DOI 10.35775/PSI.2025.122.10.023
УДК 32.327

Г.В. РЫСУХИН
аспирант кафедры американских исследований
факультета международный отношений института международных отношений
и политических наук Российского государственного
гуманитарного университета (РГГУ),
Россия, г. Москва
E-mail: glebrysuhin@mail.ru

ХАКЕРСКИЕ ГРУППИРОВКИ КАК ПРОКСИ СИЛЫ В СОВРЕМЕННЫХ ГИБРИДНЫХ ВОЙНАХ

В статье анализируется роль хакерских группировок как прокси-сил в гибридной войне. В современном мире, в эпоху цифровизации, когда информационные технологии проникли во все сферы, жизни общества и человек не может обойтись без гаджета или компьютера, а в государствах разрабатываются отдельные стратегии по кибербезопасности и информационной безопасности, по развитию информационных технологий и искусственного интеллекта, тема хакерских группировок стоит особенно остро. Раскрывается понятие гибридной войны и кибервойны в доктринах и публикациях российских и американских военных и экспертов. Методология исследования включает в себя анализ официальных документов ведущих стран, посвященных информационной безопасности и враждебным хакерским группировкам, заявления представителей хакерских группировок, их идеологии, анализ последствий их атак. Результаты данного исследования могут быть ценными в области изучения гибридной войны в целом и кибервойны в частности.

Ключевые слова: *гибридная война, кибервойна, хакерские группировки, прокси-силы, информационные технологии, Россия, США.*

Хакерские группировки играют немалую роль в современных международных отношениях в силу влияния информационных технологий во всех сферах жизни общества. В новостных сводках часто присутствуют сообщения о различных взломах, фактах кибершпионажа, кибератаках на критическую инфраструктуру. Потенциал злоумышленников в цифровой сфере достиг такого уровня, что даже стратегически важные объекты, такие как атомное оружие и другие передовые оборонные системы, оказываются под угрозой. Свидетельством тому служит недавний инцидент с взломом кодов французской фирмы «Naval», занимающейся строительством военно-морских судов, а также кодов французских боевых комплексов, оснащенных ядерным вооружением. Исходя из этих фактов, хакерские группировки представляют серьезную угрозу для национальной безопасности государств и являются эффективным инструментом гибридной войны между государствами в современных международных отношениях.

Следует подчеркнуть, что в работах российских и зарубежных авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [1; 2; 3; 5; 7; 10; 11; 12; 13; 16; 19; 20; 23].

Однако проблему хакерских группировок как прокси-сил в гибридной войне нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Понятия гибридной войны. Карл фон Клаузевиц, знаменитый немецкий военный теоретик, сравнивал войну с хамелеоном, подчеркивая ее способность меняться в зависимости от обстоятельств [9]. Гибридные войны и конфликты, представляют собой одну из форм адаптации к трансформациям, затрагивающим современное общество и развитие технологий. Новейшие технологические достижения позволяют различным участникам устанавливать контроль и даже в определенной степени подчинять себе целые государства, избегая прямой оккупации или открытого применения военной силы. Все большее количество современных столкновений классифицируются как «гибридные», и, по мнению экспертов, эта форма конфликтов может стать преобладающей в текущем столетии.

Концепции «гибридного конфликта», «гибридных угроз» и «гибридных операций» начали разрабатываться экспертами из ведущих стран НАТО в конце 1990-х годов. Фрэнк Хоффман, один из ключевых авторов, предложивших концепцию гибридной войны, описывал ее как «широкий спектр разнообразных методов ведения войны, включающих традиционные военные средства, регулярные тактические приемы и формирования, террористические акты, характеризующиеся неизбирательным насилием и элементами принуждения, а также криминальные проявления нестабильности» [26].

Элементы, уникальные для гибридной войны, и их применение на протяжении всей истории описаны в монографии Мюррея и Мансура [30]. Хотя некоторые элементы гибридной войны не являются новыми и применялись в войнах прошлого, последовательность этих элементов уникальна в современном мире, как и их применение в условиях развития современных информационно-коммуникативных технологий и растущей информации.

В 2005 г. генерал-лейтенант Корпуса морской пехоты Соединенных Штатов Джеймс Мэттис в сотрудничестве с отставным подполковником морской пехоты США Фрэнком Хоффманом представил работу под названием «Война будущего: восхождение гибридных войн» (Future Warfare: The Rise of Hybrid Wars) [26]. В дальнейшем в своем анализе Фрэнк Хоффман предположил, рост гибридных войн в будущем, в ходе которых противники будут использовать смешанные методы и средства – конвенциональные (обычные вооружения) и неконвенциональные (гибридные) способы воздействия на противника.

Согласно определению Хоффмана, гибридные войны характеризуются многообразием применяемых подходов, охватывающих как классические вооружения, так и нестандартные тактики, формации, террористические акты,

неизбирательное насилие и давление, а также элементы преступности. Эти компоненты могут использоваться различными группами или одним формированием, однако, как правило, они оперативно и тактически контролируются и согласуются в рамках основного театра боевых действий для достижения комплексного эффекта [25].

Согласно определению, представленном Лондонским международным институтом стратегических исследований, суть гибридной войны заключается в применении как военных, так и невоенных средств в рамках скоординированной кампании. Цель такой кампании – достижение неожиданности, перехват инициативы и получение психологического превосходства за счет использования дипломатических рычагов, масштабных и скоростных информационных, электронных и кибернетических операций. Кроме того, активно применяются методы маскировки и сокрытия военной и разведывательной деятельности, подкрепляемые экономическим давлением [28].

Хотя концепция гибридной войны изначально привлекла некоторое внимание экспертов, ее прорыв произошел в 2014 г. с воссоединением Крыма с Россией. Гибридная война была немедленно связана с ныне известной речью генерала Валерия Герасимова, начальника Генерального штаба Вооруженных сил России, и на Западе стала использоваться взаимозаменяемо с (совершенно мифической) доктриной, названной в его честь, – «доктрина Герасимова».

В статье «Ценность науки в предвидении» В. Герасимов сформулировал концепцию так называемой «нелинейной войны», в ходе которой военно-политические цели достигаются невоенными подрывными методами (работой с общественным мнением, политической оппозицией, организацией «цветных революций») [6].

На саммите НАТО в Уэльсе в сентябре 2014 г. гибридная война оказалась в центре дискуссии среди военных. В 2016 г. НАТО допустила применение 5-й статьи при гибридной агрессии и договорилась с ЕС о совместном противодействии таким угрозам. Позднее в структурах НАТО появился отдел мониторинга и анализа гибридных угроз, а Европейский Союз совместно с НАТО в 2017 г. создал в Хельсинки Европейский центр передового опыта.

Последующие события привели к тому, что гибридная война стала синонимом противодействия Запада в отношении России, которая воспринимается странами НАТО как самая непосредственная угроза безопасности.

Таким образом, сегодня гибридную войну можно определить, как вид враждебных действий, при котором нападающая сторона не прибегает к классическому военному вторжению, а подавляет своего оппонента, используя сочетание скрытых операций, диверсий, включая кибератаки (кибервойны), а также оказывая поддержку повстанцам, действующим на территории противника.

Кибер-война в стратегии ведущих государств. Кибервойна – это использование кибероружия и других киберсистем и средств для нанесения ущерба, разрушения или оказания влияния на международных субъектов и/или объекты. Что касается стратегии ведения кибервойн, то здесь можно выделить два

основных подхода: **революционный и эволюционный.** С позиций революционного подхода, кибероружие представляет возможность наносить атаки посредством вредоносного кода, и мыслится не иначе как «революция в военном деле», обладающее потенциалом радикальной трансформации стратегии и мощи государств.

Сторонники **эволюционного** подхода рассматривают кибероружие как тактическое новшество, исходя из убеждения, что военное дело и стратегия не претерпели кардинальных изменений: государства по-прежнему стремятся к власти и влиянию в международных отношениях и готовы бороться за них. С этой точки зрения главное изменение в кибервойне носит не стратегический, а тактический и технологический характер, независимо от того, какое оружие используется – конвенциональное (огнестрельное, бомбы, ракеты) или неконвенциональное (вредоносный код) [29].

Национальная киберстратегия США, принятая в сентябре 2023 г., является примером эволюционного подхода [27]. В документе подчеркивается, что в новом десятилетии США «переосмыслят киберпространство как инструмент для достижения наших целей в соответствии с нашими ценностями: экономической безопасностью и процветанием; уважением прав человека и основных свобод; доверием к нашей демократии и демократическим институтам; а также справедливым и разнообразным обществом» [27]. Достижение этих целей основано на двух ключевых принципах: 1) распределить ответственность за защиту киберпространства с частных лиц, малого бизнеса и местных органов власти на организации, которые обладают наибольшими возможностями и лучше всего подготовлены к снижению рисков; 2) скорректировать стимулы в пользу долгосрочных инвестиций, соблюдая баланс между защитой от актуальных угроз и стратегическим планированием и инвестированием.

В документе под названием «Доктрина информационной безопасности Российской Федерации», утвержденной Президентом РФ 5 декабря 2016 г., указывается на наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса [8]. При этом в документе не используется термин «кибервойна», а кибер пространство рассматривается в более широком контексте информационной войны, которая включает в себя деструктивное воздействие на компьютерные сети, радиоэлектронную борьбу, психологические и информационные операции противника.

Одной из значимых составляющих гибридной войны являются кибероперации и кибервойна. При этом одними из значимых акторов кибервойны выступают хакерские группировки, действующие в интересах того или иного государства. Они могут определяться не как структуры, принадлежащие государствам, а как их проксисилы.

В основе привлекательности использования хакерских группировок в качестве прокси-сил лежит концепция правдоподобного отрицания (**plausible deniability** – организация системы тайных операций, которая позволяет политикам и государственным чиновникам в любой момент сказать, что они ничего не знали, так как не были посвящены в план действий и детали) [24]. Государства, поддерживающие или направляющие эти группировки, могут избежать прямого обвинения в злонамеренных кибердействиях. Эта двусмысленность позволяет им поддерживать видимость соблюдения международного права и избегать потенциальных экономических или дипломатических последствий. Кроме того, использование прокси-сил позволяет государствам диверсифицировать свои кибервозможности и распределять риски, поскольку эти группировки часто обладают специализированными навыками и знаниями конкретных целей или технологий [4. С. 61-74].

Для того, чтоб оценить влияние хакерских группировок на ход кибервойны, можно рассмотреть следующие примеры.

24 февраля 2022 г. президент Российской Федерации Владимир Владимирович Путин объявил о начале проведения Специальной военной операции на Украине [17]. Начало СВО дало толчок глубокому кризису отношений России со странами Евросоюза и НАТО, в результате которого страны ЕС и НАТО не только усилили давление на Россию в виде санкций, но и стали оказывать дополнительную военную и финансовую помощь и поддержку Украине с целью нанесения «стратегического поражения России». В киберпространстве также произошел всплеск киберактивности, а количество кибератак, различных операций, проводимых западными спецслужбами и кибервойсками в отношении России, значительно увеличилось. В стороне от ситуации не остались также и хакерские группировки, которые оказались вовлеченными геополитическую борьбу в киберпространстве. Так хакерская группировка «Anonymous» выступила с обращением к Владимиру Путину [14], в котором они объявили, что теперь находятся в состоянии кибервойны против России, и с обращением к гражданам России [15], где объявили о том, что снимут все деньги со счетов российских граждан и направят их на помощь Вооруженным силам Украины.

При этом сайты Федеральной антимонопольной службы, Кремля, российского канала «Russia Today» и многие другие правительственные сайты России были подвергнуты мощной DDoS-атаке.

В ответ российская хакерская группировка «KillNet» выложила видео с обращением [18], где объявила о том, что вся информация о взломах банков является фейковой информацией и информационной бомбой, которая не несет никакого конкретного вреда гражданам России. Таким образом, эти события свидетельствуют о том, что началось вступление независимых хакерских группировок в геополитическую борьбу и кибервойну.

Атака хакера «KillMilka» на военно-промышленную корпорацию «Lockheed Martin». В августе 2022 г. лидер российской хакерской группировки «KillMilk» анонсировал масштабную кибератаку на американскую

военно-промышленную корпорацию Lockheed Martin [21]. В своем заявлении хакер обратился к американцам с просьбой помочь ему в деле уничтожения этой компании, чтобы, по его словам, очистить планету от корпорации, которая зарабатывает на смерти людей, и создать мир на Земле. По заявлениям «KillMilk» в результате кибератаки были достигнуты следующие цели: был обрушен сайт корпорации и получены данные кандидатов на работу в компанию, взломаны системы авторизации для сотрудников компании и уничтожены без возможности восстановления полученные данные. Также одним из значимых результатов можно отметить, что система защиты Akamai, которая ранее считалась одним из лучших кибероружий оборонительного характера было преодолено и «отвалилось от Lokcheed Martin» [22].

На основе этих примеров можно сделать следующие выводы. Сегодня с помощью кибероружия можно получить разведданные колоссальной важности, среди которых информация о размещении войск, штабов командования, транспортных узлов, промышленных объектов противника. С помощью компьютера, не тратя огромных усилий, можно не только свести на нет преимущество противника, в которое он вкладывает огромные средства (спутники, программное обеспечение, высокие передовые технологии), но и обратить это преимущество против него самого. Американские программы защиты от киберугроз, несмотря на пристальное внимание к обеспечению кибербезопасности, не являются неуязвимыми и имеют много слабых мест.

В современном мире хакерские группировки являются активными негосударственными международными акторами, способными изменять баланс сил в международных отношениях. Хакерские группировки, действующие в качестве прокси-сил, стали значимым инструментом в арсенале гибридной войны. Использование киберпространства для достижения политических и военных целей без объявления войны представляет собой серьезную угрозу для международной безопасности. Для противодействия этой угрозе необходимы скоординированные усилия международного сообщества, направленные на укрепление кибербезопасности, разработку механизмов атрибуции и установление правил поведения в киберпространстве. Только тогда можно будет обуздать использование хакерских группировок как прокси-сил и обеспечить безопасное и стабильное будущее для всех в цифровом мире.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Алаудинов А.А.** Цели и задачи России в специальной военной операции на Украине и в гибридной войне с коллективным Западом // Вопросы политологии. 2024. № 5.
2. **Алаудинов А.А., Манойло А.В.** Когнитивная и ментальная составляющие современной гибридной войны // Вопросы политологии. 2024. № 2.

3. **Апарин С.В., Суховерхова А.А., Григорян Д.К.** Цифровые войны: роль черного пиара // Вопросы национальных и федеративных отношений. 2025. № 1.
4. **Бартош А.А.** Прокси-война как определяющий фактор военных конфликтов XXI века // Военная мысль. 2023. № 5.
5. **Гавров С.Н., Еремкин М.П.** Использование искусственного интеллекта в контексте информационной войны // Вопросы политологии. 2025. № 2.
6. **Герасимов В.** Ценность науки в предвидении // Военно-промышленный курьер 02.07.2013 // https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html.
7. **Дзахова Л.Х., Кадзова Н.** Трансформация угроз национальной безопасности в условиях усиления деструктивных сообществ в российском сегменте сети Интернет // Вопросы национальных и федеративных отношений. 2025. № 1.
8. Доктрина информационной безопасности Российской Федерации утверждена Указом Президента РФ № 646 от 5 декабря 2016 г. // http://www.scrf.gov.ru/security/information/document5/.
9. **Клаузевиц К.** О войне: Пер. с нем. М.: Издательская корпорация «Логос»; «Наука», 1994.
10. **Кочеринский Д.Ю.** Внешняя политика России в области информационной безопасности: региональное измерение // Евразийский Союз: вопросы международных отношений. 2025. № 8.
11. **Медведев Н.П.** Неклассические войны: современные подходы к ведению гибридных войн. Часть 1 // Вопросы национальных и федеративных отношений. 2025. № 2.
12. **Муравых А.И., Никитенко Е.Г., Стародуб И.В.** Интегральная мировая война (Часть 1) // Вопросы политологии. 2025. № 3.
13. **Никитин Н.А.** Основные подходы к определению понятия «киберпространство» в контексте международных отношений – зарубежный опыт // Вопросы политологии. 2025. № 6.
14. Обращение к Путину. anonymous // Youtube-канал 5.10 TV. 26.02.2022 // https://www.youtube.com/watch?v=nNgATppC0mQ.
15. Обращение от Anonymous к россиянам хакеры обещают опустошить счета. 03.03.2022 // Youtube-канал ЛАЙФХАКЕР-LIFEHAKER. 28.02.2022 // https://www.youtube.com/watch?v=gLRSOPIB3xo.
16. **Петров Д.Ю.** Информационные войны: пути и механизмы влияния на примере глобальных политических конфликтов // Евразийский Союз: вопросы международных отношений. 2025. № 6.
17. **Путин В.В.** Обращение Президента Российской Федерации // Президент России. 24.02.2022 // http://www.kremlin.ru/events /president/transcripts/statements/67843.

18. Русские Хакеры из группировки Killnet, положили сайт Анонимусов. Ukraine // Russia. Youtube-канал Последние Новости. 01.03.2022 // https://www.youtube.com/watch?v=gHADMBGIR0E.
19. **Слизовский Д.Е., Медведев Н.П.** Информационные, гибридные и прокси-войны: обзор новейших исследований // Вопросы политологии. 2024. № 12.
20. **Сурма И.В.** Взаимодействие государств-членов Шанхайской организации сотрудничества в области международной информационной безопасности // Евразийский Союз: вопросы международных отношений. 2025. № 5.
21. Телеграм-канал KillMilk. 01.08.2022 // https://t.me/killmilk_channel/17.
22. Хакеры уничтожили данные производителя систем залпового огня HIMARS // Cnews.10.08.2022 // https://eurasiantimes.com/russian-hackers-launch-cyber-attacks-on-lockheed-martin/.
23. **Чжао Лэй.** Сотрудничество в области кибербезопасности и борьбы с кибертерроризмом в рамках ШОС // Евразийский Союз: вопросы международных отношений. 2024. № 5.
24. **Canfil Ju.K.** The illogic of plausible deniability: why proxy conflict in cyberspace may no longer pay // Journal of Cybersecurity. 2022. Vol. 8. No. 1. DOI 10.1093/cybsec/tyac007.
25. **Frank G. Hoffman.** Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007 // https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.
26. **Mattis J.N., Hoffman F.** Future Warfare: The Rise of Hybrid Wars // Proceedings, November 2005 // https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars.
27. National Cyber Security Strategy. The White House. Washington DC. March, 2023 // https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
28. The Military Balance 2015. The International Institute for Strategic Studies (IISS). 1st Edition.
29. **Valeriano B., Jensen B.M., Maness R.C.** Cyber strategy: The evolving character of power and coercion. Oxford University Press, 2018.
30. **Williamson Murray and Peter R. Mansoor, eds.** Hybrid warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge University Press, 2012.

G.V. RYSUKHIN
Postgraduate Student, Department
of American Studies, Faculty of International Relations,
Institute of International Relations and Political Science,
Russian State University for the Humanities (RSUH),
Moscow, Russia

HACKER GROUPS AS PROXY FORCES IN MODERN HYBRID WARS

This article analyzes the role of hacker groups as proxy forces in hybrid warfare. In the modern world, in the age of digitalization, when information technology has permeated all spheres of society and people cannot function without a gadget or computer, and governments are developing separate strategies for cybersecurity and information security, as well as for the development of information technology and artificial intelligence, the topic of hacker groups is particularly pressing. The concept of hybrid warfare and cyberwarfare is explored in the doctrines and publications of Russian and American military officials and experts. The research methodology includes an analysis of official documents from leading countries on information security and hostile hacker groups, statements by hacker group representatives, their ideologies, and an analysis of the consequences of their attacks. The results of this study may be valuable for the study of hybrid warfare in general and cyberwarfare in particular.

Key words: *hybrid warfare, cyberwarfare, hacker groups, proxy forces, information technology, Russia, USA.*