Отныне мы живем в мире кибервойн, кибервойск и командований официально, как недавно стало известно из заявления министра обороны. Первопроходцами тут были США, оседлавшие технологическую волну информационных технологий — но кто при этом помнит, что одним из теоретиков информационного оружия был советский маршал? Это самое тихое оружие на свете, но оно может оказаться и самым эффективным, невиданным образом сочетая в себе физические и гуманитарные научные принципы

Войска информационных операций
В Вооруженных силах России существуют войска информационных операций, сообщил министр обороны страны Сергей Шойгу во время своего выступления на «правительственном часе » в Госдуме 22 февраля. Обычно министр обороны выступает в Госдуме в закрытом режиме, но накануне Дня защитника Отечества заседание решено было сделать открытым.

В ходе обсуждения Владимир Жириновский предложил не забывать и о контрпропаганде — в советское время в структуре Минобороны было специальное седьмое управление, напомнил он, и его можно воссоздать. «Сейчас нужна спецпропаганда, чтобы не только знать армию противника, но и подготовиться к работе с населением», — заявил Жириновский.

«Просто хочу вам сказать, что четыре года как создано. Правда, оно не седьмое называется, а немножко по-другому. За это время созданы войска информационных операций, что гораздо эффективнее и сильнее всего того, что раньше мы создавали в направлении, которое называлось контрпропагандой. Потому что пропаганда должна быть тоже такой умной, грамотной», — рассказал в ответ министр.

По словам главы комитета Госдумы по обороне Владимира Шаманова, войска информационных операций созданы прежде всего «для защиты интересов национальной обороны и противоборства в информационной сфере».

Конечно, для специалистов не секрет, что еще с начала 2000-х годов в России организованы курсы для офицеров, целью которых было повышение информационной грамотности. В 2014 году, приказом министра обороны РФ Сергея Шойгу, были созданы и получили штатную структуру в армии войска информационных операций, а при генеральном штабе создано кибернетическое командование. 12 мая 2014 года ТАСС со ссылкой на свой источник в Минобороны опубликовал следующее сообщение: «Предложение о создании такой структуры, предназначенной для кибернетического и информационного противоборства с вероятным противником, находилось в проработке не один год. Прошлогодние разоблачения экс- сотрудником ЦРУ Эдвардом Сноуденом глобальной электронной слежки со стороны АНБ США только ускорили процесс принятия решения».

По словам собеседника агентства, в состав войск информационных операций должны были войти части и подразделения в военных округах и на флотах, укомплектованные высококвалифицированными специалистами: математиками, программистами, инженерами, криптографами, связистами, офицерами радиоэлектронной борьбы, переводчиками и другими.

Теперь не только о наличии, но и о высоком уровне новых, можно даже уточнить - принципиально новых войск официально объявил министр. Экс-начальник Генштаба Вооруженных сил РФ (2004-2008 гг.) генерал армии Юрий Балуевский, комментируя заявление Сергея Шойгу, сказал, что победа в информационном противоборстве зачастую имеет большее значение, чем в классической войне. «Победа над противником в этой войне может быть намного важнее, чем победа в классическом военном противостоянии, так как она бескровна, а эффект поразительный, обескровливающий и парализующий все органы власти государства-противника», — сказал Балуевский агентству РИА Новости.

Кибервойна — пятая область войны, после земли, моря, воздуха и космоса
Каждый день количество людей получающих доступ к интернету, в масштабах всего земного шара, неуклонно растёт. К 2017 году, по разным данным от 42 до 48% населения земли будут иметь возможность зайти в международную сеть. В день отправляются миллиарды электронных писем и сообщений, даже самые упертые ретрограды, уже не могут отрицать торжество информационной эпохи на планете Земля.

Но все эти сообщения, в том числе и секретные, могут быть уязвимы. Британский журнал The Economist описал кибервойну как «пятую область войны, после земли, моря, воздуха и космоса». Но насколько в действительности реальна угроза вторжения в киберпространство любого государства, какие это несет опасности, и какие перспективы у этой, наиболее футуристичной части современной гибридной войны?

Совсем недавно, на фоне постоянно приходящих новостей о вмешательстве «российских хакеров», в дела государств Евросоюза и США, был опубликован доклад международной фирмы Zecuricon Analytics. «Коммерсантъ» приводит данные, согласно которым Россия тратит на свои киберподразделения до 300 млн. долларов в год. Суммарная численность служащих в соответствующих подразделениях сотрудников доходит до тысячи человек.

Несмотря на высокий потенциал, Россия находится лишь на пятом месте, в неофициальном зачете по кибервойскам. США, Китай, Великобритания и Южная Корея, последовательно расположились в первой четверке. Причем количество служащих может доходить и до 20 тыс. человек, как в Китае, а финансирование — до 7 млрд долларов как США. Стоит отметить, что и в иных странах есть свои, порой даже нашумевшие подразделения кибербезопастности, к примеру, отряд 121 в Северной Корее, запомнившийся взломом американских серверов, на которых хранился шуточный фильм о Ким Чен Ыне.

Первопроходцами были американцы. Глава Агентства национальной безопасности США (АНБ, или NSA) генерал-лейтенант Кит Александр заявил о начале формирования кибервойск, как специального подразделения Стратегического командования США, 5 мая 2009 года. Главной задачей подразделения, по словам генерала, должна была стать защита страны от атак через компьютерные сети и обеспечение безопасности электронных систем. Однако как продемонстрировал Эдвард Сноуден, работавший на ЦРУ и то же АНБ, США использовали свой силовой компьютерный потенциал не только для защиты сетей и систем, но и для достаточно активных действий, создав невиданную сеть глобальной слежки.

Два поля боя и два принципа кибервойны
Известно что в 21-м веке многие науки перешли на междисциплинарные условия существования, это значит, что для рассмотрения какой либо проблемы, нам необходимо исследовать её не только в рамках одной науки, но подключить и смежные дисциплины, а возможно и самые неожиданные подходы. Исключением не стала и военная наука. Многие слышали такие термины как гибридная, сетецентрическая, информационная война. Кибервойна в данном случае, синергетически, как в теории действия сложных систем, входит в каждый из вышеописанных видов войн. В данном случае мы подразумеваем не классические средства радиоэлектронной борьбы, а именно информационные системы.

Начальник Генерального штаба Вооруженных сил России генерал армии Валерий Герасимов подробно разъяснял, что «в современных конфликтах все чаще акцент используемых методов борьбы смещается в сторону комплексного применения политических, экономических, информационных и других невоенных мер, реализуемых с опорой на военную силу». Писал генерал в опубликованной в газете «Военно-промышленный курьер» статье «По опыту Сирии» от 9 марта 2016 года.

Связанные глобальной сетью, спутниковыми передатчиками данных позиционирования, многоуровневой разведывательной системой из беспилотников-разведчиков, самолётов управления и спутников шпионов, современные армии развитых государств действуют как единое целое на неограниченном пространстве. В перерыве между иракскими кампаниями, проводимыми США, суммарная полоса пропускания военной сети Пентагона выросла в 7 раз, до 3 ГГц. И это за 12 неполных лет с 1991 по 2003 год. К сожалению, данные по современному развитию информационных военных систем в США недоступны, что по своему говорит об их важности.

Во время операции по принуждению Грузии к миру в 2008 году российское командование допустило многочисленные вынужденные ошибки в управлении частями на поле боя. Беспилотных систем практически не было, связь работала неудовлетворительно, время принятия решений затягивалось. Дошло до того, что командующий 58 армией генерал Хрулёв из-за отвратительно проведенной разведки попал в засаду и был ранен.

За неполные 8 лет была проделана колоссальная работа по устранению этих недостатков. Вот что министр обороны РФ Сергей Шойгу рассказал о проведенной работе депутатам Госдумы 22 февраля: «В 3 раза повышена оперативность принятия решений по критически важным вопросам. Улучшены характеристики систем обработки данных. Для сравнения: российский Национальный центр превосходит объединённый центр управления вооружёнными силами Франции “Балар” в 19 раз по суммарному объёму хранимых данных и в 3 раза по вычислительной мощности. При этом комплекс зданий Минобороны России построен в 3 раза быстрее и в 2,6 раза дешевле, чем французский центр» — сказал Сергей Шойгу.

Информационная платформа Национального центра позволила собрать в единую систему межведомственного взаимодействия 73 федеральных органа исполнительной власти, органы власти всех 85 субъектов Российской Федерации, 1320 государственных корпораций и предприятий оборонно-промышленного комплекса. Отдельно остановился глава военного ведомства на качественных возможностях Национального центра управления обороной, который круглосуточно осуществляет мониторинг и координацию 6500 мероприятий Плана деятельности Вооружённых Сил: «Впервые создано единое защищённое информационное пространство на федеральном, региональном и местном уровнях», — отметил Сергей Шойгу.

Но информационная война многолика. Во время и после упомянутого конфликта между Россией и Грузией информационная сфера тоже стала полем боя. Не только в боевых операциях и на дипломатических переговорах, но и в ходе «баталий» на сайтах, в прессе и в телестудиях решалось, какая завершающая черта будет поведена под итогами скоротечной войны.

Сам принцип ведения кибервойны разделен на два направления: шпионаж и атаки. Главной целью шпионажа служит как можно менее заметное проникновение во вражескую сеть и похищение необходимой информации. Атаки же проводятся по многим направлениям и могут отличаться друг от друга. Это может быть вандализм сайтов и серверов, например, с подменой их реального содержания на всевозможные непристойности. Это атаки на инфраструктуру, компьютерную сеть, отказ сервисов с целью нарушить нормальную работу ведомства или целого государства. И, наконец, растет роль пропаганды, учитывая современные возможности воздействовать на умы поверх границ.

В развитых странах, включая Россию, интернет давно стал неотъемлемой частью не только повседневной жизни граждан, но и таких серьезных систем как биржи или системы управления, вплоть до городского транспорта или банка. Атака на подобные системы, правительственные серверы, может повлечь за собой вполне серьезные бедствия или социальные потрясения, внести разлад в повседневную жизнь страны, нарушить управление военной или гражданской инфраструктурой.

Как пишет эксперт по безопасности правительства США Ричард Кларк в своей книге «Кибервойна»: «кибервойна — действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения». Сети, добавим, не только инфраструктурные, но и медийные.