Информационное общество и СМИ

# «КИБЕР ПЁРЛ-ХАРБОР» В СМИ США И РОССИЙСКО-АМЕРИКАНСКИЕ ОТНОШЕНИЯ 2001–2014 ГГ.

Статья рекомендована к публикации главным редактором Т.В. Ершовой 21.09.2022.

**Левин Ярослав Александрович**

*Кандидат исторических наук*
*Самарский государственный технический университет, кафедра «Философия и социально-гуманитарные науки», доцент*
*Самара, Российская Федерация*
*yaroslavlevin1992@mail.ru*

**Аннотация**

*Такое историческое событие, как нападение японского флота на американскую военную базу в бухте Пёрл-Харбор имело огромное значение и, помимо чисто политических последствий, оставило заметный след в культуре Соединённых Штатов. В рамках данной статьи предпринята попытка рассмотреть одну из трансформаций сформировавшегося медиа-шаблона, а именно, «Кибер Пёрл-Харбор» – идею и публицистический троп о внезапной мощной хакерской атаке на важные для США объекты. На конкретных примерах рассмотрено, как сформировалась эта конструкция, как применялась СМИ и актуализировалась политиками. Помимо этого, также рассмотрено, как данная конструкция использовалась медиа и политическими деятелями в контексте сложных и многообразных отношений России с США. Статья базируется на литературе и источниках по теме.*

**Ключевые слова**

*«Кибер Пёрл-Харбор»; СМИ; США*

## Введение

События 7 декабря 1941 г. в бухте Пёрл-Харбор оказали огромное влияние на историю США. Включение Америки во Вторую мировою войну, усиление геополитических позиций этой страны в мире и противостояние США и СССР на протяжении всей второй половины XX века оказали большое влияние на всю сферу культуры, на средства массовой информации и международные отношения [1, p. 23].

Поэтому не удивительно, что метафора Пёрл-Харбора стала достаточно устойчивым и повторяющимся сочетанием в медиадискурсе США, в разное время возвращаясь как значимая конструкция, применяемая прессой и другими СМИ Соединённых Штатов по отдельным особо важным и острым темам, как способ мотивировать и, возможно, подстегнуть усилия политиков по тем вопросам, где использовалась эта метафорическая форма [2, p. 1-52].

Учитывая сложности и разнообразие сюжетов в российско-американских отношениях, не удивительно, что данная метафора применялась и при описании этой части внешней политики США. Представленное исследование касается такой важной и актуальной в современном мире сферы, как кибербезопасность в контексте отношений современной России и Соединённых Штатов.

## 1 Формирование «Кибер Пёрл-Харбора»

Само понятие «Кибер Пёрл-Харбор» или «Цифровой (англ. Digital) Пёрл-Харбор» сформировалось в англоязычных (преимущественно американских) СМИ в начале нового тысячелетия, на рубеже



https://doi.org/10.52605/16059921_2023_02_96

2000 – 2002 гг. и первоначально не выходило за пределы профессионального сообщества специалистов по безопасности компьютерных систем, хакеров и программистов. Более того, судя по всему, изначально это понятие носило откровенно ироничный характер. Под «кибер Пёрл-Харбором» понимается внезапное масштабное и мощное негативное воздействие на жизненно важные для США компьютерные сети, сервера и иные хранилища данных, которое способно привести к реальным потерям в области инфраструктуры, энергетической, военной или гражданской безопасности, влекущее, в том числе и реальные человеческие жертвы [3]. Изначально, такая масштабная хакерская атака считалась сценарием близким к фантастическому, поэтому указание на Пёрл-Харбор и было своего рода иронией.

## 2 От формирования к первичной актуализации

Отношение к компьютерной безопасности и такому сценарию, как масштабная хакерская атака, способная серьёзно навредить потенциалу страны, стала восприниматься намного серьёзнее после трагических событий 11 сентября 2001 г. Более того, в этот период метафора «кибер Пёрл-Харбор» часто употреблялась в смеси с более, на тот момент, актуальной и злободневной метафорой «кибер 9/11» [4, p. 2]. Отойдя от первичного шока, целый ряд американских изданий начал рассуждать о других формах агрессии со стороны международного терроризма и всех иных недоброжелателей Америки [5, p. 1]. Журналисты в это время считали многочисленные перебои в работе Интернета, «обрушения» сайтов, в том числе новостных и сайтов госучреждений, звеньями одной цепи и дополнительной целью террористов, атаковавших Башни-близнецы. Впрочем, эти опасения достаточно быстро были развеяны администрацией президента Джорджа Буша-мл. и различными ведомствами, специализировавшимися на информационной безопасности. Например Агентством национальной безопасности (АНБ), а также ЦРУ и ФБР, не раз выступившим в прессе с убеждением, что все неудобства, с которыми столкнулись простые граждане в этот период в плане пользования Интернетом, не более чем следствие высокой нагрузки, которую испытали различные ресурсы в период атаки [6, p. 2].

В контексте российско-американских отношений обращает на себя внимание то, что в этот период Российская Федерация не только категорически не рассматривалась как возможный автор подобной масштабной кибер-атаки на американские сети, но и воспринималась как союзник, и притом довольно важный, как в деле компьютерной безопасности, так и в целом в борьбе с международным терроризмом. Впервые потенциальные кибер-угрозы для США были обозначены в показаниях Джорджа Тенета, директора ЦРУ (1997-2004), данных комитету по разведке Сената США, относительно потенциальных опасностей для безопасности страны и способности разведки оперативно на них реагировать. Что интересно, Тенет в своих показаниях лишь указывал на регионы (Ближний Восток и некоторые страны Азиатского региона) откуда может исходить опасность для компьютерной инфраструктуры страны и подтвердил, что, по мере развития высоких технологий, такая угроза будет становиться всё реальнее. Публикация «New York Times», посвящённая этим показаниям, попыталась рассмотреть более пристально показания главы американской разведки и конкретизировать возможные угрозы для кибер-безопасности Америки. В очерченном в прессе списке фигурировали как все те страны, которые уже попали в «оригинальный» список стран «Оси Зла» – Ирак, Иран и КНДР, так и страны, которые позднее (2004-2005 гг.) дополнили этот перечень – Куба, Ливия, Сирия, также упоминалась и республика Белоруссия [7, p. 32; 8, p. 1-3]. В целом американская пресса считала наиболее опасными угрозами стабильности Интернета и стратегических компьютерных систем такие страны как Иран, Ирак и КНДР. Что интересно, Ирак в этом списке уступал Ирану, который воспринимался как более богатое и технологически развитое государство, а следовательно, более высокая хакерская угроза. Достаточно парадоксальным выглядит и нахождение в этом списке КНДР – государства крайне закрытого и, на тот момент, очень слабо включённого в мировые информационные процессы. Хотя в списке возможных компьютерных угроз и присутствует Белоруссия, её потенциал в качестве кибер-угрозы оценивается как, в целом, «довольно малый, хотя и возможный» [8, p. 1-3].

Уже эти первые наблюдения позволяют сделать выводы, что, появившись как шутка, сценарий «кибер Пёрл-Харбора» после терактов 11 сентября 2001 г. достаточно быстро и небезосновательно стал рассматриваться высшими эшелонами власти в Америке, как вполне реальный. В своих показаниях перед комитетом по разведке Тенет особо отмечал, что: «уже к концу этого десятилетия до 35-40% важнейших инфраструктурных проектов и служб нашей страны будет работать в преимущественно цифровом формате, в дальнейшем эта цифра будет только расти».

Обращает на себя внимание, что Джордж Тенет намеренно в своём выступлении попытался избежать указаний на конкретные страны, от которых может исходить подобная угроза, однако, буквально несколькими днями ранее, сам президент Джордж Буш-мл. чётко обозначил список недружественных Вашингтону стран ярко пометив их эпитетом «Ось Зла». Представляется, что в данном случае Тенет выступал с заранее заготовленным текстом, который был написан до выступления президента, а потому не содержал конкретики. Однако речь главы Овального кабинета перед Конгрессом 29 января 2002 года достаточно чётко локализовала круг государств, на которые должны быть направлены усилия Америки по противодействию хакерским атакам. Журналисты просто расшифровали и проанализировали достаточно общую по своей сути открытую для прессы часть показаний Тенета и сделали свои выводы, идущие вслед за президентским посланием.

Тем не менее, вплоть до 2012 года метафора «кибер Пёрл-Харбор» или её более «злободневный» аналог «кибер 9/11» в СМИ встречается достаточно редко, лишь спорадически о чём-то подобном американская пресса рассуждает в общем контексте информационной безопасности или геополитики [9, p. 2]. Значительные перемены в отношении к информационной безопасности происходят после 11-12 октября 2012 года. В этот день поздно ночью министр обороны США (2011-2013) Леон Панетта в своей речи, произнесённой на конференции по случаю тридцатилетия исследовательской организации BENS, отметил, что «угроза от кибератак на интересы США растет», а также, что «вирус [10], появившийся этим летом в Заливе, вывел из строя 30 000 компьютеров, нарушив работу крупнейших нефтегазовых компаний». Отдельно Панетта остановился на том, что хакеры, уничтожив информацию на компьютерах, заменили «рабочий стол» на повторяющуюся анимацию с горящим американским флагом под некую «весёлую музыку». Закончил свою речь глава министерства обороны фразой о том, что «одновременные атаки на «критическую инфраструктуру» в будущем, вместе с какими-то реальными агрессивными действиями, могут привести к «кибер Перл-Харбору» [11, p. 2].

Обращает на себя выбор мероприятия, на котором министр обороны, до этого также занимавший пост директора ЦРУ (2009-2011), выступил с подобной речью. BENS (англ. абб. Business Executives for National Security, Представители бизнеса за национальную безопасность) – это одна из крупнейших в Соединённых Штатах неправительственных организаций, занятых исследованиями в области высоких технологий с целью экспертной консультации правительства. То есть, по сути своей, BENS представляет собой мощное объединение специалистов из различных высокотехнологичных, и не только отраслей, которые занимаются разнообразными исследованиями в тесной связи, а часто и по прямому заказу государства. Эта своеобразная «фабрика мысли» в сущности является более либерально организованным вариантом корпорации RAND [12, p. 110] и других подобных предприятий. Тесная связь с государством подчёркивается наличием в разное время в консультативном совете при совете директоров BENS таких крупных государственных деятелей, как Генри Киссинджер (бывший госсекретарь и советник президента), Роберт Рубин (бывший министр финансов), Майкл Хайден (бывший директор АНБ, позднее ЦРУ), Уильям Уэбстер (бывший директор ФБР, позднее ЦРУ) и многие другие [13, p. 215]. Кроме того, следует обратить внимание на то, что свою речь Леон Панетта произносил в конце торжественной части мероприятия, на которой присутствовали практически все руководители крупнейших IT-компаний Америки. Таким образом, министр донёс основные идеи и страхи государства до руководства сферы высоких технологий и Интернета, которое, по мере усиления влияния корпоративных гигантов, в большей степени стало беспокоиться об информационной безопасности. Метафора «кибер Пёрл-Харбор» здесь использована как наиболее понятный широкой массе сюжет-аналогия, избежать повторения которой – задача крупного бизнеса и государства.

После выступления Панетты, метафора «кибер Пёрл-Харбор» в различных вариациях закрепилась в медиасфере и стала частью дискурса США по вопросам безопасности в сфере высоких технологий, часто используясь различными авторами, пишущими на эти темы, а также журналистами, публицистами и колумнистами крупных изданий, рассуждающих о вопросах национальной и внутренней безопасности страны, а также в научных исследованиях учёных и даже студентов [14, p. 3-20].

Обращает на себя внимание также, что оборот «кибер Пёрл-Харбор» использовался Панеттой и ранее, ещё в бытность директором ЦРУ, например 11 февраля 2011 г. он в числе других представителей разведывательного сообщества США на общем совещании руководителей

основных ведомств выразил общую озабоченность спецслужб «усиливающейся чувствительностью наших компьютерных систем перед лицом кибер-угроз». Хотя сам текст не содержит цитаты Панетты о «кибер Пёрл-Харборе» она вынесена в заголовок материала «ABC News» со ссылкой именно на него [15]. Таком образом, можно сделать вывод, что разведывательное сообщество Америки в целом в период с 2009-2011 гг. усиливало интерес к сфере компьютерной безопасности. На момент общего совещания у спецслужб уже была некая общая позиция по этому вопросу т.к., судя по выступлениям директора ФБР (2001-2013) Роберта Мюллера, самого Панетты и директора национальной разведки (2010-2017) Джеймса Клэппера, руководитель Центрального разведывательного управления просто удачно выразил общие опасения своих коллег [16, p. 8]. Получив 1 июля 2011 г. должность министра обороны, Леон Панетта впоследствии использовал наработки со своей предыдущей работы и просто актуализировал их в условиях своего более значимого и высокого статуса в иерархии принятия решений, донеся сформулированную им ранее мысль до широкой общественности и лидеров IT-индустрии. Именно это и способствовало такому пристальному вниманию и вхождению этого оборота в медийную повестку Соединённых Штатов.

Кроме этого, материал Джейсона Райана для «ABC News» интересен и в контексте российско-американских отношений, поскольку впервые Россия артикулировано вписана в список кибер-угроз для США. В тексте статьи присутствует следующая цитата, также принадлежащая Леону Панетте: «Другие страны развивают значительный потенциал в этой области [кибер-атак – прим Я.Л.], будь то Россия или Китай или Иран. Сейчас мы являемся объектом буквально сотен тысяч атак, которые происходят в попытке получить информацию. Мы должны разработать не только защиту от этого, но мы должны разместить наши активы в местах, где мы можем обеспечить достаточное предупреждение о том, что эти атаки грядут» [15].

Обращает на себя внимание круг стран, который обозначен директором ЦРУ. Нахождение в нём Ирана – наследие ещё «оригинальной» «Оси Зла» сформулированной Джорджем Бушем-мл., упоминание этой страны связано с поступательно ухудшающимися отношениями Америки и Исламской республики, на которую оказывалось серьёзное санкционное давление, вынуждавшее власти поощрять любые формы получения значимой технической информации для собственных нужд [17, p. 104-110].

Появление Китая в этом перечне тоже вполне объяснимо и неслучайно, поскольку об опасности для Америки усиления этой страны и её роли в международных отношениях, а также, что важнее, в мировой экономике, крупнейшие американские интеллектуалы писали ещё в середине 1990-х гг.[ 18, с. 148] Практика показала, что предсказания о «возвышении» КНР оказались верны, что естественно, вело к столкновениям интересов Вашингтона и Пекина очень во многих сферах: от политики и экономики, до информационной безопасности. С учётом сильных позиций Белого дома в IT-индустрии и общей тенденции роста стратегической важности промышленного шпионажа в этой сфере, в которой Китай наиболее активно стремится «подвинуть» Соединённые Штаты, рост настороженности со стороны спецслужб и министерства обороны вполне понятен [19, p. 3-51].

Наконец, появление в этом списке Российской Федерации, ещё, по историческим меркам, совсем недавно воспринимавшейся как союзник в делах международной безопасности, также вполне объяснимо. Это связано с многократно возросшей субъектностью России на международной арене, что привело к целому ряду противоречий с США по многим темам. Российское руководство не поддержало кампанию по свержению режима Саддама Хусейна, поступательно усилило своё влияние в регионе стран бывшего СССР, что показала, например, конфликтная ситуация между прозападной Грузией и частично признанной республикой Южная Осетия, в которой Россия в августе 2008 г. выступила с операцией по принуждению мира, защитив свои стратегические интересы в Закавказском регионе.

Вполне понятно, что подобная самостоятельность страны, ещё десятилетие назад воспринимавшейся в Штатах как дипломатически и стратегически ограниченная, не могла не вызвать подозрений и роста настороженности, особенно с учётом тяжкого наследия Холодной войны.

## 3 «Кибер Пёрл-Харбор» и СМИ в 2012-2014 гг.

Выступление Леона Панетты вписало метафору «кибер Пёрл-Харбор» в медиапространство США. В 2012-13 гг. она достаточно часто возникает на страницах печатных американских СМИ и звучит в

телеэфирах и различных Интернет-проектах [20]. Обращает на себя внимание, что Россия всё чаще упоминается как одна из возможных угроз информационной безопасности Америки, однако отнюдь не в первых рядах. Чаще всего американские публицисты, журналисты и эксперты в сфере высоких технологий опасаются широкомасштабных внезапных хакерских атак от арабских государств (чаще всего звучат Иран, позднее Сирия), террористических организаций радикального ислама, а также Китая и Северной Кореи. Последние два государства вызывают у авторов публикаций наибольшие опасения.

Рост опасений насчёт КНР вполне вписывается в уже озвученные выше взгляды американской и, в целом, западных общественно-политических наук, которые активно отмечали рост влияния этой страны в экономике, за которым неминуемо последует усиление политического противостояния как с США, так и с Европой [21, p. 17-35, 125-143].

Северная Корея в таких публикациях изображается репортёрами как государство настолько закрытое и доведённое изоляцией до предела, что нельзя исключать никаких, даже самых радикальных, сценариев в отношениях с ней.

Такой взгляд привёл к тому, что американские СМИ в период 2014-15 гг. всерьёз опасались различных агрессивных действий, в том числе и хакерских атак со стороны Северной Кореи в ответ, например, на выход комедии «Интервью» (2014, реж. Э. Голдберг, С. Роген) в которой глава корейского государства Ким Чен Ын изображался в откровенно пародийном виде, равно как и сама Северная Корея в этом фильме представала собранием самых разных штампов и стереотипов об этой стране в западном мире [22].

Наиболее ироничным оказалось то, что эти опасения в некоторой степени подтвердились, когда некая хакерская группировка, назвавшая себя «Хранители мира» 24 ноября 2014 г. действительно устроила хакерскую атаку на сервера компании «Sony Pictures Entertainment», требуя на плохом английском снятия фильма с проката [23]. Итогом этой атаки стал массовый «слив» информации о множестве текущих проектов компании «Sony», а также, что оказалось интереснее – переписка между генеральным директором «Sony Pictures Entertainment» Майклом Линтоном и старшим аналитиком по вопросам обороны корпорации «RAND» Брюсом Беннеттом, которая вполне чётко доказывала пропагандистский подтекст данной комедии [24].

Ещё одним примером рассмотрения идеи «кибер Пёрл-Харбора» можно считать статью в «The Washington Post» с достаточно говорящим заголовком «кибер Пёрл-Харбор – это миф». Автор статьи – профессор университета Джона Хопкинса Генри Фарелл. В своём очерке он вспоминает о том, как Леон Панетта привнёс в медиа пространство эту конструкцию и как его выступление в 2012 спровоцировало новую волну обсуждений способности США противостоять угрозам в Интернет-пространстве [25]. Прежде всего, автор дискутирует самой идеей подобного нападения, опираясь на наиболее «свежую» на тот момент публикацию Эрика Гарцке, специалиста по информационной безопасности, выпустившего статью для журнала «International Security», которая опровергала многие мысли высказанные Панеттой и другими видными представителями госаппарата, спецслужб и IT-индустрии о реальности массовой атаки на сервера и иные информационные ресурсы Америки, которые могут иметь и реальные человеческие жертвы [26, p. 41-73.]. Поскольку автор сам является специалистом в области информационной безопасности и международных отношений, его мнение выглядит достаточно взвешенным. В частности, Фарелл пишет о том, что «на сегодняшний день подобный сценарий – это нечто абсолютно фантастическое». Он считает, что, во-первых, наиболее критические структуры Соединённых Штатов многократно дублируются, так что «даже при серьёзной, критической атаке на важнейшие ресурсы, существуют резервы». Кроме того, он отмечает, что наиболее важные системы, такие как банковская, инфраструктурная, военная и некоторые другие по большей части являются замкнутыми, полностью или частично лишёнными связи с Интернетом, а значит намного менее уязвимыми для атак извне [25]. По мнению Фарелла и Гарцке, данные опасения, беспочвенность которых ясна всем в профессиональном сообществе, стали удобным мотивом для выманивания огромных бюджетных средств различными корпорациями, которые играют на невежестве власти. Кроме того, автор отмечает, что эффективность подобной массовой хакерской атаки могла бы достигнуть масштабов, сопоставимых с Пёрл-Харбором, только в случае традиционной военной атаки, что представляется совсем уж невероятным и нереалистичным сценарием [25].

## Заключение

Таким образом мы можем судить, что с 2001 г. преломление трагедии в Пёрл-Харборе в кибер пространстве прошло значительный путь от узкопрофессиональной шутки до вполне серьёзной концепции, озвучиваемой как в публицистике, так и на высоком государственном уровне. На наш взгляд, такая апелляция не случайна, поскольку любому американцу со школьной скамьи история нападения Японии 7 декабря 1941 г. известна как одна из наиболее серьёзных и страшных трагедий в американской истории XX века. Данная метафора эффективно обращается к эмоциям и исторической памяти граждан. Вместе с тем, в контексте российско-американских отношений мы видим, что вплоть до 2014 г. она постепенно становится важной в контексте российско-американских отношений и их репрезентации в СМИ, хотя и имеет в этот период второстепенное значение.

## Благодарности

Работа выполнена в рамках реализации гранта Президента РФ «Русский “Перл-Харбор”: роль исторической метафоры в российско-американских отношениях 2001–2020 гг.» (МД-764.2022.2).

## Литература

1. Shepley N. Red Sun at War: Pearl Harbor and Japan's Pacific Gamble. Vol 1&2. London (UK). Andrews UK Limited. 2015. 512 p.
2. Kosa G. The Sea of Fire as a Chinese Manichaean Metaphor: Source Materials for Mapping an Unnoticed Image // Asia Major. Third Series. 2011. Vol. 24, No. 2. P. 1-52.
3. Technopedia. Dictionary. Cyber Pearl Harbor. 8 November 2012. URL: https://www.techopedia.com/definition/29052/cyber-pearl-harbor (дата обращения: 12.06. 2022).
4. The New York Times. 17 November, 2001. 23 p.
5. The Daily Reporter. 19 September, 2003. 20 p.
6. The New York Times. 11 February, 2003. 25 p.
7. Lausten M. Language at War. A Critical Discourse Analysis by Speeches of Bush and Obama on War and Terrorism. N.Y. GRIN Verlag. 2016. 56 p.
8. The New York Times. 6 February, 2002. 22 p.
9. Buchanan P.J. Saddam’s gone; who’s next on the neocons “Axis of Evil” // The free Lance-Star. 24 August, 2004. 22 p.
10. Kubecka C. How to Implement IT Security after a Cyber Meltdown. Analysis from specialist of “HypaSec NL”. URL: https://www.youtube.com/watch?v=WyMobr_TDSI (дата обращения: 14.06.2022).
11. The New York Times. 11 October, 2012. 22 p.
12. The Future of Think Tanks and Policy Advice in the United States / Ed. by McGann J. N.Y. Springer International Publishing. 2021. 342 p.
13. Watson C.A. U.S. National Security: A Reference Handbook. N.Y. ABC-CLIO. 2002. 281 p.
14. Sisler P. Should There Be Rules Regarding the Rise of Cyber-Warfare Techniques by Rival Nations. Fort Hays (KS). Fort Hays State University Press. 2013. 30 p.
15. Ryan J. CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor // ABC News. 11 February 2011. URL: https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905 (дата обращения: 12.06.2022).
16. Best Jr. R.A. Intelligence Reform After Five Years: The Role of the Director of National Intelligence (DNI). Congressional Research Service (CRS). 7-5700. R41295. 22 June 2010. 14 p.
17. U.S.-Iran Relations / Ed. by Hurt A.E. N.Y. Greenhaven Publishing. 2017. 149 p.
18. Валлерстайн И. Анализ мировых систем и ситуация в современном мире/Пер. с англ. П. М. Кудюкина под общей ред. Б. Ю. Кагарлицкого. – СПб.: Университетская книга, 2001. 416 с.
19. Pauken T.W. US vs. China: From Trade War to Reciprocal Deal. NY. World Scientific Publishing Company. 2019. 344 p.

20. Roiland P. Is cyber Pearl Harbor real? // CNN News. 13 September 2013. URL: https://edition.cnn.com/news/archive/is-cyber-pearl-harbor-real/story?id=14554492 (дата обращения: 22.06.2022).
21. Bush R.C, O'Hanlon M.E. A War Like No Other: The Truth About China's Challenge to America. NY. Wiley. 2007. 240 p.
22. Child B. North Korea rubbishes Seth Rogen comedy The Interview // The Guardian. 20 June 2014. URL: https://www.theguardian.com/film/2014/jun/20/seth-rogen-north-korea-the-interview-kim-jong-un (дата обращения: 24.06.2022).
23. Ashford W. Computer-killing malware used in Sony attack a wake-up call // ComputerWeekly.com. 3 December 2014. URL: https://www.computerweekly.com/news/2240235919/Computer-killing-malware-used-in-Sony-attack-a-wake-up-call-to-business?asrc=EM_MDN_37122786 (дата обращения 28.06.2022).
24. Sony Hack: Michael Lynton Discussed 'The Interview' With State Department Official // The Hollywood Reporter. 17 December 2014. URL: https://www.hollywoodreporter.com/business/business-news/sony-hack-michael-lynton-discussed-758816/ (дата обращения: 2.07.2022).
25. Farell H. Cyber-Pearl Harbor is a myth // The New York Times. 11 November 2013. Available at URL: https://www.washingtonpost.com/news/monkey-cage/wp/2013/11/11/cyber-pearl-harbor-is-a-myth/(дата обращения: 8.07.2022).
26. Gartzke E. The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth // International Security. 2013. Vol. 38, No. 2. P. 41-73.

# "CYBER PEARL HARBOR" IN THE US MEDIA AND RUSSIAN-AMERICAN RELATIONS 2001–2014

**Levin, Yaroslav Alexandrovich**

*Candidate of historical sciences*
*Samara State Technical University, Department "Philosophy, social sciences and humanities", associate professor*
*Samara, Russian Federation*
*yaroslavlevin1992@mail.ru*

**Abstract**

*Such a historical event as the attack of the Japanese fleet on the American military base in Pearl Harbor Bay was of great importance and, in addition to purely political consequences, left a noticeable mark on the culture of the United States. As part of this article, an attempt was made to consider one of the transformations of the formed media template, namely, Cyber Pearl Harbor, an idea and journalistic trail about a sudden powerful hacker attack on objects important to the United States. Based on specific examples, it is considered how this design was formed, how the media was used and updated by politicians. In addition, it is also considered how this construction was used by media and political figures in the context of Russia's complex and diverse relations with the United States. The article is based on literature and sources on the topic.*

**Keywords**

*"Cyber Pearl Harbor"; media; USA*

## References

1. Shepley N. Red Sun at War: Pearl Harbor and Japan's Pacific Gamble. Vol 1&2. London (UK). Andrews UK Limited. 2015. 512 p.
2. Kosa G. The Sea of Fire as a Chinese Manichaean Metaphor: Source Materials for Mapping an Unnoticed Image // Asia Major. Third Series. 2011. Vol. 24, No. 2. P. 1-52.
3. Technopedia. Dictionary. Cyber Pearl Harbor. 8 November 2012. URL: https://www.techopedia.com/definition/29052/cyber-pearl-harbor (дата обращения: 12.06. 2022).
4. The New York Times. 17 November, 2001. 23 p.
5. The Daily Reporter. 19 September, 2003. 20 p.
6. The New York Times. 11 February, 2003. 25 p.
7. Lausten M. Language at War. A Critical Discourse Analysis by Speeches of Bush and Obama on War and Terrorism. N.Y. GRIN Verlag. 2016. 56 p.
8. The New York Times. 6 February, 2002. 22 p.
9. Buchanan P.J. Saddam's gone; who's next on the neocons "Axis of Evil" // The free Lance-Star. 24 August, 2004. 22 p.
10. Kubecka C. How to Implement IT Security after a Cyber Meltdown. Analysis from specialist of "HypaSec NL". URL: https://www.youtube.com/watch?v=WyMobr_TDSI (дата обращения: 14.06.2022).
11. The New York Times. 11 October, 2012. 22 p.
12. The Future of Think Tanks and Policy Advice in the United States / Ed. by McGann J. N.Y. Springer International Publishing. 2021. 342 p.
13. Watson C.A. U.S. National Security: A Reference Handbook. N.Y. ABC-CLIO. 2002. 281 p.
14. Sisler P. Should There Be Rules Regarding the Rise of Cyber-Warfare Techniques by Rival Nations. Fort Hays (KS). Fort Hays State University Press. 2013. 30 p.
15. Ryan J. CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor // ABC News. 11 February 2011. URL: https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905 (дата обращения: 12.06.2022).
16. Best Jr. R.A. Intelligence Reform After Five Years: The Role of the Director of National Intelligence (DNI). Congressional Research Service (CRS). 7-5700. R41295. 22 June 2010. 14 p.
17. U.S.-Iran Relations / Ed. by Hurt A.E. N.Y. Greenhaven Publishing. 2017. 149 p.

18. Vallerstajn I. Analiz mirovyh sistem i situacija v sovremennom mire/Per. s angl. P. M. Kudjukina pod obshhej red. B. Ju. Kagarlickogo. – SPb.: Universitetskaja kniga, 2001. 416 c.
19. Pauken T.W. US vs. China: From Trade War to Reciprocal Deal. NY. World Scientific Publishing Company. 2019. 344 p.
20. Roiland P. Is cyber Pearl Harbor real? // CNN News. 13 September 2013. URL: https://edition.cnn.com/news/archive/is-cyber-pearl-harbor-real/story?id=14554492 (дата обращения: 22.06.2022).
21. Bush R.C, O'Hanlon M.E. A War Like No Other: The Truth About China's Challenge to America. NY. Wiley. 2007. 240 p.
22. Child B. North Korea rubbishes Seth Rogen comedy The Interview // The Guardian. 20 June 2014. URL: https://www.theguardian.com/film/2014/jun/20/seth-rogen-north-korea-the-interview-kim-jong-un (дата обращения: 24.06.2022).
23. Ashford W. Computer-killing malware used in Sony attack a wake-up call // ComputerWeekly.com. 3 December 2014. URL: https://www.computerweekly.com/news/2240235919/Computer-killing-malware-used-in-Sony-attack-a-wake-up-call-to-business?asrc=EM_MDN_37122786 (дата обращения 28.06.2022).
24. Sony Hack: Michael Lynton Discussed 'The Interview' With State Department Official // The Hollywood Reporter. 17 December 2014. URL: https://www.hollywoodreporter.com/business/business-news/sony-hack-michael-lynton-discussed-758816/ (дата обращения: 2.07.2022).
25. Farell H. Cyber-Pearl Harbor is a myth // The New York Times. 11 November 2013. Available at URL: https://www.washingtonpost.com/news/monkey-cage/wp/2013/11/11/cyber-pearl-harbor-is-a-myth/(дата обращения: 8.07.2022).
26. Gartzke E. The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth // International Security. 2013. Vol. 38, No. 2. P. 41-73.