Издаётся с 1924 года

РАДИО®

12•2022

МАССОВЫЙ ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

"Радиолюбитель"—"Радиофронт"—"Радио"

"Radio" is monthly publication on audio, video, computers, home electronics and telecommunication

12+

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ:
АНО «РЕДАКЦИЯ ЖУРНАЛА «РАДИО»
Зарегистрирован Министерством печати и информации РФ 01 июля 1992 г.
Регистрационный ПИ № ФС77-82030

Главный редактор В. К. ЧУДНОВ
Редакционная коллегия:
А. В. ГОЛЫШКО, А. Н. КОРОТОНОШКО, К. В. МУСАТОВ,
И. А. НЕЧАЕВ (зам. гл. редактора), Л. В. МИХАЛЕВСКИЙ,
С. Л. МИШЕНКОВ, О. А. РАЗИН

Выпускающий редактор: С. Н. ГЛИБИН
Обложка: В. М. МУСИЯКА
Вёрстка: Е. А. ГЕРАСИМОВА
Корректор: Т. А. ВАСИЛЬЕВА

Адрес редакции: 107045, Москва, Селивёрстов пер., 10, стр. 1
Тел.: (495) 607-31-18.
E-mail: **ref@radio.ru**
Приём статей — e-mail: **mail@radio.ru**
Отдел рекламы — (495) 607-31-18; e-mail: **advert@radio.ru**
Распространение — (495) 607-77-28; e-mail: **sale@radio.ru**
Подписка и продажа — (495) 607-77-28
Бухгалтерия — (495) 607-87-39

Наши платёжные реквизиты:
получатель — АНО "Редакция журнала "Радио", ИНН 7708187140,
р/сч. 40703810538090108833
Банк получателя — ПАО Сбербанк г. Москва
корр. счёт 30101810400000000225 БИК 044525225
Подписано к печати 25.11.2022 г. Формат 60×84 1/8. Печать офсетная.
Объём 8 физ. печ. л., 4 бум. л., 10,5 уч.-изд. л.
В розницу — цена договорная.

Подписной индекс:
Официальный каталог ПОЧТА РОССИИ — П4014;
КАТАЛОГ РОССИЙСКОЙ ПРЕССЫ — 89032.

Отпечатано в ОАО «Подольская фабрика офсетной печати»
142100, Моск. обл., г. Подольск, Революционный проспект, д. 80/42.
Зак. 04304-22.

Интернет для войны

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"Выживает не самый сильный и не самый умный, а тот, кто лучше всех приспосабливается к изменениям".

Чарльз Дарвин

В начале августа 2019 г. появились сообщения, что научно-исследовательская лаборатория сухопутных войск США изучает, как можно использовать возможности и инфраструктуру "умного города" на поле боя. Лаборатория тестировала сеть для Интернета вещей (Internet of Things — IoT) LoRaWAN (протокол, часто используемый в "умных городах" для объединения устройств и датчиков IoT в районах с высокой плотностью населения). Собственно, это был лишь пролог, потому что дальнейшие действия продемонстрировали высокую динамику, и тому были серьёзные причины.

С начала первой мировой войны все последующие конфликты (глобальные и региональные) в значительной степени использовали информационно-коммуникационные технологии (ИКТ) для доминирования в боевом пространстве, а также для поддержания тактического и стратегического превосходства над противником. Внедрение современных винтовок, военно-воздушных сил и др. сыграло важную роль в этом процессе. Однако важным фактором, который часто недооценивается, является сила информации и связи, преобразуемая непосредственно в военную разведку и осведомлённость, которая затем предоставляется в распоряжение командования и управления.

Не так давно Объединённый комитет начальников штабов США разработал новый вариант "Национальной военной стратегии". Прошлый вариант, опубликованный в 2015 г., по большей части был в открытой печати, а вот новая версия засекречена и не попадёт в средства массовой информации. Тем не менее, как свидетельствуют военные эксперты, главы штабов время от времени дают отрывочные сведения, каким они видят будущее войны и вооружённых сил и что будет включено в новую военную стратегию. По сути, они рисуют такую картину: все технические элементы вооружённых сил должны быть объединены в общую "нервную" систему, начиная от датчиков самолётов F-35 и заканчивая электронными девайсами в карманах солдат на поле боя. Объединение должно происходить не только внутри того или иного рода войск, но и во всех вооружённых силах США. ВВС видят всё то, что видят ВМФ, и так далее.

Причина подобного подхода была озвучена начальником штаба американских сухопутных войск генералом Марком Милли. Вероятный конфликт с технологически развитыми равными державами (Россией и Китаем) требует повышенной мобильности на поле боя. Иначе говоря, больше нельзя просто сидеть на базе, как в Ираке и Афганистане, и оттуда следить за ситуацией. В войне будущего нахождение на одном месте на протяжении двух-трёх часов, и особенно в компании с высшими офицерами, будет означать верную смерть. Если ты обнаружен, то очень быстро будешь уничтожен высокоточным оружием или залпом огня. Следовательно, необходимо понимать, как меняется ситуация в режиме реального времени, и получать информацию из

всех возможных источников. И уметь автоматически делиться ей. То есть, по сути, создать военный IoT.

Один из главных идеологов данной концепции — начальник штаба ВВС США генерал Дэвид Голдфейн. В своё время генерала очень впечатлила презентация Илона Маска о работе компании Tesla над тем, чтобы машины общались между собой и тем самым составляли общую картину происходящего на дорогах. Точно так же должны общаться боевые машины и военнослужащие на поле боя. Поэтому использование концепции IoT в армиях многих стран мира стало технологическим трендом текущего десятилетия, своего рода показателем современности и инновационности их вооружённых сил.

В эпоху дальнейшего стремительного развития IoT выяснилось, что "вещи" приносят гораздо больше пользы, когда они не только активно обмениваются информацией друг с другом и с командирами, но хотя бы постоянно подтверждают, что они есть в наличии в конкретном месте в известном количестве. Это напрямую касается интеллектуальной техники на полях боевых сражений — Интернета боевых вещей (Internet of Battle Things — IoBT), которому в обозримом будущем предстоит охватить всю военную инфраструктуру, включая и поле боя.

На полях сражений будущего будут действовать всевозможные устройства, как "разумные", так и не очень, которым предстоит решать широкий круг задач, регистрируя и обрабатывая оперативную информацию, а также взаимодействуя друг с другом и людьми. Среди этих устройств будут датчики, снаряжение, оружие, транспортные средства, роботы и носимая техника, способные избирательно получать и обрабатывать информацию, выполнять посреднические функции при выяснении содержания полученных данных, вести скоординированные с различными родами войск оборонительные операции, а также различными способами воздействовать на противника. Все эти задачи будут решаться совместно — устройства станут непрерывно общаться, координировать и согласовывать свои действия, разрабатывая и выполняя боевые задания.

Уже появилось несколько различных терминов для описания использования технологии IoT для разведки, наблюдения за окружающей средой, ведения беспилотных боевых действий и других боевых целей. Эти термины включают в себя Военный интернет вещей (Military IoT — MioT), Интернет военных вещей (Internet of Military Things — IoMT) и Интернет боевых вещей (IoBT). Сколько, кем и какой амуниции привезено, сколько выдано, сколько и каких именно снарядов отстреляно, в каком месте, кто отдавал приказы и т. д. и т. п. И это не только удар по встречающимся во многих уголках мира разгильдяйству и воровству, но и важнейшая информация об имеющихся военных ресурсах. Современные возможности обнаружения противника и высокоточное вооружение вынуждают военных к высокой мобильности и быстрому принятию решений. Для этого нужно получать информацию из разных источников в режиме real-time и оперативно делиться ею со всеми задействованными в операции подразделениями. IoT-устройства широко используются в различных обучающих и тренинговых программах для военнослужащих в режиме виртуального боя.

Для решения всех указанных выше задач требуется, в частности, обеспечить между вещами гибкую связь, которая бы адаптировалась к условиям быстро меняющейся ситуации на поле боя. Понадобится организовать управление большим количеством динамичных активов (устройств, каналов, виртуальных объектов, программного обеспечения, приложений и т. п.), допуская при этом множество сложных компромиссов. При этом адаптация сети, управление ею и её реорганизация должны происходить по большей части автономно, без привлечения для её поддержки и без того занятых на поле боя людей, а также сопровождения. Буквально речь идёт о появлении военных автономных операторов связи.

IoMT — это разновидность IoT для ведения боевых действий и ведения войны. Это сложная сеть взаимосвязанных объектов или "вещей" в военной сфере, которые постоянно взаимодействуют друг с другом для координации, обучения и взаимодействия с физической средой для выполнения широкого спектра действий более эффективным и информированным образом. Концепция IoMT в значительной степени основана на идее, что в будущих военных сражениях будут доминировать машинный интеллект и кибервойна. Создавая миниатюрную экосистему интеллектуальных технологий, способных обрабатывать сенсорную информацию и автономно управлять несколькими задачами одновременно, IoMT концептуально спроектирован так, чтобы разгрузить большую часть физической и умственной нагрузки, с которой сталкиваются военнослужащие в боевых условиях.

Вообще, в современном мире огромную роль играет скорость. Причём скорость во всём. Ну, а в современной войне это один из ключевых факторов. От того, как скоро можно получить разведданные, сообщить их командованию боевой единицей и принять решение о нанесении удара, а также оперативно сменить место, где были только что расположены средства ведения огня, зависит очень и очень многое — почти всё. Отсюда колоссальная роль БПЛА и дронов, спутниковой связи, времени передачи и точности координат противника, мобильности боевых единиц, а также скорости донесения приказов до исполнителя. К примеру, появились публикации американских СМИ о том, что некая фирма Palanti разработала систему, позволяющую с помощью специального ИТ-продукта (MetaConstellation), собирающего всевозможные данные с пролетающих спутников: радиосигналы, изображения в инфракрасном свете или аэрофотоснимки, определять местоположение объектов в реальном времени, после чего туда наводятся ракеты земля-земля.

Французский философ Поль Вирильо, изучавший значение скорости для современной технической цивилизации, предложил особый термин — дромократия. От греческого дромос (скорость) и кратос (могущество, власть). Теория Вирильо строится на утверждении, что в новых цивилизационных условиях побеждает не тот, кто сильнее, умнее, оснащённее, а тот, кто быстрее. Именно скорость решает всё. Отсюда стремление любыми путями повышать быстродействие процессоров, и соответственно, все цифровые операции. Именно на это и обращена преимущественно техническая инновационная мысль сегодня. Все соревнуются именно в скорости.

Современный мир — это борьба за ускорение. И тот, кто оказывается быстрее, получает самый главный приз — власть. Во всех её смыслах и измерениях — политическую, военную, технологическую, экономическую, культурную. При этом наиболее ценной в структуре дромократии является информация. Именно скорость передачи информации и является конкретным выражением власти. Это касается как функционирования мировых бирж, так и ведения военных действий. Тот, кто смог сделать нечто быстрее, получает над тем, кто замешкался, полную власть.

При этом дромократия, как сознательно выбранная стратегия, то есть попытка господства над временем как таковым, может привести и к странным эффектам. В действие вступает фактор будущего. Отсюда феномен фьючерсных сделок и связанных с ними хеджинговых фондов, а также другие финансовые механизмы аналогичного толка, в которых основные операции проводятся с тем, чего ещё нет.

Идеалом дромократии в области СМИ было бы первыми сообщить о событии, которое ещё не произошло, но которое, вполне вероятно, вот-вот произойдёт. Это не просто фэйк, это — работа с областью возможного, вероятного. Если принимать вероятное будущее событие за уже случившееся, мы выиграем время, а значит, приобретём власть. Другое дело, что этого может и не произойти. Да, и это возможно, конечно, но подчас провал ожидания не критичен, зато подтверждённый прогноз, принятый за свершившийся факт заранее, даёт колоссальные преимущества.

При развитии сверхскоростей сама реальность искривляется, и в ней начинают действовать законы неклассической физики — предвосхищённые в теории относительности Эйнштейна и в ещё большей степени в квантовой физике. Предельные скорости меняют физические законы. И именно в этой сфере разыгрывается сегодня, по Вирильо, планетарная борьба за власть.

Аналогичные теории встречаются и в более прикладной и менее философской области — в теории сетецентричных войн (Network-centric warfare), главной особенностью которых является быстрота передачи информации между отдельными единицами и центрами командования. Для этого военнослужа-

щие и другие боевые единицы снабжаются многочисленными разноориентированными камерами и другими датчиками, информация от которых сходится в единой точке. Сюда добавляются данные с коптеров, БПЛА и спутников, включая теперь спутниковый интернет Starlink от Илона Маска, которые интегрированы напрямую с боевыми и огневыми единицами. И такая полная сетевая интеграция обеспечивает преимущество в скорости — будь то ракетные системы или диверсионно-разведывательные группы.

Планка милитаризации IoT была высоко поднята Пентагоном, когда ведомство начало разработку теорий сетецентрической войны и многодоменной битвы (Multi-Domain Battle), которые предусматривают совершенно новый способ проведения военных операций, при котором все участники (техника, живая сила, штабы и т. д.) связаны единой информационной сетью.

При этом речь идёт не о соединении различных военных сетей с целью повышения эффективности конкретных операций, а о создании глобальной сети, позволяющей одновременно работать на всех театрах военных действий, в том числе и в киберпространстве. Все технические устройства, находящиеся на вооружении, должны быть связаны в одну общую систему, начиная с датчика БПЛА и завершая носимым устройством в амуниции солдата. Причём акцент делается именно на объединении не внутри отдельного подразделения или вида войск, а по всем вооружённым силам сразу. Предполагается, что объединение в глобальную сеть даст командованию возможность оперативного принятия решений о проведении наступательных, оборонительных и других активностях на всех театрах военных действий.

Справедливости ради следует признать, что в теории сетецентричных войн быстрота принятия решений часто идёт в ущерб их оправданности. Случается и очень много просчётов. Но если действовать стремительно, то, даже совершив ошибку, всегда есть время её исправить. Здесь используется принцип хакерского взлома или DDoS-атаки — главное, долбить по всему расположению войск противника, выискивая слабые места — back door. Потерь может быть довольно много, но и результаты, в случае успеха, оказываются весьма значимыми.

Далее сетецентричные войны как свою интегральную составляющую включают открытые каналы информации — прежде всего социальные сети. Они не просто сопровождают ведение боевых действий, сообщая, естественно, только то, что выгодно, а что не выгодно, скрывая или искажая до неузнаваемости, но и оперируют с вероятностным будущим. И здесь снова принцип дромократии. То, что мы сегодня воспринимаем как фейки, есть ни что иное, как прощупывание и искусственная стимуляция возможного будущего. Множество фейков оказываются пустыми, как часто тщетными бывают попытки пробить защиту при взломе, но время от времени они достигают цели — и тогда система может быть захвачена и подчинена.

Чтобы эта грандиозная картина стала реальностью, требуется решить целый ряд задач — в частности, обеспечить между вещами гибкую связь, которая бы адаптировалась к условиям быстро меняющихся ситуаций на поле боя. Для этого понадобится организовать управление большим числом динамичных активов (устройств, каналов и т. п.), допуская при этом множество сложных компромиссов. Адаптация сети, управление ею и её реорганизация должны происходить по большей части автономно, без привлечения людей для её поддержки и сопровождения.

Кроме того, необходимость разбираться в потоках информации, генерируемой IoBT, сильно усложнила бы выполнение боевой задачи для людей, находящихся в условиях экстремальной когнитивной и физической нагрузки. Поэтому IoBT должен помогать людям извлекать пользу из океана данных, принимая во внимание меняющиеся задачи миссии.

Естественно, противник не только будет физической угрозой для людей и IoBT, но и попытается проникнуть в саму сеть. Таким образом, сам IoBT станет полем боя с участием обороняющихся и атакующих. Здесь необходимо управлять рисками и снижать неопределённость в условиях враждебной среды. Кстати, если готовиться, к примеру, к фронтальному противостоянию с НАТО и одновременно полагаться на технологические элементы (те же процессоры и прочую микроэлектронику), разработанные и производимые либо в странах НАТО, либо на территории государств, зависящих от США, — это станет одним из самых больших рисков.

Учитывая огромные масштабы IoBT, понадобятся новые теоретические исследования, модели, концепции и технические подходы. Число сетевых узлов IoBT для боевого отряда может быть на несколько порядков больше, чем вообще когда-либо рассматривалось в рамках исследований. Особенно это проявится в ситуациях, когда участники боевых акций решат задействовать сетевые устройства и каналы, им не принадлежащие, к примеру, доступные гражданским устройствам IoT. А ведь в таком случае придётся иметь дело с миллионом вещей на каждый квадратный километр.

Столь большой масштаб IoBT может быть полезным в теоретическом и практическом отношении. В частности, наличие огромного числа плотно размещённых датчиков позволяет решить проблему обеспечения постоянной доступности устройств, а для этого нужны теоретические исследования с выяснением степени детерминированности, доступной в рамках очень большого ансамбля вещей и данных. IoBT будет также характеризоваться высокой гетерогенностью: локальные сети вещей состоят из множества коммерчески доступных устройств, а оборудование, которым люди будут пользоваться в боевых условиях, скорее всего, тоже будет основано на коммерческих разработках. Необходимо будет пользоваться широким набором протоколов и коммуникационных технологий, поддерживаемых различными производителями. В гетерогенной, высокодинамичной и труднопредсказуемой среде понадобятся новые способы быстрого обнаружения, выяснения характеристик доступных вещей и отслеживания их во времени и пространстве. Необходимо, чтобы эти сведения собирались и обновлялись в ходе военной операции автоматически. Между тем военнослужащие тоже являются важными элементами IoBT, и чтобы обеспечить их эффективную работу, нужно динамически распознавать, идентифицировать, характеризовать и предсказывать поведение солдат с обеих сторон и нейтральных гражданских лиц.

Масштаб, динамизм и высокий уровень сложности IoBT будут влиять на связь между вещами — для поиска каналов организации связи между огромным числом разнородных, зачастую непредсказуемых вещей, и управления этими каналами понадобятся совершенно новые подходы. И это ещё в условиях вероятного противодействия и подавления со стороны противника. Поэтому для непрерывного резервирования и перенастройки ресурсов сети связи потребуются высокоинтеллектуальные средства автоматизации. Необходимо будет автоматически составлять и обновлять стратегии и правила обмена информацией, регламентирующие длительность и привилегии связи, и уже с ними гармонизировать всю систему управления войсками. Также понадобятся высокомасштабируемые архитектуры и протоколы и надёжные методы определения и подтверждения их свойств. Но в первую очередь понадобится соответствующий искусственный интеллект, способный справиться со всеми упомянутыми задачами.

В экстремальных ситуациях, когда в IoBT происходит катастрофический сбой, делающий его недоступным или ненадёжным (например, в результате действий противника), автономные механизмы управления должны обеспечивать автоматическое восстановление, после которого можно продолжить работу, пусть и с деградацией функциональности.

Дополнительные сложности возникнут в связи с ограничениями связи по времени. Какие-то коммуникации допустимо отложить на несколько часов, но для других типов связи (например, для передачи информации между датчиками и системами реагирования) нужна работа в режиме реального времени. К тому же доступность каналов связи будет сильно варьироваться. Специалистами прогнозируется, что через 30 лет в гражданском мире данные будут гарантированно проходить по беспроводной связи 5G/6G до надёжных кабельных соединений дистанцию лишь в несколько метров, тогда как военным необходимы беспроводные каналы с охватом в десятки километров.

Картина общего состояния IoBT должна оперативно обновляться в автоматическом режиме, для чего понадобятся новые методы извлечения необходимого объёма сведений о сложных системах, основанные на регистрации относительно небольшого числа параметров. Для эффективного управления IoBT нужно учитывать разнообразие его функций и применений. Некоторые из них ясны, например, военная логистика и распределённые вычисления. Другие будут порождены самим IoBT, и его можно будет применять для нужд обнаружения, навигации, расчёта времени, а также в качестве дополнения или замены систем навигации.

В настоящее время лидерство по применению IoBT и разработке новых решений с его использованием принадлежит американской армии. Уже известно об успешных испытаниях многоцелевых самолётов, способных получать и передавать большие потоки данных от работающих в их зоне видимости боевых "умных" устройств и другой техники. Активно используется мобильное приложение ATAK (Android Tactical Assault Kit), позволяющее накапливать данные в режиме real-time и накладывать их на известный всем Google Maps. В зоне боевых действий это решение используется для коммуникации наводчика на цель, пилота самолёта или оператора БПЛА. Пентагон вообще планирует заменить все некоммуницирующие между собой сети на единую всеармейскую.

ВМС США провели учения по высадке на берег роботизированных боевых машин, при этом особый упор делался на тестирование каналов связи и взаимодействие беспилотных систем как на воде и земле, так и в воздухе. Проведены успешные испытания нового типа брони, способной после попадания в неё информировать другую технику, солдат и командный центр, участвующих в операции, о мощи и направлении обстрела.

Техническим прорывом называют использование в боевых условиях возможностей смартфонов и планшетов с помощью системы Nett Warrior. С её помощью командир подразделения имеет возможность обмениваться информацией по вертикали и горизонтали, что значительно увеличивает осведомлённость о ситуации в зоне боестолкновения с противником. Кроме того, наличие навигации (к примеру, от спутниковой системы GPS) позволяет отмечать расположение солдат на карте, которая изображается в прикреплённом к шлему дисплее, а также получать обновлённые карты местности и другую информацию из командного центра. Правда, для всего этого на местности нужна как минимум сеть 4G, но ведь и она может быть оперативно развёрнута с помощью каких-нибудь мобильных базовых станций.

Люди не могут и не должны анализировать весь объём данных, генерируемых IoBT, поэтому им нужны только высокоуровневые сведения, например, указания и предостережения по текущей ситуации и миссии. Реагировать на все сведения, требующие внимания, в контексте IoBT невозможно. В сущности, один из ключевых рисков IoBT состоит в предоставлении информации, которая приведёт к действиям с более негативными последствиями, чем если бы этой информации вообще не было.

Колоссальный массив данных IoBT необходимо уменьшать до приемлемого уровня, выделяя действительно ценное содержание, готовое для передачи людям и "умным" вещам. По некоторым оценкам, объём информации придётся уменьшить путём компрессии и консолидации в 10^{15} раз. Один из путей решения этой непростой задачи — дополнить IoBT многоуровневой иерархией информационных посредников, которые будут агрегировать, консолидировать, интерпретировать и пересылать нужную информацию. Процесс консолидации нужно начинать на самом нижнем уровне — например, все вещи, генерирующие информацию, следует снабдить локальными средствами фильтрации, интерпретации и объединения данных. Такая система посредников может затруднить извлечение данных нижнего уровня, но, похоже, эту цену неизбежно придётся заплатить, чтобы получать конструктивные сведения в приемлемом объёме.

Чтобы информационные посредники справлялись со своей задачей, они должны знать, какая именно информация полезна. Источником этих знаний могут быть процедуры планирования военной миссии и полевые учения, в рамках которых можно определить, какие именно сведения нужны людям и машинам. А для сохранения этих знаний нужен специальный язык выражения информационных потребностей для IoBT, доступный для машинной обработки, формальный, с широкой сферой применения и понятный военным. В ходе планирования и учений не вся нужная информация может быть получена, и IoBT должен уметь самостоятельно выяснять, какие сведения необходимы для конкретной миссии и её участников. Для этого потребуются подходы, основанные на машинном обучении и семантических знаниях.

Впрочем, преимущества IoBT соседствуют с рядом уязвимостей. В частности, необходимо создание специальных устройств, обладающих повышенной степенью защиты. Любое мобильное или сетевое приложение, обеспечивающее работу IoBT-устройств, как и сами они, должно быть максимально защищено от постороннего вмешательства. Попытки американских военных развить глобальную сеть также наталкиваются на проблемы уязвимости IoBT-сетей, которые не в меньшей степени, чем боевая техника или солдаты, могут становиться объектом атаки. Уязвимость отдельных элементов системы может быть спровоцирована различными доступными противнику или хакерам способами: физический и сетевой взлом, прослушка, радиоэлектронная борьба, направленная энергия и т. п. Впрочем, объём и характер трафика IoBT потребуют значительно большего радиочастотного спектра, чем доступно сегодня. Очевидно, появится совместное использование спектра и управление спектром.

Перед военными стоит задача — добиться, чтобы при принятии на вооружение IoBT-устройств не оставалось возможностей манипуляции ими или сетью, кражи, нарушения потока данных или физического уничтожения. Сделать это сейчас непросто, учитывая отношение многих производителей "умных" устройств к обеспечению их безопасности, а также тесное переплетение стационарных, мобильных и спутниковых сетей, что способствует наличию массы точек входа и незащищённых мест. Очевидно, военным ведомствам рано или поздно, но придётся работать с поставщиками и производителями IoBT-устройств с целью принуждения их к введению более надёжных стандартов безопасности. Возможно даже, что вся электронная промышленность будущего попросту перейдёт в ведение военных.

В заключение добавим, что сегодня руководство Минобороны РФ осознаёт важность внедрения инновационных методов и решений при ведении боевых действий. Информационное преимущество позволяет обойти даже превосходящего по численности противника, быть всегда на несколько шагов впереди. Поэтому Россия стремительно подходит к методам ведения сетецентрической войны и готовится к их реализации.

По материалам ***osp.ru, tadviser.ru, habr.com/ru/company/unet/blog, navoine.info, sell-off.livejournal.com, topwar.ru, k-politika.ru, новости-сша.ru-an.info, army-guide.com, idstch.com/military***