ВЕСТНИК ВОЕННОГО ИННОВАЦИОННОГО ТЕХНОПОЛИСА «ЭРА», 2022, том 3, № 2, с. 182–194

ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

УДК 355/359

“При разработке новой госпрограммы вооружений важно тщательно учитывать основные мировые тенденции в развитии военной техники и вооружений. Прежде всего это внедрение передовых информационных, био-, когнитивных технологий, …, в том числе за счет применения искусственного интеллекта и, конечно, …, робототехники”

Президент Российской Федерации В.В. Путин.
Заседание Военно-промышленной комиссии. 10.11.2021 г.

ТЕНДЕНЦИИ МОДЕРНИЗАЦИИ ВС США НА ОСНОВЕ ПРОРЫВНЫХ КОНВЕРГЕНТНЫХ ТЕХНОЛОГИЙ

© 2022 г. А. П. Чаднов[1, *]

[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного, Санкт-Петербург, Россия

E-mail: chadap@yandex.ru

Поступила в редакцию 23.12.2021 г.
После доработки 14.01.2022 г.
Принята к публикации 17.01.2022 г.

Усиление геополитического противоборства между США, с одной стороны, и Россией с Китаем – с другой, а также развитие прорывных конвергентных технологий и их внедрение обусловливают необходимость совершенствования этими государствами своих вооруженных сил, способов боевого применения систем и комплексов вооружения, военной и специальной техники в “беспилотных, интеллектуальных” войнах будущего. Проведен анализ доктринальных документов США по модернизации их вооруженных сил, в процессе анализа выявлены основные направления модернизации, базовые прорывные конвергентные технологии, особенности стратегии цифровой модернизации, модернизации систем командования, управления и связи министерства обороны США, кибербезопасности объединенной информационной среды.

DOI: 10.56304/S2782375X22010119

ВВЕДЕНИЕ

Изменение военно-политического и экономического положения в мире, поспешное широкомасштабное развертывание научно-исследовательских и опытно-конструкторских работ по совершенствованию в вооруженных силах (**ВС**) США для удержания глобального доминирования в “новом” мире обусловливают необходимость исследования основных направлений модернизации ВС США с целью адекватного реагирования и осуществления успешного противоборства нашей страны в “беспилотных, интеллектуальных” войнах будущего.

ОСНОВНЫЕ НАПРАВЛЕНИЯ МОДЕРНИЗАЦИИ ВС США

В течение последних четырех лет, начиная с 2018 по 2021 г., министерством обороны (**МО**) США принят ряд стратегий и концепций модернизации ВС.

В открытом доступе опубликованы как изложения (с учетом изъятия закрытых материалов) секретных материалов, так и несекретные материалы следующих доктринальных документов: стратегии национальной обороны (National Defense Strategy, NDS) [1] – в 2018 г.; концепции боевого применения сухопутных войск США в многодоменных операциях [2] – в 2018 г.; стратегии цифровой модернизации МО США (Digital Modernization Strategy, **DMS**) [3] – в 2019 г.; стратегии модернизации сухопутных войск [4] – в 2020 г.; стратегии модернизации командования, управления и связи [5] – в 2020 г.; стратегии данных МО США (DoD Data Strategy, **DDS**) [6] – в 2021 г.; стратегии доминирования в электромагнитном спектре [7] – в 2020 г.; концепции совместных операций в электромагнитном спектре (Joint Electromagnetic Spectrum Operations, **JESO**) [8] – в

2020 г.; концепции объединенного всепространственного командования и управления (Joint All-Domain Command and Control, **JADC**) [9] – в 2021 г.; стратегии искусственного интеллекта [10] – в 2018 г.; стратегии облачных вычислений [11] – в 2018 г.; стратегии кибербезопасности [12] – в 2018 г.; основных принципов корпоративной разработки ПО, безопасности и операций (Development, Security and Operations, **DevSecOps**) [13] – в 2021 г.; объединенной системы связи [14] – в 2019 г.; технологии спутниковой связи [15] – в 2020 г.

Следует отметить отсутствие в этих доктринальных документах упоминания о сетецентрических войнах (Network-Centric Warfare, NCW), которые до этого были широко обсуждаемы как в иностранной, так и в отечественной открытой печати. Кроме того, самого определения понятия "сетецентризма" в последнем "Словаре военных терминов и словосочетаний МО США, с изменениями на 15 февраля 2016 года" [16] не приведено. Это свидетельствует о том, что тема сетецентрических войн, предложенная еще в конце прошлого века вице-адмиралом ВМС США Артуром Цебровски, концепции сетецентрических сред [17, 18] и стратегии сетецентрических сервисов [19], опубликованных МО США в 2005 и 2007 годах соответственно, не получила дальнейшего официального развития.

Прописав в своей стратегии национальной обороны [1] тезис о возрождении соперничества великих держав, США приступило к перестройке ВС под новые задачи эпохи ведения "беспилотных, интеллектуальных" войн будущего в любом пространстве мира, где американскому доминированию в наземном, морском, воздушном, космическом, киберпространстве и в электромагнитном спектре брошен вызов равными по силе вероятными противниками. Поставлена целевая задача по обеспечению боеспособности ВС США "сражаться и побеждать" в войнах в любом из указанных выше пространств и в целом с привлечением союзников и партнеров.

Все стратегии разделяют общую тему "возврата к стратегическому противоборству великих держав", которая утверждает, что "Россия и Китай являются вероятными противниками США и обе эти страны стремятся опрокинуть нынешний международный порядок, основанный на правилах".

В процессе анализа материалов указанных выше доктринальных документов выявлены основные направления (тенденции) модернизации, в которых предусматриваются:

1) реализация МО США основных видов деятельности ВС (ведение войны и боевых действий) на принципах полносетевых систем масштаба корпорации (*Fully Networked Enterprise Systems*, FNES) с реализацией базовых телекоммуникационных услуг и прикладных информационных сервисов [14];

2) переход от ведения военных операций во многих доменах (*multi-domain*) [2] к всепространственным (*all-domain*) [9]: в наземном, морском (включая надводное и подводное), воздушном, космическом и киберпространстве с выполнением в каждом из перечисленных пространств и в целом критически важных объединенных корпоративных операций с электромагнитным спектром (*Electromagnetic Spectrum Operation*, **EMSO**) [7, 8] глобально на различных географических театрах военных действий (**ТВД**);

3) выделение операций с электромагнитным спектром как критически важного показателя в достижении превосходства в пространствах боевых действий [8];

4) осуществление операций объединенным всепространственным командованием и управлением (JADC2) [9] во всех пространствах на ТВД как в кибернетической форме, так и в физическом виде;

5) трансформация существующих систем командования, управления и связи (*Command, Control and Communications*, **C3**) в полносетевые системы командования, управления и связи (*Fully Networked Command, Control and Communications*, FNC3) [5] с обеспечением сквозного обмена мультисервисной информацией (данными, аудио, видео и их сочетанием, а также информационными сигналами и др.) между различными источниками и потребителями информации и обработки ее в интересах получения в реальном времени или близко к реальному времени (в зависимости от вида предоставляемых услуг и сервисов) сведений о ситуационной осведомленности и принятия адекватных решений на основе этой информации;

6) трансформация существующих систем командования, управления, связи, компьютеров (программно-аппаратных комплексов), разведки, в полносетевые системы командования, управления и связи (*Fully Networked Command, Control, Communications, Computers, Intelligence*, FNC4I) с акцентом на обмен мультисервисной разведывательной информацией;

7) совершенствование наряду с ядерным оружием специальной сети связи, оповещения и предупреждения ядерного командования, а также управления с высокой степенью живучести (*Nuclear Command, Control and Communications*, NC3);

8) переход от традиционного ведения электромагнитной войны (*Electromagnetic Warfare*, **EW**) как отдельного от управления использованием спектра (*Electromagnetic Spectrum Management*, EMSM) к операциям с электромагнитным спектром (EMSO) с обеспечением свободы действий и доминирования в данной среде, одновременно

разделяя спектр с военными и коммерческими партнерами, а также снижая его уязвимость;

9) отнесение EW к военным действиям вовлечения использования электромагнитной и направленной энергии для управления электромагнитным спектром и атаками на противника, а также определение данной войны в составе трех составных частей (ранее эти части были разделены): электромагнитная атака (*Electromagnetic Attack*, EA), электромагнитная защита (*Electromagnetic Protection*, EP) и электромагнитное обеспечение (*Electromagnetic Support*, ES) и, как следствие, стирание границы между обороной и нападением;

10) определение управления электромагнитным спектром в виде трех взаимосвязанных функций: распределение частот (*Frequency Management*, FM), координация использования спектра со страной размещения войск (сил) (HNC) и урегулирование помех в совместно используемом спектре (*Joint Spectrum Interference Resolution*, JSIR);

11) переход от модели статического распределения частот к когнитивным функциям совместного использования спектра и маневра его параметрами (некоторой полосой частот в конкретной географической зоне и в определенное время) несколькими его потребителями путем выполнения соглашений (в части политики, протоколов и/или процессов) по снижению вредных электромагнитных помех для удовлетворения растущего спроса на доступ ко все более и более перегруженному и физически ограниченному электромагнитному спектру (*Electromagnetic Spectrum*, EMS);

12) модернизация сети связи информационных систем МО США (*Defense Information Systems Network*, **DISN**), основного компонента сети информационных систем МО США (*DoD Information Network*, **DODIN**) в части транспортной инфраструктуры, коммутации пакетов на основе интернет-протокола версии 6 (**IPv6**) и многопротокольной коммутации по меткам (**MPLS**), а также применение оборудования плотного спектрального мультиплексирования (**DWDM**) на волоконно-оптических линиях;

13) развертывание пассивной оптической сети (*Passive Optical Network*, PON), реализующей конфигурацию “точка–многоточка” с использованием пассивных оптоволоконных разветвителей;

14) создание масштабируемой защищенной среды облачных вычислений МО США масштаба корпорации в составе центральных и граничных центров обработки данных (**ЦОД**) общего назначения (*General Purpose cloud*) и ЦОД специального назначения (*Fit For Purpose cloud*);

15) создание объединенной тактической сети (*Joint Tactical Grid*, **JTG**) для всех ТВД в мире с обеспечением удаленного доступа через сеть связи информационных систем МО США (DISN) к ресурсам сети информационных систем (DODIN);

16) модернизация сети спутниковой связи (**SATCOM**);

17) криптографическая модернизация (CM). Целью криптографической модернизации является обеспечение надлежащего состояния (уровня) безопасности для систем национальной безопасности путем применения сквозных криптографических возможностей, соответствующих оперативным требованиям и условиям выполнения задания. На первом этапе (CM1) этой модернизации планируются списание криптографических средств возрастом более 20–30 лет, переход от систем “точка–точка” к сетевым криптографическим системам, а также принятие контрмер в ответ на расширение возможностей противника. В настоящее время МО и агентство национальной безопасности (*National Security Agency*, **NSA**) США готовятся к криптографической модернизации второго этапа (CM2) по опережению уязвимостей в системе мер обеспечения безопасности и защиты от новых угроз, таких как квантовые вычисления;

18) улучшение точности местоположения, навигации и времени (*Position, Navigation and Timing*, **PNT**), предоставленных в настоящее время глобальной системой позиционирования (*Global Positioning System*, GPS) и наземными атомными часами, а также для проведения навигационной борьбы (*Navigation Warfare*, NAVWAR), поиска решений по определению местоположения, навигации и определения времени в средах, где отсутствует указанная система;

19) развитие подходов по усилению кибербезопасности (*cybersecurity*) объектов критически важной инфраструктуры США, проведение американскими кибервойсками (силами) операций в киберпространстве (*cyberspace*) против вредоносных действий Китая, России, северной Кореи и Ирана в этом пространстве с учетом появления новых угроз и выявления собственных уязвимостей, а также поддержка актуальной киберосведомленности МО США;

20) признание данных как стратегического актива, поддержка их актуальности для выполнения любых процессов в ВС США, принятие решений и поддержка ситуационной осведомленности;

21) обеспечение боеспособности военнослужащего (*soldier lethality*) “будущего” с использованием новых защищенных технологических решений в части разведки, управления и связи, встраиваемых в его боевую экипировку (жилет, экзоскелет) и интегрированных в перспективные тактические сети, а также в зависимости от боевого применения использование дополнитель-

ных к жилету модульных элементов (например, средств виртуальной реальности, средств первой медицинской помощи, рюкзаков разного типа), объединенных в подсистемы.

КОНВЕРГЕНТНЫЕ ТЕХНОЛОГИИ ДОСТИЖЕНИЯ ГЛОБАЛЬНОГО ПРЕВОСХОДСТВА ВС США В "БЕСПИЛОТНЫХ, ИНТЕЛЛЕКТУАЛЬНЫХ" ВОЙНАХ БУДУЩЕГО

Для достижения глобального превосходства ВС США в "беспилотных, интеллектуальных" войнах будущего и обеспечения технологического преимущества МО США сделало ставку на прорывные конвергентные технологии как военного, так и гражданского назначения. Основой выбора прорывных гражданских (коммерческих) технологий является степень их соответствия военным требованиям, а также возможность их доработки и адаптации под боевые условия применения в ВС США.

В открытых материалах стратегий модернизации МО США не полностью приведен пакет прорывных конвергентных технологий, но можно предположить вхождение в этот пакет наряду с новыми оружейными технологиями следующих многообещающих информационных (**ИТ**) и совмещенных инфотелекоммуникационных технологий (ИТК):

а) искусственный интеллект (*Artificial Intelligence*, AI) и машинное обучение (*Machine Learning*, ML). Относится к способностям машин (платформ) выполнять задачи, для которых обычно требуется человеческий интеллект – распознавать закономерности, учиться на опыте, делать выводы и прогнозы, предпринимать действия и многое другое – как в цифровом виде, так и в виде интеллектуального программного обеспечения, лежащего в основе автономных физических систем;

б) реализация IP-протокола IPv6 является стратегическим приоритетом МО США. Существующего адресного пространства IP-протокола версии 4 (IPv4) недостаточно для ожидаемого спроса технологии взаимодействия "все по IP" (*Everything over IP*, EoIP) и дальнейшего роста Интернета, мобильной связи, облачных вычислений и Интернета вещей. Кроме того, перспективные технологии, представляющие интерес для МО США, такие как интеллектуальная инфраструктура, облачные сервисы, автомобильный *Ethernet*, технологии мобильной связи 5-го поколения (**5G**) используют протокол IPv6. Этот протокол обеспечивает расширенное адресное пространство, а также выигрыш по производительности, эффективности управления и поддержку новых возможностей и услуг. Например, он уменьшает размер таблиц маршрутизации и делает ее более эффективной и иерархичной, устраняет проблемы с конфликтом адресов;

в) аналитика больших данных (*Big Data Analytics*, BDA). Подход МО США к аналитике больших данных основан на безопасной, расширяемой, масштабируемой, гибкой и открытой инфраструктурной платформе больших данных (*Big Data Platform*, BDP), предназначенной для обеспечения распределенных вычислений;

г) технология автоматизации процессов безопасной интеграции задач во все этапы жизненного цикла программного обеспечения от проектирования до интеграции, тестирования и его развертывания (*DevSecOps*);

д) гиперконвергентная инфраструктура (*Hyper-Converged Infrastructure*, HCI), объединяющая хранилище, вычислительные и сетевые ресурсы ЦОД в единую систему и обеспечивающая трансформацию парадигмы управления от аппаратного подхода к подходу, ориентированному на приложения, с централизованным управлением, политиками и мобильностью на уровне виртуальных машин;

е) внесерверная или управляемая событиями обработка данных (*Serverless, or Event-driven, Computing*, CEC). В ответ на реальные события необходимый программный код облачных сервисов автоматически загружается и выполняется на сервере ЦОД;

ж) квантовые вычисления (*quantum computing*). Квантовые вычисления, когда они будут воплощены в реальность, станут революционной технологией из-за уникальных возможностей, предоставляющих квантовой механикой. МО США интересуют свойства, которые позволяют кубитам оставаться коррелированными на больших расстояниях, а также способность обрабатывать огромное количество вычислений одновременно и быть в миллионы раз мощнее, чем самые мощные современные суперкомпьютеры, быстро и эффективно решать сложные задачи, которые считались невозможными для классических компьютеров;

з) технология интернета вещей (*Internet of Things*, **IoT**). Интернет вещей важен, так как объект, который может представлять себя в кибернетическом (цифровом) виде, больше не относится только лишь к своему пользователю, но становится связанным с окружающими объектами и информацией базы данных. Ассортимент встроенных датчиков (сенсоров) и подключенных устройств, входящих в состав Интернета вещей, позволяет технологиям обретать способность ощущать, прогнозировать и реагировать на потребности, а также может быть интегрирован в

процессы принятия решений и естественного поведения;

и) технология программно-определяемой сети (SDN) – это общий термин, охватывающий несколько видов инфотелекоммуникационных технологий, направленных на то, чтобы сделать сеть такой же динамичной и гибкой, как виртуализированный сервер и инфраструктура хранения. Ключевые принципы данной технологии – разделение функций передачи, управления, хранения, а также программируемость, виртуализация физических сетевых ресурсов;

к) инфотелекоммуникационные технологии, такие как технологии мобильной/беспроводной связи 5-го и 6-го поколений (5G/6G) и технологии декаметровой связи, а также их возможности, особенно решения по искусственному интеллекту (**ИИ**) технологии 6G как в ее сетях радиодоступа, так и в опорной сети, позволяющие предоставить базовые услуги, и на их основе прикладные интеллектуальные сервисы сетей беспроводной связи объектам обслуживания (различным машинным и человеческим абонентам) в соответствии с их потребностями (например, прикладные тактильные сервисы различных видов виртуальной реальности, удаленной хирургии и много кардинально новых) с необходимой динамически изменяемой пропускной способностью, минимально возможной задержкой обслуживания, теоретически обусловленной только физическими ограничениями скорости света (особенно для связи с высокоскоростными мобильными объектами), выделением виртуальных и физических подсетей в рамках сети беспроводной связи с необходимыми параметрами качества обслуживания (скоростью, задержкой, джиттером), а также помехоустойчивой и помехозащищенной интеллектуальной адаптацией этих сетей к условиям электромагнитной обстановки с учетом естественных и преднамеренных помех;

л) поддержка операций с электромагнитным спектром (**EMSO**) на основе технологий ИИ, реализующих когнитивные функции зондирования атмосферы для оценки ее состояния и прохождения радиосигналов, прослушивания эфира с определением работающих радиоэлектронных средств и принятия решений по вариантам совместного сосуществования и использования частот.

Разработка и внедрение указанных выше технологий и новых оружейных технологий окажет существенное влияние на все сферы деятельности МО США, включая боевое применение, кибербезопасность и обучение войск (сил), командование, управление, связь, компьютеры (программно-аппаратное комплексы), разведку (*Command, Control, Communications, Computers*, C4I), киберпространственные операции и многое другое.

ОСОБЕННОСТИ СТРАТЕГИИ ЦИФРОВОЙ МОДЕРНИЗАЦИИ МО США

Для обеспечения преимуществ в противоборстве великих держав и успехов в постоянно развивающихся глобальных угрозах модернизация цифровой среды ВС является одной из важнейшей задач МО США.

В общем виде модернизация цифровой среды ВС США включает в себя цели, приоритеты и направления достижений приоритетов.

Цели модернизации, приоритеты и направления их достижений показаны на рис. 1.

К целям модернизации относятся: внедрение инноваций для достижения преимуществ в конкурентной борьбе, проведение работ по оптимизации для расширения возможностей и повышения эффективности, развитие кибербезопасности для обеспечения гибкой и устойчивой позиции по вопросам обороны и развитие талантов.

К приоритетам модернизации отнесено: кибердоминирование, кибербезопасность, командование, управление и связь, искусственный интеллект и облачные вычисления.

Направлениями достижений приоритетов модернизации являются повышение боеспособности, расширение партнерства и реформирование.

В процессе модернизации реформированию подлежит: реформирование сетей, услуг данных сетей и прикладных сервисов, организуемых на основе этих услуг, для достижения наилучшего качества обслуживания; оптимизация облачных вычислений и центров обработки данных; реформирование политики и практики управления рисками кибербезопасности.

ОБЪЕДИНЕННАЯ ИНФОРМАЦИОННАЯ СРЕДА

Цифровая модернизация ВС США проводится МО США в соответствии с комплексной программой “Объединенная информационная среда” (*Joint Information Environment*, JIE), включающей в себя ряд программ, проектов и инициатив для поддержки комплексной модернизации во всех структурах МО США и продвижения информационного превосходства общим, скоординированным способом. Объединенный комитет начальников штабов (*Joint Chiefs of Staff*, JCS) одобрил объединенную информационную среду как безопасную сетевую структуру, состоящую из базовой инфраструктуры, корпоративных услуг и сервисов, а также единой архитектуры безопасности.

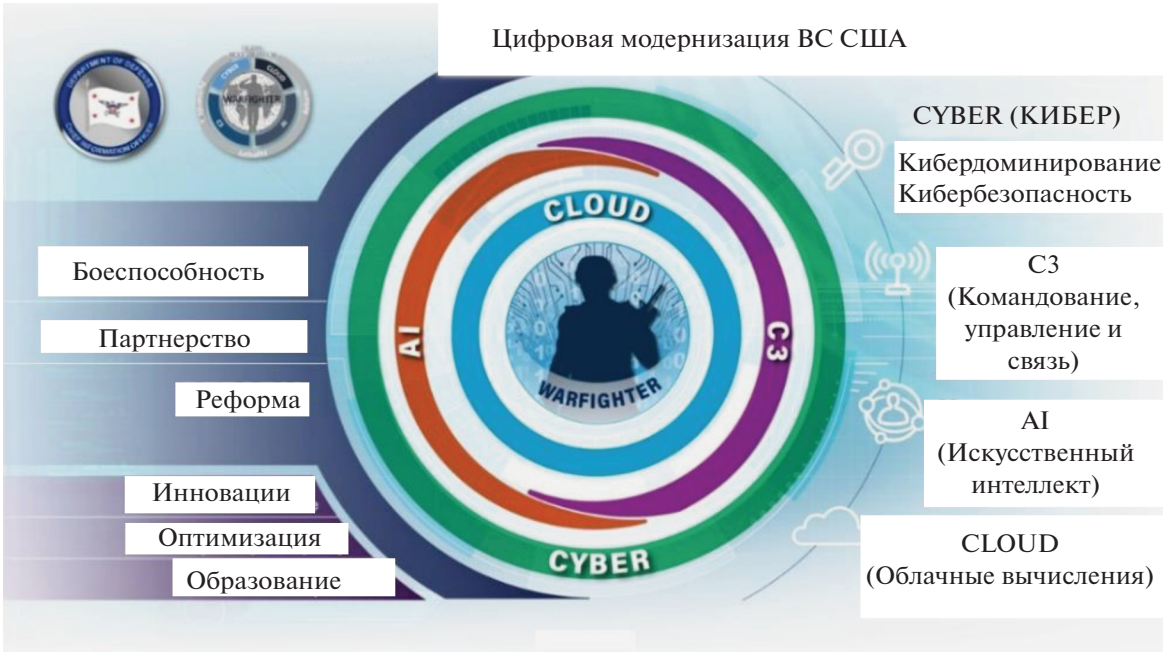

Рис. 1. Общее представление цифровой модернизации ВС США.

В соответствии с этой программой объединенная информационная среда предназначается для повышения эффективности выполнения боевых задач (миссии), усиления кибербезопасности, улучшения взаимодействия, своевременного предоставления возможностей (телекоммуникационных услуг и прикладных информационных сервисов), а также для повышения эффективности применения технологий.

Указанной выше программой вводятся: новые возможности кибербезопасности, включая защиту от кибератак и сетевых вторжений; возможности сети для неподвижных и мобильных абонентов; ряд новых корпоративных (масштаба корпорации) информационных сервисов; многоуровневая структура центров управления сетью и обеспечения безопасности сети.

Сфера действия объединенной информационной среды состоит из десяти целей по наращиванию возможностей, составляющих структуру данной среды. Каждая цель включает в себя одно или несколько основных мероприятий (инициатив), помогающих определять важные аспекты для достижения поставленной цели (табл. 1).

Базовая инфраструктура объединенной информационной среды включает в себя:

– маршрутизируемую сеть несекретной связи на основе интернет-протокола (*Non-classified Internet Protocol Router Network*, NIPRNet) и маршрутизируемую сеть секретной связи на основе интернет-протокола (*Secret Internet Protocol Router Network*, SIPRNet), являющихся двумя из шести основных сетей связи информационных систем МО США (DISN). Оставшиеся четыре включают в себя коммутируемую сеть МО США (*Defense Switched Network*, DSN), закрытую коммутируемую сеть правительственной связи США (*Defense Red Switched Network*, DRSN), объединенную глобальную систему связи разведки (*Joint Worldwide Intelligence Communications System*, JWICS) и сеть управления спутниками (*Satellite Control Network*, **SCN**);

– коалиционные сети, обрабатывающие вплоть до секретной и секретной/разрешенной для передачи (S/REL) информацию;

– развернутые сети связи оперативно-тактического звена управления, подключенные к базовой инфраструктуре.

Инфраструктура объединенной информационной среды приведена на рис. 2. Кроме перечисленного выше в состав данной среды входят основные компоненты, такие как узлы доступа в интернет (*Internet Access Point*, IAP), объединенные стеки региональной безопасности (*Joint Regional Security Stack*, **JRSS**), ЦОД различного назначения, спутниковые шлюзы (*Satellite Gateway*, SATGW), шлюзы поддержки мобильности (*Mobility Gateway*, MGW), шлюзы партнерской среды миссии (*Mission Partner Gateway*, MPG), а также оборудование многопротокольной коммутации по меткам (MPLS) и оборудование плотного спектрального мультиплексирования (DWDM) на волоконно-оптических линиях для сети связи информационных систем (DISN).

Таблица 1. Цели и мероприятия объединенной информационной среды

Цели	Основные мероприятия
1. Модернизация инфраструктуры сети	Модификация оптической транспортной сети Развитие маршрутизаторов многопротокольной коммутации по меткам (*Multi-protocol Label Switching*, MPLS) Упразднение коммутаторов с асинхронным способом передачи (*Asynchronous Transfer Mode*, ATM) и низкоскоростных каналов с мультиплексированием и с временным разделением (*Time Division Multiplexing,* TDM) Модернизация шлюзов спутниковых сетей (*Satellite Communication*, SATCOM), Применение интернет-протокола версии 6 (IPv6)
2. Управление сетью масштаба корпорации	Создание глобальных и региональных центров управления сетью Создание сети управления (администрирования) объединенной информационной среды Объединение решений по управлению ИТ-сервисами Переход от компонентно-центричной к общекорпоративной модели боевых и военных действий
3. Реализация региональной безопасности	Реализация объединенного стека региональной безопасности (*Joint Regional Security Stack*, JRSS) Реализация объединенной системы управления (*Joint Management System*, JMS)
4. Формирование и поддержка партнерской среды миссии (MPE)	Приложения, услуги и сервисы Транспорт Шлюзы ЦОД
5. Оптимизация инфраструктуры ЦОД	Рационализация приложений в ЦОД
6. Реализация согласованных мер по обеспечению безопасности	Возможности по защите периметра сети Безопасность облачных вычислений Защита конечных точек безопасности Аналитические возможности ситуационной осведомленности о кибербезопасности (*Cyber Situational Awareness Analytic Capabilities*, CSAAC) Управление идентификацией, учетными данными и доступом (*Identity, Credential, & Access Management*, **ICAM**)
7. Повышение мобильности в сети	Совершенствование секретности беспроводной мобильной связи Общий набор мобильных приложений МО США
8. Регламентация управление снабжением продуктами ИТ	Соглашение о корпоративном ПО Соглашение о корпоративных лицензиях Соглашение о корпоративном оборудовании Управление ИТ-активами
9. Предоставление услуг и сервисов абонентам	Базовые услуги и сервисы масштаба корпорации (*Enterprise Collaboration and Productivity Services*, ECAPS): набор 1 (офисные), набор 2 и 3 (голос и видео), а также услуги экстренной связи (*Next Generation 9–1–1 Service*): голос видео и текст
10. Предоставление гибридных облачных вычислительных сред	Облачные сервисы

В дополнение к базовой инфраструктуре объединенная информационная среда охватывает тактические компоненты (корабли, летательные аппараты, транспортные средства и т.д.), которые предназначены работать как в соединении с данной инфраструктурой, так и функционировать автономно при потере связи (соединения) с ней.

Подход МО США к кибербезопасности задокументирован в эталонной архитектуре кибербезопасности (*Cybersecurity Reference Architecture*,

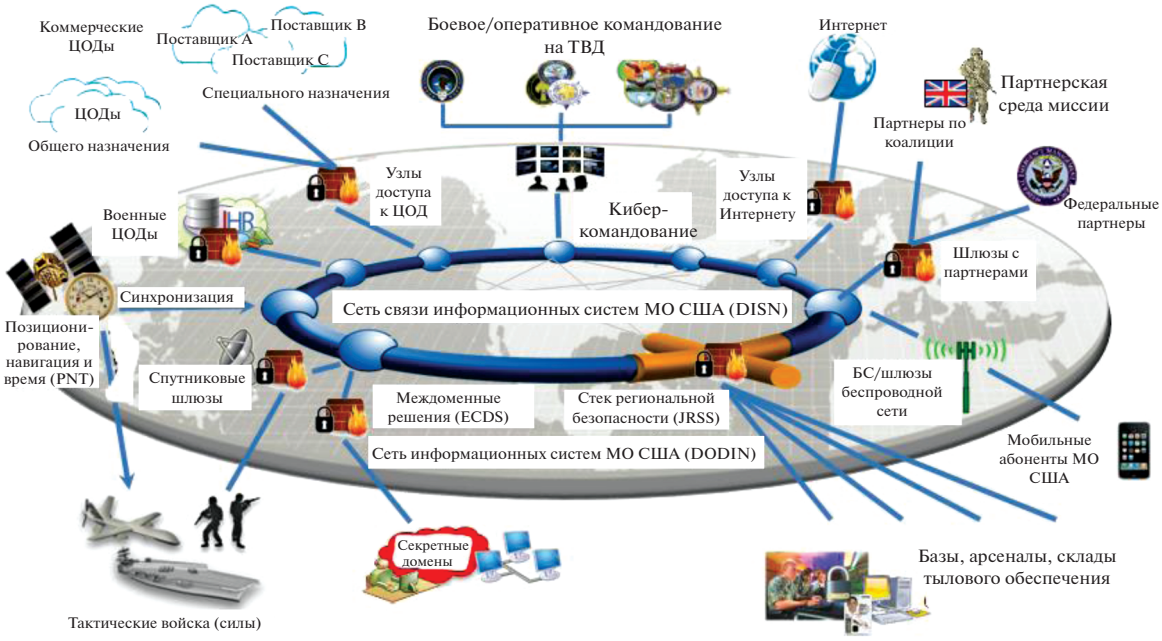

Рис. 2. Инфраструктура объединенной информационной среды ВС США.

CSRA), в которой отражены следующие ключевые принципы кибербезопасности: изоляция, сдерживание, избыточность, уровни защиты, минимальные привилегии, ситуационная осведомленность и физическая/логическая сегментация сетей, сервисов и приложений.

Эталонная архитектура кибербезопасности позволяет обеспечить работу командования и управления, информировать о ситуационной осведомленности, а также обеспечить действия мер внутренней защиты кибероперации (*Defensive Cyber Operations-Internal Defense Measures*, DCO–IDM), повысить уровень кибербезопасности во всех структурах МО США.

Результаты внедрения средств защиты кибербезопасности: информационная сеть МО США (DODIN), включая данные в сети, защищается как единая виртуальная информационная среда с помощью общих процессов и возможностей; средства защиты киберпространства распознают внешние и внутренние угрозы и реагируют на них, принимая соответствующие меры по исправлению, смягчению и восстановлению; командование и управление войсками, которые используют информационную сеть МО США, обеспечиваются общей ситуационной осведомленностью о кибербезопасности сети в целом.

Элементы эталонной архитектуры кибербезопасности: защита периметра сети, безопасность конечных точек беспроводной связи, безопасность средних и конечных точек, безопасность данных (для облачных вычислений в ЦОД), безопасность платформ больших данных, управление идентификацией, учетными данными и доступом (ICAM).

Защита периметра сети масштаба корпорации (*Enterprise Perimeter Protection*, EPP) консолидирует услуги безопасности шлюзов, сокращая расходы и повышая безопасность благодаря централизованному управлению. Данная защита устанавливает защитный барьер между Интернетом, сетями партнеров миссии и коммерческими облачными сервисами, предоставляя возможность обнаруживать, проверять, блокировать и собирать (формировать) трафик в соответствии с политиками безопасности.

Также эта защита обеспечивает основу для маршрутизации интернет-трафика через точку доступа к интернету, маршрутизацию трафика партнеров по миссии через их шлюзы, маршрутизацию несекретного/секретного интернет- и мобильного трафика конечных абонентов через шлюз мобильности и маршрутизацию облачного трафика через точку доступа к облаку.

Необходимо развернуть коммерчески доступные средства мобильной безопасности для защиты конечных точек беспроводной связи от мобильных угроз и улучшенного управления безопасностью мобильными устройствами на базе операционной системы Android.

Ключевым элементом безопасности средней точки или региональной безопасности являются объединенные стеки региональной безопасности (JRSS). С помощью такого стека весь поступающий и выходящий трафик с помощью набора датчиков (сенсоров) безопасности проверяется на

наличие угроз кибербезопасности. Помимо местного анализа полученные данные по безопасности предоставляются более широкому аналитическому потенциалу МО США с целью проведения корпоративного анализа для более быстрого и эффективного реагирования на угрозы кибербезопасности.

Безопасность конечных точек обеспечивается объединенной группой людей, процессов и технологий, работающих вместе для предотвращения несанкционированного доступа к конечным точкам, выявления и устранения вредоносных кодов и несанкционированных программ, а также предотвращения выполнения данных программ. Кроме того, безопасность конечных точек защищает авторизованные платформы/устройства, которые подключаются к информационной сети (DODIN), позволяя авторизованным абонентам получать безопасный доступ к ресурсам объединенной информационной среды из любого места и в любое время, используя любое аутентифицированное устройство.

Управление идентификацией, учетными данными и доступом (ICAM) реализуется четырьмя основными компонентами: управление цифровой идентификацией: создание цифровой идентификации и управление жизненным циклом; управление учетными данными: выдача физического или электронного токена в качестве заместителя (прокси) для достоверной цифровой идентификации; аутентификация: подтверждение личности с помощью учетных данных и подтверждение подлинности этих учетных данных; авторизация: санкционирование доступа на основе цифровых политик и достоверной информации о запрашиваемых удостоверениях личности и доступном ресурсе.

С целью кардинального повышения уровня кибербезопасности МО США совместно с агентством оборонных информационных систем (*Defense Information Systems Agency*, DISA), американским киберкомандованием (*U.S. Cyber Command*, USCYBERCOM) и агентством национальной безопасности (NSA) начиная с 2019 г. вплотную исследуют новую стратегию кибербезопасности, именуемую как “безопасность с нулевым доверием” (*Zero Trust Security*, ZTS). Ориентированная на данные модель этой стратегии исключает понятие о доверенных и недоверенных сетях, устройствах, абонентах, процессах и переходит к многопараметрическим (многокритериальным) уровням доверия, которые позволяют проводить политику аутентификации и авторизации в соответствии с концепцией наименее привилегированного доступа.

МОДЕРНИЗАЦИЯ СИСТЕМ КОМАНДОВАНИЯ, УПРАВЛЕНИЯ И СВЯЗИ МО США

Ввиду основополагающего значения систем командования, управления и связи (С3) во всех военных операциях ВС США проанализирована стратегия модернизации данных систем [5]. Необходимость модернизации данных систем обусловлена следующими факторами:

– существующие системы командования, управления и связи ВС США, основанные на столбовых платформенноцентричных подходах, не только не успевают за угрозами вероятных противников, но и не удовлетворяют постоянно растущим потребностям объединенных войск (сил) в устойчивом, надежном, своевременном обмене необходимой информацией, а также обработке, хранении и предоставлении данной информации в различных прикладных сервисах и услугах связи;

– растущими потребностями объединенного всепространственного командования и управлением (**JADC2**) в новых знаниях и концепциях ведения “беспилотной, интеллектуальной” войны будущего, в прорывных конвергентных технологиях, в экспериментах и устойчивых инвестиций;

– проблемами тактической сети и систем, разрабатываемых начиная с 2002 г. в ходе трех этапов программы управления проектом “боевая тактическая информационная сеть” (*Project Manager Warfighter Information Network-Tactical*, **PM WIN-T**) [20] с применением технологий [21], устаревших за 16 лет разработок в рамках данной программы. 27 сентября 2017 г. конгрессом США [22] предложено приостановить финансирование дооснащения тактической сети и двух систем решениями, разрабатываемые по третьему этапу данной программы;

– неудовлетворенность сухопутных войск США [23] услугами тактической сети: перечнем услуг, качеством обслуживания, особенно в режиме “движения”, уровнями предоставления (батальонный, ротный) услуг наземными, воздушными и спутниковой компонентами данной сети, возможностью удаленного доступа к ресурсам информационных систем в местах их постоянной дислокации, а также возросшей уязвимостью кибербезопасности сети к угрозам современных средств радиоэлектронной борьбы вероятного противника (особенно России).

С целью поддержки эффективных совместных, многонациональных операций объединенного всепространственного командования и управления (JADC2) данная стратегия сфокусирована на построении полностью сетевых систем командования, управления и связи (*Fully Networked Command, Control, and Communications*,

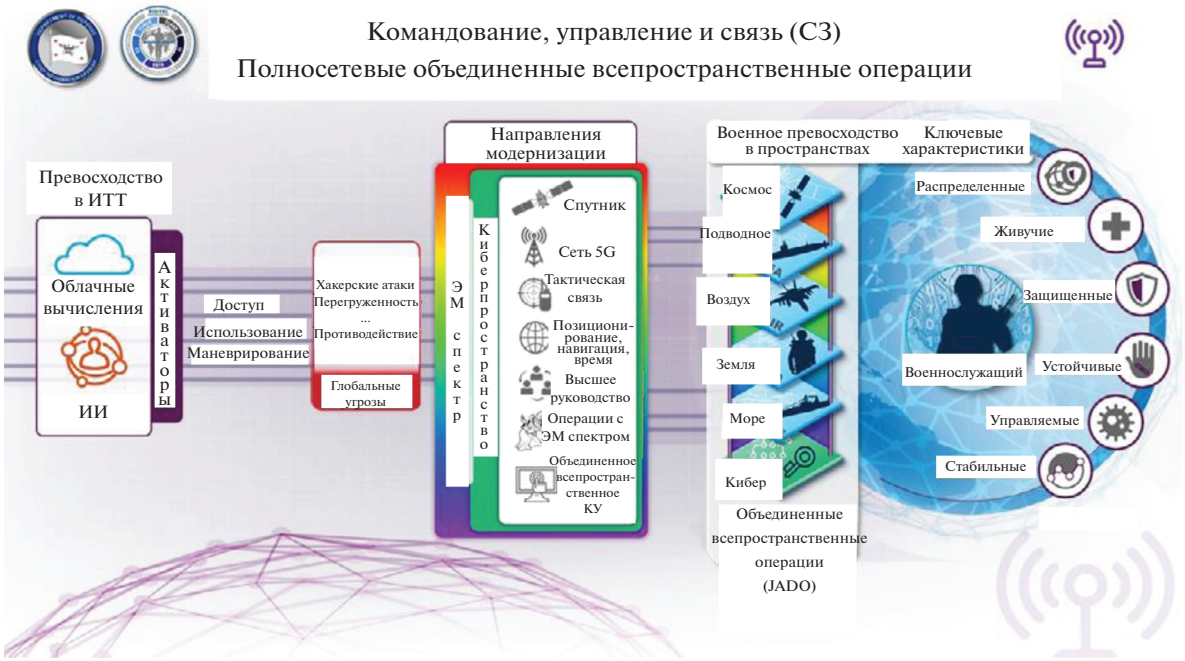

Рис. 3. Модернизация командования, управления и связи ВС США.

FNC3) с переходом от столбовых подходов к сетевым решениям (рис. 3).

Цели, представленные в данной стратегии, согласованны со стратегией **DMS** МО США и с другими руководящими документами более высокого уровня, например с концепцией операций объединенных войск (сил).

В стратегии определены девять целей и для каждой цели определены несколько задач в виде направлений действий (*Lines of Effort*, **LOE**):

1) разработка и внедрение гибких операций с электромагнитным спектром (EMSO);

2) повышение качества доставки и устойчивости информации о положении, навигации и времени (PNT);

3) укрепление командного потенциала национального руководства (*National Leadership Command Capability*, **NLCC**);

4) обеспечение интегрированных и функционально совместимых возможностей связи вне прямой видимости (*Beyond-Line-of-Sight Communications*, **BLOS**);

5) ускорение и координация поступления на вооружение модернизованных систем тактической связи;

6) создание и внедрение экосистемы связи общественной безопасности МО США (*Public Safety Communications*, **PSC**);

7) создание условий для ускоренного развертывания инфраструктуры беспроводной сети мобильной связи 5G и использование сетей данного поколения за пределами США;

8) обеспечение создания устойчивых и быстро реагирующих (оперативных) систем командования и управления (*Command and Control*, **C2**);

9) предоставление возможностей и сервисов партнерской среды миссии (*Mission Partner Environment*, **MPE**).

Из указанных выше целей модернизации систем командования, управления и связи отметим наиболее критически важные новые подходы к операциям с электромагнитным спектром и технологические подходы к модернизации и развитию сетей.

РАЗРАБОТКА И ВНЕДРЕНИЕ ГИБКИХ ОПЕРАЦИЙ С ЭЛЕКТРОМАГНИТНЫМ СПЕКТРОМ

Операции в электромагнитном спектре и работа по модернизации с ним, показанные на рис. 4, будут осуществляться за счет облачных технологий и технологий ИИ с предоставлением возможностей и сервисов, позволяющих осуществлять динамический доступ к электромагнитному спектру и маневрирование его параметрами.

Исходя из критически важных операций с электромагнитным спектром в “беспилотных, интеллектуальных” войнах будущего МО США сконцентрировало задачи разработки и внедрения гибких операций с данным спектром в пять направлений действий:

1) улучшение сбора и агрегирования данных об электромагнитном спектре для предоставления

Рис. 4. Операции с электромагнитным спектром.

точной, актуальной, видимой, понятной и достоверной информации;

2) разработка аналитической обработки данных с использованием ИИ для повышения качества принятия решений в операциях с электромагнитным спектром;

3) совершенствование компетенции в понимании ситуационной осведомленности об электромагнитном спектре для определения и уменьшения рисков в перегруженной и противоборствующей электромагнитной среде;

4) разработка когнитивных, динамических возможностей доступа к спектру и совместного использования частот;

5) внедрение в спектрально-зависимые системы стандартных интерфейсов динамического управления рисками доступа к электромагнитному спектру.

ОБЕСПЕЧЕНИЕ ИНТЕГРИРОВАННЫХ И ФУНКЦИОНАЛЬНО СОВМЕСТИМЫХ ВОЗМОЖНОСТЕЙ СВЯЗИ ВНЕ ПРЯМОЙ ВИДИМОСТИ

В настоящее время за пределами зоны прямой радиовидимости спутниковая связь (SATCOM) МО США является основным средством связи для передачи больших объемов данных по всему миру.

Однако, несмотря на постоянные усилия по запуску новых спутниковых группировок и использование пропускной способности коммерческих спутников на контрактной основе, сегодняшние возможности за пределами зоны прямой радиовидимости в эфире с отказами-отключениями, с прерывистой и низкой пропускной способностью, а также с существенной задержкой недостаточны для будущих всепространственных операций. Уязвимость спутниковой связи к атакам электромагнитной войны порождают риски в условиях противоборства в электромагнитном спектре.

Исходя из данного обстоятельства МО США планирует реагировать на эту ситуацию путем модернизации технологий спутниковой связи и поиска новых технологий, поддерживающих [15] связь за пределами зоны прямой радиовидимости. Из шести задач по обеспечению интегрированных и функционально совместимых возможностей связи вне прямой видимости, за исключением организационных действий, можно выделить три технические задачи:

1) постановка на вооружение модернизированных комплексов спутниковой связи МО США (включая абонентские терминалы) для доставки услуг до ротных уровней тактической сети;

2) информированное и оперативное управление ресурсами спутниковой связи МО США;

3) разработка перспективных технологий поддержки высокочастотной (декаметровой) связи для сред с отсутствием прямой радиовидимости и спутниковой связи.

УСКОРЕНИЕ И КООРДИНАЦИЯ ПОСТУПЛЕНИЯ НА ВООРУЖЕНИЕ МОДЕРНИЗОВАННЫХ СИСТЕМ ТАКТИЧЕСКОЙ СВЯЗИ

Существующая панорама сетей тактической связи на ТВД сложна и фрагментирована. Она включает в себя множество разнообразных комплексов (систем), которые в целом не обеспечивают производительность, совместимость и безопасность тактических сетей. В результате на ТВД представлена смесь аналоговых и цифровых комплексов, состоящая из более чем миллиона терминалов, установленных на нескольких платформах военных ведомств, союзников и партнеров по коалиции, которые соединяются с использованием шлюзов сотнями различимых форм сигналов и протоколов с многочисленными подвариантами.

Быстрый прогресс в инфотелекоммуникационных технологиях и изменение характера войн будущего требуют более разумного и скоординированного подхода к созданию сетей тактической связи, которые должны обеспечить объединенному всепространственному командованию (JADC2) решающее информационное преимущество над вероятными противниками.

Для достижения цели по ускорению и координации поступления на вооружение модернизованных систем тактической связи предусмотрены четыре задачи, две из которых приведены ниже:

– руководство созданием объединенной тактической сети (JTG) со сменой акцента от устаревших стволовых, платформенно-центричных подходов на поддержку полносетевых тактических систем командования, управления и связи масштаба корпорации (*fully-networked enterprise tactical*, C3);

– развитие объединенной тактической сети (JTG) на основе перспективных инфотелекоммуникационных технологий.

МО США активно поддерживает поставленную советом национальной безопасности США цель по улучшению цифровой инфраструктуры Америки путем развертывания на военных объектах страны технологии мобильной связи 5G и экспериментирования с ней в ответ на обязательство, выраженное в 2019 г. президентом США сделать Америку не только первой в мире по применению данной технологии, но и по обеспечению лидерства в разработке аналогичной технологии 6G.

Задачи, начиная от координации политики и заканчивая исследованиями в области концепции сетей 5G, включают:

– определение спектра 5G в дополнение к уже имеющемуся;

– гармонизацию спектра 5G по всему миру;

– разработку стандартов 5G, политики в области кибербезопасности;

– ускорение МО США адаптации и внедрение технологии 5G.

После опубликования указанной выше стратегии модернизации командования, управления и связи стартовал экспериментальный этап крупномасштабных экспериментов по прототипированию и продвижению технологий мобильной связи пятого поколения. Для этого на первом этапе проекта выделено 600 млн. долларов. Испытание планируется проводить на пяти военных испытательных полигонах США. Цель данного проекта – в краткие сроки создать масштабируемую, устойчивую и надежную беспроводную сеть мобильной связи пятого поколения как лабораторию для проведения различных экспериментов в интересах ВС США. Партнерами в экспериментах являются телекоммуникационные и оборонные компании, в частности оператор мобильной связи AT&T Inc. и оборонный подрядчик General Dynamics Corp.

Для осуществления американского превосходства в мире (в первую очередь над Китаем) и поддержки всех функций ведения военных и боевых действий в цифровых “беспилотных, интеллектуальных” войнах будущего МО США планирует усовершенствовать технологию мобильной связи пятого поколения 5G и инвестировать солидные средства в будущие технологии беспроводной связи шестого поколения 6G/Network 2030. Для продвижения глобального лидерства Северной Америки в развитии 6G МО США принимает активное участие в программе “Next G Alliance” организации ATIS (Alliance for Telecommunication Industry Solutions) [24].

ЗАКЛЮЧЕНИЕ

С целью достижения глобального доминирования в мире США вступило в новую технологическую эру геополитического противоборства с Россией и Китаем. Для выполнения данного целеполагания и успешного ведения военных и боевых действий в “беспилотных, интеллектуальных” войнах будущего глобально во всех пространствах мира МО США принят ряд стратегий и концепций модернизации ВС на основе прорывных конвергентных технологий.

Выявленные направления и технологические особенности модернизации ВС США позволят Российской Федерации учесть их в концепциях войн будущего.

СПИСОК ЛИТЕРАТУРЫ

1. Summary of the 2018. National Defense Strategy of the United States of America. Sharpening the American Military’s Competitive Edge. https://dod.de-

fense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
2. TRADOC Pamphlet 525–3–1. U.S. Army in Multi-Domain Operation 2028. December 2018. https://info.publicintelligence.net/USArmy-Multidomain-Ops2028.pdf
3. DoD Digital Modernization Strategy. CLEARED for Open Publication. Jul. 2019. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF
4. The Army's Modernization Strategy: Congressional Oversight Considerations. February 7, 2020. https://sgp.fas.org/crs/natsec/R46216.pdf
5. C3 Modernization Strategy. September 2020. https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf
6. Executive Summary: DoD Data Strategy. Unleashing Data to Advance the National Defense Strategy. Sep 2020. CLEARED for Open Publication. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF
7. Department of defense. Electromagnetic Spectrum Superiority Strategy. October 2020. https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF
8. Department of defense. Joint Electromagnetic Spectrum Operations. May 2020. https://irp.fas.org/doddir/dod/jp3_85.pdf
9. Joint All-Domain Command and Control: Background and Issues for Congress. Updated August 12, 2021. https://crsreports.congress.gov/product/pdf/R/R46725
10. Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF
11. DoD Cloud Strategy. December 2018. UNCLASSIFIED. https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF
12. SUMMARY. DEPARTMENT OF DEFENSE CYBER STRATEGY. 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
13. DoD Enterprise DevSecOps Fundamentals. Unclassified. CLEARED for Open Publication. May 12.2021. https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsFundamentals.pdf
14. Joint Publication 6–0. Joint Communications System. 10 June 2015. Incorporating Change 1. 04 October 2019. https://irp.fas.org/doddir/dod/jp6_0.pdf
15. ATP 6–02.54. TECHNIQUES FOR SATELLITE COMMUNICATIONS. NOVEMBER 2020. https://irp.fas.org/
16. Joint Publication 1–02. 8 November 2010 (As Amended Through 15 February 2016). Department of Defense Dictionary of Military and Associated Terms. https://irp.fas.org/doddir/dod/jp1_02.pdf
17. Net-centric Operational Environment JOINT INTEGRATING CONCEPT, Version 1.0, 31 OCTOBER 2005) https://dodcio.defense.gov/Portals/0/Documents/netcentric_jic.pdf
18. Net-centric Environment Joint Functional Concept, 07 February April 2005) http://extras.sltrib.com/Utah_Data_Center/netcentric_jfc-1.pdf
19. Department of Defense Net-Centric Services Strategy. Strategy for a Net-Centric, Service Oriented DoD Enterprise. March 2007. Prepared by the DoD CIO. https://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf
20. Project Manager Warfighter Information Network-Tactical. https://military.wikia.org/wiki/PM_WIN-T
21. ATP 6–02.60. 3 February 2016. TECHNIQUES FOR WARFIGHTER INFORMATION NETWORK-TACTICAL. https://irp.fas.org/doddir/army/atp6-02-60.pdf
22. The Army's Warfighter Information Network-Tactical (WIN-T) Program. October 10, 2017. https://www.everycrsreport.com/files/20171010_IN10799_4f753f0d27c8020000750bec410a073034988c56.pdf
23. RECORD VERSION STATEMENT BY LIEUTENANT GENERAL BRUCE T. CRAWFORD ARMY CHIEF INFORMATION OFFICER. https://docs.house.gov/meetings/AS/AS25/20170927/106451/HHRG-115-AS25-Wstate-CrawfordB-20170927.pdf
24. Next G Alliance an ATIS initiative. Building the foundation for North American leadership in 6G and beyond. https://nextgalliance.org/