ЗМІСТ

Операции в киберпространстве и радиоэлектронная борьба. Боевой устав армии США FM 3-12. Ворожою мовою

Анотація

Боевой устав FM 3-12 определяет и описывает принципы и тактику решения задач в оперативной обстановке, а также даёт представление о боевых действия (операциях) в киберпространстве, ведении РЭБ, их планировании, внедрении и согласовании в рамках оперативного процесса (операций). В нём описываются части и подразделения, проводящие эти операции, и то, как они обеспечивают достижение целей командиров в боевых действиях (операциях) сухопутных войск.

БОЕВОЙ УСТАВ АРМИИ США FM 3-12

Издательский дом
«С В А Р О Г»
Киев — 2024

УДК 621.396.663
О-60

О-60 **Операции в киберпространстве и радиоэлектронная борьба. Боевой устав армии США FM 3-12. Ворожою мовою**. — Киев: Изд. дом «СВАРОГ», 2024. — 228 с.

ISBN 978-611-01-3456-9

Боевой устав FM 3-12 определяет и описывает принципы и тактику решения задач в оперативной обстановке, а также даёт представление о боевых действия (операциях) в киберпространстве, ведении РЭБ, их планировании, внедрении и согласовании в рамках оперативного процесса (операций). В нём описываются части и подразделения, проводящие эти операции, и то, как они обеспечивают достижение целей командиров в боевых действиях (операциях) сухопутных войск.

ISBN 978-611-01-3456-9 УДК 621.396.663

Оглавление

ВСТУПИТЕЛЬНОЕ СЛОВО

За последние два десятилетия незатухающих конфликтов сухопутные войска развернули самые мощные системы связи за всю свою историю. В течение этого времени вооружённые силы США продолжали доминировать в киберпространстве и электромагнитном спектре, проводя операции в Афганистане и Ираке против противника, не способного оспорить технологическое превосходство США. Однако, в последние годы региональные соперники продемонстрировали внушительный потенциал в гибридных войнах. Эти возможности угрожают доминированию сухопутных войск США как в киберпространстве, так и в электромагнитном спектре.

Информационная сеть министерства обороны – сухопутные войска США является неотъемлемой площадкой для ведения боевых действий и критической составляющей системы командования и управления, на которой строится успех операций сухопутных войск. Эффективная эксплуатация, обеспечение безопасности и защита сети для поддержания доверия к её конфиденциальности, целостности и доступности является залогом успеха командиров на всех уровнях. Командир, не имеющий доступа к коммуникационным и информационным системам и данным, рискует потерять жизни подчинённых, утратить критически важные ресурсы или провалить боевую задачу.

В то же самое время противник также все больше полагается на сети и системы вооружения, связанные с сетевыми технологиями. Сухопутные войска, как часть объединённых (межвидовых) сил, должны быть готовы использовать или лишить противника оперативных преимуществ, которые предоставляют эти сети и системы.

По мере того, как сухопутные войска переключают своё внимание на крупномасштабные боевые действия против региональных соперников, мы должны понимать, что противник будет постоянно пытаться получить доступ, найти уязвимости и ухудшить состояние наших сетей и данных.

В будущем, по мере роста возможностей противника, наше продолжающееся господство в киберпространстве и электромагнитном спектре станет менее очевидным, в то же время наша способность получать доступ к киберпространству и зависящим от спектра возможностям станет, как более сложной, так и более важной для борьбы и победы в различных доменах.

Эффективное использование поражающих факторов киберпространства и РЭБ на всех этапах противоборства является ключом к достижению относительных преимуществ в киберпространстве и электромагнитном спектре, при одновременном лишении противника аналогичных возможностей. Для достижения таких относительных преимуществ командиры должны внедрять и согласовывать операции в киберпространстве и ведение РЭБ с прочими силами и средствами вооружённой борьбы путём совместных действий различных родов войск.

Кроме того, для успешного планирования, согласованности и проведения операций в киберпространстве и ведения РЭБ, критически важными являются разведывательная и информационная деятельность, средства связи, а также космический и огневой потенциал. Командиры и штабы осуществляют внедрение и согласование этих возможностей в различных доменах и аспектах боевого обеспечения для достижения максимального взаимодополняющего поражающего воздействия в киберпространстве и электромагнитном спектре.

Боевой устав FM 3-12 определяет и описывает принципы и тактику решения задач в оперативной обстановке, а также даёт представление о боевых действия (операциях) в киберпространстве, ведении РЭБ, их планировании, внедрении и согласовании в рамках оперативного процесса (операций). В нём описываются части и подразделения, проводящие эти операции, и то, как они обеспечивают достижение целей командиров в боевых действиях (операциях) сухопутных войск.

В связи с быстрым развитием своих возможностей, тактики, техники и процедур в киберпространстве и электромагнитном спектре, Головной центр кибероперацій будет пересматривать и обновлять Боевой устав FM 3-12 и вспомогательные публикации, чтобы не отставать от постоянно меняющейся оперативной обстановки.

Нейл С. Херси (NEIL S. HERSEY)

генерал-майор, командование сухопутных войск США

ВВЕДЕНИЕ

Боевой устав FM 3-12 предусматривает реализацию доктрины сухопутных войск по использованию кибер-электромагнитной деятельности для внедрения и согласования боевых действий (операций) в киберпространстве и ведения РЭБ в рамках операций при управлении выделенными участками электромагнитного спектра в интересах совместных наземных операций. Боевой устав FM 3-12 определяет и даёт понимание кибероперациий сухопутных войск, ведения РЭБ, уставных и должностных полномочий, ролей, отношений, обязанностей и возможностей для обеспечения боевых действий (операций) сухопутных войск и объединенных операций. В нём раскрываются методы СВ ведения наступательных и оборонительных кибероперациий, а также рассматриваются способы внедрения командирами и штабами возможностей киберпространства и РЭБ в рамках всего спектра военных операций.

Боевой устав FM 3-12 охватывает и обосновывает доктрину по объединённым кибероперациям и РЭБ и публикацию ADP 3-0: Доктрина Сухопутных войск – «Операции» (ADP 3-0, Operations) и содержит положения доктрины для рассмотрения взаимосвязи между оперативным процессом сухопутных войск и кибероперациями и РЭБ. Для понимания основ внедрения и согласования кибероперациий и РЭБ читатель должен быть знаком с изданиями: ADP 2-0, ADP 3-0, ADP 3-19, ADP 3-37, ADP 3-90, ADP 5-0, ADP 6-0, FM 3-09, FM 3-13, FM 3-55, FM 6-0, ATP 2-01.3, JP 3-12, и JP 3-85.

Боевой устав FM 3-12 раскрывает, как личный состав, участвующий в кибер-электромагнитной деятельности, внедряет и согласовывает функционал и возможности кибероперациий и РЭБ в рамках боевого обеспечения, защищает сеть и предоставляет командирам критически важные возможности на всех уровнях в ходе совместных наземных операций.

Боевой устав FM 3-12 содержит четыре главы и семь приложений.

В главе 1 описывается как кибероперации и РЭБ обеспечивают поддержку сухопутных войск при проведении совместных наземных операций. В ней даётся обзор аспектов оперативной обстановки, в которой части и подразделения проводят кибероперации и ведут РЭБ. В данной главе также подробно представлено, как кибероперации и ведение РЭБ оказывают поддержку в боевом обеспечении сухопутных войск.

В главе 2 подробно рассмотрены виды кибероперациий и РЭБ, а также связанные с ними задачи и общие поражающие факторы. В ней также рассматривается взаимосвязь кибероперациий и РЭБ с другими видами операций сухопутных войск.

В главе 3 представлен обзор организационных структур объединённых сил и сухопутных войск, осуществляющих кибероперации и РЭБ. В ней также описываются роли и обязанности специального отделения кибер-электромагнитной деятельности на различных уровнях. В этой главе рассматривается взаимодействие отделения кибер-электромагнитной деятельности с другими структурными подразделениями штаба и объясняется роль рабочей группы по кибер-электромагнитной деятельности.

В главе 4 рассмотрено, каким образом командиры и штабы осуществляют внедрение и согласование кибероперацій и РЭБ в рамках оперативного процесса. Далее в главе более подробно представлены ключевые исходные и выходные данные, связанные с разведывательной подготовкой района боевых действий, сбором информации, целеуказанием, управлением рисками и информацией.

В Приложении А описаны две наиболее распространённые методики принятия решений в сухопутных войсках (Методика выработки комплексных решений и процесс принятия военных решений) и порядок их применения для планирования, внедрения и согласованности кибероперацій и РЭБ с оперативным и интеграционным процессами.

В Приложении В описаны правила ведения боевых действий и соответствующие разделы Кодекса США, связанные с кибероперациями и РЭБ. Оно включает таблицу, в которой приведены все кибероперации и РЭБ, относящиеся к законодательству США (титульные полномочия). Приложение В содержит таблицу с перечнем федеральных законов, защищающих информацию и права граждан США на неприкосновенность частной жизни.

В Приложении С рассматриваются вопросы, связанные с проведением кибероперацій и РЭБ в составе объединённых сил или с другими участниками совместных действий[1].

В Приложение D рассматриваются национальные силы и средства, силы и средства министерства обороны и резерва СВ США, которые обеспечивают кибероперации. В данном приложении также приводится обзор Киберкомандования США и подчинённых ему объединённых структурных подразделений, обеспечивающих поддержку кибероперацій и РЭБ общевойсковых командиров, использующих силы и средства для выполнения задач в киберпространстве.

В Приложении Е рассматривается, каким образом подразделения сухопутных войск осуществляют запрос на поддержку кибероперацій и РЭБ при совместных действиях. Графические изображения отображают процессы запроса на поддержку как при наступательных, так и при оборонительных кибероперациях.

[1] Участники совместных действий (*англ. unified action partners*) – военные силы, правительственные и неправительственные организации, а также составляющие частного сектора, с которыми вооружённые силы осуществляют планирование, взаимодействие, согласование и внедрение своих действий во время проведения операций – прим. пер.

В Приложении F представлен общий порядок действий для улучшения приёмов и возможностей РЭБ. В нём описаны четыре фазы улучшения приёмов и возможностей РЭБ и их три основные категории и действия.

В Приложении G приводится обзор подготовки военнослужащих и более подробно рассматривается подготовка тех, кто стремится получить профессию в области кибероперациий и ведения РЭБ.

ГЛАВА 1. ОБЩЕЕ ПРЕДСТАВЛЕНИЕ ОБ ОПЕРАТИВНОЙ ОБСТАНОВКЕ

В данной главе описаны аспекты оперативной обстановки, в которой сухопутные войска проводят кибероперации и РЭБ. Рассмотрены их прямые обязанности и изложены фундаментальные принципы ведения кибероперациий и РЭБ. В главе представлены взаимосвязи между кибероперациями, РЭБ и другими аспектами боевого обеспечения.

Общее представление об оперативной обстановке

1-1. Кибероперации и РЭБ играют важную роль в проведении сухопутными войсками совместных наземных операций в составе объединённых сил и во взаимодействии с другими участниками совместных действий.

Кибероперации *(англ. Cyberspace operations, CO)* – это использование средств воздействия на киберпространство, основной целью которых является достижение целей в киберпространстве или с его помощью (JP 3-0).

Радиоэлектронная борьба *(англ. Electromagnetic warfare, EW)* – это военные действия, связанные с использованием электромагнитной и направленной энергии для контроля электромагнитного спектра или для нападения на противника (JP 3-85).

1-2. Киберпространство является одной из пяти сфер, в которых ведутся боевые действия. Операции проводятся в части электромагнитного спектра ((далее – ЭМС) (*англ. electromagnetic spectrum*, *EMS*), например, Bluetooth, Wi-Fi, спутниковый трафик. Поэтому кибероперации и РЭБ требуют распределения радиочастот, управления ими и взаимодействия между операторами средств РЭБ, через которые осуществляются операции по управлению электромагнитным спектром. Операции по управлению спектром состоят из четырёх ключевых функций: управление спектром, распределение частот, взаимодействие со страной пребывания войск и соблюдение правил. Операции по управлению спектром включают предотвращение и уменьшение конфликтов в радиосети и электромагнитных помех (далее – ЭМП) (*англ. electromagnetic interference, EMI*) между своими войсками и войсками страны пребывания во время операций сухопутных войск (см. Наставление ATP 6-02.70).

Киберпространство и электромагнитный спектр

1-3. Киберпространство и ЭМС имеют решающее значение для успеха в современной оперативной обстановке. Как силы США, так и силы противника в значительной степени полагаются на киберпространство и технологии, зависящие от ЭМС, для управления и контроля, сбора информации, понимания ситуации и целеуказания. Достижение относительного превосходства в киберпространстве и ЭМС даёт командирам преимущество перед противником. Проводя кибероперации и РЭБ, командование может ограничить доступные противнику варианты действий, снизить его способность мобилизовывать силы, ослабить его командование и управление, а также снизить его способность эффективно действовать в других доменах.

1-4. Командиры должны использовать возможности киберпространства и РЭБ, применяя силы и средства вооружённой борьбы путём совместных действий различных родов войск овладевать, удерживать и использовать оперативную инициативу.

Эффективное использование кибероперацій и РЭБ требует от командиров и штабов проведения кибер-электромагнитной деятельности (*англ. cyberspace electromagnetic activities, CEMA*).

Кибер-электромагнитная деятельность[2] (далее CEMA) – это процесс планирования, внедрения и согласования кибероперацій и РЭБ для обеспечения совместных наземных операций (ADP 3-0).

Внедряя и согласуя кибероперации и РЭБ, свои войска получают информационное преимущество в различных доменах и направлениях деятельности.

На рис. 1-1 показано, какой вклад вносят кибероперации и РЭБ в операции сухопутных войск.

[2] *Далее в настоящем Боевом уставе вместе с термином «кибер-электромагнитная деятельность» или вместо него используется аббревиатура CEMA (прим. переводчика).*

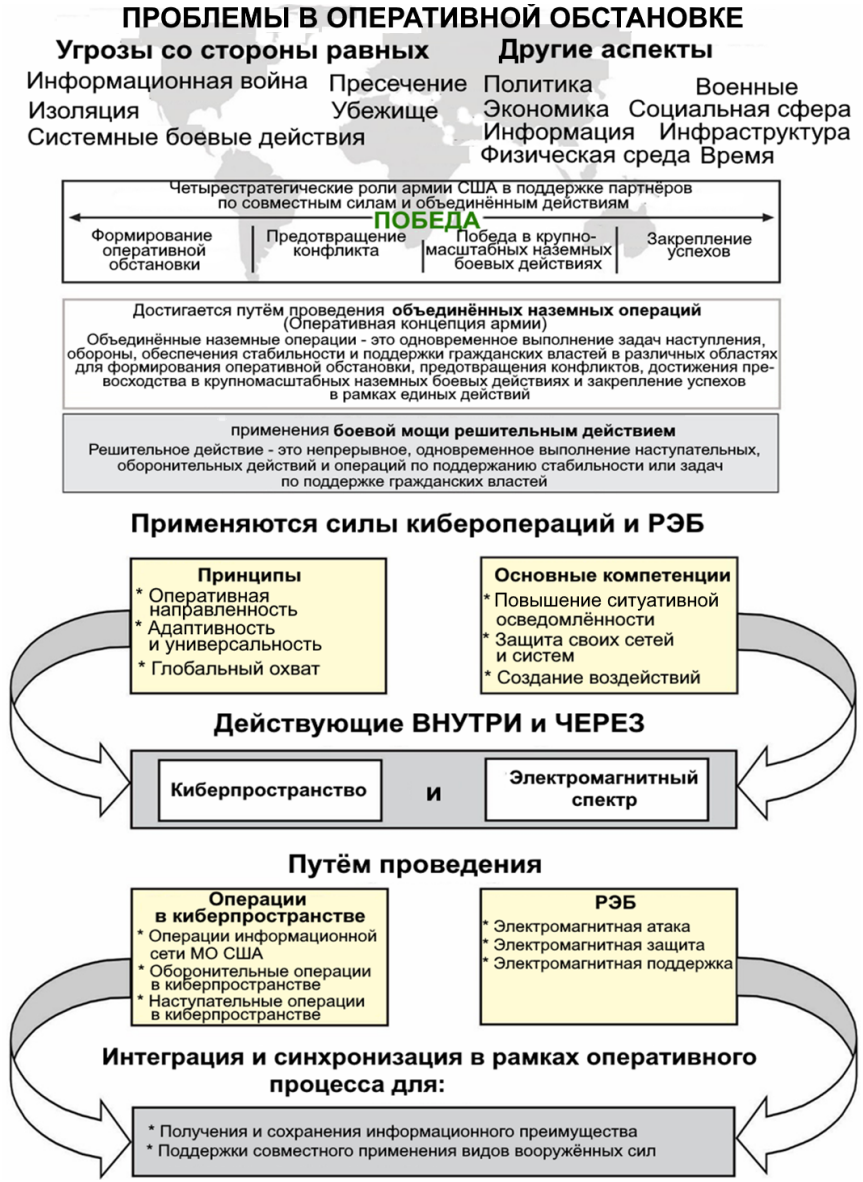

Рис. 1-1. – *Логическая схема кибероперации и РЭБ*

ПРЕДИСЛОВИЕ

Боевой устав FM 3-12 содержит тактику и порядок взаимодействия, внедрения и согласования боевых действий (операций) сухопутных войск (далее – СВ) в киберпространстве и РЭБ для обеспечения совместных наземных и объединённых операций. Боевой устав FM 3-12 объясняет основы, термины и определения боевых действий (операций) в киберпространстве (далее – кибероперации) и радиоэлектронной борьбы (далее – РЭБ) сухопутных войск. В данном издании описывается, каким образом командиры и штабы осуществляют внедрение кибероперацийи РЭБ в совместные наземные операции. Издание представляет собой всеобъемлющее руководство для командиров и штабов по кибероперациям и РЭБ сухопутных войск на всех уровнях. Издание заменяет Боевой устав FM 3-12 от 11 апреля 2017 года.

Основной целевой аудиторией Боевого устава FM 3-12 являются все представители соответствующего рода войск. Командиры и личный состав штабов сухопутных войск, действующих в качестве объединённой оперативно-тактической группы или многонационального штаба, также должны применять совместную или многонациональную доктрину в отношении всего диапазона военных операций и объединённых или многонациональных сил. Издание также будет полезно инструкторам и преподавателям всех родов сухопутных войск.

Командиры, штабы и их подчинённые обеспечивают соблюдение применимых законов и правил Соединённых Штатов, международных, а также, в некоторых случаях, законов и правил страны пребывания войск. Командиры всех уровней должны следить за тем, чтобы их военнослужащие действовали в соответствии с законами войны и правилами ведения боевых действий (см. Боевой устав FM 6-27). Они также, должны придерживаться военной этики, описанной в Наставлении ADP 1.

В Боевом уставе FM 3-12 в необходимых случаях используются единые термины. Общая и военная терминология и определения приведены как в словаре, так и в тексте. Настоящее издание не является пропагандой каких-либо военных терминов. Термины и определения, для которых Боевой устав FM 3-12 является первоисточником, выделены в тексте жирным шрифтом. Для других определений, приведённых в тексте, термин выделен курсивом, а после определения указан номер публикации его разработчика.

Боевой устав FM 3-12 распространяется на действующий личный состав СВ, Национальной гвардии СВ США, а также на резерв СВ США, если не указано иное.

Разработчиком Боевого устава FM 3-12 является Головной центр кибероперацийСВ США. Подготавливающим органом является Отдел развития доктрин из состава Головного центра кибероперацийСВ США.

Комментарии и предложения предлагается направлять по адресу: ********

1.1. Основные компетенции и фундаментальные принципы

1-5. Зависимость сухопутных войск от сетевых систем и вооружений требует наличия высококвалифицированных специалистов для защиты боевых систем и сетей, зависящих от доступа к киберпространству и электромагнитному спектру. Киберпространство и ЭМС могут быть сильно перегружены из-за использования их противником, нейтральными субъектами и своими войсками, а также постоянных действий противника.

1-6. Противник продолжает разрабатывать современные виды вооружения и сетевые системы, которые проецируют мощь через киберпространство и ЭМС, или зависят от них. Сухопутные войска задействуют возможности киберпространства и РЭБ в рамках сил и средств вооружённой борьбы и путём совместных действий различных родов войск и видов вооружённых сил наносят поражение действиям угрозы (противника) в киберпространстве и ЭМС, защищают свои войска и обеспечивают свободу действий в их интересах на протяжении всего конфликта. Кибервойска и войска РЭБ сухопутных войск отвечают за свои основные компетенции и применяют следующие основополагающие принципы для завоевания и удержания позиций относительного преимущества своими войсками.

1.1.1. Основные компетенции

1-7. Кибервойска и специалисты по РЭБ организованы, обучены и оснащены в целях реализации функционирования областей, которые обеспечивают важные и долговременные возможности сухопутных войск:

- обеспечение понимания ситуации;
- защиту личного состава, сил и средств;
- нанесение поражающих воздействий.

1.1.1.1. Обеспечение понимания ситуации

1-8. Кибервойска осуществляют разведку, наблюдение и рекогносцировку киберпространства в информационной среде и через неё с целью выявления и изучения сетей, систем и процессов противника. Эта информация позволяет командирам лучше понять возможности и уязвимости противника, что повышает их способность определять приоритеты и наносить поражающее воздействие.

1-9. Специалисты РЭБ ведут наблюдение за электромагнитным спектром для сбора боевой информации, используемой для характеристики применения ЭМС противником и понимания особенностей интеграции излучающих систем противника на разных уровнях. Эта информация позволяет определить свои уязвимые места и возможности угроз, а командованию – расставить приоритеты и нанести поражающее воздействие.

1.1.1.2. Защита личного состава, сил и средств

1-10. Кибервойска обеспечивают защиту сетей, боевых платформ, сил и средств, а также данных от текущей или надвигающейся злонамеренной активности в киберпространстве. Защищая критически важные сети и системы, кибервойска помогают поддерживать способность сухопутных войск проводить операции и проецировать силу во всех сферах.

1-11. Войска РЭБ во взаимодействии со структурным подразделением штаба G-6 или S-6 и в поддержку директивы командира осуществляют и усиливают меры по защите своего личного состава, объектов, боевых платформ, сил и средств от неблагоприятных воздействий в ЭМС.

Войска РЭБ предлагают к принятию меры по маскировке или контролю излучения своих сил и средств от обнаружения противником и лишают его возможности обнаруживать и идентифицировать свои подразделения. Войска РЭБ обнаруживают и ослабляют атаки противника в ЭМС в целях обеспечения способности сухопутных войск проводить операции и проецировать силу во всех сферах.

1.1.1.3. Нанесение поражающих воздействий

1-12. Кибервойска оказывают киберпространственные поражающие воздействия на сети, системы и вооружение противника. Эти воздействия повышают способность сухопутных войск вести боевые действия (операции), снижают боевые возможности противника и позволяют проецировать силу во всех сферах.

1-13. Специалисты РЭБ оказывают воздействия на сети, системы и вооружение противника в рамках ЭМС. Эти действия снижают боевые возможности противника, обеспечивают защиту своих войск и усиливают их поражающие способности.

1.1.2. Фундаментальные принципы

1-14. Фундаментальные принципы – это основные правила или предположения, имеющие центральное значение и определяющие подход специалистов по кибероперациям и РЭБ к проведению киберопераций и ведению РЭБ.

Фундаментальными принципами являются:

- оперативная направленность;
- адаптивность и универсальность;
- глобальный охват.

1.1.2.1. Оперативная направленность

1-15. Кибервойска и войска РЭБ выполняют задачи в поддержку основного оперативного замысла командующего. При правильном внедрении и согласовании в рамках сил и средств вооружённой борьбы и путём совместных действий различных родов войск, средства воздействия киберпространства и РЭБ могут создавать многоуровневые проблемы для противника в различных доменах и изменять его относительные боевые возможности. Для достижения этой цели штабы, занимающиеся вопросами кибероперацій и РЭБ, должны уметь осуществлять взаимодействие по всем направлениям боевых действий.

1.1.2.2. Адаптивность и универсальность

1-16. Кибервойска и войска РЭБ ведут боевые действия (операции), используя возможности, адаптируемые к различным требованиям задачи. Возможности сил кибероперацій и войск РЭБ различаются как по численности применяемых сил, так и по величине или масштабу создаваемых ими поражающих факторов. В зависимости от задачи возможности кибероперацій и РЭБ могут использоваться как главные или поддерживающие воздействия для решающих, формирующих или обеспечивающих операций.

1.1.2.3. Глобальный охват

1-17. Характер киберпространственной сферы увеличивает оперативный охват сил кибероперацій и войск РЭБ. Силы, выполняющие боевые задачи, и специалисты по РЭБ обеспечивают стратегическое, оперативное или тактическое воздействие по всему миру с удалённых, совместных или передовых оперативных позиций.

1.2. Оперативная обстановка

1-18. ***Оперативная обстановка*** (*англ. operational environment, OE*) – это совокупность условий, обстоятельств и факторов, которые влияют на применение сил и средств и принятие решения командиром (JP 3-0). Условия в киберпространстве и ЭМС часто быстро меняются и могут как положительно, так и отрицательно влиять на способность командира достичь поставленных целей. Действия своих сил, нейтральных субъектов и противника в киберпространстве и ЭМС могут создавать практически мгновенные последствия на поле боя или в расположении гарнизона. Учитывая глобальный характер киберпространства и ЭМС эти действия могут оказывать влияние на оперативную обстановку командира в зоне ответственности, даже если они могут зарождаться или заканчиваться за пределами этой оперативной обстановки. Воздействия в киберпространстве и РЭБ также пересекаются между собой и оказывают влияние на несколько доменов одновременно.