Издаётся с 1924 года

РАДИО®

"Радиолюбитель"—"Радиофронт"—"Радио"

8•2021

МАССОВЫЙ ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

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

12+

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ: ЗАО «ЖУРНАЛ «РАДИО»

Зарегистрирован Министерством печати и информации РФ 01 июля 1992 г.

Регистрационный ПИ № ФС77-50754

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**

Группа работы с письмами — (495) 607-08-48

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 — ЗАО "Журнал "Радио", ИНН 7708023424,

р/сч. 40702810438090103159

Банк получателя — ПАО Сбербанк г. Москва

корр. счёт 30101810400000000225 БИК 044525225

Подписано к печати 23.07.2021 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. 02239-21.

Если завтра война...

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

"Теперь, с появлением лука, война стала слишком ужасной. Наступила эра вечного мира".

Гарри Гаррисон "Абсолютное оружие"

Для начала уместно вспомнить вот такое высказывание Эйнштейна: "Я не знаю, каким оружием будут сражаться в Третьей мировой войне, но в Четвёртой будут использовать камни и палки". Несомненно, учёный находился под впечатлением от только что созданной атомной бомбы и последствий её испытаний.

Горячие и холодные, интеллектуальные и тотальные, кабинетные и гуманитарные, асимметричные и эшелонные, партизанские и на истощение, информационные и кибернетические — это далеко не всё из военного арсенала гомо сапиенс, как вершины эволюции. Однако же последний его тренд — кибервойна и другие виды войн с элементами этой.

Войны ближайшего будущего вряд ли будут похожи на то, что мы видим в фантастических фильмах. Говорят, генералы всегда готовятся к прошедшей войне, но это далеко не так. Скорее простые граждане ошибочно понимают, что такое та же кибервойна. Ведь "говорящие головы" с экранов и дезинформация в новостях представляют собой элементы политики или войны информационной, которая сопровождает человечество на всём пути развития цивилизации. Настоящая же кибервойна начнётся в тот момент, когда в самом цифровом любовно обустроенном мире всевозможных сервисов и вселенских знаний в одночасье исчезнут все эти сервисы, потому что пропадут мобильная связь и Интернет вместе с телетрансляцией, остановятся заводы, начнут отказывать объекты энергетики и далее везде...

Впрочем, открутим время назад. В сентябре 2010 г. компьютерный вирус Stuxnet нанёс значительный ущерб иранской ядерной программе. Этот программный червь "весом" всего лишь в 500 Кб стал причиной повреждения 1368 из 5000 центрифуг для обогащения урана и отбросил выстроенную в течение десяти лет ядерную программу Ирана примерно на два года назад. По уровню ущерба действие вредоносной программы специалисты сравнили с полноценной атакой боевой авиации. А вот по уровню затраченных ресурсов сравнить попросту не с чем, так как не наблюдалось никакого риска для живой силы атакующего и его военной техники, не тратились боеприпасы и горючее, не выпускали офицеров военные академии, не обучали рядовой состав сержанты. Получается, для подобной атаки не нужно ничего, кроме куска программного кода. И вот уже минуло десятилетие после "первого звоночка" кибервойн, но до сих пор неясно, насколько серьёзный ущерб могут причинить подобные атаки. Хотя военные стратеги, понятное дело, планируют делать это по максимуму.

В 2013 г. американцам из Ирана прилетела "ответка" — иранские хакеры успешно атаковали программную инфраструктуру небольшой дамбы на севере Нью-Йорка. И это было настолько неожиданно, что, к примеру, ФБР попросту

не успело среагировать и, как впоследствии выяснилось, тем самым фактически расписалось в своей беспомощности с таким комментарием в СМИ: "Если бы террористы попытались перехватить контроль над плотиной Bowman Avenue, то, скорее всего, им бы это удалось". Правда, никакой стратегической ценности плотина не имеет, но при этом успешная диверсия показала США опасность кибервойны, в том числе, для них самих. Неспроста они решились рассказать о той атаке лишь три года спустя. С другой стороны, в США есть и другие плотины, в том числе и такие, что вместе с потенциально затапливаемой территорией контролируют чуть ли не четверть энергетических мощностей страны.

Из самого последнего. 7 мая компания Colonial Pipeline — оператор трубопровода протяжённостью более 8800 км, через который поставляется чуть ли не половина бензина, дизельного топлива и других нефтепродуктов на Восточное побережье США, признала, что подверглась кибератаке. Атакующие использовали так называемые программы-вымогатели, которые блокируют компьютерные системы и требуют от жертвы взлома плату за их разблокировку. Компания была вынуждена приостановить подачу топлива по трубопроводу несмотря на то, что злоумышленники не проникли в жизненно важные системы, непосредственно управляющие его работой. Вряд ли последствия работы хакеров чем-то отличаются от военных действий, тем более что на заблокированном топливе функционирует вся военная техника.

Некоторые эксперты оценивают сегодня угрозу кибервойн настолько высоко, что она чуть ли не "заставляет их просыпаться ночью" от видений тотального уничтожения экономики вместе с шахтами межконтинентальных ракет. Ведь, по сути, ни у одной из стран нет достаточной защиты от киберугроз. И прежде всего у той, где всё это зародилось вместе с Интернетом. Да и кто сегодня откажется от Интернета вместе со всей "цифровой" экономикой? Понятно, что режимные объекты не имеют выходов в сеть и охраняются куда строже. Но от человеческого фактора и многоступенчатых диверсий это не уберегает.

В целом, у любого режимного объекта очень сложная техническая структура. Однако периодически им тоже нужна техническая модернизация. Контролировать их производство на каждом отдельном этапе практически невозможно. В создании, к примеру, ПО принимают участие сотни и тысячи людей. Заразить даже партию чипов на стадии производства проще, чем может показаться. И если заражённый чип попадёт куда-нибудь в панель управления, то его в перспективе можно использовать для кибератаки.

Хорошо, пусть стратегические объекты вроде ядерных шахт и атомных электростанций надёжно защищены, но возможности кибератак развиваются значительно быстрее, чем навыки защиты от них (всё в точном соответствии с развитием кибермошенничества). Ответом на это стала всеобщая забота о критической информационной инфраструктуре (КИИ), как основе экономики и безопасности государства. В частности, в РФ действует Федеральный закон №-187 "О безопасности критической информационной инфраструктуры (КИИ) Российской Федерации", который вступил в силу 1 января 2018 г.

Под КИИ подразумеваются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов, а также сети электросвязи, используемые для организации их взаимодействия. В свою очередь, субъекты КИИ — это компании, работающие в стратегически важных для государства областях, таких как здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также организации, обеспечивающие взаимодействие систем или сетей КИИ. Компьютерная атака на КИИ определяется как целенаправленное вредоносное воздействие на её объекты для нарушения или прекращения их функционирования, а компьютерный инцидент — как факт нарушения или прекращения функционирования объекта КИИ и/или нарушения безопасности обрабатываемой объектом информации.

Отсечь КИИ в киберпространстве от прочей инфраструктуры и окружить её защитным барьером — основная забота кибероборонны. У инициаторов кибервойн прямо противоположные цели. Известный футуролог Рэй Курцвейл, в частности, считает, что киберпространство станет главным полем боя в будущем, а целостность и безопасность — ключевыми стратегическими вопросами. Классические войны будут происходить реже. Децентрализованная коммуникация вроде Интернета по своей природе является демократизирующей силой и двигает мир к большей демократии. Разумеется, это не идеальная система, но демократии не склонны воевать друг с другом. Будущие конфликты будут происходить между небольшими группами тех, кто пытается усилить своё влияние через поиск уязвимостей в нашей технологической инфраструктуре . Как говорится, блажен, кто верует. Как будто поиском уязвимостей озабочены исключительно отдельные зловредные группы хакеров, а не страны, уже давно создавшие у себя киберкомандование со всей подчинённой иерархией. Или же прослушивание лидеров и похищение содержимого баз данных вполне себе "демократических" государств другими "демократическими" государствами вовсе не имели места в истории.

Одной из главных опасностей кибервойн считают Интернет вещей (IoT). Допустим, не все его фрагменты относятся к КИИ, но чем больше устройств подключено к глобальной сети, тем шире возможности использовать их во вред. Как отмечают специалисты, пока ещё безопасность IoT настолько слаба, что опасность может представлять интеллектуальный чайник, холодильник или даже унитаз. Возможно, авторы детективов уже обдумывают будущие сюжеты вроде "Смерть на унитазе" или "Холодильник-убийца", но остальным гражданам всё это вряд ли понравится. Впрочем, нападать на обычных граждан таким способом вряд ли кому-нибудь нужно, а у тех, кто представляет интерес для потенциального противника, все "вещи", безусловно, будут надёжно защищены.

Ещё одна серьёзная проблема — реакция государства на кибератаки. В мае 2019 г. израильские ВВС уничтожили здание в г. Газа, в котором размещались основные компьютерные мощности Хамаса — организации, признанной террористической в Израиле. При этом авиаудар был нанесён по вполне себе жилому кварталу. Конечно, один из основных принципов военных действий гласит, что ответ на атаку должен быть пропорционален самой атаке. Однако сложность заключается в том, что оценить перспективную угрозу невозможно.

К примеру, разведывательный дрон или спутник может оценить число боевых подразделений и тяжёлого вооружения, а также их возможные цели, после чего стратеги разработают меры противодействия. А вот как выяснить мощности и цели кибератак? Даже если учесть, что целью кибератак могут стать стратегические пункты вроде ядерных шахт или электростанций, подобные превентивные удары по компьютерным базам не отвечают принципам ведения военных действий. Да и можно ли с высокой точностью определить настоящий источник компьютерной атаки?

Мировому сообществу уже давно пора осознать, что кибервойна может быть не менее опасной, чем полноценное военное столкновение между государствами. Здесь другие плацдармы, другие воины, другие боеприпасы. Но смысл один — война. Наверное, вполне в наших силах не допустить её. В связи с этим ООН и различные военные блоки могли бы разработать международные законы ведения кибервойн ещё лет пять назад. Но, по состоянию на начало 2021 г., их всё ещё нет. И, очевидно, вовсе не потому, что до сих пор неясно, насколько опасной может быть кибервойна и как вообще её можно регулировать (говорят, что есть только рекомендательные правила, которые не имеют законодательной силы), а потому что продолжается ухудшение в регулировании горячих войн. Поэтому развитые страны разрабатывают собственные доктрины кибербезопасности. Как правило, это только внутренние правила, что считать элементами кибервойн, как защищаться от кибератак и как на них реагировать.

Футуролог Кевин Келли отметил ещё большие риски в ведении кибервойн: "Мое главное опасение — кибервойны между странами в будущем. Я боюсь их, потому что у нас нет никаких соглашений о допустимых способах войны в этой реальности. Конечно, странно, что у нас есть соглашения по ведению

войны, но это лучше, чем бои без правил. У нас нет никаких договорённостей о том, как вести кибервойны, тем более, когда в них задействован искусственный интеллект".

Искусственный интеллект (ИИ) можно рассматривать как "усилитель" кибервойн и как "усилитель" киберзащиты. Не так давно в редакцию журнала NewScientist попал отчёт ООН, согласно которому в прошлом году в Ливии военный беспилотный летательный аппарат впервые выследил и уничтожил человека без непосредственного участия оператора. Атака произошла во время конфликта между ливийскими правительственными войсками и отколовшейся от них фракцией под руководством Халифы Хафтара. В инциденте, произошедшем в марте 2020 г., участвовал квадрокоптер Kargu-2 производства турецкой компании STM. В отчёте говорится, что он атаковал одного из солдат Хафтара, пытавшегося отступить.

Оснащённый боезарядом Kargu-2 может самостоятельно обнаруживать и поражать цели, а оператору остаётся лишь направить его в определённую зону. Оператор при необходимости может отменить атаку дрона или перенаправить его на другую цель. Боезарядом может быть осколочный заряд для поражения личного состава противника и других небронированных целей, кумулятивный для атаки на легкобронированную технику, термобарический для поражения целей в замкнутом пространстве. Как говорится в отчёте, летальное автономное вооружение запрограммировано атаковать цели без обмена данными между оператором и оружием. Военные называют такую систему "нашёл, выстрелил и забыл" (FFF — Find, Fire & Forget). В общем этот инцидент демонстрирует необходимость срочного обсуждения потенциальных ограничений на использование автономного оружия.

Несколько лет назад Стивен Хокинг, Илон Маск и другие известные в научном мире лица в открытом письме об автономном оружии написали: "Автономное оружие способно выбирать и атаковать цели без участия человека. Сегодня оно включает вооружённые квадроциклы, которые могут находить и устранять людей по определённым критериям, но не учитывают крылатые ракеты или дистанционно управляемые беспилотные летательные аппараты, где цель определяют люди. Ставки чрезвычайно высоки: многие утверждают, что автономное оружие — это революция в войне после пороха и ядерного оружия. Начинать гонку вооружений с искусственным интеллектом — плохая идея. Мы считаем, что для её предотвращения нужно полностью запретить создание автономного оружия, находящегося вне реального контроля человека. Автономное смертельное оружие грозит стать третьей революцией в войне. Однажды созданное, оно позволит вооружённым конфликтам вестись в больших масштабах, чем когда-либо раньше, и быстрее, чем люди способны осознать. Оно может стать оружием террора, которое направят против невинного населения, оружием, которым можно пользоваться как хочется. У нас есть немного времени, но как только этот ящик Пандоры откроется, его будет сложно закрыть".

Тоби Уолш, профессор ИИ Университета Нового Южного Уэльса, в свою очередь, заявил: "Возьмите существующие сегодня дроны и замените человека, который ими управляет, компьютером. Слабое звено в дронах — радиосвязь с базой. Избавь их от неё, и вы получите дрон, который может отслеживать свою цель 24/7. Он никогда не спит. У него сверхчеловеческая точность и реакция. Дроны станут идеальным оружием для подавления гражданского населения. В отличие от людей, они без колебаний начнут истреблять целые группы". И вот уже сценаристы, журналисты и прочие создатели контента рисуют картины, где небо покроется сплошным дымом, как поля сражений во время наполеоновских войн, над дымной пеленой полетят стаи хищных дронов, выслеживающих свою добычу, атмосфера начнёт искрить от работ систем электронного подавления (в этом месте радиоинженеры могут улыбнуться), а солдаты с автоматами, возможно, исчезнут как класс. Главными целями станут операторы дронов и центры управления. Если там вообще останутся люди. В общем, новые технологии позволяют интеллектуальным барражирующим боеприпасам самим решать боевые задачи.

Сама идея стай барражирующих боеприпасов — беспилотников с боевой частью, способных зависать над полем боя, отыскивать и поражать цели, пришла в голову англичанам в конце 1990-х. Первый такой экземпляр Fire Shadow выполнил свой демонстрационный полёт 30 апреля 2008 г. и привлёк внимание разве что военных журналистов. Сегодня самым известным (хотя не самым результативным) считается американский одноразовый ударный беспилотник или дрон-камикадзе AeroVironment Switchblade. Малая масса (2,7 кг) и удобный трубчатый контейнер для запуска делают его персональным оружием пехотинца. Крылья дрона разворачиваются уже в воздухе, дальность полёта — до 10 км, его продолжительность — до 10 мин. Управление современными армейскими беспилотниками интуитивно понятно для поколения, выросшего на компьютерных играх.

Пока такие боеприпасы применяются одиночно. Качественный скачок произойдёт тогда, когда они получат возможность действовать роем (примерно, как в фильме "Падение ангела"). Эта технология очень близка к конечной реализации, достаточно посмотреть в Интернете многочисленные ролики, в которых сняты мировые рекорды по управлению стаями дронов. Ими управляют системы с ИИ, а операторы лишь назначают цели.

То есть на подходе новая грозная инновация — роевые группы беспилотников, действующие под управлением ИИ. Американцы много лет работают над такими системами оружия, они уже добились не только автономного, без управления человеком, маневрирования, но и самообучения роботов прямо в полёте. Совсем недавно фирма "Боинг" провела успешные автономные полёты своих беспилотников с отработкой указанных алгоритмов. Отсутствие необходимости в живом операторе позволит применять дешёвых роботов в огромных количествах. Как с этим бороться, пока точно неизвестно. А вот то, что одномоментный удар тысячами таких аппаратов по последствиям сравним с ядерным оружием, уже очевидно. Появление всего этого над полем боя — вопрос буквально нескольких следующих лет. В общем, беспилотная воздушная война уже начала менять облик современных армий, и это только начало.

Пол Шарре, руководитель программы технологий и национальной безопасности Центра новой американской безопасности, предупреждает об объективной опасности новых технологий: "Иногда кажется, что технологии — это отличное решение для войн. Вы думаете: "Да, с такими технологиями мы станем эффективнее на поле боя и спасём наших солдат!" Но когда они есть и у второй стороны — так уже было с автоматами, — война становится ещё более страшным местом. Такая же проблема — с автономным оружием и робототехникой. Мы рискуем ввязаться в новую гонку вооружений, когда по отдельности страны добиваются различных военных достижений, но в совокупности они делают войну менее управляемой и этим вредят человечеству".

Возможно, что не всё ещё потеряно для нашей цивилизации, если представители военных ведомств задумываются о последствиях вреда всему человечеству. Впрочем, всем и всегда полезно помнить о таком оружии, как бумеранг. Это лишь на первый взгляд стая дешёвых беспилотников кажется неуязвимой. Специалисты сходятся во мнении, что данная технология полностью изменит характер военных конфликтов, но никто точно не может сказать, как. Да и какими бы ни были групповые применения дронов, группе нужна связь, оптическая или по радиоканалу. К примеру, если информационный обмен в группе будет нарушен, это приведёт к сбою, что многократно увеличивает ценность систем радиоэлектронной борьбы (РЭБ). Ещё один сравнительно дешёвый и довольно старый способ борьбы — дым, который давно используется для защиты от высокоточного оружия, например танков. Наведение на цели небольших дронов-убийц пока осуществляется оптическими или недорогими тепловизионными головками наведения, для которых дым является нерешаемой проблемой, а радиолокационное самонаведение пока стоит чрезвычайно дорого.

Если есть операторы беспилотников, то можно уничтожать и их. В частности, израильские исследователи из Университета Бен-Гуриона недавно продемонстрировали технологию ИИ на основе глубоких нейронных сетей, позволяющую вычислять координаты операторов, используя только данные траектории движения беспилотников. При скорости ударных беспилотников около 100 км/ч остаётся запас по вре-

мени для уничтожения оператора ракетным или артиллерийским ударом. То есть против ИИ может с успехом использоваться также ИИ.

В США начались испытательные полёты боевого самолёта нового поколения, создаваемого по программе NGAD (Next Generation Air Dominance — воздушное доминирование следующего поколения). Это концептуально новый подход к воздушной войне. Теперь в воздушное пространство противника засылается малозаметный разведчик-убийца, трудноуязвимый для противника в силу своей малозаметности. Такая машина, оснащённая ИИ, способна обнаруживать воздушные цели и обеспечивать применение по ним ракет истребителями старых типов как на предельную дальность, так и без включения их радиолокационных станций, т. е. скрытно для противника. При этом этот летательный аппарат и сам более чем способен вести воздушный бой и сбивать те истребители противника, которые его всё-таки обнаружили. Как и многие другие военные инициативы, эта развивается не только США, поэтому военные эксперты сходятся в одном, что последние инновации способны резко изменить характер военных действий. Впрочем, это не последняя инновация в военном деле.

Современные автоматизированные системы управления (АСУ) позволяют организовывать взаимодействие боевых единиц и различных уровней командования в вооружённых силах на небывало высоком уровне, позволяя им действовать как единый организм. В частности, в США разрабатывается концепция многодоменного противостояния (Multidomain Operation) — одновременное ведение войны в различных физических средах (доменах): на поверхности, на воде (под водой), в воздухе, в космосе и даже в киберпространстве. По сути, это расширенная версия сетецентрической войны, которая предполагает глубочайшую интеграцию между собой боевых единиц, входящих в состав военно-воздушных сил, военно-морских сил, сухопутных войск и других элементов вооружённых сил.

В рамках многодоменной боевой операции вооружение, запускаемое одним видом войск, например, с корабля или подводной лодки, может получать целеуказание от боевой единицы другого вида войск в автоматизированном режиме. Планирование ведения боевых действий и управление войсками также ведётся с учётом преимуществ и недостатков всех элементов доменов. Зона боевых действий в рамках многодоменного противостояния делится на боевые зоны и зоны поддержки. В рамках многодоменной стратегии формируются дополнительные горизонтальные информационно-управляющие связи, которые, с одной стороны, повышают скорость взаимодействия, а с другой стороны повышают достоверность разведывательной информации, что обеспечивает принятие верных решений.

Можно выделить несколько ключевых отличий многодоменного противостояния:

— горизонтальные связи управления, обеспечивающие непосредственно взаимодействие между боевыми единицами разных видов и родов вооружённых сил;

— применение развитых систем связи, в том числе спутниковой, с многократным резервированием и широкими высокоскоростными каналами передачи данных;

— применение систем управления с элементами ИИ, обеспечивающее автоматизацию принятия решений.

Глубокая интеграция доменов позволит повысить оперативность управления войсками за счёт синергетического эффекта от получения и обработки всей доступной информации всех участников многодоменного взаимодействия. Собственно существуют два основных способа достижения конкурентных преимуществ: сделать в количественном измерении свои циклы действий более быстрыми, что вынудит вашего противника реагировать на ваши действия, или же улучшить качество принимаемых решений, т. е. принимать решения, в большей степени соответствующие складывающейся ситуации, чем решения вашего противника.

Таким образом, при столкновении противников с примерно равными по характеристикам вооружениями преимущество получит тот, кто будет лучше координировать действия своих сил на всех уровнях, быстрее получать и обрабатывать разведывательную информацию, принимать решения. В общем, быстрее думать (очевидно, последнее будет лучше получаться у ИИ). В результате противник с меньшим количеством вооружений может получить преимущество над противником с большим количеством вооружений за счёт более эффективного управления ведением боевых действий. Разумеется, ключевым здесь является слово "может".

Не исключено также, что однажды не в меру развитый ИИ осуществит перехват управления человеческой цивилизацией и начнёт осуществлять его по-своему. И это может стать новым вызовом для будущих генералов.

По материалам ***rbc.ru, topwar.ru, habr.ru, vpk.name, popmech.ru***

Приём статей: mail@radio.ru
Вопросы: consult@radio.ru