мог находиться в двух состояниях. Данная система исчисления помогла объединить логику и арифметику, тем самым заложив основу всей цифровизации в дальнейшем.

Так как промежуток накопления научной базы для цифровизации длился несколько веков, стоит выделить наиболее значимые события данного явления (таблица 1).

Таблица 1 – Научная база для цифровизации [33]

Год	Исследователь	Открытие или изобретение
Начало XVII в.	Джон Непер	Логарифмы
1640 г.	Блез Паскаль	Механическое устройство сложения
1698 г.	Вильгельм Лейбниц	Ступенчатый калькулятор
1705 г.	Вильгельм Лейбниц	Двоичная система исчисления
1837 г.	Чарльз Бэббидж	Аналитическая машина
1854 г.	Джордж Буль	Законы Мышления (булева алгебра)
1933 г.	Клод Шеннон	Развитие булевой алгебры
1937 г.	Клод Элвуд Шеннон	Символический анализ релейных соединений и соединение с коммутацией каналов
1936 г.	Алан Тьюринг	Формализация алгоритмов
1946 г.	Нейман	«Архитектура фон Неймана»
1947 г.	Клод Элвуд Шеннон	Математическая теория коммуникации
1948 г.	Норберт Винер	«Кибернетика»

Второй этап цифровизации был связан с развитием аппаратного обеспечения. Зачатками развития аппаратного обеспечения для цифровизации послужило создание первых электромеханических цифровых компьютеров. Разработка велась независимо сразу в нескольких государствах таких как Германия, Великобритания и США.

В 1936 г. немецкий инженер Конрад Цузе начал работу над компьютером серии Z. Первому и второму поколению Z-компьютеров так и не удалось выйти в свет из-за начавшейся Второй мировой войны и уничтожения последующих наработок Z2 в результате бомбардировок «Союзников». В 1941 г. была завершена работа над первым в мире программируемым компьютером Z3. Дальнейшая работа над Z4 которая велась в промежутках между 1942–1946 гг. была замедлена в результате отступления и поражения Германского Рейха, в свет Z4 вышел только в 1950 г. в Швейцарии. Так же для данного компьютера был создан первый в мире высокоуровневый язык программирования Планкалкюль [9].

Говоря про британские и американские наработки в этой сфере, можно выделить Эдасак, у которого была записана программа в памяти компьютера «*Whirlwind I*» с работой в реальном времени.

Развитие второго поколения аппаратного обеспечения стало возможным благодаря изобретению транзистора в 1947 г. [33]. В отличие от компьютеров первого поколения, данное аппаратное обеспечение обладало относительным быстродействием, в нем стала широко использоваться магнитная лента, а позже появились и дискеты. Компьютеры второго поколения по-прежнему использовались только университетами, правительствами, крупными корпорациями.

Третье поколение аппаратного обеспечения получило возможность к развитию благодаря изобретению интегральной схемы в 1952 г. [33]. В целом, как и на предыдущих поколениях компьютеров, на них производились расчеты, но более специализированные под различные задачи. Было реализовано мультипрограммирование.

Развитием четвертого поколения аппаратного обеспечения послужило создание центрального процессора, то есть использование вместо множества интегральных схем одной, где все операции будут записаны в машинном коде [33]. По сей день используются, развиваются и используются компьютеры 4 поколения в военных и мирных целях.

Третий этап цифровизации заключался в развитии программного обеспечения (ПО). Первое программное обеспечение было написано на языке ассемблер, которое носило название «*UNIX*», на основе которого строилось другое ПО. В дальнейшем над развитием ПО работала компания «*Microsoft*». *PC-DOS* и *MS-DOS*, вышедшие в 1981–1982 гг., стали основоположниками современного «*Windows*», которые являлись инновационными. Во-первых, благодаря графическому интерфейсу. Во-вторых, благодаря возможности запускать одновременно несколько программ, а также переключаться между ними.

Основой четвертого этапа цифровизации послужило развитие сетей. После создания аппаратного обеспечения и ПО появилась необходимость в разработке сетей для передачи данных. Министерство обороны США в 1957 г. в условиях Холодной войны посчитало, что армии необходима надежная система для передачи данных. Так, первой попыткой связать ЭВМ на больших расстояниях занялся Пол Бэран, проект назывался «*ARPANET*». В связи с тем, что на больших расстояниях

невозможно передать аналоговый сигнал без искажений, была предложена альтернатива, заключающаяся в передаче цифровых данных пакетами.

В 1969 г. была создана экспериментальная сеть, соединившая 4 узла, которая постепенно охватила все США. В дальнейшем была разработана первая программа для отправки электронной почты по сети [33].

В 1983 г. закрепляется термин «Интернет». В 1990 г. Тим Бернерс-Ли опубликовал предложения по системе гипертекстовых диаграмм, дав ей название «*World Wide Web*», которая дословно звучит как «Всемирная паутина». Объединение цифровой паутины на первоначальном этапе выглядело привлекательным из-за отсутствия единого руководства, а также благодаря открытости технических стандартов Интернета, что делало сети на тот момент независимыми от бизнеса и конкретных компаний [26].

В целом, можно подвести итог, сказав, что цифровизация мира была длительным процессом. Всю историю цифровизации можно разделить на четыре этапа. Первый этап был связан с накоплением научной базы, второй с развитием аппаратного обеспечения, третий – развитие ПО для аппаратного обеспечения, четвертый – связи аппаратного обеспечения между собой.

В целом, можно подвести итог, что цифровизация дала огромный толчок в развитии коммуникации, изучении различных дисциплин, упрощении жизни, но постепенно стала зависеть от крупного бизнеса, корпораций и государственного вмешательства.

1.2 Цифровизация международных отношений

Цифровые технологии быстро вошли в жизнь человечества, став её неотъемлемой частью. Одним из важнейших направлений современного глобального развития является «ускорение» и «сжатие» времени. Цифровые технологии оказали огромное влияние на государственную систему, экономику и политику. «Цифровое государство», «цифровая экономика», «цифровая

дипломатия», «цифровая цивилизация» – эти понятия не так давно вошли в научную и публицистическую лексику [30].

От цифровых технологий не остались в стороне и международные отношения как в инструментальном, техническом плане, так и в появлении новых методов дипломатии в мировой политике. «COVID-19» ускорил цифровизацию в глобальном масштабе в большей степени не как объективный процесс, а как способ решения многих задач которые невозможно было решить, находясь на карантине [5].

Говоря про саму цифровизацию международных отношений стоит отметить что, «*World Wide Web*» – информационная компьютерная сеть Интернет – все более явно и осязаемо становится новой электронной средой обитания человеческой цивилизации. Человечество на современном этапе развития становится более зависимым от виртуального цифрового пространства, данная тенденция принимает повсеместный и необратимый характер [34].

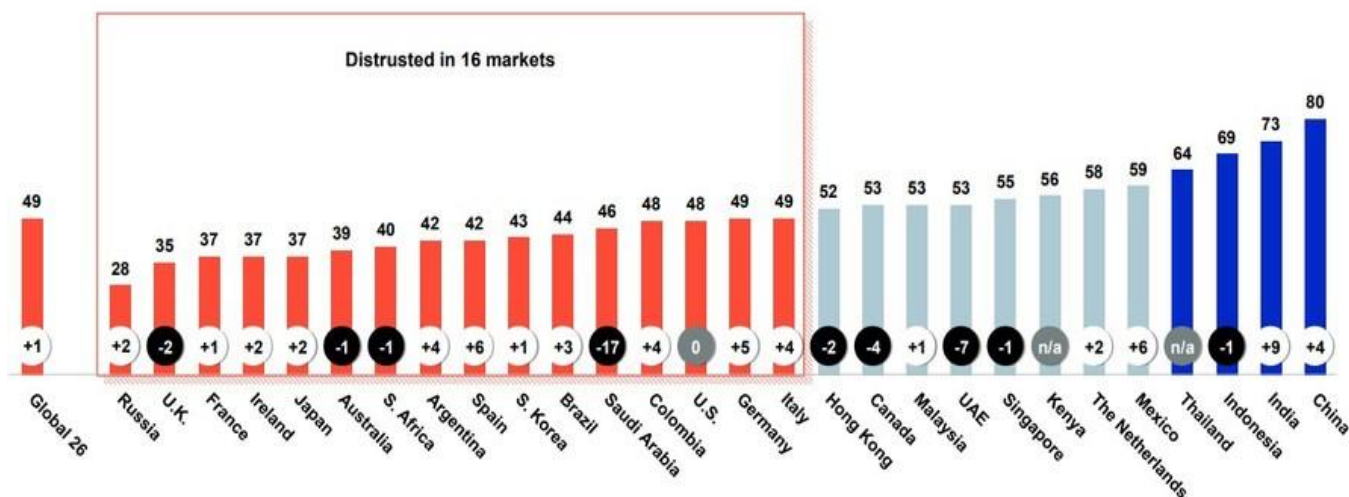
Глобальные сети как один из элементов цифровизации и виртуализации планетарного масштаба превращаются постепенно из инструмента внутренней и внешней политики в акторов международных отношений. От эффективной работы органов государственной пропаганды в цифровых медиа во многом зависит имидж государства как внутри страны в глазах граждан государства, так и у иностранцев. Так же эффективная работа органов государственной пропаганды в эпоху цифровизации может эффективно проводить политику дестабилизации в чужих странах.

С развитием цифровых технологий социальные сети претерпели огромные изменения. Большое значение приобрела информационная функция – социальные сети становятся главным источником новостей, превосходя телевидение, рост доверия к которому у населения России и большинства развитых стран достаточно мал, исключением является коммунистический Китай, при этом в интернет – пространстве, в частности социальных сетях, присутствует «свобода выбора» источника самой информации.

Данные о доверии к средствам массовой информации в России и мире представлены на рисунке 1.

TRUST IN MEDIA RISES, IN 16 OF 26 MARKETS

Percent trust in media



2020 Edelman Trust Barometer. TRU_INS. [Media in general] Below is a list of institutions. For each one, please indicate how much you trust that institution to do what is right. 9-point scale: top 4 box, trust. General population, 26-mkt avg.

Edelman | 42

Рисунок 1 – Доверие к СМИ в мире [42]

Использование интернет – пространства и социальных сетей растёт в геометрической прогрессии. Так, согласно ежегодному отчету *Global Digital* за 2022 г. количество пользователей сети интернет достигло 4,95 млрд чел., а пользователей различных социальных сетей достигает 4,62 млрд чел. Более подробный прирост пользователей интернета и социальных сетей можно увидеть на рисунках 2 и 3.

Для связи с внутренней и внешней аудиторией государства развёртывают специальные группы – кибервойска, которые проводят анализ общественных настроений, получают необходимую информацию от пользователей, вбрасывают и распространяют пропагандистские сообщения, создают контент для продвижения нужных политических идей [28].

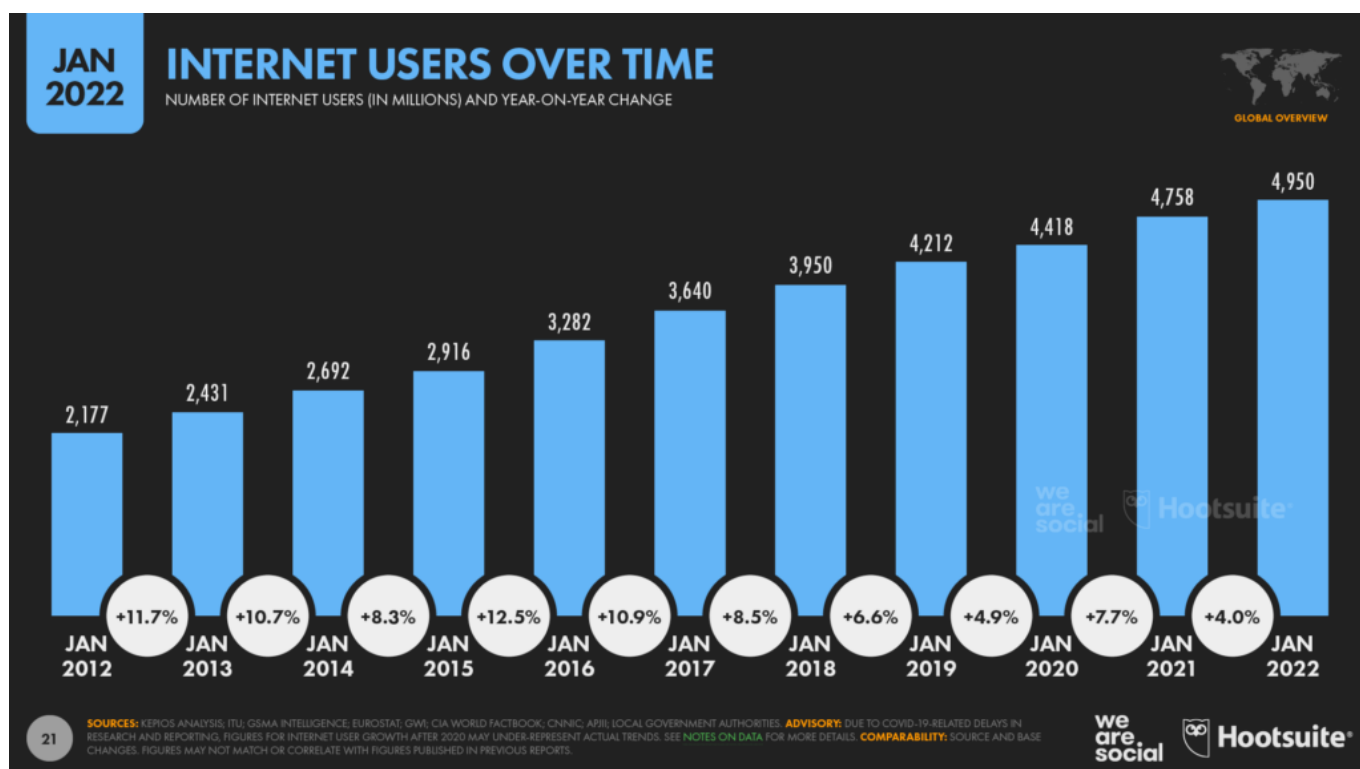


Рисунок 2 – Рост числа пользователей интернета [37]

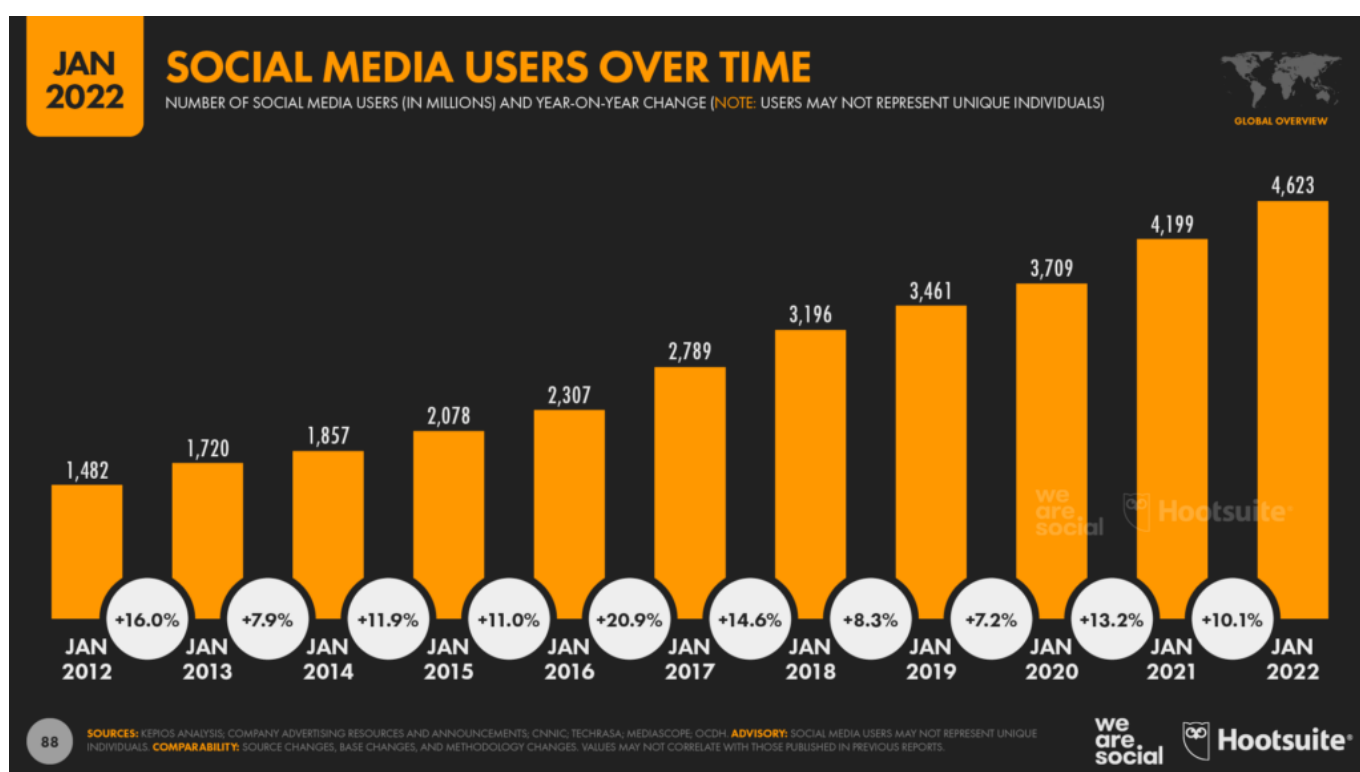


Рисунок 3 – Рост числа пользователей социальных сетей [37]

Высоким потенциалом кибервойск, а значит, способностью формировать информационное пространство, обладают Китай, Египет, Иран, Израиль, Мьянма, Россия, Саудовская Аравия, Сирия, Объединённые Арабские Эмираты, Венесуэла, Вьетнам и США. Правящая верхушка и политики используют социальные сети для своих внутривластных целей, например, проведения пропагандистских кампаний, дискредитации оппозиции, подавления политического инакомыслия, влияния на выборы.

Так же социальные сети стали одним из инструментов международной дипломатии. Так, начиная с 2020 г. со вспышкой «коронавируса» большая часть дипломатической активности переместилась в онлайн платформы и социальные сети. Социальные сети под действием политических процессов стали новым инструментом и изменили форму восприятия дипломатических процессов [18]. Благодаря цифровому формату взаимоотношения между социальными сетями и внешнеполитическими ведомствами стали трансформироваться в современное явление, показывающее, что социальные сети могут играть как отрицательную (*twitter*-революции, социальная нестабильность, формирование негативного общественного мнения и т. п.), так и положительную роль в выстраивании благоприятных отношений и обеспечении мира между странами [31].

Также цифровизация международных отношений стала отличной почвой для подмены фактов в цифровом пространстве. В целом, цифровые технологии в политической борьбе оказывают колоссальное влияние на политические процессы в мире, в первую очередь – на выборы в различные органы государственной власти. Это наглядно продемонстрировали две последние кампании по выборам президентов США 2016 г. [23], а также президентская гонка во Франции 2022 г.

Хотя информационные войны были главной особенностью многих вооружённых конфликтов в до цифровую эпоху, во время становления и развития цифровых технологий данный способ ведения информационной войны приобрёл совершенно новый характер и по-другому стал влиять на акторов международных отношений. Виртуализация как глобальная мегатенденция перенесла всю тяжесть борьбы за умы людей в блогосферу, в интернет-пространство. На данном этапе

цифровое пространство является неразделенным, и в результате чего происходят конфликты интересов акторов международных отношений [20].

Информационная безопасность в условиях стремительной цифровизации международных отношений также является важной задачей. Сегодня проблемы создания, внедрения, использования цифровых технологий тесно связаны с национальной безопасностью государства. Цифровые технологии являются по своей сути интеллектуальными ресурсами государства, в первую очередь человеческий капитал, определяющие его конкурентоспособность на глобальном уровне. Важным является вопрос комфортной среды для привлечения, воспроизводства и развития интеллектуального человеческого капитала и вовлечения его в нужное «русло». Первостепенной задачей современного государства является мобилизация человеческих ресурсов извне, формирование собственного интеллектуального капитала, чтобы в будущем успешно конкурировать в глобальном масштабе.

Итак, развитие цифровых технологий создаёт новое измерение международной политики, которое не стремится заменить классические методы дипломатии, а дополняет их и старается сделать более открытыми. Решение задачи мобильности человеческого капитала требует комплексного стратегического взгляда, и в этом смысле развитие транспортной инфраструктуры совместно с распространением телекоммуникационных и информационных технологий может стать катализатором изменений и задаст вектор для опережающего движения на пути построения социально-экономической системы следующего десятилетия.

1.3 Цифровизация международных конфликтов

Главной особенностью войн и конфликтов конца XX – начала XXI вв. – это массовое внедрение цифровых технологий. Так во время военных конфликтов в Югославии, Афганистане, Ираке, Ливии и Сирии проходили испытания высокотехнологического оружия, воздушно-космических сил, военно-морского флота и военной техники. Как показала практика данных войн и конфликтов –

новые виды вооружения по большей части базировались на достижениях цифровой эпохи.

Данные о развитии цифровой инфраструктуры за 2020 г. приведены «*Global Connectivity Index*». Расчет индекса осуществляется на основе 40 показателей, отражающих степень развития страны, рост инвестиций в ИКТ инфраструктуру и т.д.

Рейтинг стран по развитию цифровой инфраструктуры приведен на рисунке 4.

FRONTRUNNERS				ADOPTERS				STARTERS			
RANK	COUNTRIES	SCORE		RANK	COUNTRIES	SCORE		RANK	COUNTRIES	SCORE	
1	United States	87		21	United Arab Emirates	62		58	Indonesia	39	
2	Singapore	81		22	China	62		59	Philippines	38	
3	Switzerland	81		23	Spain	61		60	Morocco	38	
4	Sweden	80		24	Estonia	61		61	Ecuador	38	
5	Denmark	77		25	Portugal	61		62	Paraguay	37	
6	Finland	76		26	Italy	60		63	India	37	
7	Netherlands	75		27	Lithuania	58		64	Egypt	36	
8	United Kingdom	75		28	Czech Republic	57		65	Venezuela	35	
9	Japan	75		29	Slovenia	56		66	Jordan	35	
10	Norway	73		30	Chile	54		67	Lebanon	32	
11	Australia	72		31	Hungary	54		68	Bolivia	32	
12	New Zealand	72		32	Slovakia	54		69	Algeria	32	
13	South Korea	71		33	Saudi Arabia	53		70	Kenya	31	
14	Luxembourg	70		34	Malaysia	53		71	Botswana	31	
15	Germany	70		35	Greece	52		72	Ghana	30	
16	France	70		36	Bulgaria	52		73	Bangladesh	30	
17	Canada	70		37	Bahrain	51		74	Namibia	28	
18	Ireland	69		38	Croatia	51		75	Pakistan	28	
19	Belgium	66		39	Poland	51		76	Nigeria	27	
20	Austria	66						77	Uganda	26	
								78	Tanzania	25	
								79	Ethiopia	23	

Рисунок 4 – Рейтинг стран по цифровой инфраструктуре за 2020 г. [39]

Западные аналитики отмечают: цифровая информация стала и оружием, и ключом к достижению успеха в вооруженной борьбе. «Цифровая эпоха начала проявлять себя в вооруженных силах США, – писал еще в 1992 г. бывший председатель Комитета начальников штабов США генерал К. Пауэлл. – Всего несколько лет назад облик солдата с винтовкой в одной руке и компьютером в другой приводил всех в шок. Но именно это можно было видеть в песках

Саудовской Аравии в 1990 и 1991 гг. Информационные системы стали сегодня неотъемлемыми слагаемыми успеха боевых операций на поле боя» [29].

Война в Персидском заливе 1990–1991 гг., по оценки американских публицистов и военных деятелей, явилась последней традиционной и первой сетецентрической (*networkcentric*) войной. Так в ходе военной операции со стороны военных США и коалиции было задействовано более 300 систем телефонной и спутниковой связи и более 30 компьютерных сетей. Ежедневно осуществлялось около 700 тыс. телефонных разговоров и передавалось более 150 тыс. информационных сообщений. В 1998 г. была принята доктрина «Объединенная доктрина информационных операций» которая ознаменовала новый этап в развитии теории и практики информационного противоборства в целях достижения информационного доминирования в мирное и военное время [29].

Необходимость доктрины заключалось в том, чтобы разработать единую концепцию информационных операций, которые включали бы в себя такие сферы как экономика, политика, война и т.д.

В начале XXI в. в США стала массово проводится цифровизация всех процессов подготовки и ведения боевых действий на суше, море, в воздухе и космосе. Процесс цифровизации заставил изменить ранее существующую концепцию о вооруженных силах. Летом в 2002 г. были проведены широкомасштабные военные учения «*Millennium Challenge 2002*» «Вызов нового тысячелетия», основной целью которых была практическая отработка принципиально новой концепции изменения всей структуры вооруженных сил. К проведению данных военных учений министерство обороны США подготавливались около двух лет [12].

В ходе проведения военных учений «*Millennium Challenge 2002*» предусматривалось, что цифровые технологии позволят обеспечить сбор детальной информации обо всех объектах противника, так же сможет обрабатывать все данные в режиме реального времени, а также позволит командирам постоянно оставаться на связи со всеми своими подчиненными, которые участвуют в военных операциях. Военные учения «*Millennium Challenge 2002*» для США проходили под большим

грифом секретности, об этом свидетельствует тот факт, что союзников по НАТО не приглашали. Сведения о работе новой системы остаются закрытыми, то о новинках уже можно судить по качеству и скорости отработки конкретных задач и принятии решений. На рисунке 5 представлены новые системы цифровых технологий в военном деле.

По замыслу организаторов, учения «*Millennium Challenge 2002*» отрабатывали события, который происходили ранее, такие как война в Персидском заливе 1990 г., вторжение в Югославию в 1999 г., и конкретно воплотились во время второго вторжения в Ирак в 2003 г. и вторжения в Ливию в 2011 г.

Linkway TDMA – широкополосная система радиосвязи с временным разделением каналов заменит несколько устаревшую систему с частотным разделением каналов.

RTV – система оперативной визуализации профиля местности. На основании снимков высокого разрешения генерируется трехмерное изображение профиля местности с любым уровнем детализации.

TACSPASE – широкополосная система получения и обработки графической информации с военных спутников. Специальное программное обеспечение (*BRITE*) позволяет командирам подразделений оперативно запрашивать и получать цветные снимки участков местности в очень высоком разрешении.

JAWS – портативное компьютерное рабочее место. Этот своеобразный «мобильный армейский офис», обеспечен всеми необходимыми периферийными и коммуникационными устройствами, а также соответствующим программным обеспечением.

CROP – интегрированная компьютерная система. Мощный компьютерный центр, непрерывно получающий и обрабатывающий в режиме реального времени данные от всех доступных источников.

Рисунок 5 – Новые цифровые системы вооружения [12]

Цифровая ЭВТ стала столь же базовой вещью, как и автоматическая винтовка. Подчеркивая практическую значимость и объем добываемой информации, генерал Вильям Кернан, командующий объединенными вооруженными силами США, подчеркивал: «Мы должны знать о нашем противнике как можно больше – больше, чем он сам о себе знает, – кем бы этот противник ни оказался. Мы создаем

вооруженные силы, способные наносить удары по многим целям многими способами. Мы будем обладать решимостью и возможностями действовать быстрее и решительнее, чем, когда бы то ни было раньше. Мы должны быть умнее и быстрее, использовать хитрость и все возможности информационных технологий для того, чтобы вмешаться в процесс принятия решений противника и повлиять на ход операции».

В армии США такие термины как «информационные операции» и «информационная война» стали широко употребляются в СМИ и в том числе, в официальных военных документах. «Информационно-цифровые операции – это акции, предпринимаемые против информации и информационных систем противника, с одновременной защитой своей информации и своих информационных систем» [16].

С информационно-цифровыми операциями тесно связано понятие «информационная война». В «Словаре военных терминов» Комитета начальников штабов определяется: «Информационная война – информационно-цифровые операции, проводимые в периоды кризисов или конфликтов для достижения или обеспечения определенных целей в борьбе с определенным противником или противниками». Армия США уже имеют определенный опыт организации и проведения информационных операций в разных условиях. По современным американским взглядам, военно-технологическое превосходство должно быть достигнуто, прежде всего, за счет «прыжка» в развитии информационно-коммуникационных составляющих систем вооружения:

- сокращения времени между получением информации и наведением на цель боевой платформы – до 10 мин;

- разработки в рамках Боевой системы будущего (*Future Combat System*) высокоскоростной информационной сети, интегрированной как в вертикальном, так и в горизонтальном измерениях [12].

Так во время войны в Ираке 2003 г. классическая аналоговая радиосвязь практически уже не использовалась в качестве связи и управления войсками. На смену аналоговой радиосвязи пришли беспроводные пакеты передачи данных

которые позволяли получать не только количественные данные о расходах боеприпасов и топлива, но и позволяли получить оценку ведения боевых действий с помощью БПЛА, самолетов с радиоэлектронным оборудованием, а также участвующие в сборе информации в местах ведения военной операции.

Основным преимуществом сетецентрической доктрины или как ее называют военные эксперты «современная доктрина войны» является то, что военные в ходе боевых действий могут оперативно получать данные разведки и в последующем вступать в бой проходя противника, так же пропадает необходимость заботы о тыловом снабжении, которое доставляется в нужное время. Но у данной доктрины есть и негативные моменты такие как высокая зависимость от цифровых технологий, которые могут давать сбой тем самым нарушая план всей операции или оставляя солдат без снабжения.

США впервые использовали новую распределительную информационную систему боевого управления *FBCB2 (Force XXI Battle Command or Below)*, охватывающую уровень бригады, батальона и роты, которая собирает и распределяет данные, поступающие от всех источников разведывательной информации: спутника, самолета, вертолета, танка и даже отдельного пехотинца. Так во время вторжения в Ирак в 2003 г. одна из лучших американских дивизий – «Железный конь», специально переброшенная для взятия столицы Багдад, была полностью оборудована для работы с этой системой. Для водителей бронетранспортеров и другой техники перед началом штурма столицы Ирака до начала ведения боевых действий и во время войны складывались менее охраняемые противником маршруты предвещения, а также использовалась практика нанесения высокоточных ударов по для подрыва боевого духа противника.

Все командиры боевых подразделений и передовые артиллерийские наводчики для ориентирования на местности и передачи боевых донесений получили в свое распоряжение персональные переносные мини компьютеры (500 МГц/4 Гб). Военнослужащие в зоне боевых действий имели приемоиндикаторы спутниковой навигационной связи, способные точно определить местонахождение бойца в любой точке и в любых условиях. Впервые они использовались в таких

масштабах для наведения высокоточного оружия на цель независимо от погоды и времени суток. В настоящее время в США создается система глобальной геопространственной информации (СГГИ). Пользователь сможет связываться с единым источником данных. Хранилища цифровой информации планируется связать с единой системой управления на театре военных действий вплоть до роты. Использование спутниковой технологии в топогеодезическом обеспечении повседневной и боевой деятельности вооруженных сил имеет революционное значение [11].

Цифровые технологии на современном этапе развития смогли изменить характер ведения войны. Вооруженные силы США в ходе вторжения в Ирак в 2003 г. стали массово применять цифровые технологии для сбора информации, слежки и нанесения точных ракетных ударов в режиме реального времени. Данные действия позволяли анализировать ситуацию и контролировать действия подчиненных на фронте. Благодаря изменению облика ведения войны и тотальной цифровизации, США смогли достигнуть поставленных целей в кратчайший период.

Вооруженные силы, оснащенные передовыми цифровыми технологиями, имеют боевой потенциал, в три раза превышающий эффективность боевого применения обычных воинских частей. В США, вопреки расхожему мнению, именно государством затрачены огромные усилия на диффузию научных знаний и технологий из государственных учреждений и, прежде всего из министерства обороны, в частный сектор и обратно. При Совете безопасности США, в частности, действует специальная консультативная группа, в которую входят руководители восьми американских корпораций, успешно действующих в сфере высоких технологий.

Глава 2 Международные конфликты в условиях цифровизации

2.1 Гибридная война в эпоху цифровизации

Анализ современных событий показывают, что в настоящее время происходит трансформация искусства ведения войны. Процессы, которые были вызваны применением цифровых технологий, позволяют использовать различные стратегии в ходе вооружённых конфликтов. Новые методы в сочетании с традиционным пониманием войны и безопасности часто обозначаются как гибридная война.

Гибридные войны современности представляют собой сочетание как конвенциональных, так и неконвенциональных методов ведения войны.

Способ ведения современной гибридной войны в эпоху цифровизации, лучше всего описал Янис Берзиньш, который наглядно иллюстрирует переход от «традиционной» к гибридной войне. В таблице 2 представлена иллюстрация перехода от традиционной к гибридной войне.

Таблица 2 – Переход от традиционной войны к гибридной войне [40]

Традиционная война	Гибридная война
Прямое разрушение	Прямое влияние
Прямое уничтожение оппонента	Внутренний распад оппонента
Война с помощью оружия и технологий	Война ценностей
Война с помощью регулярной армии	Война специально подготовленными силами
Традиционного поля сражений	Информационная/ психологическая война
Прямых столкновение	Бесконтактная война
Поверхностная и секторная война	Тотальной война во всех сферах
Война в физической среде	Война за человеческое сознании и в киберпространстве
Симметричная война	Асимметричная война
Определенный период времени	Перманентная война

Конвенциональная война или конвенционная война – представляет собой вооруженный конфликт двух или нескольких государств, ведущийся в соответствии с нормами международного права. Традиционная конвенционная война отличается от асимметричной войны наличием различий между вооруженными силами и

гражданским населением, наличием морального равенства сторон, при котором противники придерживаются общих правил ведения войны, а также отказом от использования запрещенных мер.

Конвенциональные методы вооруженных конфликтов долгое время базировались на индустриальном веке военных технологий, в которых механические системы воплощали и доставляли военную силу. Индустриальная эпоха была сформирована, в частности, тремя революциями в военном деле (*RMA*), то есть появлением прорывных технологий, которые превосходили существующие на тот момент военные концепции и возможности, требующие переосмысления того, как, чем и кем ведется война.

На рисунке 6 представлена революция в военном деле конвенциональных методов гибридного конфликта.

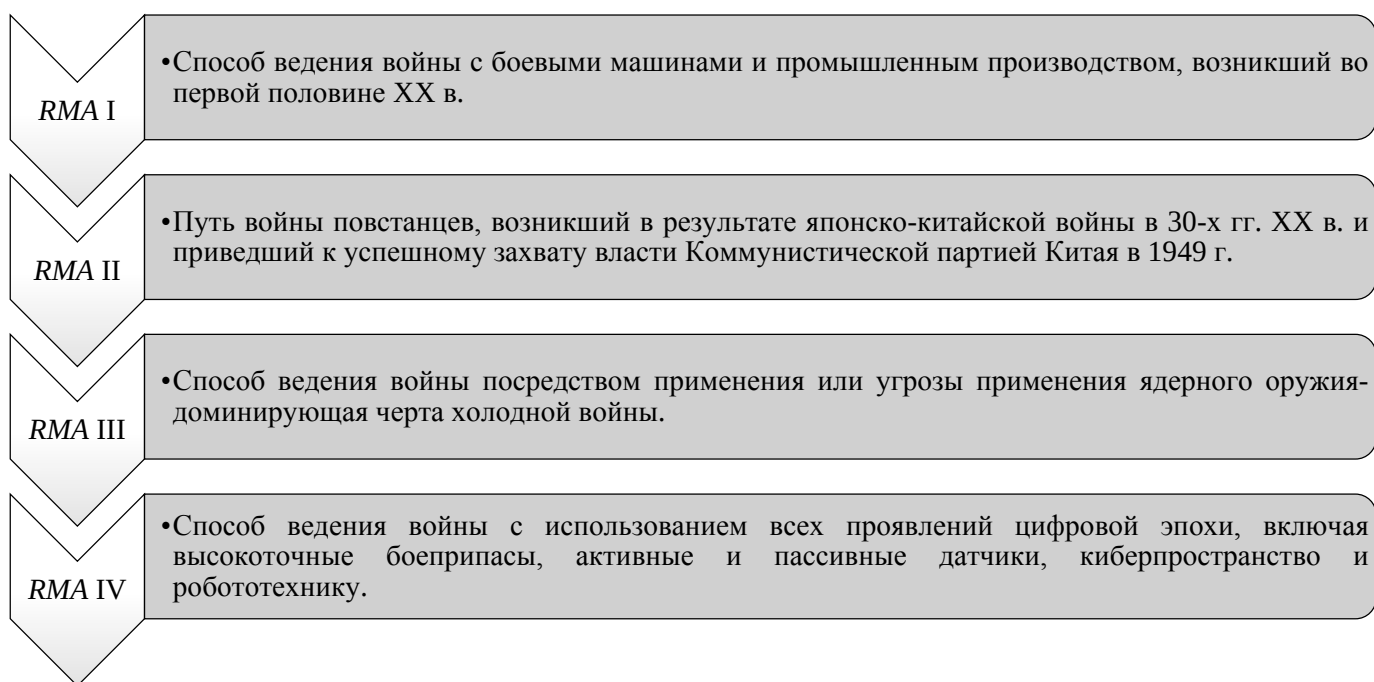


Рисунок 6 – Революция в военном деле [11]

Акторами конвенциональных гибридных конфликтов являются комбатанты (вооруженные силы страны обладающие юридическим статусом) и нерегулярные комбатанты (террористы, преступники, милиция, наемники, движения сопротивления, партизаны и т.д.), данные представлены в таблице

Таблица 3 – Акторы конвенциональных конфликтов [33]

Акторы	Кейсы	Тип гибридной ситуации с наибольшей эффективностью	Ресурсная база	Роль в социальном конструировании	Роль в информационных войсках
Ополчения	Сирия Ирак Египет Ливия	Гражданская война	Местное население – локальный уровень. Самообеспечение	Средняя – обеспечивают стабильность на определенной территории, но не устойчивую лояльность	Низкая – не являются активными игроками
ЧВК	Сирия Ирак Ливия	Гражданская война. Гражданская нестабильность после окончания гражданской войны	Внесистемные элементы у себя на родине. Контрактные отношения	Низкая – выделены из социального пространства, изолированы от социальных процессов	Низкая
Официальные военизированные формирования	Иран Сирия	Начальная фаза гражданского конфликта	Активисты локального и регионального уровня	Могут обозначать варианты официальной политической позиции	Средняя – могут быть источником политических коммуникаций
Криминальные структуры	Сирия Украина Гонконг США	Гражданские беспорядки на фазе нарастания	Локальный уровень	Основа для структур, альтернативных власти	Низкая

Нетрадиционные боевые действия или неконвенциональная война – данный термин обозначает проведение различных операций, которые сильно отличаются от обычных военных действий.

В отличие от конвенционального конфликта, цель которого – уничтожение военной и гражданской инфраструктуры, тактика нетрадиционных методов ведения войны является попыткой достичь военной победы путём мирного договора, капитуляции, или тайной поддержки одной из сторон существующего конфликта.

Неконвенциональный конфликт отличаются от методов обычной войны тем, что их силы или цели скрыты, или не очень хорошо определены, а общие или долгосрочные цели направлены на капитуляцию или же уничтожения противника малой кровью.

Неконвенциональные методы ведения войны представлены на рисунке 7.



Рисунок 7 – Неконвенциональные методы ведения гибридной войны [8]

Концепция неконвенциональных методов гибридной войны основывается на способности оказывать целенаправленное воздействие на удаленные объекты и процессы нетрадиционными военными средствами, в особенности на процессы и объекты, являющиеся критически важными для функций государства и вооруженных сил. В качестве асимметричного подхода неконвенциональные методы направлены на достижение победы или же нанесения максимального урона противнику с использованием минимальных средств. Например, подрыв линий снабжения противника или создания образа несправедливой войны для предотвращения получения политической поддержки населения страны.

Применение асимметричного подхода в военных действиях направлено на наиболее критические важные и уязвимые места в инфраструктуре государства. Наиболее частые нападения государственными и негосударственными акторами осуществляются на уязвимые точки идеологий и институций, а также использования социальное недовольство граждан как инструмента для уравнивания сил во время войны [11].

При гибридных конфликтах используется стратегия координации мягких действий с использованием более целостной стратегии, которая варьирует в плане

интенсивности на различных этапах (инициирование, острая фаза, решение). Конечной целью является подрыв данного государства путем стимулирования дестабилизации экономики, разочарования и недовольства населения, отчуждения меньшинств или обиженных групп населения, создания условий для контролируемой и неконтролируемой миграции, подавления гражданского сопротивления и подрыва критической инфраструктуры.

Как можно заметить из вышеизложенного, гибридная война современности подразумевает собой увеличение внутренней нестабильности во многих сферах государства (рисунок 8).

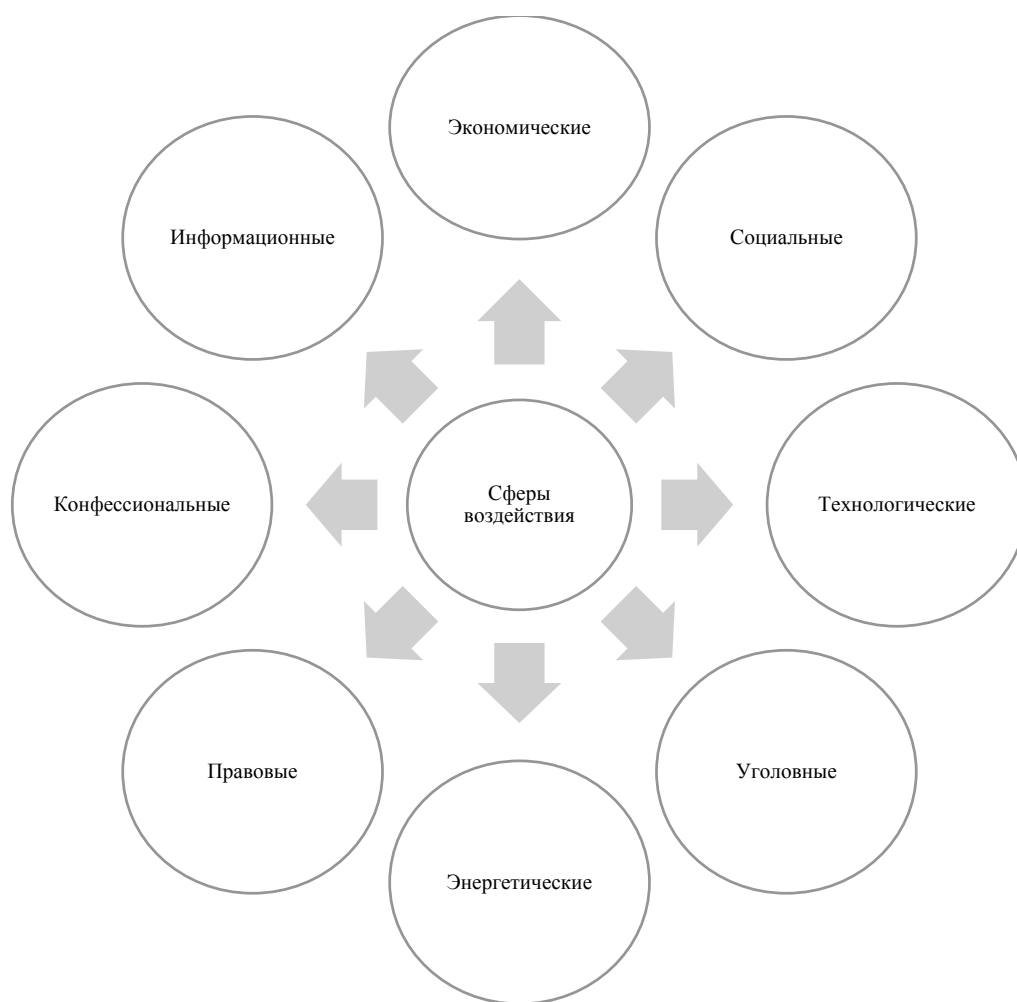


Рисунок 8 – Сферы воздействия гибридных войн [8]

Желаемое воздействие может включать повышение недоверия к институтам и общим ценностям, упадку экономической активности и доверия, приведение в

замешательство объективности, экспертизы, идеологии и других источников социальной кохезии.

Сохранение доминирования и конкурентоспособности на международной арене требует высокой экономической независимости или же контролирование огромных рынков сбыта за счет уникальности продукции и невозможности ее замещения, а также высокого уровня развития инновационных технологий. Государства, которые не имеют доступа к ресурсам, теряют темпы экономического развития в следствии чего и к потере цифрового развития и обороноспособности страны, данные события неизбежно приводят к утрате конкурентоспособности и затем к поглощению более могущественными акторами. В таблице 4 представлены данные стран с наиболее высокой экономической мощностью по номинальному показателю ВВП за 2021 г.

Таблица 4 – Рейтинг стран по номинальному ВВП за 2021 г. [39]

Рейтинг	Страна	ВВП (трлн долл.)
1	США	22,9
2	Китай	16,9
3	Япония	5,1
4	Германия	4,2
5	Великобритания	3,1
6	Индия	2,9
7	Франция	2,9
8	Италия	2,1
9	Канада	2
10	Южная Корея	1,8
11	Россия	1,6

В таблице 5 представлены данные международной бизнес-школы *INSEAD* по индексу инновации. Глобальный индекс инноваций охватывает 82 компонента таких как количество школ, вузов, уровень экономических свобод, уровень грамотного населения, вложения в инновационные разработки и т.д. Показание индекса можно разделить на два главных показателя «*Innovation Input*» и «*Innovation Output*» которые можно объединить в семь блоков: институты, человеческий капитал

и исследования, инфраструктура, развитие внутреннего рынка, развитие бизнеса развитие технологий и экономики знаний, результаты творческой деятельности.

Таблица 5 – Рейтинг стран по глобальному индексу инноваций за 2021 г. [38]

Рейтинг	Страны	Индекс
1	Швейцария	65,5
2	Швеция	63,1
3	США	61,3
4	Великобритания	59,8
5	Южная Корея	59,3
6	Нидерланды	58,6
7	Финляндия	58,4
8	Сингапур	57,8
9	Дания	57,3
10	Германия	57,3
12	Китай	54,8
45	Россия	36,6

Исходя из данных таблицы 4 и 5, можно сказать, что в условиях ведения современной гибридной войны самыми высокими потенциалами научной и экономической базы являются страны НАТО, Китай, Россия. Основываясь на этом, можно сделать вывод: данные страны обладают высокой конкурентоспособностью по сравнению с другими странами.

Попытка захвата контроля стратегически важных ресурсов в стране миноре или, наоборот, предотвращение такого развития ситуации, приводит к нарушению сфер влияния между странами гегемонами и в результате этого происходит опасное сближение сфер влияния центров мирового могущества с неизбежным конфликтом их интересов.

В таблице 6 рассмотрены приблизительные краткосрочные и долгосрочные цели гибридной войны трех государств.

Таблица 6 – Цели гибридной войны трех государств [7]

США и Запад		Россия		Китай	
Долгосрочные	Краткосрочные	Долгосрочные	Краткосрочные	Долгосрочные	Краткосрочные
Поддержание глобальной гегемонии	Противодействие России и Китаю	Создание великой державы	Бизнес-контракты	Статус великой державы	Бизнес-контракты
Поддержание статуса единственной супердержавы	Борьба с политикой Ислама	Укрепление в качестве нового архитектора общеевропейской безопасности	Ослабление экономических санкций	Архитектор новой азиатской безопасности	Контроль за стратегической инфраструктурой
Продолжение расширения НАТО	Изменение антизападного режима	Создание региональной гегемонии	Ослабление НАТО и ЕС	Глобальное экономическое превосходство	Сотрудничество на негосударственном уровне населения Китая с остальными странами
Контроль над ключевыми глобальными органами	Уничтожение нейтрального пространства в международной политической системе	Распад ЕС и НАТО	Заполнение стратегического вакуума после снижения влияния США в мире	Глобальное присутствие и учет интересов государства во всех регионах	Формирование новой мировой политической системы

Вышеперечисленные противоречия между странами стоит рассматривать как столкновения цивилизаций, в которых культурные и религиозные различия народов являются первичным источником конфликтов в мире после распада биполярной системы мира. Сэмюэль Хантингтон утверждал, что последующие конфликты и войны будут вестись не странами, а между культурами [8].

Данные столкновения могут быть также макиавеллевскими попытками подрыва стратегических противников, поскольку лидеры часто будут ощущать потребность развивать проекцию военной силы, которая не будет приводить к *ultima ratio regum* [8] решениям, при которых вооруженный конфликт может привести к уничтожению обеих сторон.

Цифровые технологии обеспечивают современные государства (цивилизации) тайными инструментами давления при которых государство не может доказать вину страны агрессора.

На рисунке 9 представлены данные о цивилизациях и их возможной эскалации интересов в будущем.

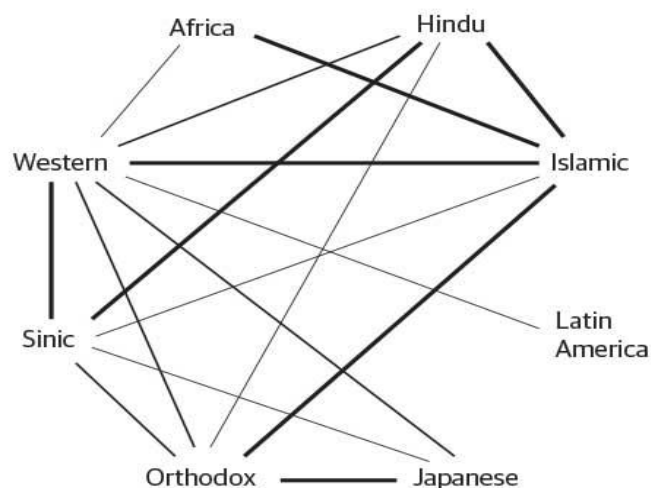


Рисунок 9 – Цивилизации и их возможные эскалации интересов [16]

Цифровые технологии дают возможность достигать стратегических целей неконвенциональными и когнитивными эффектами (технологии социального влияния и манипулирования, кибер сфера, информационное оружие, возможности нанесения существенного вреда системам управления государства). Такие технологии как социальные медиа сделали возможным, чтобы заинтересованный актор мог дистанционно оказывать влияние на все основные институты и на инфраструктуру государства. Это стало основой для неконвенциональных посягательств на территорию, часто даже без использования конвенциональных военных компонентов. Или их присутствие сделало возможным использование организованных и поддерживаемых извне движений сопротивления и террористических движений, которые тоже могут способствовать достижению стратегической цели создания нестабильности и нанесению ущерба институтам без применения военного насилия [14].

Таким образом, «гибридная война» рационально сочетает конвенциональные и неконвенциональные компоненты с упором на использование множества источников и режимов нападения, синергию результатов и высокий уровень неопределенности для оппонентов относительно конечных стратегических целей.

В гибридных конфликтах основными целями являются захват контроля над обществом, осуществление влияния на умонастроения людей, манипулирование

людьми, которые отвечают за принятие важных решений в государстве. Противник пытается манипулировать основными ценностями, мотивационными факторами, культурным базисом и стратегической, коммуникационной и критической инфраструктурой страны. Это достигается комплексным, сбалансированным осуществлением влияния с использованием мягкой и жесткой силы. Вот почему критические элементы систем, другими словами, объекты асимметричных действий в гибридных конфликтах, являются важными для ключевых элементов систем (компонентов, подсистем) государства, политических, дипломатических, социальных, технических, социотехнических, энергетических, финансовых, кибер, социо-кибер, информационных и других систем. Влияние на них в пределах оптимальных мер и корреляций параметров пространства, времени и ресурсов для оказывающей это влияние стороны приводит к желаемым, целенаправленным, быстрым, каскадным, синергетическим и деструктивным для этих систем изменений (нарушений) в их отношениях, структурах, процессах и результатах функционирования

2.2 Анализ крупнейших войн с использованием цифровых технологий

Войны и международные конфликты в эпоху цифровизации в отличие от прошлого столетия приняли совершенно новый характер, по своей сути все они являются частью гибридной войны или же войны нового времени. Теперь помимо типичной военной конфронтации, войны и конфликты посредством цифровых технологий стали затрагивать почти все сферы, при этом традиционные боевые действия до сих пор остаются актуальными. Примером областей, подверженных влиянию военных конфликтов, стали:

- технологическая (затрагивающая и экономическую составляющую);
- информационная.

Технологическая война – это международный конфликт нового уровня, технологическая гонка, которая неизбежно изменит не только лицо войны

будущего, но и повлияет на картину мира в целом - от политики до промышленности.

Несомненно, технологическое противостояние крупных держав было всегда, начиная от создания первого огнестрельного оружия и заканчивая изобретением оружия массового поражения, тем самым изменяя кардинально принципы ведения войны. Но именно сейчас технологическое развитие в цифровой среде сильно изменило облик ведения войны и сильно влияет на выживание государства. Уже сейчас активно практикуется тактика применения беспилотных систем, которые действуют удаленно, сводя к минимуму прямое боестолкновение. Таким примером может послужить вторая война за Карабах, где Азербайджан массово использовал беспилотных дронов разведывательного и боевого (камикадзе) типа. В частности, «*Bayraktar*» и «*Kargu*», которые навсегда изменят облик малых и крупных войн [32].

Говоря про технологическую войну в XXI в., стоит отметить недавно случившийся конфликт 2017–2020 гг., заключавшийся в противостоянии между такими крупными державами как Китайская Народная Республика (КНР) и США. Среди движущей силы американо-китайской технической войны можно выделить три ключевых фактора: геополитическое противостояние, торговая война и секьюритизации технологий.

Наиболее очевидно фактором является геополитическое содержание. Данный фактор связан с задачей ограничения потенциала КНР. Удар по китайскому цифровому и технологическому сектору был направлен на ограничение военно-технических возможностей Китая и его совокупного потенциала. Также политика США направлена на снижение потенциала развития китайской экономики и предотвращение возможности ее перехода на более высокий уровень. Эта цель определяется ролью производства и экспорта цифровой продукции для экономики Китая, структурообразующим значением ИКТ и крупнейших корпораций (*Huawei*, *ZTE*, *Alibaba*, *Tencent* и др.) для развития сектора хай-тек КНР и китайской инновационной системы. Данные действия с точки зрения США можно лишь трактовать как маккиндеровскую геополитическую формулировку: «кто контролирует цифровые технологии X, тот доминирует в мире».

Далее, можно обратиться к анализу технологического противостояния в контексте двусторонних торгово-инвестиционной борьбы.

Прежде всего, речь идет о международно-экономическом и глобальном измерениях национальной конкурентоспособности США: о борьбе за перспективные глобальные технологические рынки и контроль над ними, в том числе в части экспорта наукоемких цифровых услуг и оборудования, инвестиционной экспансии, включая поглощение стартапов, иных перспективных технологических компаний. Отдельным вопросом в связи с этим является снятие барьеров на доступ технологических корпораций США на рынки КНР. Эта задача тем более значима, что в КНР до недавнего времени были де-юре и остаются до сих пор де-факто с ограниченными возможности иностранных инвестиций во многие стратегические секторы экономики. Кроме того, по политическим в виде цензуры (рисунок 10) и экономическим (поддержка национальных компаний) причинам на китайском рынке запрещены или серьезно ограничены возможности работы американских интернет-сервисов (*Facebook, Google, Amazon* и др.). То же можно сказать и об импорте и реализации различных американских аппаратных решений (ранее – в том числе мобильных телефонов), включая нетарифные ограничения в виде системы уникальных национальных технических стандартов. Опасения усиления КНР до уровня, когда она сможет сместить США с позиции ведущей сверхдержавы. личных американских аппаратных решений (ранее – в том числе мобильных телефонов), включая нетарифные ограничения в виде системы уникальных национальных технических стандартов.

Данные о политической цензуре по состоянию за 2022 г. можно увидеть на рисунке 10.

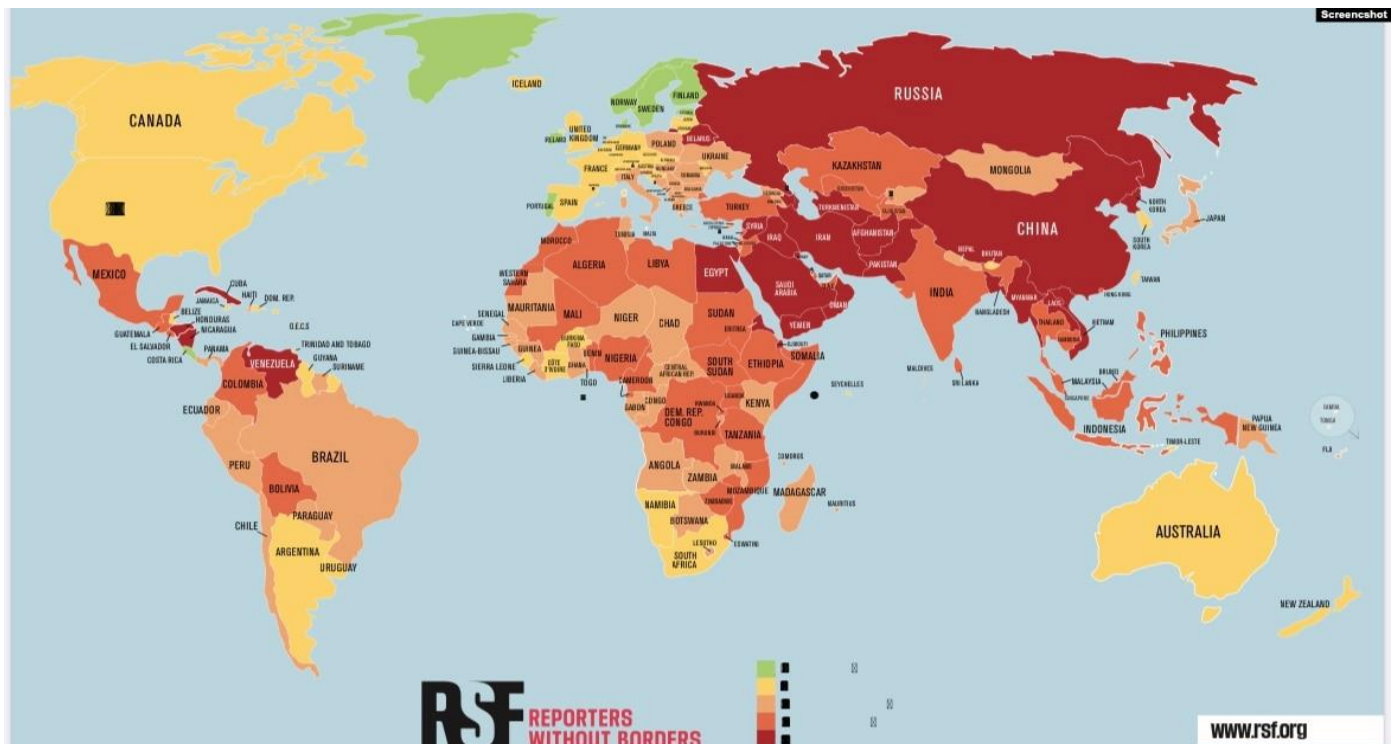


Рисунок 10 – политическая цензура в мире по состоянию на 2022 г. [23]

Во-вторых, наряду с предотвращением нечестной конкуренции наблюдаются и классические протекционистские мотивы, связанные с защитой национального рынка и американского технологического бизнеса от китайской экспансии в принципиально важных для будущего экономики технологических областях. Можно отметить что большинство американских цифровых корпораций проявляют очень сдержанную позицию относительно технологических санкций Белого дома (в силу собственных бизнес-интересов в КНР), часть из них объективно заинтересована в ограничении китайской конкуренции. Показательным примером в данном отношении является роль, приписываемая основателю и руководителю *Facebook* М. Цукербергу, в продвижении идей о запрете *TikTok* в США. Другим важным индикатором значимости этого мотива является давно дискутируемый вопрос о дефиците США в торговле высокотехнологичной продукцией с КНР, хотя немалая его часть – импорт продукции американских фирм. В Вашингтоне как минимум с конца 2000-х гг. обсуждается проблема потерь американской экономики, включая сектор хай-тек, от агрессивной торговой политики КНР, усиленной скрытой

господдержкой, демпингом, кражей интеллектуальной собственности и иными нечестными практиками [23].

В качестве специфического мотива технологического противостояния США и Китая выступают процессы секьюритизации. Это касается как собственно прорывных цифровых гражданских и «двойных» технологий, так и научно-технологических ресурсов (кадры, компетенции, венчурный и иной умный капитал, образовательная система и проч.). Можно уверенно сказать, что секьюритизация играет огромную роль в разматывании маховика американо-китайской технологической войны. Хотя формально проблематика секьюритизации занимает подчиненное положение относительно более общих геополитических факторов, в части прорывных технологий она приобретает до некоторой степени самостоятельное значение.

Главная цель санкций США направлена на попытку снизить потенциальный рост китайской и не только технологической мощи как угрозы для первенства США. По этому США активно используют санкции для сохранения своего лидерства на международной арене.

Данные о санкциях США по отношению к другим странам за 2022 г. можно увидеть на рисунке 11.

Подводя промежуточный итог можно отметить, что те пределы возможностей и угроз современных цифровых технологий, часть американских военных и властных элит опасается уязвимости перед растущей цифровой мощью КНР. Одновременно она стремится максимально капитализировать ситуацию пока еще сохраняющегося лидерства США в цифровом сегменте (включая его финансовые, институциональные и другие аспекты). Это, в свою очередь, стимулирует и геополитические, и торгово-экономические конфликты.

Следующая сфера войн в XXI в. затрагивает информационно-кибернетическое пространство. Киберпространство – метафорическая абстракция, используемая в философии и в компьютерных технологиях и являющаяся виртуальной реальностью, – второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей.

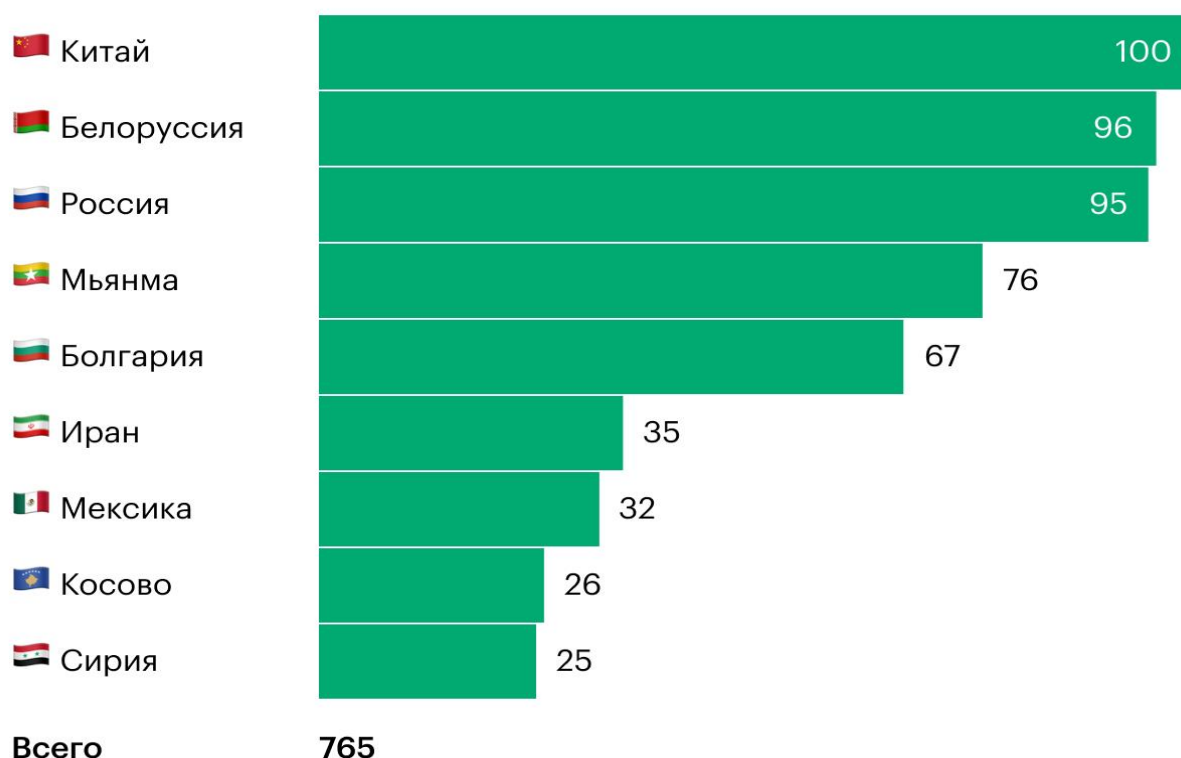


Рисунок 11 – Санкции США по отношению к другим странам за 2022 г. [41]

Следующая сфера войн в XXI в. затрагивает информационное-кибернетическое пространство. Киберпространство – метафорическая абстракция, используемая в философии и в компьютерных технологиях и являющаяся виртуальной реальностью, – второй мир как «внутри» компьютеров, так и «внутри» компьютерных сетей.

Кибервойна – война и противостояние в цифровом пространстве, в том числе компьютерное противостояние в Интернете.

Информационную войну в цифровом пространстве можно разделить на два вида (рисунок 12).

Теперь на данных категориях можно остановится более подробно.

Кибершпионаж – термин, обозначающий, несанкционированное получение информации с целью получения личного, экономического, политического или военного превосходства, осуществляемый с использованием взлома систем компьютерной безопасности, с применением вредоносного программного обеспечения и шпионских программ.



Рисунок 12 – Виды кибервойны [13]

Примером кибершпионажа может послужить инцидент который произошел в 2013 г. Бывший сотрудник АНБ Эдвард Сноуден раскрыл сведения, что правительство США взломало сервера китайских компаний-провайдеров мобильной связи для сбора текстовых сообщений, а также занималось шпионажем за университетом Цинхуа, и скачивало данные из сети *China Education and Research Network (CERNET)*, где имеют аккаунты миллионы китайцев. По словам Сноудена, американские спецслужбы ведут электронный шпионаж за Китаем и Гонконгом в течение многих лет [13].

Вандализм предполагает под собой использование хакерами интернета для порчи интернет-страниц, замены содержания оскорбительными или пропагандистскими картинками.

Пропаганда – рассылка обращений пропагандистского характера или вставка пропаганды в содержание других интернет-страниц. В задачи групп могут входить создание тем и сообщений на интернет-форумах, постов и комментариев в блогах и социальных сетях, оставление комментариев на страницах интернет-СМИ, зачастую в форме агрессивного издевательства над оппонентом.

Сбор информации – взлом частных страниц или серверов для сбора секретной информации и/или её замены на фальшивую, полезную другому государству. Ярким примером послужила хакерская атака в марте 2013 г. в ходе неё были взломаны

компьютерные сети ряда крупных банков Южной Кореи – *Shinhan Bank*, *Woori Bank* и *Nonghyup Bank*, а также многих телерадиокомпаний – *KBS*, *YTN* и *MBC*, в общей сложности было затронуто более 30 тыс. компьютеров; это была наиболее мощная кибератака в истории Южной Кореи. Хотя ответственности за сбор информации не удалось установить, самым очевидным вариантом остается главный противник Южной Кореи – КНДР [3].

Отказ сервиса – хакерские атаки правительственными и неправительственными организациями целью которых является нарушение работы сайта или сервисных составляющих сайта.

Вмешательства в работу оборудования – атаки на компьютеры, которые занимаются контролем над работой гражданского или военного оборудования, что приводит к его отключению или поломке.

Атаки на пункты инфраструктуры – атаки на компьютеры, обеспечивающие жизнедеятельность городов, их инфраструктуры, таких как телефонные системы, водоснабжения, электроэнергии, пожарной охраны, транспорта и т.д. Примером такой операции может послужить кибератака 2010 г. на Иран. Жертвой спланированной атаки стала компьютерная сеть фабрик по обогащению урана в Нетензе с помощью компьютерного вируса *Stuxnet* [3]. Данная кибератака привела к повреждению более 1000 ядерных центрифуг, и, по оценкам экспертов журнала *Business Insider*, «атомная программа Ирана была отброшена по меньшей мере на два года назад»

Война в киберпространстве затрагивает не только все ключевые элементы инфраструктуры, но и борется за сознание человека. Победа или же доминирование в киберпространстве в эпоху цифровизации дает государствам место под солнцем.

Хотя в цифровую эпоху традиционные войны и конфликты сильно преобразовались, они по-прежнему составляют большую часть войн.

На рисунке 13 представлены данные о видах конвенционных войн в эпоху цифровизации.

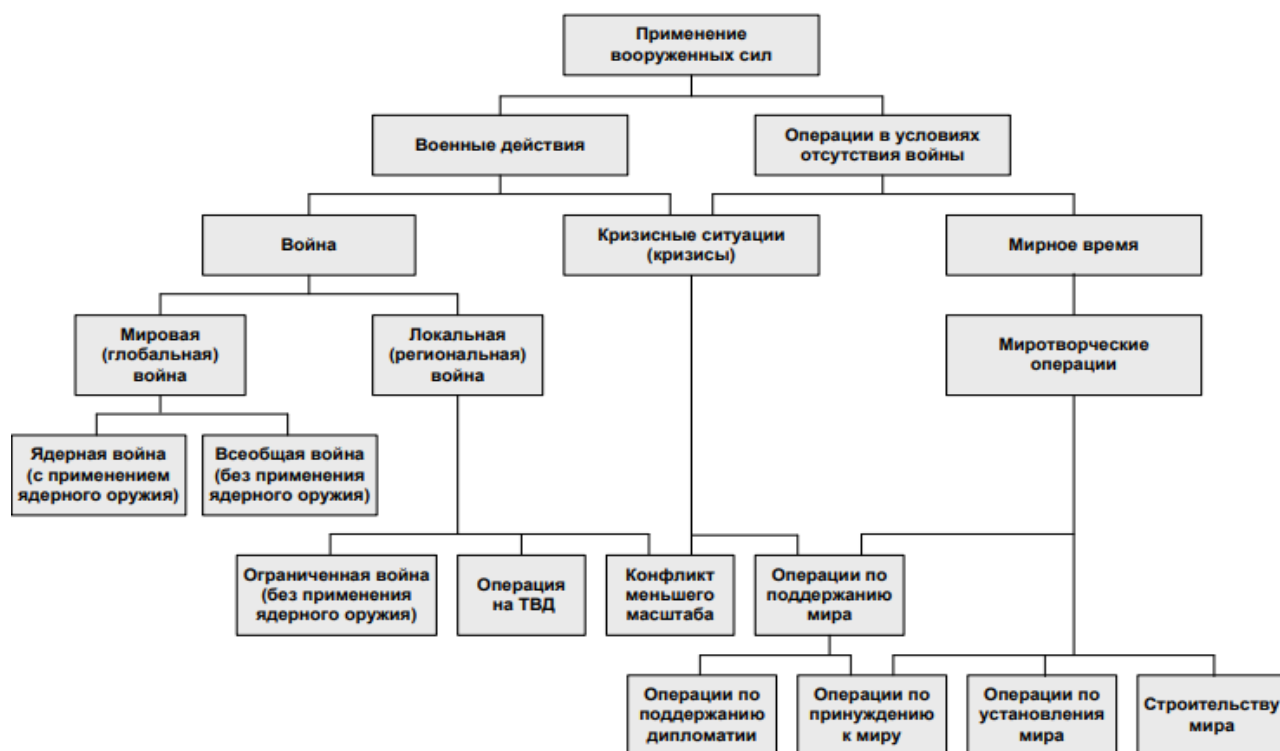


Рисунок 13 – Виды войн и конфликтов [11]

Ярким примером «современной войны в цифровую эпоху» является конфликт на Донбассе. Отличительным он является тем, как широко он занял все аспекты общественной жизни, сколько широкомасштабной, многомерной и мультифакториальной информации сконцентрировалось в психологических и кибер источниках. Хорошим примером такой деятельности являются новаторское и высокотехнологическое оружейное и военное оборудование, использованное при возвращении Крыма в 2014 г.

Стратегия с использованием новаторских кибер технологий в координации с тщательно спланированными действиями неконвенциональных и нерегулярных сил на месте привели в 2014 г. к потере Крыма Украиной и к конфликту на Донбассе.

В ответ на неконвенциональные и конвенциональные угрозы безопасности большинство стран, располагающих способностями для быстрого реагирования, сосредотачиваются на двух основных компонентах аппарата безопасности.

Потенциал сдерживания, состоящий из конвенциональных видов вооруженных сил (сухопутные силы, военно-воздушные силы, военно-морские силы).

Неконвенциональный военный потенциал. Этот потенциал включает военное оборудование и личный состав Сил для специальных операций, информационно-психологические операции и средства электронной борьбы, а также кибер силы (кибер разведка, кибер безопасность и кибер операции), службы разведки (электронные средства разведки, разведка с использованием открытых источников (РИОС), технические виды разведки, наблюдения и рекогносцировки и т.д.), коммуникацию для оперативного контроля, военные подразделения, которые оборудованы роботизированными (беспилотные летательные аппараты) комплексами и средствами для противодействия для соответствующих нападений, другие высокотехнологические ресурсы и меры [11].

Таким образом, сущность и характер военных конфликтов в цифровую эпоху позволяют сделать вывод о том, что при уменьшении вероятности развязывания широкомасштабной войны с применением ядерного оружия вероятность возникновения военных конфликтов регионального и локального характера не снизится. В этих условиях для реализации эффективной политики сдерживания необходим более широкий спектр соответствующих сил и средств, включающих как традиционные силы сдерживания, так и нетрадиционные (санкции, кибер атаки и т.д), гарантирующих нанесение противнику ощутимого, но соразмерного ущерба. Кроме того, быстро меняющаяся обстановка потребует при отстаивании национальных интересов прибегать не только к сдерживанию потенциальных агрессоров, но и к своевременному проведению превентивных действий.

2.3 Оценка и последствия международных конфликтов в цифровую эпоху

Международные конфликты в цифровую эпоху стали затрагивать все сферы деятельности государства. Конфликты и войны в цифровую эпоху не обязательно заканчиваются путем военного вторжения, где победившая сторона насильственным путем диктует свои условия. Ключевой особенностью является только тот факт, что война в цифровую эпоху не имеет фактического начала и конца, при этом

последствия поражения войны в цифровую и до цифровую эпоху обладают малыми отличиями.

Для выявления последствий войны в цифровую эпоху будут взяты несколько наиболее крупных конфликтов XXI в. в неконвенциональной сфере конфликтов – гибридная война России и США, и в конвенциональной – война Югославии, Ираке и Ливии.

Говоря про неконвенциональные последствия гибридной войны между США и Россией стоит отметить тот факт, что каждая из сторон конфликтов претендует на глобальную гегемонию. При этом между Россией и США после распада СССР складывались теплые отношения, после начала косовского кризиса и прихода Примакова в МИД отношения постепенно стали накаляться. Предвестником разрыва дипломатических отношений послужил Украинский кризис 2014 г. фактический, данная дата послужила началу гибридной войны между США и Россией. Преимущественно данный конфликт затрагивал технологическую, экономическую и кибер сферу.

Инструментами данного противостояния послужили экономические санкции в отношении критических важных отраслей промышленности и экономики России в частности: космическая, нефтегазовая, транспортная, фармацевтическая, банковская, энергетическая и т.д. Так же инструментами данного противоборства послужила цифровая сфера и вытекающие из нее. В частности, демонизация врага которая присуща всем сторонам конфликта через медиа и интернет пространство, создание образа непобедимой армии для психологического воздействия. Еще одним инструментом противоборства является военные учения с демонстрацией нового вооружения вблизи границ недружественного государства.

Про окончательные последствия данного противостояния говорить рано, так как противостояние еще находится в самом разгаре и неизвестно как события будут разворачиваться дальше.

В таблице 7 будут рассмотрены последствия противостояния США и России.

Таблица 7 – Последствия конфликта США и России [11]

США и Запад	России
Инфляция	Инфляция
Снижение дохода от импорта	Рост уровня безработицы (уход иностранных компаний из России)
Продовольственный кризис	Дефицит аппаратного и программного обеспечения
Энергетический кризис	Отставание в высокотехнологичной сфере

Следующий тип конфликтов будет затрагивать конвенциональные способы ведения войны и их последствия для государств. Наиболее явно характер сетцентрической войны с организацией военного управления на основе новых цифровых технологиях проявились в ходе вооруженных конфликтов в Югославии, Ираке, Ливии, проводимых США, НАТО и их союзниками в период с конца XX по начало XXI вв. При этом военные действия проходили с помощью ограниченного состава континентальных войск и преимущественно с использованием воздушно-космических сил и военно-морского флота, в результате чего на начальном этапе достигались геостратегические цели. Это связано не только с применением новейших высокотехнологических систем вооружения, но и с достаточно глубокой проработкой вопросов теории современной цифровой войны в научном и практическом планах.

В таблице 8 отражены конфликты с участием НАТО и США в концепции новой войны с использованием цифровых технологий.

Таблица 8 – Военные конфликты с использованием цифровых технологий [11]

Тип конфликта	Временной промежуток	Актеры	Регион
Война в Югославии	1999 г.	США и НАТО, Югославия	Балканы
Иракская война	2003 г.	США и НАТО, Правительство Ирака.	Ближний восток
Гражданская война в Ливии	2011 г.	Правительство Ливии, оппозиция, НАТО.	Северная Африка

Война США на Балканах против Югославии стала первой коалиционной войной в Европе после второй мировой войны. Данное противостояние от последующих конфликтов отличалось тем, что оно носила лишь испытательный

характер новой доктрины ведения боев и не ставило целью свержения правительства. Данное противостояние можно разделить на два этапа, которые будут представлены на рисунке 15.

Испытания в реальных боевых условиях новых высокоточных систем оружия, систем разведки, управления, связи, навигации, всех видов обеспечения, а также взаимодействия различных сил и средств.

- Первый этап

Нанесение высокоточных ударов по объектам гражданской и военной инфраструктуры, при помощи небольшой военной группы, преимущественно бесконтактными способами

- Второй этап

Рисунок 14 – Этапы конфликта в военных действиях против Югославии [11]

Инструменты, которые использовали страны НАТО для борьбы с Югославией можно разделить на два типа. Первый тип был инструментов относится к новейшим вооружениям основанных на цифровых технологиях представлен на рисунке 16.

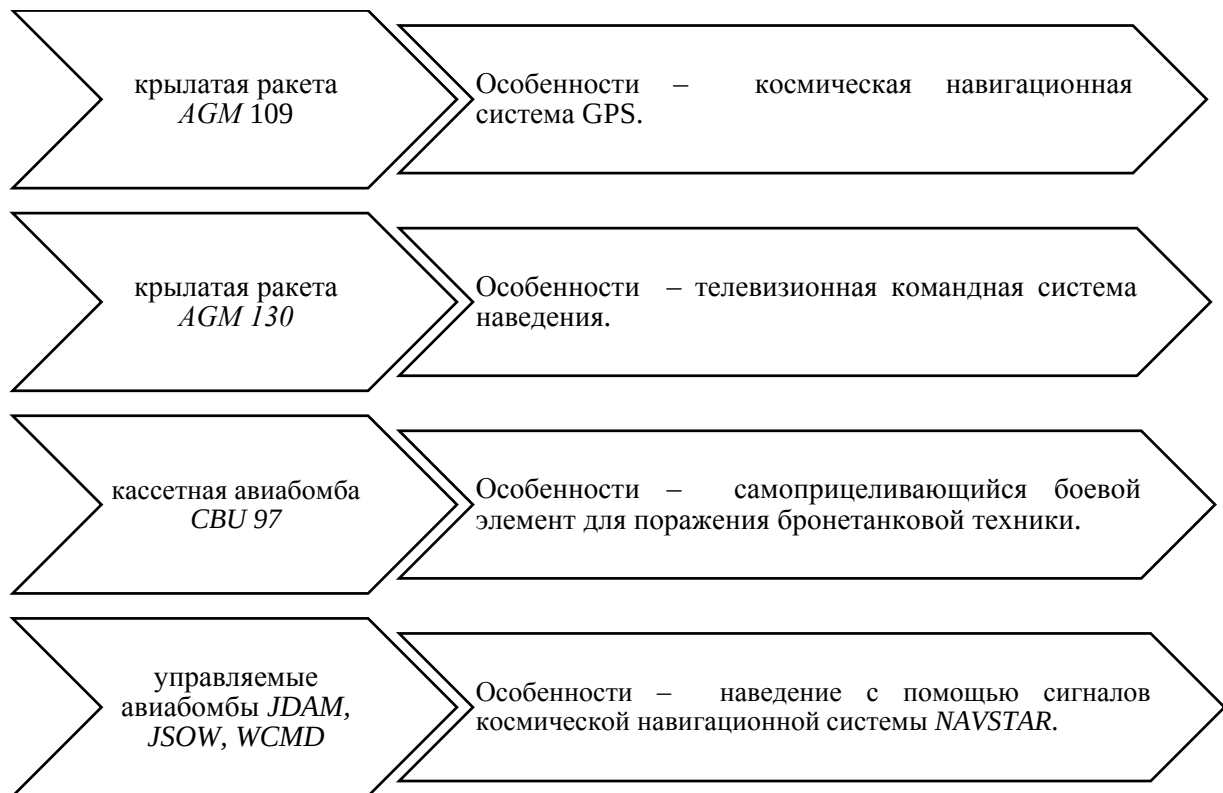


Рисунок 15 – Новейшие вооружения стран НАТО в 1999 г. [11]

Второй тип инструментов относится к неуправляемым авиабомбам прошлого поколения. Тем самым страны НАТО избавлялись от старого оружия, входе этого военный конфликт был затянут на несколько месяцев.

Так же для проведения операции «решительная сила» НАТО использовало средства радиоэлектронной борьбы, средства управления, средства разведывательного и навигационного обеспечения и информационно-психологических операций. Данные средства представлены на рисунке 16.



Рисунок 16 – Средства воздействия в ходе операции «решительная сила» [11]

Последствия этой войны для Югославии стала полностью разрушенная инфраструктура такая как: 100 % нефтяная промышленность, 50 % индустрии боеприпасов, 70 % авиационной промышленности, 40 % танковой и автомобильной промышленности, 40 % нефтехранилищ, 100 % мостов через Дунай, 70 % транспортных сетей и конечном итоге отделение Косово от состава страны. В последующем окончательный распад страны на Сербию и Черногорию и геноцид сербского народа в Косово.

Войну в Ираке нельзя рассматривать изолированно от экономического противоборства, главным содержанием которого стала блокада Ирака. С 1991 г. в соответствии с резолюцией Совета Безопасности ООН осуществлялось эмбарго на

торговлю Ирака с другими государствами, из-за этого военный и технологический потенциал страны заметно пострадал. Поэтому вполне закономерно, что к началу боевых действий в 2003 г. общее соотношение основных сил и средств коалиционной группировки и Ирака составляло 4,5:1, а по авиации – 8:1.

При подготовке к войне США в ходе операции «Шок и трепет» в Ираке в 2003 г., применив военную хитрость, сумев ввести в заблуждение иракское руководство о том, что они собираются вести войну в рамках сухопутной наземной операции. Вооруженные силы Ирака готовились к такому варианту войны и ушли в глубокую оборону, ожидая наземных военных действий. Однако США и их союзники начали против Ирака бесконтактную войну с активным применением средств высокоточное оружие.

В ходе этой войны НАТО стало более активно применять цифровые технологии в военном деле. Совершив в обеих Иракских операциях примерно одинаковое количество боевых вылетов (41 тыс. – в 1991 г. и 46 тыс. – в 2003 г.) с применением практически одинакового числа высокоточных средств поражения, авиация поразила, по данным американской прессы, почти в 4,5 раза больше целей, чем 12 лет назад (4 500 и 19 900 соответственно) [29].

Так же в ходе данного конфликта были использованы новые средства радиоэлектронной борьбы, спутниковой связи и системы БПЛА. Так же использовались высокоточное оружие как:

- *CBU-105 WCMD SFW* (контейнерные, корректируемые по ветровому отклонению, с сенсорным взрывателем);
 - *CBU-107 WCMD* (контейнерные, корректируемые по ветровому отклонению);
 - *AGM-86D CALCM* (КРВБ с проникающей БГЧ по заглубленным целям);
 - *Storm Shadow* (Великобритания) (КРВБ с «проникающей» БГЧ);
 - *JDAM (Joint Direct Attack Munition)* (высокоточные авиационные бомбы).
- Боеприпасы *JDAM* применялись палубными самолётами F-14D; бомбы *Mark 82* – бомбардировщиками B-2.

Эффективность применения боевой авиации, оснащенной высокоточным оружием, в операциях и локальных войнах конца XX в. и начала XXI в. приведена в таблицах 9 и 10.

Таблица 9 – Применение авиационных средств поражения США и НАТО в ряде военных операций [11]

Показатель	«Буря в пустыне» (Ирак, 1991 г.)	«Решительная сила» (Югославия, 1999 г.)	«Несокрушимая свобода» (Афганистан, 2001 г.)	Военная операция США и их союзников против Ирака (Ирак, 2003 г.)
ракет и бомб	256 000	23 000	22 000	29 000
высокоточных боеприпасов	20 500	8 000	12 500	20 000
доля высокоточного оружия, %	8	35	57	67

Таблица 10 – Результаты применения крылатых ракет в операциях против Ирака [11]

Показатель	1991	2003
Применение крылатых ракет: количество пусков	330	800
КРМБ количество пораженных целей	60	790
Применение боевой авиации: количество вылетов	41 300	45 600
количество пораженных целей	4550	19 900
Потери летательных аппаратов коалиционных сил:		
боевых самолетов	38	1
боевых вертолетов	16	6

Вместе с тем высокая технологичность и компьютеризированность боевых действий формирует слабые места вооруженных сил. Опыт боевых действий в Ираке показал, что в цифровой войне все виды. Вооруженные силы в огромной степени зависят от космических средств разведки, связи и навигации. Именно это предопределяет их уязвимость, так как данные виды обеспечения могут быть нейтрализованы путем создания соответствующих помех. В ходе операции в Ираке были случаи, когда десант, высадка которого планировалась в Иракской пустыне, оказался в Иране, ракеты, выпущенные по Багдаду, попадали на территорию

Турции, а 27 марта штурмовик А-10А расстрелял свою же колонну бронетехники. Данные факты подтверждают, что самая совершенная техника не может функционировать без человека и зачастую именно человеческий фактор должен вносить определяющую роль в принятие решений на поле боя.

Последствия вторжения в 2003 г. в Ирак неоднозначные, так с одной стороны войска коалиции выполнили цель по свержению Каддафи как «террориста» номер один и смогли установить лояльную администрацию для себя. Конфликт затянулся с 2003 по 2011 гг. вызвав рост исламского радикализма и в последующем приведший к гражданской войны с 2011 по 2017 гг. с ИГИЛ. В результате этой войны экономика Ирака была уничтожена, культурное наследие страны было разграблено и уничтожено.

Последним будет проведен анализ последствий вторжения НАТО в Ливию.

Военная операций «Одиссея. Рассвет» и «Союзный защитник», проведенных в Ливии в 2011 г., можно констатировать абсолютное техническое превосходство США и стран НАТО в космической группировке, средствах РЭБ, крылатых ракетах морского и воздушного базирования.

Причиной вторжения и поддержки многих политиков послужили информационные атаки на М. Каддафи и развернутая в мире кампания дезинформации о ливийских событиях. Данная кампания ввела в заблуждение многих крупных мировых политиков, выступивших с заявлениями, осуждающими нынешний ливийский режим за «непропорциональное» применение силы, нарушения прав человека и т.д. Никто даже не попытался глубоко разобраться в сути происходивших событий, причинах столь быстрого обострения обстановки, источниках и происхождении оружия у оппозиции и принадлежности членов боевых отрядов оппозиции.

В результате под давлением информационных операций, проводимых западными СМИ, 17 марта 2011 г. Совет безопасности ООН принял резолюцию № 1973 об объявлении ливийского воздушного пространства бесполетной зоной и об ужесточении экономических санкций против Ливии. А уже 19 марта 2011 г. заблаговременно созданные коалиционные силы (США, Великобритания, Франция,

Италия, Канада, Бельгия, Испания, Дания, Норвегия, Катар) начали против Ливии военную операцию, получившую название «Одиссея. Рассвет».

Военный сценарий в Ливии разворачивался по следующим пунктам:

- концепции управляемого хауса – посредством массовой дезинформационной пропаганды с помощью цифровых технологий – спланированные демонстрации в нескольких крупных городах;

- концепции обезоруживающего удара – уничтожение с помощью ВТО систем ПРО и ПВО;

- концепции информационного превосходства – новейшие средства связи, разведки и сбора информации;

- использование беспилотных и робототехнических средств – в задачи БПЛА входил сбор информации о противнике, а также нанесение ракетных ударов, разведка и доразведка целей, наблюдение за полем боя – средства превосходства: *MQ-1B Predator* и *RQ-4 Global Hawk*;

- применение радиоэлектронной борьбы и информационно-технических воздействий – проведена серия информационно-технических операций, позволивших коалиции получить доступ к сети сотовой связи операторов Ливии, а также провести мониторинг телефонов, принадлежащих военнослужащим ливийской армии – средства превосходства: самолеты разведки и радиоэлектронной борьбы *RC-135*, *EC-130Y*, *EC-13J*, *EA-18G*, *EP-3E*;

- информационно-психологические операции – запугивания, угрозы, манипуляции, пропагандистские листовки – средствами достижения послужили взломанные ранее операторы Ливийской сотовой связи и интернет [11].

Последствия войны для Ливии оказались разрушительными, как и в предыдущих конфликтах, которые развязали США и коалиция. Так вместо единого государства образовалось несколько независимых «государств», произошел рост исламского радикализма, экономические последствия для Ливии стали такими же катастрофическими как для Ирака. Так страна из развивающейся экономики, постепенно стала страной должником. А война операция по свержению Каддафи,

обернулась очередной кровавой гражданской войной, как и в сценарии с Ираком и последующем конфликте в Сирии.

В целом подводя итоги последствий международных конфликтов в цифровую эпоху можно отметить следующие. Итоги военного вторжения в Югославию, Ирак и Ливию свидетельствуют о том, что страны НАТО готовы применять неконвенциональные методы которые перерастают в конвенциональные войны для достижения своей гегемонии. Война в Ираке и Ливии подтвердила намерения США и их союзников возглавить «борьбу народов за демократию», направляя процесс «демократического переустройства» против антизападных режимов в регионе.

Так же конфликт в Ираке и Ливии подтвердил основные тенденции развития военного искусства западных стран и позволил им на практике проверить ряд новых концептуальных подходов к ведению современных и будущих войн. Кроме того, он показал, что одним из решающих факторов, обеспечивающих победу в войне, становятся мероприятия, связанные с информационно-психологическим и экономическим воздействием на противника.

Опыт ливийской кампании выявил ряд новых тенденций, которые с высокой степенью вероятности будут использоваться Западом в дальнейшем. В частности, при достижении военно-политических целей на первый план выдвигаются информационно-психологические, дипломатические и экономические формы воздействия на неугодные режимы.

Одновременно ливийская кампания и в последующем ситуация в Украине подтвердила возрастающее значение информационно-пропагандистского фактора, особенно в современных условиях, когда СМИ играют существенную роль в формировании общественного сознания.

Заключение

Мировой процесс цифровизации, начавшийся в конце 1950-х – начале 1960-х гг. в Европе и Америке, охватил все страны земного полушария. Цифровая эпоха развивалась постепенно, начиная от научных исследований, разработкой аппаратного обеспечения и персонального обеспечения, заканчивая подключением мира к цифровому пространству. Процесс цифровизации коснулся всех сфер деятельности человека, начиная от гуманитарных наук и заканчивая конфликтами и войнами. Цифровизация международных отношений в эпоху всеобщей цифровизации было лишь вопросом времени. Сама цифровизация международных отношений сделала политику более доступной для масс. Затрагивая вопрос цифровизации международных конфликтов, стоит отметить что самым первым государством, которое стало массово внедрять цифровые технологии в армию стали США, тем самым внося свою лепту в военную историю.

Гибридная война рационально сочетает конвенциональные и неконвенциональные компоненты с упором на использование множества источников и режимов нападения, синергию результатов и высокий уровень неопределенности для оппонентов относительно конечных стратегических целей.

Сущность и характер военных конфликтов в цифровую эпоху позволяют сделать вывод о том, что при уменьшении вероятности развязывания широкомасштабной войны с применением ядерного оружия вероятность возникновения военных конфликтов регионального и локального характера не снизится.

Итоги военной кампании в Югославии, Ираке и Ливии свидетельствуют о том, что страны Запада готовы применять военно-силовые методы для достижения своих военно-политических и военно-стратегических целей в будущем. Война в Ираке и Ливии подтвердила намерения США и их союзников возглавить «борьбу народов за демократию», направляя процесс «демократического переустройства» против антизападных режимов в регионе.

Так же конфликт в Ираке и Ливии подтвердил основные тенденции развития военного искусства западных стран и позволил им на практике проверить ряд новых концептуальных подходов к ведению современных и будущих войн. Кроме того, он показал, что одним из решающих факторов, обеспечивающих победу в войне, становятся мероприятия, связанные с информационно-психологическим и экономическим воздействием на противника.

Опыт ливийской кампании выявил ряд новых тенденций, которые с высокой степенью вероятности будут использоваться Западом в дальнейшем. В частности, при достижении военно-политических целей на первый план выдвигаются информационно-психологические, дипломатические и экономические формы воздействия на неудобные режимы. Непосредственно в ходе военного конфликта будут комплексно применяться в первую очередь высокоточные средства поражения, в том числе большой дальности, позволяющие минимизировать ответные действия противника и не допустить существенных потерь своих сил и средств.

Одновременно ливийская кампания подтвердила возрастающее значение информационно-пропагандистского фактора, особенно в современных условиях, когда СМИ играют существенную роль в формировании общественного сознания. Так, в интересах обоснования необходимости вмешательства международного сообщества в разрешение кризиса в Ливии Западом активно проводилась целенаправленная дезинформация, когда акцент делался на «преступлениях» одной из противоборствующих сторон, замалчивая при этом деструктивные и противозаконные действия другой.

Список использованных источников

- 1 Алейников А. В., Милецкий В. П., Пименов Н. П., Стребков А. И. Феномен «фейк-ньюс» и трансформация информационных стратегий в цифровом обществе // Научно-техническая информация. 2019. № 6. С. 1–7.
- 2 Бедрицкий А. В. Новые подходы к развитию вооруженных сил США. М. : РИСИ, 2008. 28 с.
- 3 Белоус А., Солодуха В. Кибероружие и кибербезопасность. О сложных вещах простыми словами. М. : ЛитРес, 2021. 220 с.
- 4 Белоус А., Солодуха В. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. М. : ЛитРес, 2021. 210 с.
- 5 Васильева М. Современные международные отношения. М. : ЛитРес, 2022. 310 с.
- 6 Военная операция в Сирии. URL: www.rbc.ru/rbcfreenews/604f15fe9a79478247f233a0 (дата обращения: 20.04.2022).
- 7 Гибридная война в XXI веке: анализ западных концепций. URL: <http://csef.ru/ru/oborona-i-bezopasnost/348/gibridnaya-vojna-v-xxi-veke-analiz-zapadnyh-konczenczij-9081> (дата обращения: 29.04.2022).
- 8 Даник Ю. Гибридная Война: Хай-Тек, Информационные и Кибер Конфликты. URL: <http://connections-qj.org/ru/article/gibridnaya-voyna-hay-tek-informacionnye-i-kiber-konflikty> (дата обращения: 14.03.2022).
- 9 Конрад Цузе: мечтатель, создавший первый компьютер. URL: <https://habr.com/ru/company/ua-hosting/blog/386247/> Конрад Цузе: мечтатель, создавший первый компьютер (дата обращения: 25.04.2022).
- 10 Коньков А. Е. Цифровизация политики vs политика цифровизации // Вестник Санкт-Петербургского университета. Международные отношения. 2020. Т. 13. Вып. 1. С. 47–68.
- 11 Макаренко С. И., Иванов М. С. Сетецентрическая война – принципы, технологии, примеры и перспективы. Монография. СПб. : Наукоемкие технологии, 2018. 898 с.

- 12 Новые правила войны. URL: <http://www.foreignpolicy.com/articles> (дата обращения: 29.04.2022).
- 13 Овчинский В., Ларина Е. М. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М. : Книжный мир, 2020. 300с.
- 14 Овчинский В., Ларина Е. М. Крах однополярного мира. М. : ЛитРес, 2020. 320 с.
- 15 Подберезкина А. И. Некоторые аспекты анализа военно-политической обстановки: монография. М. : МГИМО, 2019. 874 с.
- 16 Попов И. М., Хамзатов М. М. Война будущего: концептуальные основы и практические выводы. Очерки стратегической мысли. М. : Кучково поле, 2016. 836 с.
- 17 Почепцов Г. Г. Виртуальные войны. Фейки. М. : Glagoslav Distribution (A), 2019. 512 с.
- 18 Почепцов Г. Г. Информационные войны. Новый инструмент политики. М. : Алгоритм, 2018. 320 с.
- 19 Почепцов Г. Г. Как ведутся тайные войны психологические операции в современном мире. М. : Консум, 2000. 198 с.
- 20 Почепцов Г. Г. Когнитивные войны в соцмедиа, массовой культуре и массовых коммуникациях. М. : Glagoslav Distribution (A), 2020. 320 с.
- 21 Почепцов Г. Г. Пропаганда 2.0. М. : Фолио, 2019. 210 с.
- 22 Революция в военном деле и «армейские операции вне условий войны»: обоюдоострое оружие. URL: <https://www.perspektivy.info/print.php?ID=36310> (дата обращения: 14.04.2022).
- 23 Рябченко Н. А., Малышева О. П., Гнедаш А. А. Управление политическим контентом в социальных сетях в период предвыборной кампании в эпоху постправды // Полис. 2019. № 2. С. 92–106.
- 24 Сафонов А. История (конец XX – начало XXI века) 2-е изд. М. : ЛитРес, 2022. 320 с.
- 25 Сафонов А. История: международные конфликты в XXI веке. М. : ЛитРес, 2022. 300 с.

- 26 Скиннер К. Четвертая революция в истории человечества, которая затронет каждого. М. : «Манн, Иванов и Фербер», 2020. 304 с.
- 27 Слоботчиков О. Война и мир в эпоху становления цифровой цивилизации. М. : ЛитРес, 2021. 320 с.
- 28 Соловей В. Д. Особенности политической пропаганды в цифровой среде // Гуманитарные науки. Вестник Финансового университета. 2018. № 1. С. 81–87.
- 29 Суворов С. Советское и американское оружие в иракской войне // Техника и вооружение. 2003. № 10. С. 15–18.
- 30 Сурма И. В. Цифровая дипломатия в мировой политике // Государственное управление. 2015. № 49. С. 220–249.
- 31 Туронов. С. Политический анализ и прогнозирование. М. : ЛитРес, 2022. 320 с.
- 32 Форбс (США): что можно узнать о войне в Нагорном Карабахе из открытых источников. URL: <https://inosmi.ru/20201026/248405246.html> (дата обращения: 20.04.2022).
- 33 Цехановский В. Информационные технологии. М. : Юрайт, 2021. 326 с.
- 34 Шваб К., Дэвис Н. Технологии Четвертой промышленной революции. М. : Эксмо, 2022. 230 с.
- 35 Шпитцер М. Антимозг: цифровые технологии и мозг. М. : АСТ, 2020. 320 с.
- 36 Frank G. «Hybrid Warfare and Challenges» // Joint Forces. 2009. № 52. P. 34–39.
- 37 Global Digital 2022: вышел ежегодный отчёт об интернете и социальных сетях – главные цифры. URL: <https://www.sostav.ru/publication/we-are-social-i-hootsuite-52472>. (дата обращения: 26.04.2022).
- 38 Global innovation index 2021: Tracking innovation through the COVID-19 crisis. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021.pdf (дата обращения: 26.04.2022).
- 39 Global Connectivity Index 2020 URL: <https://www.huawei.com/minisite/gci/en/index.html> (дата обращения: 18.04.2022).

40 Rising Caseloads, A Disrupted Recovery, and Higher Inflation. URL: <https://www.imf.org/en/Publications/WEO/Issues/2022/01/25/world-economic-outlook-update-january-2022> (дата обращения: 14.04.2022).

41 Russian New Generation Warfare. URL: https://www.researchgate.net/publication/331530391_Russian_New_Generation_Warfare (дата обращения: 29.04.2022).

42 International sanctions during the 2022 Russian invasion of Ukraine. URL: <https://home.treasury.gov/> (дата обращения: 05.05.2022).

43 2020 Edelman Trust Barometer URL: <https://www.edelman.com/trust/2020-trust-barometer> (дата обращения: 05.05.2022).