DOI 10.24412/1026-8804-2024-4-47-59
УДК 327+94

Кибервойска НОАК как составная часть национальной безопасности Китая

Егор Александрович Разумов,
старший лаборант с высшим образованием Центра глобальных и региональных исследований Института истории, археологии и этнографии народов Дальнего Востока ДВО РАН, Владивосток.
E-mail: razumov@yeboshi.ru

Данная статья посвящена рассмотрению политики Китая по созданию кибервойск как составной части национальной безопасности КНР. Рассмотрен процесс создания и развития специализированных кибервойск, включая ключевые моменты формирования Сил информационной поддержки в 2024 г. Проанализирована доктринальная база и функции официальных кибервойск в составе Народно-освободительной армии Китая, а также выявлены тенденции в развитии кибербезопасности в Китайской Народной Республике. Особое внимание уделено стратегическим аспектам кибербезопасности, включая интеграцию передовых технологий, таких как искусственный интеллект и большие данные, в военные операции. В статье подчёркивается значимость кибервойск для обеспечения национальной безопасности и защиты критически важных инфраструктур от кибератак и шпионажа. Рассматривается, как кибервойска способствуют модернизации вооружённых сил Китайской Народной Республики, повышая их способность к управлению военными операциями и их координации. В заключении статьи акцентируется внимание на необходимости дальнейших исследований в области кибервойсковых подразделений Китайской Народной Республики. Подчёркивается важность интеграции инновационных технологий в военную доктрину для поддержания технологической независимости и усиления национальной безопасности. Отмечается, что дальнейшее развитие кибервойск Народно-освободительной армии Китая будет играть ключевую роль в модернизации вооружённых сил и укреплении позиций Китая на международной арене, способствуя его превращению в ведущую кибердержаву. Делается вывод о том, что кибербезопасность и развитие кибервойск становятся неотъемлемыми элементами стратегии национальной безопасности Китайской Народной Республики.
Ключевые слова: Китай, НОАК, кибербезопасность, кибервойска, национальная безопасность, военное строительство, искусственный интеллект.

The PLA Cyber Units as a Part of China's National Security.

Egor Razumov, Institute of History, Archeology and Ethnology of the Peoples of the Far East, FEB RAS, Vladivostok, Russia. E-mail: razumov@yeboshi.ru.

This paper attempts to analyze the Chinese policy for establishing cyber units as a part of PRC's national security. The paper examines the process of creation and development of specialized cyber forces, including key moments in the establishment of the Information Support Forces in 2024. The doctrinal basis and functions of the official cyber forces within the People's Liberation Army of China are analyzed, and trends in the development of cybersecurity in the People's Republic of China are identified. Special attention is paid to the strategic aspects of cybersecurity including the integration of advanced technologies such as artificial intelligence and big data into military operations. The paper emphasizes the significance of cyber forces in ensuring national security and protecting critical infrastructure from cyberattacks and espionage. It examines how cyber forces contribute to the modernization of the armed forces of the People's Republic of China by enhancing their capability to manage and coordinate military operations. The conclusion of the paper highlights the need for further research in the field of cyber units in the People's Republic of China. The importance of integrating innovative technologies into military doctrine to maintain technological independence and strengthen national security is underscored. It is noted that the further development of the cyber forces of the People's Liberation Army of China will play a crucial role in the modernization of the armed forces and the strengthening of China's position on the international stage, contributing to its transformation into a leading cyber power. Thus, cybersecurity and the development of cyber forces become the integral elements of the national security strategy of the People's Republic of China.

Keywords: China, PLA, cybersecurity, cyber warfare, national security, military construction, artificial intelligence.

В последние годы Китай сделал значительные шаги в области военных технологий, уделяя особое внимание развитию кибервойск для укрепления своей обороноспособности. Кибервойска стали ключевым элементом современной военной стратегии Китая, выполняя задачи по защите критически важных инфраструктур, атаке на информационные системы противника и обеспечению информационной безопасности страны.

Использование искусственного интеллекта (ИИ) явилось важным дополнением в деятельности китайских кибервойск и значительно повысило их эффективность. ИИ применяется для анализа огромных массивов данных, прогнозирования угроз и автоматизации процессов защиты и нападения в киберпространстве.

Интеграция ИИ в критическую инфраструктуру позволяет китайским кибервойскам оперативно реагировать на возникающие угрозы и повышает их общую боеспособность. Таким образом, Китай стремится занять лидирующие позиции в области кибервооружения, внедряя передовые технологии и методы для обеспечения своей национальной безопасности в цифровую эпоху.

Целью данной статьи является оценка стратегии руководства КНР по формированию и деятельности киберподразделений Народно-освободительной армии, а также выявление тенденций развития кибербезопасности в КНР. В работе рассматривается исключительно политический аспект вопроса, без углубления в его техническую часть.

Для достижения цели статьи автор решает следующие задачи:

1. Провести анализ доктринальной базы по формированию специализированных киберподразделений Китайской Народной Республики.
2. Описать формирование и функции официальных кибервойск в составе Народно-освободительной армии Китая, в частности Сил стратегической поддержки.
3. Дать оценку возможным тенденциям дальнейшего развития кибербезопасности КНР в условиях появления нового вида кибервойск — Сил информационной поддержки НОАК.

Необходимо отметить, что тематика кибервойсковых подразделений в отечественной науке исследована недостаточно. Некоторые отечественные авторы предприняли попытки проанализировать вопросы обеспечения кибербезопасности и подготовки вооружённых сил КНР к ведению боевых действий в киберпространстве. Так, С.В. Кулинич, А.Б. Шелест и А.В. Сучков [2] в своей статье рассмотрели формирование новых подразделений в составе НОАК, а В.Б. Кашин и А.А. Кокошин изучали китайское киберпространство как вероятное поле кибербаталий [1].

Среди зарубежных исследователей, работающих над этой темой, можно отметить Колтона [5], Триоло, Хаксли и Дибба. М. Колтон анализирует военные кибервозможности Китая и стратегические последствия его киберполитики. А. Сегал исследовал проводимые китайской стороной кибероперации [7]. Хан Сармад Али и Аббаси Сайра Наваз рассматривали возможный киберконфликт между КНР и США [4].

Тематика кибервойск НОАК в китайском сегменте научных публикаций практически не представлена. Китайские авторы рассматривают мировой опыт создания и использования киберподразделений, но не учитывают возможности вооружённых сил в информационном пространстве. Цзян Тянцзяо была предпринята попытка определить основные направления киберстратегии Китая и вероятного создания специализированных киберподразделений [3].

ПОЛИТИЧЕСКИЙ КУРС КНР ПО ФОРМИРОВАНИЮ КИБЕРВОЙСК

Политическое руководство Китайской Народной Республики ещё с начала 90-х гг. XX в. уделяло особое внимание технологическому развитию страны. На мнение китайских властей повлияли не только события на площади Тяньаньмэнь 1980-х гг., но также и появление сети Интернет на территории страны, что поставило государственные структуры перед необходимостью реагировать на новый вид угроз для национальной безопасности — киберугрозы.

Необходимость в формировании собственных киберподразделений обосновывалась нуждами во внутренней политике. Так, развитие экономики и дальнейшая интеграция Китая в глобальные мировые процессы требовали модернизации производства и внедрения технологических инноваций. Учитывая весьма слабое технологическое развитие внутри Китая, правительство предприняло попытку формирования собственных киберподразделений для ведения технической разведки, предполагающей проведение операций против иностранных технологических компаний для дальнейшего использования полученной информации в собственном производстве [8].

Несмотря на то, что политическим руководством был принят ряд вышеописанных решений, не было централизованного управления подобными структурами. Так, в период с 1990 по 2012 г. на территории КНР функционировала следующая система киберподразделений:

1. Гражданские хакеры — обычные граждане.
2. Специалисты Министерства общественной безопасности, представляющие собой отдельные группы сотрудников, выполняющие отдельные задачи министерства по обеспечению внутригосударственной безопасности и расследованию вероятных киберконфликтов.
3. Отдельные военизированные части Народно-освободительной армии Китая, которая в рассматриваемый период была одной из квалифицированных структур, имеющих возможность реализовать поставленные руководством задачи в области информационной безопасности [6].

Подобная система работала до 2012 г., когда к управлению страной пришёл председатель КНР Си Цзиньпин. Начиная с этого момента Пекин стал уделять более пристальное внимание технологическому развитию страны, что потребовало от властей активных действий в области информационной безопасности.

Председатель КНР не раз в своих программных выступлениях озвучивал необходимость строительства «сильного и большого кибергосударства» [9], предполагающего наличие собственных технологических мощностей для обеспечения киберсуверенита,

а также специализированных структур, способных реализовывать политические и идеологические установки. Таким образом, курс Си Цзиньпина на укрепление кибербезопасности, развитие кибервойск и искусственного интеллекта стал частью более широкой стратегии Китая по укреплению национальной безопасности и технологической независимости.

В области кибербезопасности Китай сделал несколько значительных шагов. Законодательство и регулирование играют ключевую роль: принятые законы, такие как Закон о кибербезопасности 2017 г., требуют от компаний защиты пользовательских данных и предоставления их правительству по запросу. Национальная стратегия кибербезопасности, опубликованная в 2016 г., подчёркивает важность кибербезопасности для национальной безопасности в целом и экономического развития. В рамках этой стратегии активно развиваются инфраструктура и системы защиты данных, включая создание центров по киберзащите.

Развитие искусственного интеллекта также является приоритетом для Китая. В 2017 г. была опубликована национальная стратегия развития ИИ до 2030 г., которая предусматривает создание в КНР ведущей мировой ИИ-индустрии. Целью является достижение лидерства в области ИИ к 2030 г. Китай активно инвестирует в соответствующие исследования и разработки, поддерживая стартапы и крупные технологические компании, а также создавая государственные и частные исследовательские центры. ИИ внедряется в различные сектора экономики, включая здравоохранение, транспорт, образование и оборону. Особое внимание уделяется использованию ИИ для повышения уровня кибербезопасности. Кроме того, Китай разрабатывает этические и правовые нормы использования ИИ, создавая благоприятную регуляторную среду, которая стимулирует инновации и обеспечивает безопасность использования искусственного интеллекта.

Важным фактором в функционировании кибервойск КНР является военно-гражданская конверсия. Она представляет собой стратегическую инициативу, направленную на интеграцию гражданских и военных секторов для обеспечения взаимного обмена технологиями и ресурсами. Эта концепция играет ключевую роль в модернизации и усилении боеспособности Народно-освободительной армии Китая, а также в развитии национальной экономики и технологического потенциала страны. Китай активно использует достижения гражданских технологий для укрепления своих вооружённых сил. Современные технологии, такие как искусственный интеллект, беспилотные системы, кибербезопасность и квантовые вычисления, находят широкое применение в военном секторе, что позволяет значительно улучшить оперативные возможности НОАК и найти более эффективные и инновационные решения для выполнения военных задач [14].

Военные подразделения активно внедряют ИИ для улучшения управления войсками, разведки, планирования операций и обеспечения безопасности. Китай также интенсивно разрабатывает и внедряет беспилотные системы, которые используются как в гражданских, так и в военных целях. Беспилотные летательные аппараты (БПЛА) применяются для разведки, наблюдения, доставки грузов и выполнения боевых задач, причём технологии, разработанные для гражданского рынка, находят быстрое применение в военном секторе.

В условиях роста киберугроз Китай уделяет большое внимание развитию кибербезопасности. Гражданские разработки в области киберзащиты и защиты данных интегрируются в системы национальной обороны, обеспечивая высокий уровень безопасности военной информации и коммуникаций. Современные системы управления войсками и контроля за полем боя, разработанные с использованием ИИ, позволяют повысить оперативность и точность принятия решений. Эти системы интегрируются с гражданскими технологиями, обеспечивая более эффективное использование ресурсов и улучшение координации между различными подразделениями [13].

Перспективные оперативные концепции в области кибербезопасности указывают на то, что НОАК будет развивать сетевые возможности для точечных ударов в рамках интегрированных совместных операций в условиях информатизированной локальной войны в ближайшее десятилетие. Однако стратегические планы Си Цзиньпина и его команды выходят за пределы «полной модернизации», которой планируется достигнуть к 2035 г. Их целью является разработка военной теории и концепций для создания «вооружённых сил мирового класса» к 2050 г. [9]. Этот амбициозный план совпадает со столетием основания КНР в 2049 г. и является ключевым элементом более широкой стратегии «возрождения китайской нации».

Председатель КНР не рассматривает модернизацию китайской армии как простое соревнование с мировыми лидерами в этой области. Цели на 2050 г. указывают на стремление Китая стать лидером в военном деле. Это отражено в концепции «интеллектуализированной» войны, где режим противостояния эволюционирует от «системного противостояния» к «алгоритмическому». Преимущество в алгоритмах позволит доминировать в конфликтах за счёт гибридных операций человек — компьютер и принятия решений на основе нейронных сетей, технологий «облачного мозга» и «виртуальных складов». Хотя искусственный интеллект не рассматривается как полная замена человеческим командирам, он может выполнять роль «цифрового штабного офицера», способного собирать и анализировать разведданные, определять намерения противника и контролировать операции [9].

Будущая китайская военная доктрина будет подчёркивать важность инноваций. Концепция военно-гражданского слияния, поднятая Си Цзиньпином до уровня «стратегии национального развития» в 2015 г., направлена на ускорение технологических инноваций в оборонном секторе. Эти инновации будут сосредоточены на новых сферах ведения войны, таких как космос, киберпространство и когнитивная сфера человека. Основой этих усилий станет использование НОАК национальных оборонных больших данных, что поддержит переход к системному или алгоритмическому подходу в вооружённом конфликте [9].

Для достижения этих амбициозных целей Китай активно инвестирует в развитие передовых технологий, включая квантовые вычисления, искусственный интеллект и гиперзвуковые системы. Эти вложения призваны обеспечить НОАК технологическое превосходство и возможность адаптироваться к быстро меняющимся условиям ведения войны. Важным аспектом этой стратегии является также международное сотрудничество и обмен технологиями, что позволяет Китаю интегрировать лучшие мировые достижения в свою военную науку и технику.

Таким образом, модернизация НОАК направлена не только на достижение паритета с ведущими мировыми военными державами, но и на установление нового стандарта в военных делах, где интеллектуальные и алгоритмические преимущества играют решающую роль. Это требует не только технологических новшеств, но и фундаментальных изменений в организационной структуре и подходах к ведению боевых действий, что позволит НОАК стать силой глобального масштаба к середине XXI в.

СТАНОВЛЕНИЕ КИБЕРВОЙСК КНР

Силы стратегической поддержки Народно-освободительной армии Китая были созданы в декабре 2015 г. в рамках масштабной реформы вооружённых сил, инициированной управленцами «пятого поколения» под руководством Си Цзиньпина. Эта реформа направлена на значительное повышение боеспособности НОАК и её готовности эффективно реагировать на современные угрозы национальной безопасности. Ключевыми направлениями реформы стали развитие космических сил и информационных военных возможностей, что отражает стратегический акцент на интеграции передовых технологий и информационного превосходства в оборонную доктрину Китая [15].

Китай рассматривает аналитику больших данных также как стратегический ресурс. Большие данные и ИИ будут способствовать улучшению возможностей НОАК и смогут обеспечить Китаю победу в будущем конфликте. Они предвещают новую эру в ведении

войны, в которой совместные операции, ориентированные на атаку и защиту данных, определяют победу. НОАК исследует программы по сбору, обработке, интеграции и обмену данными по всей силе для различных приложений, включая C4ISR, приобретает нужное оборудование, осуществляет логистику, мобилизацию, обучение, моделирование и симуляцию, а также кибероперации. Эти усилия свидетельствуют о создании инфраструктуры больших данных и применении системного инженерного подхода для использования данных, собранных, хранящихся и передаваемых в этой инфраструктуре [4].

НОАК сосредоточена на использовании аналитики больших данных и инструментов глубокого обучения для улучшения возможностей прицеливания в контексте операций точечного удара в войне на уничтожение систем радиоэлектронной борьбы противника. Улучшение осведомлённости о ситуации на поле боя для командиров НОАК на всех уровнях является неотъемлемой частью усилий по интеграции и распространению данных, с акцентом на обеспечение дальнего удара в условиях фрагментарной информации о целях, полученной от различных датчиков и источников.

Сетевая война также является одной из областей фокуса программы больших данных НОАК. В различных подразделениях НОАК — от сухопутных войск до военно-морских и военно-воздушных сил — реализуются научно-исследовательские проекты и программы, направленные на развитие технологий больших данных и аналитики, координируемые для создания комплексного подхода к сетевой войне, включая кибербезопасность и киберзащиту. Усилия по реструктуризации и модернизации НОАК охватывают более расширенное использование кибертехнологий в военных целях, выходящее за рамки традиционной киберзащиты и включающее как защитные, так и наступательные операции в киберпространстве, направленные на взлом, выведение из строя или взятие под контроль информационных систем противника для достижения информационного превосходства и улучшения собственных боевых возможностей.

Одной из вех на пути к «национальному возрождению» Китая к середине века, определённого Си Цзиньпином, является достижение глобального лидерства в технологиях и приложениях ИИ к 2030 г. Использование ИИ для создания «интеллектуализированной армии» выступает важным элементом этой стратегии. ИИ станет основой для разработки будущих возможностей ведения войны, включая автоматизированные системы поддержки принятия решений для повышения их скорости и точности. Приложения ИИ будут использоваться для создания продвинутых крылатых ракет, автономных воздушных, наземных, надводных и подводных систем дронов, систем противоартиллерийской, противовоздушной и противоракетной обороны и ряда систем управления и контроля [9].

Стремления к инновационной военной стратегии и доктрине зависят от применения передовых технологий больших данных и ИИ для военных целей и интеграции новых возможностей в существующие концепции совместных операций в рамках системной войны. Руководство КПК приоритетно и финансово поддерживает создание необходимых технологий и систем, что позволит НОАК разработать оперативную концепцию, соответствующую будущему полю боя, как в соседних с Китаем регионах, так и в глобальном масштабе.

СИЛЫ СТРАТЕГИЧЕСКОЙ ПОДДЕРЖКИ НОАК

В апреле 2024 г. Народно-освободительная армия Китая сделала значительный шаг вперёд в укреплении своих возможностей в области информационной войны, учредив Силы информационной поддержки [10]. Эти новые подразделения представляют собой интегрированную структуру, целью создания которой является обеспечение информационного превосходства в современных условиях боевых действий, где информационная составляющая становится всё более важной. Одним из ключевых направлений работы этих сил является активное использование технологий искусственного интеллекта, что открывает новые горизонты в области военной стратегии и тактики.

Китайское военное командование считает информационное пространство самостоятельной областью ведения войны, равной физическим областям воздуха, земли, моря и космоса. КПК и НОАК рассматривают операции в этих физических областях как поддержку операций в информационном пространстве. Таким образом, информационное пространство становится центром усилий. Это отличается от типичного взгляда США и их союзников.

Применение искусственного интеллекта в новых информационных подразделениях НОАК позволяет значительно повысить их боеспособность. ИИ используется для анализа больших данных, прогнозирования вражеских действий, автоматизации процессов управления и принятия решений. Системы ИИ помогают быстрее и точнее выявлять угрозы, координировать действия различных подразделений и обеспечивать защиту информационных сетей. Кроме того, ИИ играет ключевую роль в разработке и использовании кибероружия, а также в защите от кибератак.

Си Цзиньпин отмечал важность нового подразделения вооружённых сил: «Информационные поддерживающие силы — это новосозданная стратегическая сила и ключевая поддержка для координации строительства и применения сетевых информационных систем. Необходимо эффективно поддерживать операции, придерживаться информации для достижения совместной победы, обеспечивать бесперебойные информационные связи, интегрировать

информационные ресурсы, укреплять защиту информации и глубоко интегрироваться в совместную операционную систему армии» [9].

Реорганизация, ликвидировавшая Стратегические поддерживающие силы, подчеркнула необходимость более эффективного управления информационными системами НОАК. Информационные поддерживающие силы будут обеспечивать реализацию совместной информационной поддержки для создания сетевой информационной системы, отвечающей требованиям современной войны. Информационные поддерживающие силы, вероятно, будут функционировать на базе бывшей Информационной и коммуникационной базы Стратегических поддерживающих сил [11].

Причины ликвидации Стратегических поддерживающих сил остаются неясными. Возможно, это связано с независимым функционированием их элементов, таких как космические, киберпространственные и коммуникационные сети. Ликвидация Стратегических поддерживающих сил не обязательно должна рассматриваться как неудачный эксперимент, а скорее как шаг к совершенствованию возможностей военной информационной мощи [12].

Си Цзиньпин отметил, что создание Сил информационной поддержки связано с его докладом на 20-м съезде партии в 2022 г., где подчёркивалось значение сетевых информационных систем для повышения боевой эффективности армии. Придание Информационным поддерживающим силам уровня заместителя командующего театром военных действий может быть ответом НОАК на аналогичные усилия Министерства обороны США по консолидации военных информационных сетей в рамках Объединённого вседоменного командования и управления [9].

Дополнительные изменения в организацию НОАК и уточнение ролей и обязанностей в новой структуре могут быть внесены в будущем. Пресс-секретарь НОАК отметил, что «по мере развития обстоятельств и задач мы будем продолжать совершенствовать структуру современных вооружённых сил с китайскими характеристиками» [9]. Мониторинг дальнейшего развития, связанного с информационными организациями НОАК, предоставит необходимые сведения о военных возможностях, стратегии и намерениях Китая.

ВЫВОДЫ

Кибервойска Китайской Народной Республики представляют собой ключевой элемент стратегии национальной безопасности страны. Создание и развитие специализированных киберподразделений, включая ключевые этапы формирования Сил информационной поддержки в 2024 г., отражают стратегическую направленность Китая на укрепление своих позиций в киберпространстве и обеспечение технологического превосходства.

Китай активно интегрирует передовые технологии, такие как искусственный интеллект и большие данные, в свои военные операции. Это подчёркивает значимость кибервойск в защите национальной безопасности и критически важных инфраструктур от кибератак и шпионажа. Кибервойска также играют решающую роль в модернизации вооружённых сил КНР, повышая их способность к управлению военными операциями и их координации.

Важным аспектом стратегии КНР является развитие военно-гражданской конверсии, которая позволяет интегрировать достижения гражданских технологий в военную сферу, значительно повышая боеспособность и оперативные возможности НОАК. Применение ИИ для анализа больших данных, автоматизации процессов и разработки автономных систем способствует созданию инновационных решений для выполнения военных задач.

В перспективе развитие кибервойск НОАК станет критическим фактором в укреплении позиций Китая на международной арене и будет способствовать его превращению в ведущую кибердержаву. Модернизация китайской армии направлена не только на достижение паритета с ведущими мировыми военными державами, но и на установление нового стандарта в военных делах, где интеллектуальные и алгоритмические преимущества играют решающую роль.

Для достижения этих амбициозных целей Китай активно инвестирует в развитие передовых технологий, включая квантовые вычисления, искусственный интеллект и гиперзвуковые системы. Эти инвестиции призваны обеспечить НОАК технологическое превосходство и адаптивность к быстро меняющимся условиям ведения войны. Международное сотрудничество и обмен технологиями также играют важную роль в интеграции лучших мировых достижений в китайскую военную науку и технику.

Развитие кибервойск и информационных технологий становится неотъемлемым элементом стратегии национальной безопасности Китайской Народной Республики. Это требует не только технологических новшеств, но и фундаментальных изменений в организационной структуре и подходах к ведению боевых действий, что позволит НОАК стать силой глобального масштаба к середине XXI в.

ЛИТЕРАТУРА И ИСТОЧНИКИ

1. Кашин В.Б., Кокошин А.А. О подходах руководства КНР и китайских силовых структур к противоборству в киберпространстве // Военная мысль. 2022. № 6. С. 119—126.
2. Кулинич С.В., Шелест А.Б., Сучков А.В. КНР: анализ создания нового вида вооружённых сил // Научная мысль. 2020. Т. 14. № 4-1 (38). С. 80—85.