

Social Networks



# FALL 2020 COGNITIVE WARFARE

AN ATTACK ON TRUTH AND THOUGHT



Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, Olivia Madreperla



# Оглавление

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| <b>Управляющее резюме</b>                                         | <b>3</b>  |
| <b>Введение</b>                                                   | <b>5</b>  |
| <b>Эволюция некинетической войны</b>                              | <b>6</b>  |
| Истоки                                                            | 6         |
| Психологическая война (PsyOps)                                    | 7         |
| Электронная война (EW)                                            | 7         |
| Кибервойна                                                        | 8         |
| Информационная война                                              | 8         |
| Когнитивная война                                                 | 9         |
| <b>Цели когнитивной войны</b>                                     | <b>11</b> |
| Дестабилизация                                                    | 12        |
| Случай 1: Дестабилизация через замешательство.                    | 13        |
| Случай 2: Дестабилизация путем посева разделения.                 | 15        |
| Случай 3: Дестабилизация как средство воздействия.                | 17        |
| Пример 1: Воздействие на вербовку Случай 2:                       | 20        |
| Влияние на принятие политики Пример 3: Влияние                    | 21        |
| как средство дестабилизации                                       | 22        |
| <b>Будущие угрозы</b>                                             | <b>27</b> |
| Заглядывая вперед                                                 | 27        |
| Угроза 1: Простота отбора и вирусность.                           | 29        |
| Угроза 2: Новый век правды.                                       | 30        |
| Угроза 3: Кибер-индуцированный институциональный дискомфорт и     | 31        |
| недоверие Угроза 4: Биологическое и терапевтическое эмоциональное | 32        |
| манипулирование Угроза 5: Расширенная вербовка агентов            | 33        |
| <b>Рекомендации по стратегии</b>                                  | <b>35</b> |
| Структура распознавания угроз и критерии                          | 35        |
| оценки рисков                                                     | 36        |
| Организационные реализации                                        | 37        |
| Наступательные соображения                                        | 39        |
| <b>Заключительные мысли</b>                                       | <b>40</b> |
| <b>Библиография</b>                                               | <b>41</b> |

## Управляющее резюме

Война резко изменилась за последние несколько десятилетий, отойдя от физического угрозы обычной войны. Война теперь движется к социальным и идеологическим угрозам благодаря средствам массовой информации и достижениям в области технологий. Появление этого нового вида войны отличается от всего, что мы видели раньше. Хотя он берет элементы из предыдущие типы гибридной войны, охват и уровень воздействия, которыми она обладает, делают ее гораздо более опаснее своих предшественников. Мы назвали этот новый способ войны *когнитивная война*.

Когнитивная война, хотя и имеет некоторое сходство с другими нетрадиционными и некинетические виды боевых действий/операций, в конечном счете, уникальны по своему исполнению и назначению. В этой статье мы исследуем истоки некинетической войны, сначала взглянув на холодную войну и использование психологических операций (PsyOps). Мы следим за эволюцией ведения войны, отмечая, что достижения в области технологий привели к радиоэлектронной войне, а затем и к кибервойне. В качестве кибервозможности продолжали развиваться, разведка стала растущей областью, а информация военные действия начали развиваться. Однако когнитивная война идет дальше, чем просто борьба за контролировать поток информации. Скорее, это борьба за контроль или изменение того, как люди *реагировать* Информация. Когнитивная война стремится заставить врагов уничтожить себя изнутри. Мы определяем когнитивную войну как превращение общественного мнения в оружие внешней сущностью для цель (1) повлиять на общественную и государственную политику и (2) дестабилизировать общественную учреждения.

Дестабилизация и влияние — основные цели когнитивной войны. Эти цели работают с целью посеять недовольство в обществе или поощрить определенные убеждения и действия. Утечки информации о Национальном съезде Демократической партии (DNC) 2016 года — хороший пример Власть использует разногласия для дестабилизации общества. Террористические группы, такие как «Аль-Каида», демонстрируют как радикальные идеологии могут влиять на мирных жителей и вербовать их. Никогда прежде не было такого коварные манипуляции было так же легко осуществить, как и сегодня. Достижения в области подключения, оцифровка, неврология и психология принесли обществу множество благ. Пока что,

с каждой новой возможностью возникает новая угроза. Сегодня мы сталкиваемся с проблемами, которые приходят с возможностью социальных сетей передавать информацию миллиардам желающих людей в вопросе минут. Мы должны защищаться от алгоритмов, которые могут определить, кто будет самым восприимчивым к размещенным материалам, и кто наиболее готов их распространять. Современная способность к подделыванию и манипулированию информацией беспрецедентно, и недавние достижения в области искусственного разведка теперь сделала видео и аудио подозрительными. Люди не знают, что делать верить, не избавляя даже правительственные учреждения от этого неверия. Одновременно мы революционизируем то, что мы знаем о том, как наш мозг и эмоции функционируют как личности поэкспериментировать с различными формами контроля.

Поэтому мы считаем, что НАТО должна быстро и решительно адаптироваться для защиты от нынешних угрозы в сфере когнитивных войн и работу по пресечению будущих угроз. В то время как демократический общество одновременно сложно и удивительно, оно также уязвимо. Чтобы опередить эти угрозы, НАТО должна отреагировать в обороне тремя способами. Во-первых, НАТО должна работать над созданием рабочего определение или рамки для когнитивных актов войны. Это включает в себя набор критериев для обнаружения когнитивные атаки по мере их возникновения. Во-вторых, альянс должен оценить уязвимые места для когнитивные атаки на национальном и личном уровне в надежде создать и вдохновить более жизнестойкое население. В-третьих, НАТО должна создать организации для связи с технологическими компаниями и справиться с вызовами войны будущего. Дополнительным окончательным соображением будет анализ потенциально враждебных государств, против которых мы можем использовать когнитивную войну в наступательной стратегии или как средство сдерживания.

Основа демократии лежит не только в законах и гражданском порядке, но и в доверии и взаимном уважение: уверенность в том, что мы будем следовать этим законам, уважать гражданские институты и уважать друг друга и наши разные мнения. Доверие сейчас под угрозой, правда подвергается нападкам, а демократия угрожал. Время готовиться сейчас, и весь мир наблюдает.

# Введение

Люди пытались влиять на общественное мнение с момента возникновения цивилизации. Это очень важно компонент политических структур, в которые мы превратились. Тем не менее, *вооружение* общественного мнения — это новое явление, угрожающее развитию нашего взаимодействия. Появление Интернет и средства массовой информации сделали возможным крупномасштабное манипулирование населением через целенаправленный, доступный, мультимодальный обмен сообщениями, который теперь может существовать под видом анонимности.

В море миллиарда голосов определить отдельные источники стало невероятно сложно [1]. Усилие, которое в некотором роде сравнимо с трудностью определения того, кто кричал «Пожар!» в толпе. Некоторые возражают, что это задумано, утверждая, что анонимность необходима для ресурсы, которые предоставляет Интернет. Другие, однако, беспокоятся о непредвиденных последствиях, которые это отсутствие подотчетности может иметь место в долгосрочной перспективе [2].

Независимо от того, какая точка зрения верна, мы считаем, что НАТО должна знать об угрозе. что наша взаимосвязь произвела. Тактика, ориентированная на публику, со временем не исчезнет; они станут более эффективными. Они будут нацелены на более широкую аудиторию. Более того, они будут становятся все более убедительными. Технологические достижения уже продемонстрировали свое умение делать именно это. Не нужно искать дальше утечки информации DNC 2016 года. для подтверждения скорости, с которой информация приобретает и распространяется в интересах противная сторона.

Социальные сети, новостные сети, алгоритмы автоматизации, искусственный интеллект, психическое здоровье руководство и, возможно, даже наша собственная физиология, как ожидается, будут быстро развиваться в ближайшем будущем. будущее. Все это работает на то, чтобы сделать нас более связанными, более управляемыми данными и более любопытными. Это будет захватывающая новая эра человеческого взаимодействия. Однако дороги в нашем сознании не улицы с односторонним движением. Получая информацию, люди одновременно отдают ее. информация и данные. В нынешнем виде простые строки кода однажды смогут идентифицировать и опишите все о нас. Наши привычки, наши друзья, наша вера, наша культура, наши предпочтения, и даже наши пороки. Впервые война не будет иметь дело с обнаженными телами. Он будет иметь дело с открытые умы вместо этого. Именно это новое направление войны мы назвали когнитивной войной.

# Эволюция некинетической войны

## Истоки

Она начинается, как и большинство вещей в природе современной войны, в период холодной войны. Взаимно заверено разрушения (MAD) стала общепринятой глобальной доктриной, представляя тотальную войну в масштабах Второй мировой маловероятна. Прокси-война превратилась в дискуссию за ужином. Подрывная деятельность и шпионаж преобладает в повседневных международных взаимодействиях, и «правдоподобное отрицание» является термином времени.

Таким образом, ЦРУ и ФБР расширили свои первоначальные возможности, и действия в тени стали нормой [3]. Эти новые методы стали «цивилизованным» подходом. к конфликту, явно лучше, чем «варварства» ядерной катастрофы. Также здесь находится *сила слов* и *идеи*, и некинетическая война, наконец-то проявляется в полную силу. Миллионы или даже миллиардов, убедился в этом, когда Советский Союз наблюдал за падением железного занавеса, не в силах выполнить свою цель — противостоять силе «синих джинсов и рок-н-ролла». [4]. демократический нации всегда имели «домашнее преимущество» в использовании голоса общественности. Способен рекламировать своих посланий о личных свободах и обильных ресурсах западные демократии последовательно использовали свои слова и идеи в качестве оружия против более авторитарных режимов.

Возможно, доказательством эффективности такой тактики является реакция, которую она вызвала у недемократические державы. Ограничения, запреты и всеобщая цензура уже давно стали политикой такие страны, как Китай, Россия и, что гораздо более радикально, Северная Корея. Возраст Интернет только усилил их опасения. Неудивительно, что Facebook и другие социальные сети платформы сталкиваются с ограничениями, если не с полным запретом, в этих и подобных странах по всему миру.

[5][6][7]. Однако именно эти идеалы свободы прессы и свободы слова оставили Демократическую нации уязвимы перед силами, пытающимися контролировать общественное мнение. Эти народы были вынуждены перейти к обороне, так как защита ресурсов и индивидуальных свобод больше не сохраняют ту же убедительность, что и когда-то. Мировая экономика видела как США, так и Китай процветает [8]. Однако самым важным изменением со времен холодной войны стал сдвиг в как мы общаемся и делимся идеями. Мы стремимся проиллюстрировать это изменение, рассказывая о прошлых сдвигах.

так, как люди боролись за умы и информацию, завершив новую эру и  
перспект войны.

## Психологическая война (PsyOps)

В Соединенных Штатах PsyOps конкретно относится к использованию белых, серых и черных продуктов, произведенных различными родами вооруженных сил и ЦРУ или его предшественниками. Белые продукты официально идентифицируемые как полученные из США, серые продукты имеют неоднозначный источник элемент, и черные продукты должны выглядеть так, как будто они происходят из враждебного источника. Операции включают в себя пропагандистское радио, предоставление руководств по неподчинению ополчение и даже поощрение детей-солдат дезертировать, чтобы избежать конфликта [9][10].

По сравнению с когнитивной войной существует немало ключевых отличий. Во-первых, когнитивная война работает в основном с серыми продуктами. Белые и черные продукты либо слишком прозрачны, либо слишком опасны быть надежными методами воздействия на общественное мнение. Кроме того, существует определенный элемент отрицание, присущее когнитивной войне, которая теряется в белых продуктах и подвергается опасности в черных товары. Более того, в прошлом PsyOps редко имел дело с широкими слоями населения. Есть акцент на военной или подрывной деятельности в PsyOps, которая обычно не является целью познавательного тактики ведения боевых действий, которые, как правило, нацелены на гражданскую социальную инфраструктуру и правительства [9].

## Электронная война (РЭБ)

РЭБ определяется использованием электромагнитного спектра для атаки противника, создания помех противнику. атаки или идентифицировать и искать определенные активы. В некотором смысле, радиоэлектронная борьба была предшественник кибервойны. Его происхождение восходит к 1900-м годам с изобретением ранней беспроводной связи. коммуникация. Инфракрасное самонаведение, радиосвязь и растущее использование беспроводной связи технологии делают это важным тыловым подразделением в вооруженных силах. Однако это поле имеет дело с инструментами и тактическими преимуществами. Это не относится к общественному высказывать мнение или даже активно взаимодействовать с гражданским пространством за пределами помех домашнему электричеству и радио [11][12].

## Кибервойна

Кибервойна определяется как использование кибератак с целью причинения вреда активы нации. Кибервойна и ее военная классификация до сих пор широко обсуждаются [13].

Тем не менее, многие государства-члены НАТО и другие страны вложили средства в разработку кибер-возможности, как наступательные, так и оборонительные [14][15]. Некоторых беспокоит определение таких действия как войну, потому что они нацелены «только» на компьютеры. Однако глобальная тенденция к оцифровка и Интернет вещей (IoT) означают, что теперь больше функций контролируется компьютеров, чем многие могли себе представить. Все, от строительного оборудования до финансовых институты, гражданская инфраструктура и даже военные объекты теперь зависят от сложного компьютерная сеть [16]. Потеря таких компьютерных активов может стоить и уже дорого обходится ущерб не только с точки зрения времени и потери данных, но и физического ущерба, который может быть измерен в долларов и жизней [17].

Связь кибервойны с когнитивной войной в основном состоит в том, что у них общий путь операций. Были случаи, когда компьютерные вирусы распространялись через социальные сети. ориентироваться на друзей и/или контакты пострадавшего. Однако эти экземпляры лучше описать как киберпреступления, а не целенаправленные попытки кибервойны. Когнитивная война использует социальные сети совершенно по-другому. Вместо распространения вредоносного программное обеспечение, агенты когнитивной войны распространяют злонамеренную информацию. Используя аналогичную тактику используемые в DDoS-атаках, а именно ботнеты, агенты когнитивной войны могут распространять подавляющее количество ложной или вводящей в заблуждение информации через учетные записи, которые смотрят и взаимодействуют по-человечески [18]. Однако это только одна тактика, используемая в когнитивной войне. во многом там, где сходство с кибервойной заканчивается.

## Информационная война

Информационная война является наиболее связанным и, следовательно, наиболее смешиваемым типом войны с когнитивная война. Однако есть ключевые отличия, которые делают когнитивную войну уникальной. достаточно обратиться в свою юрисдикцию. Как бывший командующий ВМС США Стюарт Грин описал его: «Информационные операции, наиболее близкая существующая американская доктринальная концепция для

когнитивная война состоит из пяти «возможностей корпуса», или элементов. К ним относятся электронные боевые действия, операции в компьютерных сетях, психологические операции, военный обман и оперативная безопасность».

[19]. Вкратце, информационная война работает, чтобы контролировать поток информации.

Основное различие между информационной войной и когнитивной войной заключается в том, что первая не проводит различия между тактической информацией поля боя и информацией, направленной на общественный. Например, информационная война имеет дело с DDoS-атаками и армиями-призраками, в то время как ни один из них не попадает в сферу когнитивной войны. Возможно, более четкое разграничение заключается в том, что информационная война стремится контролировать чистую информацию во всех формах, а когнитивная война стремится контролировать, как отдельные люди и популяции *реагировать* представленной информации [20].

## Когнитивная война

Недавнее определение от декабря 2019 года, предоставленное Оливером Бэkesом и Эндрю Свабом, Белферовский центр Гарварда определил когнитивную войну следующим образом: «Когнитивная война — это стратегия, фокусируется на том, чтобы изменить образ мышления целевой группы населения и, таким образом, то, как она действует». [21]. Несмотря на преднамеренной расплывчатости этого определения, оно служит более чем подходящей основой для дальнейшего изучения когнитивной войны. Наши собственные исследования и анализ прошлого, настоящего и потенциальные будущие варианты использования этого термина позволили нам далее разделить когнитивную войну на два операционных поля. Мы также составили краткий справочный список, чтобы проверить, действительно ли ничего не попадает в сферу когнитивной войны.

|                                             |                                 |                             |                       |                            |                                |
|---------------------------------------------|---------------------------------|-----------------------------|-----------------------|----------------------------|--------------------------------|
| Характеристика                              | психологический<br>Военное дело | Электронный<br>Военное дело | Кибер<br>Военное дело | Информация<br>Военное дело | познавательный<br>Военное дело |
| Использование массы<br>тренды/данные        |                                 |                             | Икс                   | Икс                        | Икс                            |
| Имеет дело с<br><b>МЫСЛИ И</b><br>поведение | Икс                             |                             |                       |                            | Икс                            |
| Емкость для<br>крайний<br>публичный доступ  |                                 |                             | Икс                   |                            | Икс                            |
| Интерес к<br>обращение<br>Информация        | Икс                             | Икс                         |                       | Икс                        | Икс                            |

Подводя итог, можно сказать, что когнитивная война *оружие общественного мнения по внешнему объекту*, за **целью влияния** общественная и/или государственная политика **или же** с целью **дестабилизирующий** правительственные действия и/или институты.

# Цели когнитивной войны

Когнитивную войну по своей сути можно рассматривать как имеющую ту же цель, что и любой тип войны. В качестве

Карл фон Клаузевиц утверждает: «Война [является] актом силы, направленным на то, чтобы заставить нашего врага исполнять нашу волю».

Когнитивная война, в отличие от традиционных сфер войны, в первую очередь не действует на физическом уровне.

самолет. Поэтому он не использует физическую силу, чтобы заставить своих врагов. Однако это

Можно также утверждать, что цель когнитивной войны не похожа на любой другой тип войны. Скорее

чем «заставить нашего врага исполнять нашу волю», цель состоит в том, чтобы заставить врага уничтожить себя изнутри

делая его неспособным сопротивляться, сдерживать или отклонять наши цели.

В любом случае цели когнитивной войны достигаются другими методами, чем

цели обычной войны. Когнитивная война преследует две отдельные, но дополняющие друг друга цели:

дестабилизация и влияние. Хотя обе эти цели могут быть достигнуты по отдельности,

успешно использовать общественное мнение в качестве оружия, их также можно достичь совместно, используя его как средство

к другому. Целями атак когнитивной войны могут быть как целые популяции, так и

отдельные лидеры в политике, экономике, религии и науке. Далее, роль

нельзя упускать из виду менее известных общественных лидеров. Так называемые коннекторы, знатоки и

продавцы могут сыграть важную роль в применении когнитивной войны [22].

Чтобы лучше классифицировать атаки когнитивной войны, на рис. 1 представлена пара осей, по которым события могут

быть охарактеризованы. В следующем разделе мы проанализируем каждую цель в отдельности и опишем

как они переплетаются, порождая новый, более опасный, более всеобъемлющий тип ведения войны.

Затем мы подробно рассмотрим примеры сражений и стычек когнитивной войны, которые произошли или

могут произойти в будущем. Эти кампании выведут когнитивную войну на новый уровень.

мировой этап. Необходимо принять меры, создать оппозиционные кампании и принять защитные меры.

реализованы, чтобы предотвратить успех преступников.

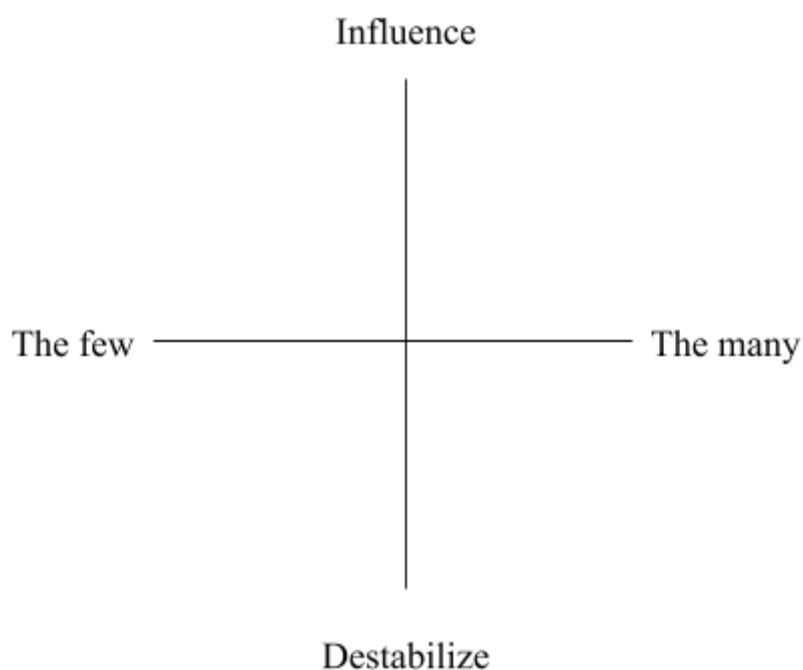


Рисунок 1. Пара осей, визуализирующих характеристики атак когнитивной войны

## Дестабилизация

Первая фундаментальная цель когнитивной войны — дестабилизировать целевые группы населения.

Дестабилизация осуществляется путем нарушения организации и единства систем населения и люди. Это приводит к резкому падению производительности и потере сотрудничества, поскольку это население теперь перегружено внутренними проблемами и меньше сосредоточено на достижении общих целей. преступники нарушить организацию и единство своих целевых групп населения, ускорив существовавшие ранее разделение внутри групп населения или внедрение новых идей, направленных на противопоставление различных группы друг против друга и усиливают поляризацию.

Лидеров можно рассматривать как объекты дестабилизации, когда они становятся источником поляризации. идеи. Преступники также могут нацеливаться на население в целом, чтобы случайным образом ввести разобщающие идеи, которые играют на ранее существовавших убеждениях или выдвигают ложные нарративы против групп

люди. Некоторые стратегии когнитивной войны, соответствующие целям дестабилизации, включают:  
но не ограничиваются следующим:

- Увеличить поляризацию
- Оживить движения/проблемы
- Делегитимация правительства/руководства
- Изолировать отдельных лиц/группы
- Прерывание ключевой экономической деятельности
- Нарушить инфраструктуру
- Запутать общение

Ниже приведены несколько случаев, демонстрирующих примеры дестабилизации как цели когнитивной войны.  
и окружающих их обстоятельств.

#### Случай 1: Дестабилизация из-за замешательства

Кампании когнитивной войны могут стремиться дестабилизировать популяции людей, вызывая массовые путаница. Хаос порождается, когда население больше не знает, что правильно и кому можно доверять. Как  
В результате гражданские лица могут начать терять веру в руководство нации, которое призвано контролировать  
их безопасности и свободы. Подрыв лидерства и создание хаоса представляет угрозу  
Западные демократии, один из самых свежих и ярких примеров, возникших в результате вспышки  
и ранние события, связанные с COVID-19.

Россия, Китай и Иран восприняли вихрь неразберихи, вызванный вирусом, как  
возможность начать кампанию когнитивной войны против Запада. Это разнонаправленный и  
многоплановая кампания, направленная на подрыв общественного доверия к западным государствам [23]. Этот  
Кампания началась со вспышки вируса и путаницы вокруг его происхождения, что  
где мы начали видеть инструменты когнитивной войны, такие как дезинформация и ложные нарративы,  
занят. Министр иностранных дел Китая Лицзянь Чжао засыпал вопросами в твиттере.  
с начала марта, направленный на США, с вопросом: «Когда в США появился нулевой пациент? Как много

люди заражены? Как называются больницы? Возможно, это армия США принесла эпидемии в Ухань» [24]. Затем он призвал последователей читать и распространять теорию заговора. с канадского веб-сайта Global Research, в котором говорится, что вирус возник в армии США.

Научно-исследовательский медицинский научно-исследовательский институт инфекционных заболеваний в Форт-Деррике, штат Мэриленд [24].

распространение этих нарративов практически без конкретных доказательств на таких ранних стадиях

Вирус функционировал только для того, чтобы посеять сомнения в умах американских граждан и их союзников. Эти инструменты когнитивной войны предназначены для того, чтобы влиять на то, как люди интерпретируют и реагируют на информацию в способ, который заставляет их сомневаться в собственном лидерстве.

Россия отреагировала таким же злонамеренным образом через свое государственное информационное агентство.

Спутник. Он выпустил пропаганду на более чем тридцати языках в соответствии со многими повествованиями.

из Китая, которые утверждали, что вирус возник в США или что США разработали и

выпустили вирус как биологическое оружие, предназначенное для ослабления экономики Китая [24]. Постоянная

поток ложных повествований варьировался от несколько правдоподобных историй до диковинных обвинений

нацелены на западные государства и правительственные организации. В этом заключается опасность познавательного

кампании: становится все труднее различать заслуживающие доверия и не заслуживающие доверия

истории, особенно когда они исходят от поддерживаемых правительством новостных сайтов, таких как Sputnik.

Кремль может рассылать тысячи разных историй с разным уровнем достоверности и

правдоподобие и посмотреть, что палочки. Эта стратегия быстро приводит к подрыву западной

правительства в том, что население может расценить как недостаток честности по отношению к своему народу в отношении

вируса или невозможность защитить их от него.

Иран является третьим крупным игроком, проводящим собственную кампанию когнитивной войны против граждан.

западных государств. Новостные сообщения, появляющиеся из Тегерана, содержали темы, похожие на сюжеты

выходя из Пекина и Москвы. Press TV — это англо-французская новостная сеть, связанная

с Радиовещательной компанией Исламской Республики Иран, которая выпустила многочисленные материалы, связывающие

Вспышка коронавируса среди военных США [24]. Командир Исламского революционера

Корпус гвардии Хоссейн Салами зашел так далеко, что заявил, что COVID-19 является острием биологическое вторжение США [24].

## Познавательные кампании Китая, России и Ирана вокруг вспышки коронавируса

все они нацелены против западных государств и содержат почти идентичные сообщения. Опасность в эти кампании являются их огромным охватом и поддержкой со стороны государственных лидеров и учреждений.

Подобные истории выпускаются на десятках языков по всему миру и выходят напрямую государственных новостных сайтов или поддерживаемых государством СМИ [24]. Но это только

происхождения, с десятками тысяч независимых сайтов и пользователей, распространяющих одни и те же

намеренно или нет, подрывают доверие к западным обществам. американцы

находить эти истории снова и снова и поощрять верить, что их правительство скрывает

информация от них. Или они перегружены историями, которые заставляют их сомневаться в национальной

способность защитить их от серьезных угроз их безопасности и личным свободам. Угроза не

только в информации, которая распространяется, а в дестабилизирующих реакция и убеждениях тех,

получая их.

## Случай 2: Дестабилизация посевным отделом

Когнитивная война часто направлена на разделение населения и усиление поляризации. Существующие ранее

разделение по линии политических партий может показаться наиболее очевидным для использования. Однако это

не всегда так, поскольку когнитивные кампании могут быть направлены на то, чтобы посеять внутренние разногласия внутри группа. Мы видим яркий пример этого в случае утечки электронной почты DNC 2016 года.

Россия несколько десятилетий тренировала свои кибервозможности, экспериментируя со странами

Европа, например Украина, чтобы проверить свое влияние на выборах. Как директор службы национальной безопасности

Организация и командующий Кибернетического командования США, адмирал Майкл Роджерс заявил: «Это было

это не было сделано случайно, это не была цель, выбранная чисто произвольно.

Это было сознательное усилие национального государства для достижения определенного эффекта» [25]. И у него был

сильное влияние на DNC и Демократическую партию в целом.

В апреле 2016 года российские киберподразделения получили доступ к внутренним серверам DNC, что позволило им для кражи конфиденциальных электронных писем и документов. Несколько месяцев спустя эти сообщения были просочились на WikiLeaks. Именно в этот момент операция из типичного шпионажа превратилась в политический саботаж. Кампании были свернуты, и внутри партии начал расти раскол. Выяснилось, что DNC поддерживал Хиллари Клинтон во время, предшествовавшее выбору. официального кандидата в президенты. Это превратило прогрессивных демократов и умеренных демократов в друг против друга. Раскол внутри демократической партии привел к смещению позиций кандидатов. поддерживать. Вместо того чтобы сосредоточиться на самом нападении русских, политические деятели были гораздо более обеспокоены содержанием и тем, что это может означать для их карьеры [26]. Избиратели начали меняться из-за проблем, поднятых этими новыми документами и опубликованными заявлениями о недовольстве. Кампания Хиллари Клинтон признала, что эта атака оказала значительное влияние на исход всеобщие выборы [23]. И это не значит, что не было дальнейшего поляризующего воздействия на линии партии, а также. Кампания президента Трампа также обратилась к содержанию хакерских атак. а не само нападение русских. В то время, когда страна не могла позволить себе реагировать партизанским путем две основные партии повернулись друг против друга и против самих себя, в результате чего одна из самые поляризованные этапы американской политики.

Российская атака выходит далеко за рамки акта кибервойны. Кибервозможности и отсутствие надлежащая безопасность была просто инструментами и возможностями, которые сделали атаку возможной. само нападение, однако, было направлено на гораздо большую цель, которая была достигнута с честью.

Американская политика пришла в упадок, и теперь Россия имеет влияние в двух самых важные институты американской демократии: выборы и независимые СМИ [25].

разногласия, возникшие и обострившиеся в результате этого события, дестабилизировали политику и избирательный процесс.

К сожалению, средства массовой информации были только взволнованы, чтобы освещать выпускаемый контент. при этом WikiLeaks был самым популярным политическим термином в октябре 2016 года [25].

Это была именно та реакция, на которую рассчитывала Россия. Их познавательная кампания была идеально нацелены на использование разногласий в американской политике и привели к обвинению и неопределенность.

### Кейс 3: Дестабилизация как средство воздействия

Виновные в когнитивной войне могут вызвать дестабилизацию, чтобы повлиять на членов населения, убеждая их, что их правительство не может обеспечить их. Исторически, экономическая мощь всегда была важным источником рычагов для наций, стремящихся вымогать борющиеся народы. Такое экономическое превосходство можно использовать с помощью санкций. Согласно теории дестабилизации и нечувствительности санкций, санкции — это «манипулирование экономическими отношениями в политических целях, направленные на угрозу или исполнение экономического наказания, чтобы заставить общество изменить свою политику или свое правительство». Есть два типа санкций согласно этой теории: принудительные и манипулятивные. В этом случае будем дальше изучать манипулятивные санкции, направленные против общества целевой страны. Цель такой санкции заключается в том, чтобы «оттолкнуть общественность от лидеров до такой степени, что последние теряют свои влиятельные позиции». Результатом является смена политики или правительства в результате отягощенного населения. В недавнем прошлом имели место случаи применения санкций против других государств. Объясняется дестабилизацией не только экономики страны, но и ее социальной и политической также ситуация [27].

Возьмем, к примеру, режим Альенде в Чили. Американское общественное мнение было против открытого применения силы против чилийского правительства. Вскоре было решено, что лучший способ свергнуть чилийское правительство значило бы возложить вину за деградирующую нацию на неполноценную социалистическую политику. Американское правительство приняло двойной подход к дестабилизации правительства Чили, нападая как на чилийскую экономику, так и на общество. Экономический натиск спровоцировал множество факторов. Американское правительство закрыло все частные американские инвестиции, новые и старые. Кроме того, американское правительство использовало свою беспрецедентную силу на мировой арене, чтобы удержать международные финансовые институты от финансирования любых чилийских операций. Это оказало решающее влияние на жизнь чилийцев как основной отрасли промышленности Чили. Меди, доминировали американские транснациональные корпорации [27].

Хотя эти изменения и оказали пагубное влияние на чилийскую экономику, спад не может дестабилизировать положение нации сам по себе. Возьмем, к примеру, Кубу. Соединенные штаты проводил столь же жесткую экономическую политику для борьбы с Кастро и его социалистическим режимом. Однако простого использования экономической зависимости недостаточно, чтобы дестабилизировать всю правительство, что подтверждается настойчивостью Кубы благодаря экономическим усилиям Америки. Кубинцы в время привыкло к скудным ресурсам и репрессивной экономической политике. Напротив, Чили имели хорошо зарекомендовавший себя средний класс, который зависел от потребительской культуры для поддержания своего уровня жизни. Альянде признавал стандарты среднего класса, а также их зависимость от Соединенных Штатов в гораздо большем количестве областей, чем просто экономика, и пытались удовлетворить на запросы среднего класса. Однако вскоре ему стало трудно поддерживать средний уровень. стандарты класса из-за американского экономического возмездия, и уровень жизни резко упал. Вскоре чилийский народ убедился, что их нынешнее правительство некомпетентно в руководства своей страны. Таким образом, падение чилийского правительства не было результатом экономическое давление со стороны Соединенных Штатов, а скорее социальные последствия последующий экономический спад[27].

По сути, Соединенные Штаты дестабилизировали экономическую систему, чтобы повлиять на население. поверить, что их правительство не может предоставить им такую же возможность. В результате такого влияние, чилийское правительство было свергнуто капиталистическим режимом без всякой вины. повернут против американских чиновников. Осуществляя разрушительную экономическую политику, Америка изменили мыслительные процессы всего населения, едва пошевелив пальцем. Санкции вызвало сомнение, сомнение зародилось в чилийском народе, и сомнение превратилось в возмездие. Это это молчаливое сшивание недоверия посредством манипуляций и превращения общественного мнения в оружие, что определяет когнитивную войну.

Помимо изображения последствий дестабилизации как средства воздействия, это дело также подчеркивает необходимость понимания входов и выходов целевой группы населения. Без полного понимания карьера в вопросе, невозможно провести эффективную атаку. Хотя подобная стратегия использовалась против Кубы, она не дала желаемого эффекта, потому что США не

учитывать отсутствие среднего класса. В нападении важно понимать цель. Для защиты необходимо знать, как ваше население может быть использовано.

С появлением Интернета способность преступника понимать население только возросла. сильнее. С помощью нескольких щелчков мыши кто-то может найти все, что нужно знать о месте и его людях. Этот неограниченный доступ приведет к возникновению подобных угроз в еще большем масштабе. Когда Никсон проводил эту экономическую политику, у него не было доступа к информации, которая могла бы ему помочь. что он будет работать в Чили, но не на Кубе. Теперь, с обширными историческими базами данных, Интернет поисковых систем, а главное, хакеров, информация о любой целевой группе может быть легко получить и использовать. Например, если бы Соединенные Штаты хотели нацелиться на страну, аналогичную в Чили было бы несложно собрать информацию о размере среднего класса и о том, является ли он была достаточно велика, чтобы обеспечить эффективное восстание. До интернета единственный способ узнать было бы поехать в Чили и познакомиться с культурой, которая выглядела бы подозрительно с самого начала. Теперь представитель американской разведки может просто провести поиск по экономическое демографическое распределение Чили, и у них будет информация, необходимая для провести эффективную атаку.

## Влияние

Вторая фундаментальная цель когнитивной войны — воздействовать на целевые группы населения. Цель влияние достигается за счет манипулирования интерпретацией и пониманием объекта мир вокруг них. Преступники могут впоследствии направлять действия своей цели таким образом, чтобы приносит пользу правонарушителю. Цель воздействия отличается от цели дестабилизации в что конечная цель состоит в том, чтобы целевая группа придерживалась единомышленников по проблеме. В наибольшей степени потенциала, преступники стремятся достичь консенсуса среди населения, обладающего достаточной властью, чтобы произвести сдвиг парадигмы, обратив свои цели против фундаментальных идей, на которых они были воспитаны.

Чтобы повлиять на мышление всего населения или сегментов населения, преступники могут

политические, экономические, академические или общественные лидеры в качестве векторов для охвата большей аудитории.

В качестве альтернативы преступники могут просто обнародовать информацию, закинув широкую сеть в надежде

охват достаточного количества людей, чтобы спровоцировать изменения. Ситуации, когда методы когнитивной войны могут быть использованы для оказания влияния, включают, но не ограничиваются следующим:

- Пропагандировать экстремистские идеологии
- Манипулировать гражданскими убеждениями
- Контролировать ключевые виды экономической деятельности
- Регулировать действия правительства
- Влиять на выборы или делегитимировать их
- Вербуйте мирных жителей в маргинальные группы
- Подавить инакомыслие

Ниже приведены несколько случаев, демонстрирующих, как можно вести когнитивную войну, чтобы повлиять на популяции и условия, окружающие каждый случай.

### Случай 1: влияние на вербовку

Кампании когнитивной войны могут быть запущены с целью вербовки гражданских лиц в дело, как это можно видеть в случае с террористическими группами. Понятие «идеологический двигатель» описывает стратегию когнитивной войны, в которой «абстрактные мотивирующие факторы сходятся воедино, чтобы произвести насилие». идеологии» [21]. Эта модель использовалась террористической группировкой «Аль-Каида» на Ближнем Востоке. Модель продвигается так называемыми «идентификационными предпринимателями»: общественными лидерами, которые не обязательно имеют большое влияние в политических или экономических институтах, но способны сопереживать и связаться с обычными членами своего целевого общества. Идентификационные предприниматели могут вербовать гражданских лиц в экстремистские идеологии, представляя нарратив, в котором избиратели обозначены как главные герои, которые улучшат общество. Эти лидеры могут нацеливаться на мирных жителей в бедных условиях жизни, убеждая их в том, что они не одиноки, что они не виноваты в своих бедность, и что виноват реальный угнетатель. В случае с «Аль-Каидой» выбранный повествование рассказывало историю падения ислама от величия и считало новобранцами тех, кто вернут их земле ее первоначальное процветание. Соответствует большинству других когнитивных войн стратегии, идеологический двигатель наиболее эффективен, когда он подпитывается *ранее существовавший* чувства против предполагаемого угнетателя.

Предприниматели, занимающиеся идентификацией, закладывают основу для акторов насилия, готовя почву для атаки на выявленный угнетатель. Стратегически террористы выбирают цель насильственной атаки, чтобы быть учреждением, вероятно, слишком остро отреагирует и применит чрезмерную силу в ответ. Такая реакция позволяет повстанцам, чтобы представить предполагаемого угнетателя в негативном свете, оправдать свое дело перед гражданскими лицами, усилить поляризацию и морально изолировать предполагаемого угнетателя. Аль-Каида сделала этот шаг провоцируя США насильственными действиями, такими как взрывы посольств США и сентябрьские 11 атак. Отсюда последовала многолетняя «война с террором», которая привела к значительным жертвам среди гражданского населения. **жертв, что дает повстанцам возможность очернить Запад.**

На заключительных стадиях таких кампаний террористы переносят рамки своей борьбы на контексте национального, культурного или религиозного долга. Таким образом, отказ человека присоединиться к сопротивлению против предполагаемого угнетателя рассматривается как предательство общественных ценностей. общества продолжают бороться не за материальную выгоду, как они, возможно, делали изначально, а за защиту идеологии. Один раз идеологический двигатель достигает этой стадии, избиратели были успешно внушены идеология личности предпринимателей.

По мере развития технологий и роста охвата Интернета идеологический двигатель будет только расти. сильнее. Взаимосвязанность обществ позволит террористическим организациям создавать глобальные сети и выходить за пределы национальных границ. Как заявил Стюарт Грин, основатель модель идеологического двигателя, «Повстанческие кампании перешли от военных кампаний, поддерживаемых от информационных операций до стратегических коммуникационных кампаний, поддерживаемых партизанскими и террористическими операциями» [19]. В эту новую эру войны физический план больше не является доминирующим. сфера, с помощью которой преступники принуждают свои цели действовать в соответствии с их волей. Вместо этого физ. насилие используется для поддержки идеологий и поддержки сражений в новейшей области войны: в сознании каждая цель.

## Случай 2: влияние на принятие политики

Методы когнитивной войны имеют большой потенциал для влияния на политику. Амбициозная нация, стремящаяся расширить свое влияние в глобальном масштабе, выиграет от мировой сверхдержавы, такой как США, приняв изоляционистскую внешнюю политику. Например, в последние месяцы Китай проводил экспансионистскую внешнюю политику, о чем свидетельствует его враждебность на китайско-индийской границе и в Южно-Китайском море [28]. Для того, чтобы действовать более агрессивно без возмездия, преступник, спонсируемый Китаем, может нацелиться на широкую общественность США с целью манипулирование гражданскими лицами с целью оказания давления на их избранных представителей, чтобы они сосредоточили свое внимание на себе и уменьшить внешнее участие.

Этот тип вмешательства в политику другой страны требует, чтобы целью была общественность, а не политики, потому что, хотя у политиков есть власть, гражданские лица должны одобрять их Действия представителей. Как было установлено ранее, цель когнитивной войны состоит в том, чтобы изменить как цели воспринимают реальность. Даже если политиков принуждали к принятию законов или решения в пользу иностранной державы, любой функционирующий представительная демократия, если гражданские лица не верят в такое дело. Такая кампания была бы особенно коварным, поскольку преступник будет действовать в обход международных организаций и типичные дипломатические сообщения, направленные непосредственно на граждан.

Для того, чтобы этот тип кампании когнитивной войны увенчался успехом, должны существовать уже существующие изоляционистские чувства, которые можно использовать. Атака когнитивной войны была бы более эффективной, если бы, например, целевая нация имела историю неудачной внешней политики или недавнее национальное смущение на мировой этап. Особое внимание уделяется этому условию, поскольку когнитивная война извлекает выгоду и процветает существующие предубеждения и взгляды. Преступнику значительно труднее посеять семена идею в миллионах голов, чем культивировать и взращивать глубоко укоренившиеся чувства. Хотя Китай, Иран и другие региональные державы могут не иметь таких возможностей и ресурсов, как когнитивная война. Российские, вполне вероятно, что они их разрабатывают. Было бы опасно недооценивать других нации как соперники в когнитивной сфере.

### Случай 3: Влияние как средство дестабилизации

Влияние может быть использовано как средство дестабилизации, когда определенные слои населения поощряются или принуждаются к принятию и продвижению определенных взглядов, особенно против взглядов других группы внутри населения. Ярким примером когнитивной войны является русское вмешательство в выборы за границей. Такие атаки являются частью более широкой кампании по снижению доверия к демократические страны во всем мире, ослабляя Запад. Впервые встречается в странах Балтии — Эстонии, Латвия и Литва — с тех пор раздавались обвинения и предупреждения России о расширении ее усилия западных держав, таких как Соединенные Штаты, Великобритания и Германия. Предполагается, что конечной целью России является вывод из строя ее противников, позволяющий ей расширить его глобальный охват. Отвлекая и поляризуя общественность в тылу западных сверхдержав, западные государства вынуждены обратиться внутрь себя, чтобы исправить беспорядок, вызванный обвинения в иностранном вмешательстве или сговоре в их выборах. С их вниманием в другом месте, такие государства могут потерять авторитет на мировой арене или оказаться не в состоянии защитить себя или своих союзников от российской агрессии. Для достижения такой цели Москва должна убедить народам демократических стран, что их правительства и избирательные системы не заслуживают доверия и незаконный. Таким образом, дестабилизация посредством воздействия.

Страны Балтии были особенно уязвимы для усилий России по когнитивной войне из-за нескольких факторы. Эстония, Латвия и Литва уникальны своей географической близостью к России, исторические связи с нацией, русское этническое население и доступ жителей к русскому языку подконтрольные государству СМИ. Воспользовавшись этими факторами, Россия запустила информационный операций против стран Балтии с момента восстановления их независимости в 1990-х гг. Москва сосредоточены на временах уязвимости, особенно на выборах, во время которых российские СМИ источники поддержали три сообщения: правительства стран Балтии были фашистами и симпатизировали нацистам; Балтика правительства были неэффективны в управлении; и страны Балтии были дискриминационными по отношению к этнические русские [21]. Такое оформление превратило значительные группы этнических русских, проживающих в Прибалтики против других граждан. Использование российских государственных СМИ и российских троллей в социальных сетях Москва могла распространять дезинформацию, подстрекательскую информацию,

и пропаганда. Воспользовавшись существующими предубеждениями, Москва обострила напряженность и еще больше поляризовал общественность Эстонии, Латвии и Литвы. Хотя западные страны не имеют таких же условий и уязвимых мест, как прибалты, у них есть уязвимые места, тем не менее. Имея опыт использования иностранных подразделений, чтобы влиять на мышление граждан, и голосовать — Россия сможет использовать аналогичную коварную тактику против западных стран.

Учитывая данное нами определение когнитивной войны, действия России отвечают Условия такой атаки. Установлено, что преступником является российское правительство и целью является широкая американская общественность. Этот случай классифицируется как дестабилизация с помощью влияния, потому что Москва пытается убедить людей не в определенных политических взглядах, а двух разделяющих понятий: сограждане оппозиционной политической партии опасны, а выборы целостность не может быть гарантирована. В последние годы такие настроения пережили всплеск. Избиратели по обе стороны политического спектра становятся все более поляризованными, что увековечивает менталитет «мы против них». Уже есть и демократы, и республиканцы, которые считают другая сторона предаст идеалы нации. Российские интернет-тролли и боты только расширились пропасть.

Концепция все большей поляризации демократов и республиканцев получила название «трайбализм» [29]. Избиратели начали относиться к политике как к командному виду спорта, отдавая приоритет партийной лояльности над политикой. Избиратели более склонны перерастать разногласия в споры и распространять вера в то, что любая идея, не выгодная для чьей-либо партии, должна быть нападением на них. Считается, что Россия использовали эти разногласия между демократами и республиканцами в прошлом.

На выборах 2016 года Москва провела свою самую масштабную когнитивную войну. Вмешательство Кремля в выборы 2016 года было сложным и коварным, направленным против многих аспекты американской политики, как видно из *Случай 2 из Дестабилизация*. Как уже упоминалось, американский спецслужбы установили, что президент России Владимир Путин отдал приказ о частном электронные письма из кампании Клинтон будут просочены, а боты в социальных сетях будут созданы для распространения экстремистские взгляды и противоречивые новости. Спустя почти три года, 18 августа 2020 г., Сенат США

опубликовал отчет, в котором говорится: «Комитет установил, что российское правительство участвовало в агрессивные, многогранные попытки повлиять или попытаться повлиять на итоги 2016 г. президентские выборы» [30]

Успеху этой атаки способствовали три основных фактора. Первый,

тогдашний кандидат от республиканцев Дональд Трамп не осудил Путина, когда его спросили, что он думает о возможности вмешательства России в выборы 2016 года. До Трампа мейнстрим

Американские политики последовательно и однозначно считали Россию угрозой для Америки.

Напротив, Трамп подчеркнул содержание просочившихся документов из Демократической партии.

Национальное собрание в связи с тем, что американский политический институт подвергся нападению со стороны иностранная власть. Во-вторых, Москва имела доступ к просочившимся электронным письмам еще до прихода Хиллари Клинтон.

выдвижение кандидатом от Демократической партии. Если бы был выдвинут другой кандидат, утечки может быть не так эффективно. В-третьих, президент Обама, демократ, не решался раскрыть

разведку или нанести ответный удар без одобрения республиканцев. Администрация Обамы была обеспокоен тем, что обнародование такой разведывательной информации незадолго до выборов может показаться

партизан, как будто сами пытались манипулировать выборами. Таким образом, условия

Президентские выборы 2016 года создали идеальный шторм для расчетливой атаки когнитивной войны на

назначить американского президента, который не будет категорически против российского вмешательства, создать хаотическую отвлечение внимания на политической сцене и разделение американцев по партийным признакам.

Чтобы подчеркнуть серьезность этой ситуации: расследования показали, что Кремль заказал

кибератака на американскую политическую организацию с целью кражи внутренних документов и

сообщения с намерением использовать их, чтобы настроить общественное мнение против этого

вечеринка организации. В предыдущие месяцы перед важными президентскими выборами Кремль

продолжал сливать украденные документы общественности, обеспечивая разногласия и посев сомнение в умах американцев относительно целостности их политических институтов.

Кроме того, Россия предприняла усилия по распространению раскольнической риторики, покупая рекламу в социальных сетях.

платформы, создание учетных записей в социальных сетях и создание нарративов для поляризации избирателей. Москва имеет

нашел метод эксплуатации самой основы функционирующей демократии: дискурс между

разнообразный спектр мнений. Новые технологии сделали эту кампанию возможной, так как армии  
Российские интернет-тролли подстрекают избирателей по обе стороны политического спектра, батальоны  
Российские боты распространяют дезинформацию и подстрекательские новости, а легионы российских хакеров  
получать и выпускать порицающие материалы.

# Будущие угрозы

## Заглядывая вперед

До сих пор мы описали несколько случаев, когда западные нации и институты пришли к под когнитивной атакой. Когнитивная война опасна в ее нынешнем виде, но истинная угроза кроется в своем будущем потенциале. Нейронаука, психология и социология находятся в зачаточном состоянии в великой Схема человеческих инноваций. Все эти науки получили развитие благодаря достижениям вычислительная мощность и возможность моделировать большое количество соединений и сценариев. Социология особенно столкнулась с революцией с появлением социальных сетей. Сама социальная сеть оказался чрезвычайно адаптируемым и быстрым в своей эволюции. Последние десять лет стали свидетелями взлет и падение более чем пяти различных платформ социальных сетей с сотнями миллионов, если не миллиарды пользователей. По мере того как ученые все ближе и ближе подходят к пониманию того, как мы думаем, как мы взаимодействуем друг с другом, как мы получаем мотивацию и, в конечном счете, кто мы как люди, мы становятся все более уязвимыми для тех, кто пытается использовать эти идеи.

Кроме того, мы представили доказательства того, что противники НАТО более чем готовы и уметь пользоваться этими методами. Они также продемонстрировали, что у них есть возможность использовать эти ресурсы и достижения. В конечном счете, мы считаем, что это будут не негосударственные субъекты, которые ведут кампании когнитивной войны, но государственные деятели. Хотя негосударственные субъекты могут использовать методы когнитивной войны, у них нет ресурсов для поддержания кампании, которая может длиться поколения. Пример такой кампании описал советский перебежчик Юрий Бесменов. в интервью 1984 года, который заявил, что идеологическая подрывная деятельность — это процесс «[изменения] восприятие действительности каждым американцем, что, несмотря на обилие информации, никто не способны прийти к разумным выводам в интересах защиты себя, своих семей, своих сообщества и своей страны» [31]. Безменов подробно рассказал, как проходил первый этап идеологическая диверсия — деморализация — занимает от 15 до 20 лет. Эти десятилетия кампании теперь могут быть сокращены до нескольких лет из-за достижений в области социальных технологий. Они

стало легче планировать, исполнять и скрывать. Если НАТО планирует сохранить саму реальность, она должны подготовиться и отомстить тем, кто ведет когнитивную войну.

Не нужно думать дальше президентских выборов в США 2020 года, чтобы увидеть потенциал для катастрофы. За месяцы до выборов уже были внутренние обвинения с обеих сторон прохода относительно легитимности предстоящих выборов.

Нынешний президент Дональд Трамп выразил обеспокоенность тем, что система голосования по почте отстаиваемой Демократической партией, может привести к «фальсификации результатов выборов». Когда его спросили, будет ли он уважая результаты выборов 2020 года в случае его поражения, он ответил: «Я должен увидеть. Нет я не собирается просто сказать да. Я не собираюсь говорить «нет», указав вышеперечисленные опасения как причину своего трепет [32]. Возмущенные этими заявлениями возглавили Демократическую партию, обвинившую его в попытка подорвать демократический процесс.

С другой стороны, демократы, как общественные, так и официальные, критиковали выборы в США. процесс, который привел к избранию Трампа президентом в 2016 году. В частности, эта критика взимаемый с коллегии выборщиков, которая дала Трампу президентское кресло, несмотря на его поражение в народном голосовании. Эта критика спровоцировала членов Республиканской партии, которые выступают за ценность Коллегия выборщиков в американской избирательной системе и власть, которую она дает малым штатам.

Независимо от того, кандидат от какой партии избран, партия проигравшего кандидата может использовать это. замешательство и недоверие, чтобы поставить под сомнение законность процесса голосования. Это эти Москва может использовать уже существующие разногласия. В распространении дезинформации и раздувании пламени политического раскола Америки, Россия снабдила каждую сторону боеприпасами, и они скорее всего воспользуюсь.

Крупные технологические компании, такие как Facebook, уже определили «очень сложные» Российские и иранские операции по вмешательству в выборы. 21 октября 2019 года Facebook объявил что он удалил четыре «сети учетных записей, страниц и групп» из социальных сетей.

платформу, идентифицировав троих как иранцев, а одного – из России. Неаутентичный

пользователи в этих сетях маскируются под местных жителей в районах, на которые они нацелены, и распространяют

дезинформация и пропаганда [33]. Поскольку выборы быстро приближаются, эти усилия будут

расширен. Для дальнейшей защиты от попыток когнитивной войны информационная безопасность должна быть

укреплять, иностранным ботам и троллям нельзя давать трибуну, а доверие к демократическому

система должна быть усилена. Ниже приведены некоторые из угроз, которые наша команда считает многообещающими.

в будущем когнитивной войны. Это не исчерпывающий список, а скорее

представление о том, как агенты когнитивной войны могут достичь целей, описанных в

предыдущие разделы. Он также обеспечит основу для областей, которыми НАТО будет заниматься.

двигаться вперед в борьбе с когнитивной войной.

## Угроза 1: Простота отбора и виральность

Недавний успех TikTok объясняется его удивительными алгоритмическими способностями. Каждое видео

предоставляется пользователям, которые, скорее всего, «взаимодействуют» с контентом посредством комментариев, лайков, обмена или

просто просмотр. Основная цель такого алгоритма — это, конечно же, максимизировать время просмотра и рекламу.

доход [34]. Однако он имел беспрецедентный успех. TikTok сам должен вставлять уведомления

напоминая зрителям периодически спать или выходить из службы [35]. Он также создал

среду, в которой пользователи могут обмениваться контентом и организовывать его с единомышленниками на

молниеносная скорость. Всего за несколько дней TikTok может создать подсообщества, которые объединятся для продвижения реформ,

собирают деньги на цели или даже организовывать и планировать протестную деятельность [36].

Это не означает, что TikTok обладает уникальными или невозпроизводимыми возможностями. Реальность такова, что

каждая существующая социальная сеть пытается улучшить свои алгоритмические рекомендации,

и все видели недавний успех. Если бы не TikTok, другая платформа социальных сетей просто бы

в конце концов наткнулась на аналогичные уровни алгоритмической технологии. Алгоритмический

Однако рекомендации — не единственный способ создания «вирусного» контента. Недавние исследования

в модели распространения пандемии помогли лучше понять «парадокс дружбы» или

«эффект суперпользователя». Эпидемиологические исследования неизменно показывают, что распространение

информация, или вирус, на самом деле в основном связаны с гораздо меньшим количеством жизненно важных «узлов».

Оказывается, во всех сетях человеческих связей есть несколько, за неимением лучшего термина, популярных люди, которые служат точкой привязки для многих других людей, которые имеют гораздо больше ограниченный круг общения. Было показано, что эти «суперпользователи» обладают беспрецедентным уровнем контроль за распространением информации и болезней [37]. Китай, в частности, уже разместил ресурсы в выявлении и выяснении того, как связаться с этими людьми [38].

В конечном счете, по мере того, как эти сети становится легче идентифицировать и использовать, возникает реальная угроза внешние силы, нацеленные на группы риска, у которых теперь есть инструменты для быстрой организации. Этот может быть опасным, например, в случае преследования бесправных политических групп. Может быть хуже, например, в случае нападения на семейную ячейку военнослужащих, особенно те, кто моложе или имеют другие факторы риска. Или это также может быть критическим, например, в случай воздействия на лиц с существующими психическими расстройствами. Особенно те из бредовые или параноидальные наклонности. В Интернете есть поговорка, что «интернет-время» бежит быстрее, чем время реального мира из-за того, как быстро распространяется информация, а тенденции растут и падают. Например, одна неделя в реальном мире может показаться годом в Интернете. По мере распространения вируса увеличивается количество информации, будет меньше предупреждений для властей. Система предупредительного оповещения есть отчаянно нуждался в том, чтобы отреагировать на эти невероятно быстрые целевые кампании.

## Угроза 2: Новый век истины

Растет интерес к возможности создавать контент, который можно выдать за истинный. Это видно по фейковым статьям, которые уже некоторое время распространяются в соц. медиа сети. Однако следующее поколение этого поддельного контента вызывает гораздо большее беспокойство. «Deepfakes» — это видео, которые пытаются создать иллюзию того, что человек делает или говорит что-то с технологией трансплантации лица. Эти видеоролики могут быть очень убедительными, и технологии только совершенствуются с течением времени. Bloomberg и PBS опубликовали примеры за последние два года, демонстрирующие быстрое развитие технологий [39][40]. Кроме того, аудиоверсии этой же технологии подделки, такие как так называемая Приложение искусственного интеллекта «Лирохвост» также получает дальнейшее развитие [41]. Сети социальных сетей, такие поскольку Facebook и TikTok уже запустили кампании по запрету дипфейкового контента [42].

Однако это решение — лишь повязка на симптомы более крупной проблемы. Беспокойство в том, что даже если поддельный контент отозван или удален, исправления и отмены не достигают всех, кто просмотрели исходный контент, так как им не хватает того же «вирусного импульса». Так как эти технологии должны быть объединены усилия по разработке точных алгоритмов обнаружения или некоторых другая форма защиты, которую мы должны применить быстро.

### Угроза 3: Институциональный дискомфорт и недоверие, вызванные киберпространством

Страны НАТО чрезвычайно продуктивны, чего и следовало ожидать от стран с одними из самых сложных социальных систем в мире. Каждый божий день граждане полагаются на экономические, медицинские и судебные учреждения должны эффективно работать для сохранения порядка и комфорта. Таким образом, чтобы нарушить этот порядок и комфорта, кибератаки, как правило, нацелены на эти самые учреждения в показательной манере. А стимул больницы восстановить свои цифровые данные и компьютерную мощность гораздо более актуален, чем те из типичной частной компании [43]. Однако существует альтернативный сценарий, когда эти кибератаки имеют те же цели, но более коварны по своим методам и целям.

Уже есть заявления о том, что эти общественные институты дискриминируют людей на основании социально-экономический статус, раса, религия и другие факторы. Можно было бы легко использовать кибермир для укреплять эти убеждения. Возможно, целевая часть населения испытывает сбой: ничего критичного, но раздражает и беспокоит. Эти небольшие ошибки могут вызывать тревогу из-за их близость к важной информации. Потерянный документ или платеж, неверные данные, возможно даже тревожные заметки или директивы, которые могли означать нечто большее. Исследования уже показывают, что как только информация становится испорченной, люди теряют доверие ко всему документу или системе [44]. Один можно увидеть, как эти эффекты могут быть усилены, если поддержка фальшивых новостей заявит об этих сбоях. быть преднамеренными попытками подрывной деятельности со стороны правительства. Недоверие может распространяться из больниц, банкам и даже судам. Если целевая группа выбрана тщательно, это может быстро дестабилизировать и без того ненадежную веру людей в влияние правительства учреждения.

## Угроза 4: Биологическая и терапевтическая эмоциональная манипуляция

Рекомендации и лечение в области психического здоровья недавно привлекли внимание международного сообщества.

сцена. Существуют различные захватывающие разработки в этой области, которые могут произвести революцию в том, как мы просматривать и лечить психические заболевания. Например, транскраниальная магнитная стимуляция (ТМС). метод использования магнитных полей для стимуляции нервных клеток при лечении симптомов депрессия [45]. Транскраниальная стимуляция постоянным током (TDCS) является родственной областью, которая применяется электрический ток на кожу головы в надежде стимулировать нервные клетки, расположенные близко к черепу, другой метод, разрабатываемый для лечения депрессии [46]. Также работают терапевты и психиатры. вместе с разработчиками приложений, чтобы придумать приложения-инструменты для лечения синдрома дефицита внимания, посттравматического стрессового расстройства, депрессия и тревога. Некоторые из них уже вышли на рынок с положительными отзывами. [47].

Несмотря на это, есть много опасений по поводу скорости внедрения некоторых из этих технологий. разрабатываются, особенно темпы их коммерциализации. ТДКС в частности относительно легкий по конструкции и эксплуатации. Различные продукты уже существуют в рынок, см. Muse [48], а требуемые детали таковы, что некоторые подростки в социальных сетях медиа-сайт Reddit уже успел сделать свои домашние версии. Это последний аспект что особенно смущает. TDCS все еще активно исследуется и разрабатывается, особенно в том, что касается функции мозга несовершеннолетних. Различные ученые и исследователи выразил беспокойство по поводу такого развития событий и призвал к более строгим правилам коммерческой деятельности. предприятия. Некоторые сообщения от первого лица о повышенном раздражении, замешательстве и гневе уже известны. порождены этими домашними версиями и коммерческими предприятиями [46]. Аналогично, в то время как некоторые терапевтические приложения спонсируются сертифицированными специалистами в области психического здоровья, пространство далеко от регулируется.

Все это говорит о том, что более прямые методы изменения когнитивного убеждения и настроения доступны на рынке таким образом, чтобы их можно было легко перехватить. Эти прямые методы

также имеют тенденцию иметь дело с группами риска, такими как ветераны с посттравматическим стрессовым расстройством, с помощью терапевтических приложений или

впечатлительные подростки, создающие домашние комплекты TDCS. Иностранная держава могла легко заполнить терапевтическое приложение с «плохими» советами очень опасными способами, или они могли загрузить немного «неправильный» TDCS руководства и инструкции на Reddit. Хотя это не обязательно мощное само по себе, это может быть за которой следует целенаправленная атака когнитивной войны, чтобы воспользоваться измененным состоянием. Если кто-то действительно понимал, что они делают, результаты могли быть заметными и ужасающими.

## Угроза 5: расширенный набор агентов

Общественное мнение трудно предсказать и управлять им. Системы, которые связывают людей друг с другом может быть чрезвычайно сложным. Однако мы уже показали, что некоторые люди в этих обширные сети имеют большее влияние, чем другие. Фактически, чтобы увидеть влияние некоторых из этих лицам, вам нужно только открыть приложение Twitter. Существуют различные формы влиятельные лица, которые теперь имеют более тесные связи с общественностью, чем когда-либо прежде. Образовательный, экономические, культурные, религиозные и политические лидеры недавно получили трибуны для публички в таких масштабах, которые были бы немыслимы еще десять лет назад. Во многих отношениях это также сделал влияние на общественное мнение намного проще, чем когда-либо прежде, сократив количество цели, с которыми приходится идти на компромисс, чтобы воздействовать на массовое мышление.

Индивидуально-специфическая когнитивная война связана с попыткой «вербовать» или скомпрометировать эти отдельных лиц в попытке вооружить общественное мнение своей аудитории. Церковь Саентология, классифицируемая некоторыми членами НАТО как опасный культ, уже продемонстрировала важность вербовки элиты и знаменитостей для пропаганды и легитимации определенных идеи и убеждения [49][50]. Новая угроза в этом небольшом количестве целей заключается в том, что прямой контроль над разумом становится все более опасной перспективой.

Существуют косвенные методы достижения этого. Синтетические дизайнерские наркотики более популярны, чем когда-либо, и их можно сделать невероятно увлекательными [51]. Привлечение знаменитости к наркотику заставляет для убедительного стимула. Более прямым методом было бы имплантирование электрических или оптогенетических стимуляторы в головном мозге. Хотя известные исследования этого прямого метода все еще находятся в крайней в младенчестве результаты испытаний на животных были невероятно убедительными. Например, ученые

удалось создать ложные воспоминания о страхе у мышей. Ученые поместят мышь в коробку А. Затем они удалят мышь, но пометят пространство памяти с помощью изображения. Затем они поместите его в коробку В и ударьте по нему током, одновременно стимулируя нейроны, связанные с блок А через оптогенетический рецептор. Когда мышь помещается обратно в коробку А, она останавливается в страх, создав ложное впечатление, что он уже испытал шок внутри ящика А. Ложное воспоминание в настоящее время создан [52]. Пользность, влияние и опасность этой технологии в когнитивной сфере. военные кампании невозможно переоценить. Конечно, имплантация электродов или оптогенетическая рецепторов в головном мозге — задача не из легких, особенно если добиться этого нужно скрытно и точно. Тем не менее, прямой характер этой манипуляции делает риск, заслуживающий внимания. чрезвычайно тесно в области когнитивной войны.

## Рекомендации по стратегии

Как указывалось выше, попытки повлиять на общественность не новы. Политики, генералы, рынок лидеры и другие влиятельные лица используют риторику, пропаганду и обмен сообщениями, чтобы годами манипулировать общественным мнением. Что нового, так это инструменты для этого, а затем достижения, которого можно достичь. Интернет, социальные сети и круглосуточный новостной цикл позволяют постоянные потоки информации, облегчающие воздействие на человеческий разум, и свободы, предоставленные гражданам стран-членов НАТО, облегчают это. Либерал, западным демократиям не только не хватает понимания когнитивной войны, они также более восприимчивы к быстро развивающейся угрозе и не готовы к ней. Чтобы переломить ход этой битвы, НАТО должна работать на различных уровнях альянса, чтобы определить и измерять когнитивные угрозы, оценивать уязвимости своих членов и ставить ключевые группы с инициативы по смягчению и реагированию на когнитивные кампании против организации.

## Структура и критерии распознавания угроз

Первый вопрос, который НАТО должна задать, когда имеет дело с когнитивной войной, заключается в том, откуда мы знаем когда нас атакуют? Чтобы ответить на этот вопрос, необходимо предпринять два шага: во-первых, добавить когнитивной войны в более широкую международную структуру ведения войны, и, во-вторых, разработка набора критериев, чтобы установить, когда когнитивная атака действительно имеет место.

Текущие международные определения ведения войны проистекают из доктрин эпохи после Второй мировой войны, а именно Устав ООН. В уставе есть два основных раздела, которые определяют пределы ведения войны. и теперь являются причиной путаницы. Статья 2(4) запрещает «угрозу силой или ее применение против территориальная целостность или политическая независимость любого государства»; Статья 51 допускает «самооборону, если происходит вооруженное нападение на члена Организации Объединенных Наций». [53]. Статьи были написаны во времена, когда летальная кинетика была главным инструментом войны [54]. С тех пор достижения и зависимость от вычислительной мощности и Интернета позволили появиться крупным масштабировать когнитивную войну, оставив такие термины, как «применение силы» и «вооруженное нападение», непригодными для

инкапсулировать угрозу. Другие военные доктрины, также подвергающиеся сомнению, - это доктрины отличия и соразмерность: как следует проводить различие между гражданскими и военными субъектами и как соответственно следует реагировать на когнитивную атаку [55]. Путаница позади как руководящие органы определяют современную войну, позволили врагам угрожать безопасности и стабильности стран-членов НАТО. По этой причине НАТО необходимо разработать свод правил или структуры, чтобы можно было определить акты некинетической войны и соответствующим образом отреагировать на них. Одна из лучших попыток сделать это исходит от структуры Шмитта, которая является попыткой отделить киберпреступления от кибервоенных действий [56]. Такой каркас может быть адаптирован для разработки юридических определений и показателей для когнитивных военных действий.

Вторая часть этой проблемы заключается в том, чтобы выяснить, когда акт когнитивной войны фактически происходит. Одно из самых больших различий между когнитивной войной и другими формами некинетической войны заключается в том, что эти другие методы часто требуют от противника передачи информации на население. С помощью когнитивной войны люди будут сталкиваться не только с «атаками», безобидно, как случайные сообщения или твиты, они затем начнут активно искать информацию, которая подтверждает их убеждения. Это похоже на разницу между выталкивающим и вытягивающим маркетингом. С ИИ и машинного обучения, технологические компании создали алгоритмы, предназначенные для удержания нашего внимания. Теперь враждебно настроенные актеры взломали код и могут создавать нарративы и истории. Использование данных для манипулирования большими массами населения без ведома читателя. Прежде чем НАТО сможет предпринять шаги по борьбе с последствиями когнитивной войны, она должна упреждающий подход к выявлению атак и разработке основы для дифференциации случайных онлайн-мнение из более крупной и коварной познавательной кампании.

## Оценка рисков

Следующий вопрос, на который НАТО должна ответить, заключается в том, насколько уязвим альянс? Это потребует более глубокое погружение не только в саму НАТО, но и в каждую из ее стран-членов. Начиная с Альянса, НАТО следует обратить внимание на любые подразделения или группировки, которые противник может использовать потенциально ослабить или даже разрушить альянс. После этого НАТО следует проанализировать каждый из его страны-члены и партнеры, чтобы увидеть, могут ли какие-либо предстоящие события и существующие разногласия быть

цели и инструменты для когнитивной атаки соответственно. Понимая состояние члена стран альянса, НАТО может активно работать над выявлением угроз, проектированием стратегии смягчения последствий и создание встречных нарративов в надежде предотвратить крупномасштабный хаос до того, как это начнется.

Меньшая, второстепенная часть этой оценки риска должна проводиться на личном уровне. Технологии, в частности, Интернет вездесущ в 21 веке. При использовании и освоении этих технологии увеличились, а просвещение об опасностях — нет. По этой причине НАТО следует поощрять граждан внутри альянса к формированию собственной личной устойчивости к когнитивным атаки. Первым шагом в этом направлении могло бы быть создание исследования, информирующего граждан о важности или опасности соответствующих тем, включая, помимо прочего, предвзятость в СМИ, проверка фактов, угрозы эхо-камер, конфиденциальность в Интернете и информационная безопасность. По повышению осведомленности об этих возможных опасностях, граждане в идеале предпримут шаги для защиты себя от будущих угроз и атак, которые исходят от связи, вызванной нашим зависимостью от техники.

## Организационные реализации

Третий вопрос, на который НАТО должен ответить, заключается в том, кому следует поручить управление и решение проблемы когнитивной войны? Технологии, психология и неврология — все началось формировать будущее войны; НАТО и администрации стран-членов должны реорганизоваться соответственно, если они хотят вести своих граждан в безопасное и надежное будущее. Первым шагом в этом является найти место для задач когнитивной войны в НАТО, будь то подразделение в Emerging Security Challenges Division или нечто большее [57]. Кроме того, НАТО и ее союзники должны создать когнитивные организации в рамках своей правоохранительной и военной организации с каналами связи, действующими через альянс, филиалы военными, а также между правительством и местными правоохранительными органами. Обязанности этих подразделений должен быть тройным: во-первых, установить текущее состояние альянса в борьбе с когнитивными атаками путем разработки схемы нападения и завершения оценки уязвимости НАТО и ее члены; во-вторых, чтобы подготовиться к ожидаемым когнитивным атакам перед важными событиями, такими как

выборы и общенациональные протесты; и, наконец, исследовать когнитивные атаки, чтобы установить нарушителя и выработать соответствующий ответ. Эта последняя обязанность может быть разделена с отдел общественной дипломатии, чтобы раскрыть общественности атаки в надежде создать более когнитивно-устойчивая популяция [58]. Помимо этого, отдел общественной дипломатии следует работать над созданием исследований в СМИ и в центре внимания, посвященных личной уязвимости и смягчение когнитивных атак против самого себя.

Еще одна второстепенная проблема, которая поднималась в этом документе, — это и растущая техническая неграмотность стран-членов. Правительства больше не могут делать вид, что они осведомлены и осведомлены о возможностях и угрозах, связанных с эволюцией технологии, и они больше не могут позволить себе отчуждать крупные технологические конгломераты, поскольку они продолжают получить власть и контроль над рынками и средствами массовой информации. Правительство должно найти способ сотрудничать с Facebook, Google и Microsoft по всему миру. Для этого член страны могут либо пойти по стопам Дании и создать офис технической дипломатии, или создать всеобъемлющий пост или офис, которому поручено поддерживать связь с кремниевыми долинами мире [59]. Например, одной из обязанностей этой организации будет установление юрисдикции при рассмотрении дезинформации на платформах социальных сетей. В настоящее время регулирование социальных сетей в западном мире разделено между правительством и СМИ. компании с несколькими определяемыми линиями. Хотя пока это может работать, технология постоянно развивается, а технологические компании набирают силу и влияние. Позволяя им единоличное регулирование конкретных сообщений на сайтах СМИ может создать опасный прецедент в будущем. За По этим причинам технические представители должны работать с медиа-конгломератами, чтобы установить правила и юрисдикции по конкретным делам, особенно когда распространение информации потенциально может угрожают здоровью человека, как это наблюдается во всем мире, с распространением ложных методов лечения коронавируса и теории заговора.

## Наступательные соображения

Все вышеперечисленные меры связаны с подготовкой и защитой от когнитивных атак, но есть

по-прежнему является наступательной стороной для рассмотрения. Существуют определенные факторы, которые можно использовать для создания

основу для разработки наступательных стратегий. Первое из них — понимание

типа войны, которая имеет место. Если это гибридная война, в которой когнитивная война

часть более крупной наступательной стратегии, когнитивные методы могут быть не лучшими методами ведения боя,

и страны, возможно, пожелают рассмотреть другие стратегии, такие как кибернетика и смертоносная кинетика, если

абсолютно необходимо. Если происходящая война — это в значительной степени война познания, то первый шаг в

Определение стратегии заключается в понимании целей кампании, как они определены в *Цели*

*Когнитивная война* раздел этой статьи. Как только цели поняты, становятся возможными векторы

яснее. Другой частью стратегии является понимание геополитического положения

врага, чтобы найти точки давления для нацеливания. Важными факторами здесь могут быть центры

богатство и власть, структура инфраструктурных систем, структура отрасли и лидеры СМИ

источники, основные фракции внутри страны и юридические лазейки. Лучше понимая эти ключевые

болевы точки, стратегии и тактики могут раскрыться и помочь уравнивать правила игры.

войны познания.

## Заключительные мысли

В своем выступлении на открытии программы «НАТО-2030» Генеральный секретарь Йенс Столтенберг подтвердил: «Поскольку мы продолжать конкурировать в более конкурентном мире, мы должны сохранять силу наших демократий». [60].

При решении повседневных задач новых форм ведения войны, будь то кибернетические или познавательные, НАТО не должно упускать из виду эндшпиль. До сих пор Запад, а именно США принял доктрину «защиты вперед» [61]. Это означает превентивное предотвращение и упреждающий поиск атак, не переходя в наступление. Аргументация: НАТО и

США считают, что они должны оставаться в рамках международных законов и правил, чтобы оставаться на высоком дипломатическом уровне. репутации и предотвращения посягательств на свободы и демократию во всем мире [61].

Враги НАТО в настоящее время меньше озабочены своим международным положением. Их цели показать, что демократия не является правдоподобным решением мировых проблем. Если на Западе привычно по умолчанию занимает оборонительную позицию, это может привести к игре в кошки-мышки, в которой НАТО и ее участники попадают в ловушку. Таким образом, НАТО должно ответить на следующий вопрос: как мы можем не только предотвращать, но сдерживать когнитивные атаки будущего, оставаясь непоколебимым примером свободы и демократии для остального мира? Вероятно, это будет основной военно-дипломатический вызов 21 века.

## Библиография

- [1] Гринемайер, Ларри. «В поисках адреса: почему кибератаки так сложно отследить до хакеров». *Научный американец*, 11 июня 2011 г., [www.scientificamerican.com/article/tracking-cyber-hackers/](http://www.scientificamerican.com/article/tracking-cyber-hackers/).
- [2] Торбет, Джорджина. «3 неопровержимые причины, почему вам нужна онлайн-анонимность». *MakeUseOf*, 3 апреля 2020 г., [www.makeuseof.com/tag/3-undeniable-reasons-need-online-anonymity/](http://www.makeuseof.com/tag/3-undeniable-reasons-need-online-anonymity/).
- [3] «Эволюция разведывательного сообщества США — исторический обзор». *ФАС*, Федерация американских ученых, 23 февраля 1996 г., [fas.org/irp/offdocs/int022.html](http://fas.org/irp/offdocs/int022.html).
- [4] Маккарти, Бриджит. «Как рок-н-ролл разрушил Советский Союз». Под редакцией Лизы Маллинз, *Мир от PRX*, Международное общественное радио, 19 мая 2011 г., [www.pri.org/stories/2011-05-19/how-rock-and-roll-brought-soviet-union-down](http://www.pri.org/stories/2011-05-19/how-rock-and-roll-brought-soviet-union-down).
- [5] Цукки, Кристина. «Почему Facebook запрещен в Китае и как получить к нему доступ». *Инвестопедия*, 22 октября 2019 г., [www.investopedia.com/articles/investing/042915/why-facebook-banned-china.asp](http://www.investopedia.com/articles/investing/042915/why-facebook-banned-china.asp).
- [6] Талмадж, Эрик. «Северная Корея блокирует Facebook, Twitter и YouTube». *Глобальные новости*, Ассошиэйтед Пресс, 4 апреля 2016 г., [globalnews.ca/news/2616449/north-korea-blocks-facebook-twitter-and-youtube/](http://globalnews.ca/news/2616449/north-korea-blocks-facebook-twitter-and-youtube/).
- [7] Сомин, Илья. «Facebook должен прекратить сотрудничество с российской государственной цензурой». *Вашингтон Пост*, Компания WP, 21 декабря 2014 г., [www.washingtonpost.com/news/voikh-conspiracy/wp/2014/12/21/facebook-should-stop-cooperating-with-russian-government-censorship/](http://www.washingtonpost.com/news/voikh-conspiracy/wp/2014/12/21/facebook-should-stop-cooperating-with-russian-government-censorship/).
- [8] Моррисон, Уэйн М. «Экономический подъем Китая: история, тенденции, проблемы и последствия для Соединенных Штатов». *EveryCRSReport*, Исследовательская служба Конгресса, 25 июня 2019 г., [www.everycrsreport.com/reports/RL33534.html](http://www.everycrsreport.com/reports/RL33534.html).
- [9] «Психологические операции: доктрина BBC 2-5.3». Под редакцией Тимоти А. Киннана, *Ивар*, BBC США, 27 августа 1999 г., [www.iwar.org.uk/psyops/resources/us/afdd2-5-3.pdf](http://www.iwar.org.uk/psyops/resources/us/afdd2-5-3.pdf).
- [10] Селигман, Лара. «Кризис детей-солдат: «Дети дешевы»». *Внешняя политика*, 8 ноября 2019 г., [Foreignpolicy.com/2019/11/08/child-soldier-crisis-kids-are-cheap-yemen-isis-my-star-sky/](http://Foreignpolicy.com/2019/11/08/child-soldier-crisis-kids-are-cheap-yemen-isis-my-star-sky/).
- [11] Рэмбо. «История радиоэлектронной борьбы». *Блогспот*, 7 декабря 2009 г., [ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html](http://ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html).
- [12] «Электронная война: совместная публикация 3-13.1». Под редакцией Уильяма Э. Гортни, *ФАС*, Объединенный комитет начальников штабов, 8 февраля 2012 г., [fas.org/irp/doddir/dod/jp3-13-1.pdf](http://fas.org/irp/doddir/dod/jp3-13-1.pdf).
- [13] «Кибервойна — существует ли она?» *Обзор НАТО*, НАТО, 13 июня 2013 г., [www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html](http://www.nato.int/docu/review/articles/2013/06/13/cyberwar-does-it-exist/index.html).

- [14] Гренобль, Райан. «Трамп отменяет правила эпохи Обамы в отношении кибератак». *ХаффПост*, 17 августа 2018 г., [www.huffpost.com/entry/trump-cyberattack-directive-20\\_n\\_5b758f76e4b0df9b093d1b06](http://www.huffpost.com/entry/trump-cyberattack-directive-20_n_5b758f76e4b0df9b093d1b06).
- [15] «Великобритания — глобальная кибердержава, — говорит директор GCHQ». Под редакцией Джереми Флеминга, *GCHQ*, 25 февраля 2019 г., [www.gchq.gov.uk/news/the-uk-is-a-global-cyber-power--says-director-gchq](http://www.gchq.gov.uk/news/the-uk-is-a-global-cyber-power--says-director-gchq).
- [16] Низкий, Винсент. «Тенденция к цифровизации». *Сержант Канон*, Канон, 2020, [sg.canon/en/campaign/business-insight/ambassador/the-trend-towards-digitisation](http://sg.canon/en/campaign/business-insight/ambassador/the-trend-towards-digitisation).
- [17] Бреннер, Сьюзан В. и Лео Л. Кларк. «ГРАЖДАНСКИЕ ЛИЦА В КИБЕРВОЙНЕ: ПОТЕРИ». *Law.UPenn*, Юридический факультет Кэри Пенсильванского университета, июль 2010 г., [www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/BrennerClarke.pdf](http://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/BrennerClarke.pdf).
- [18] Коста-Робертс, Даниэль. «Вот как обнаружить русского бота». *Мать Джонс*, 1 августа 2018 г., [www.motherjones.com/media/2018/08/how-to-identify-russian-bots-twitter/](http://www.motherjones.com/media/2018/08/how-to-identify-russian-bots-twitter/).
- [19] Грин, Стюарт А. «Когнитивная война». *Авгиевы конюшни*, Объединенный колледж военной разведки, июль 2008 г., [www.theaugeanstables.com/wp-content/uploads/2014/04/Green-Cognitive-Warfare.pdf](http://www.theaugeanstables.com/wp-content/uploads/2014/04/Green-Cognitive-Warfare.pdf).
- [20] Бернс, Меган. «Информационная война: что и как?». *CS.CMU*, Университет Карнеги-Меллона, 1999 г., [www.cs.cmu.edu/~burnsm/InfoWarfare.html](http://www.cs.cmu.edu/~burnsm/InfoWarfare.html).
- [21] Бэкс, Оливер и Эндрю Сваб. «Когнитивная война: российская угроза честности выборов в странах Балтии». Документ, Белферовский центр науки и международных отношений, Гарвардская школа Кеннеди, ноябрь 2019 г.
- [22] Гладуэлл, Малкольм. *Переломный момент: как маленькие вещи могут иметь большое значение*. Абак, 2000.
- [23] Эпштейн, Диана и Джон Д. Грэм. «Поляризованная политика и политические последствия». *РЭНД*, RAND Corporation, 26 августа 2007 г., [www.rand.org/pubs/occasional\\_papers/OP197.html](http://www.rand.org/pubs/occasional_papers/OP197.html).
- [24] Мшвидобадзе, Хатуна. «Пропаганда трио пандемии: как Китай, Россия и Иран нацелены на Запад». *ГФСИС*, Фонд Рондели, 23 апреля 2020 г., [www.gfsis.org/blog/view/1067](http://www.gfsis.org/blog/view/1067).
- [25] Липтон, Эрик и др. «Идеальное оружие: как российская кибермощь вторглась в США» *Нью-Йорк Таймс*, Нью-Йорк Таймс, 13 декабря 2016 г., [www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html](http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html).
- [26] Юхас, Алан. «Кампания Хиллари Клинтон возлагает вину за утечку электронных писем Национального комитета Демократической партии США о Сандерсе на Россию». *Хранитель*, Guardian News and Media, 24 июля 2016 г., [www.theguardian.com/us-news/2016/jul/24/clinton-campaign-blames-russia-wikileaks-sanders-dnc-emails](http://www.theguardian.com/us-news/2016/jul/24/clinton-campaign-blames-russia-wikileaks-sanders-dnc-emails).
- [27] Мером, Гил. «Демократия, зависимость и дестабилизация: потрясение режима Альенде». *Политология ежеквартально*, том. 105, нет. 1, 1990, стр. 75–95., doi: 10.2307/2151226.
- [28] Челлани, Брахма. «Китайский экспансионизм вступает в опасную фазу». *Холм*, 25 авг. 2020 г., [thehill.com/opinion/international/513574-chinas-expansionism-enters-dangerous-phase](http://thehill.com/opinion/international/513574-chinas-expansionism-enters-dangerous-phase).

[29] Пакер, Джордж и др. «Новый отчет предлагает взглянуть на трайбализм в эпоху Трампа». *Ньюйоркер*, The New Yorker, 13 октября 2018 г., [www.newyorker.com/news/daily-comment/a-new-report-offers-insights-into-tribalism-in-the-age-trump](http://www.newyorker.com/news/daily-comment/a-new-report-offers-insights-into-tribalism-in-the-age-trump).  
- Трампа.

[30] «ОТЧЕТ ИЗБРАННОГО КОМИТЕТА ПО РАЗВЕДКЕ СЕНАТА США О РОССИЙСКИХ АКТИВНЫХ МЕРАХ КАМПАНИИ И ВМЕШАТЕЛЬСТВЕ В 2016 Г. ВЫБОРЫ В США». *Intelligence.senate.gov*, Сенат, 2020 г., [www.intelligence.senate.gov/sites/default/files/documents/report\\_volume5.pdf](http://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf).

[31] Гриффин, Эдвард Г. и Юрий Безменов. «Советская подрывная деятельность в отношении прессы свободного мира». Доступ 1984.

[32] Уоллес, Крис. «Стенограмма: воскресное интервью Fox News с президентом Трампом». *ФоксНьюс*, FOX News Network, 19 июля 2020 г., [www.foxnews.com/politics/transcript-fox-news-sunday-interview-with-president-trump](http://www.foxnews.com/politics/transcript-fox-news-sunday-interview-with-president-trump).

[33] Розен, Гай. «Помогая защитить выборы в США в 2020 году». *О Facebook*, Фейсбук, 21 октября 2019 г., [about.fb.com/news/2019/10/update-on-election-integrity-efforts/](https://about.fb.com/news/2019/10/update-on-election-integrity-efforts/).

[34] Мацакис, Луиза. «Как на самом деле работает алгоритм TikTok «Для вас»». *Проводной*, 18 июня 2020 г., [www.wired.com/story/tiktok-finally-explains-for-you-algorithm-works/](http://www.wired.com/story/tiktok-finally-explains-for-you-algorithm-works/).

[35] Берк, Кэролайн. «Новое экранное время TikTok предлагает напомнить пользователям сделать передышку». *суматоха*, 19 фев. 2020, [www.bustle.com/p/tiktoks-new-screen-time-prompts-remind-users-to-take-a-breather-21816527](http://www.bustle.com/p/tiktoks-new-screen-time-prompts-remind-users-to-take-a-breather-21816527).

[36] Герман, Джон. «TikTok формирует политику. Но как?» *Нью-Йорк*, The New York Times, 28 июня 2020 г., [www.nytimes.com/2020/06/28/style/tiktok-teen-politics-gen-z](https://www.nytimes.com/2020/06/28/style/tiktok-teen-politics-gen-z).

[37] Кристакис, Николас А. и Джеймс Х. Фаулер. «Датчики социальных сетей для раннего обнаружения вспышек инфекционных заболеваний». *ПЛОС ОДИН*, об. 5, нет. 9, сентябрь 2010 г., стр. 1–8. *EBSCOhost*, doi:10.1371/journal.pone.0012948.

[38] Хуанг, Джойс. «Китайская технология отслеживания вирусов вызывает опасения по поводу конфиденциальности». *Воаньюс*, Голос Америки, 22 июня 2020 г., [www.voanews.com/covid-19-pandemic/chinas-virus-tracking-technology-sparks-privacy-concern](http://www.voanews.com/covid-19-pandemic/chinas-virus-tracking-technology-sparks-privacy-concern).

[39] Тертон, Уильям и Эндрю Мартин. «Как дипфейки делают дезинформацию более реальной, чем когда-либо: QuickTake». *Блумберг*, 7 января 2020 г., [www.bloomberg.com/news/articles/2020-01-06/how-deepfakes-make-disinformation-more-real-than-ever-quicktake](https://www.bloomberg.com/news/articles/2020-01-06/how-deepfakes-make-disinformation-more-real-than-ever-quicktake).

[40] О'Брайен, Майлз. «Почему «глубокие фейки» становится все труднее обнаружить». *PBS*, Служба общественного вещания, 12 июня 2019 г., [www.pbs.org/newshour/show/why-deepfake-videos-are-becoming-more-difficult-to-detect](http://www.pbs.org/newshour/show/why-deepfake-videos-are-becoming-more-difficult-to-detect).

- [41] *лирохвост*, 2020, [www.descript.com/lyrebird](http://www.descript.com/lyrebird).
- [42] Шед, Сэм. «Facebook запретит «глубокие подделки»». *BBC*, Британская радиовещательная корпорация, 7 января 2020 г., [www.bbc.com/news/technology-51018758](http://www.bbc.com/news/technology-51018758).
- [43] «Кибератаки: в секторе здравоохранения». *СНГБезопасность*, Центр интернет-безопасности, 27 сентября 2019 г., [www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/](http://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/).
- [44] Бернал, Алонсо и Дженнифер Окерман. «Главный инженер по когнитивным системам в Лаборатории прикладной физики Университета Джона Хопкинса». 20 июля 2020 г.
- [45] «Транскраниальная магнитная стимуляция». *Клиника Майо*, Фонд медицинского образования и исследований Майо, 27 ноября 2018 г., [www.mayoclinic.org/tests-procedures/transcranial-Magnetic-stimulation/about/pac-20384625](http://www.mayoclinic.org/tests-procedures/transcranial-Magnetic-stimulation/about/pac-20384625).
- [46] Анита Джва, Ранние последователи магического мышления: исследование сообщества пользователей транскраниальной стимуляции постоянным током (tDCS) «сделай сам» (DIY), *Журнал права и биологических наук*, Том 2, выпуск 2, июль 2015 г., страницы 292–335, <https://doi-org.proxy1.library.jhu.edu/10.1093/jlb/lsv017>
- [47] Трушель, Джессика. «25 лучших приложений для психического здоровья на 2020 год: альтернатива терапии?» *Псайком*, 13 августа 2020 г., [www.psycom.net/25-best-mental-health-apps](http://www.psycom.net/25-best-mental-health-apps).
- [48] «Медитация стала проще». *Муза*, 24 августа 2020 г., [Chooseemuse.com/](http://Chooseemuse.com/).
- [49] Саппелл, Джоэл и Роберт Уэлкос. «Ухаживание за могущественными посредниками». *Латимес*, Los Angeles Times, 27 июня 1990 г., [www.latimes.com/local/la-scientology062790a-story.html](http://www.latimes.com/local/la-scientology062790a-story.html).
- [50] Макмастер, Джефф. «Некогда процветающей церкви Саентологии грозит вымирание, — говорит Cult Tracker». *Фолио*, 11 января 2018 г., [www.folio.ca/once-thriving-church-of-scientology-faces-extinction-says-cult-tracker/](http://www.folio.ca/once-thriving-church-of-scientology-faces-extinction-says-cult-tracker/).
- [51] «Расширяющийся рынок синтетических наркотиков». *УНП ООН*, Управление Организации Объединенных Наций по наркотикам и преступности, 23 марта 2020 г., [www.unodc.org/documents/scientific/Global\\_SMART\\_23\\_web2.pdf](http://www.unodc.org/documents/scientific/Global_SMART_23_web2.pdf).
- [52] Нунан, Дэвид. «Познакомьтесь с двумя учеными, которые внедрили ложную память в мышь». *Смитсоновский журнал*, Смитсоновский институт, 1 ноября 2014 г., [www.smithsonianmag.com/innovation/meet-two-scientists-who-implanted-false-memory-mouse-180953045/](http://www.smithsonianmag.com/innovation/meet-two-scientists-who-implanted-false-memory-mouse-180953045/).
- [53] «Устав ООН». *Un*, Организация Объединенных Наций, 26 июня 1945 г., [www.un.org/en/sections/un-charter/un-charter-full-text/](http://www.un.org/en/sections/un-charter/un-charter-full-text/).
- [54] Бьенвеню, Эмили и др. «Когнитивная война». *Коув.армия*, Бухта, 19 сентября 2018 г., [cove.army.gov.au/article/cognitive-warfare](http://cove.army.gov.au/article/cognitive-warfare).
- [55] «ОСНОВНЫЕ ПРИНЦИПЫ ВОЕННОГО ПРАВА И ИХ ПОСЛЕДСТВИЯ ДЛЯ НАЗНАЧЕНИЯ». *Doctrine.af.mil*, Curtis E. Lemay Center, 15 марта 2019 г., [www.doctrine.af.mil/Portals/61/documents/Annex\\_3-60/3-60-D33-Target-LOAC.pdf](http://www.doctrine.af.mil/Portals/61/documents/Annex_3-60/3-60-D33-Target-LOAC.pdf).

- [56] Фольц, Эндрю С. «Stuxnet, анализ Шмитта и дебаты о кибер-использовании силы». *Ндупресс.нду*, Издательство Университета национальной обороны, 2012 г.,  
[ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67\\_40-48\\_Foltz.pdf](http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf).
- [57] НАТО. «Новое подразделение НАТО для решения возникающих проблем безопасности». *НАТО.int*, НАТО, 4 августа 2010 г., [www.nato.int/cps/en/natolive/news\\_65107.htm](http://www.nato.int/cps/en/natolive/news_65107.htm) .
- [58] «Коспонсорские гранты отдела общественной дипломатии НАТО». *НАТО.int*, НАТО, 6 декабря 2018 г.,  
[www.nato.int/cps/en/natohq/63610.htm](http://www.nato.int/cps/en/natohq/63610.htm) .
- [59] *Офис технического посла Дании*, 2020, [techamb.um.dk/](http://techamb.um.dk/).
- [60] Столтенберг, Йенс. «Замечания Генерального секретаря НАТО Йенса Столтенберга по поводу запуска # NATO2030 — Укрепление Североатлантического союза в условиях растущей конкуренции». *НАТО.int*, НАТО, 8 июня 2020 г., [www.nato.int/cps/en/natohq/opinions\\_176197.htm?selectedLocale=en](http://www.nato.int/cps/en/natohq/opinions_176197.htm?selectedLocale=en) .
- [61] Салмейер, Майкл и Пол М. Накасоне. «Как конкурировать в киберпространстве». *Иностранные дела*, 25 августа 2020 г., [www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity](http://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity) .