Сетевые войска

Написала:
МАРИЯ САЛЬНИКОВА

Нарисовал:
ДЖОЗЕФ АШ

Англия решила начать кибервооружение. Не является ли эта поочередная подготовка стран сигналом предстоящих военных действий, разыгрывающихся на просторах интернета?

Импульсом для активных действий по укреплению системы безопасности в сетевых ресурсах стала угроза Америки применять оружие в борьбе с хакерами. И у них есть для этого основания. Ведомство Пентагона даже готовит к публикации доктрину о кибербезопасности. Похоже, правительство США в серьез принялось за традиционное военное вооружение, только в сфереинтернет-коммуникаций. Вполне кстати, так как попытки хакерских программ проникнуть в спецбазы и секретные системы совершались неоднократно. Совсем недавно, к примеру, стало известно о кибератаке, направленной на крупнейшую авиационную корпорацию LockheedMartin. Хотя нападение отразили, стоит учитывать, что блокируя и повреждая компьютерную систему такой организации, можно создать рычаг манипулирования и дестабилизации страны. Вероятно, именно поэтому Америка так заинтересована во всевозможных капиталовложениях в исследовательские работы данного направления,а также в создании хорошо функционирующего аппарата, который бы надежно обеспечивал безопасность страны в киберпространстве.

В свою очередь, Англия, комментируя действия США по укреплению системы безопасности, призналась в ведении разработки военного инструментария для ответных атак. Министр обороны Британии, Ник Харви аргументирует важность кибервооружения тем, что хотя интернет и новое поле деятельности, там работают те же законы и нормативы, что и в реальной жизни. Довольно сильным стимулом для такой подготовки являются периодические взломы правительственных систем. Значит, чтобы противостоять иностранным кибер-разведчикам, требуется комплексная и хорошо разработанная система безопасности. Таким образом, было положено начало важной операции, под грифом «Кибервооружение». Безусловно, более детальная информация по составлению и осуществлению таких проектов строго конфиденциальна. И все же известно, что в подготовку по созданию кибер-армии включены представители правительственного аппарата и Центр кибербезопасности. Ник Харви также заметил, что даже если «хакерские полки» не приобретут особой значимости реальной армии, это все же укрепит национальную безопасность страны.

Интересно вспомнить о том, что в Китае формирование сетевых войск объясняется лишь оборонительными целями. Хотя есть предположения, что китайцы уже инициировали ряд кибер-атак, среди «жертв» которых оказались такие гиганты промышленности и научной деятельности как Россия и США. Следовательно, уязвимые для ноу-хау вирусов и шпионских программ места имеются и в мощнейших державах. А поскольку XXI век известен глобальной компьютеризацией и повсеместным проникновением интернета во все сферы повседневной жизни, кибер-оружие действительно стает важной составляющей безопасности стран. И Англия бесспорно права, признавая на государственном уровне важность формирования «сетевых вооруженных сил» для обеспечения целостной мощи страны.

СПРАВКА

Создание «кибероружия» и «кибер-войск» — это разработка новейших вирусов и шпионсикх программ, а также подготовка специалистов для «военных» операций в интернет-среде. Цель таких подготовок состоит в обеспечении возможности оборонятся и нападать в случае необходимости, с помощью компьютерных технологий. Попытки кибератак уже предпринимались, что доказывает появление технически совершенного вируса Stuxnet в Иране. Stuxnet — шпионская программа, осуществляющая несанкционированный сбор данных в компьютерной системе. Его «дебют» был направлен на остановку работы иранского завода Натанз по обогащению урана. Один из результатов действия вируса — колеблющаяся работа центрифуги в заводском механизме. Код такой «бомбы» составляет 15000 строк! Это шедевр «вирусологии» с целевым предназначением. Объектом поражения такого вируса мог бы стать любой другой завод или организация. На сегодня, считается самым опасным в мире вирусом.

Ссылки:

www.gchq.gov.uk/
— центр кибербезопасности Англии

ПОСКОЛЬКУ XXI ВЕК ИЗВЕСТЕН ГЛОБАЛЬНОЙ КОМПЬЮТЕРИЗАЦИЕЙ И ПОВСЕМЕСТНЫМ ПРОНИКНОВЕНИЕМ ИНТЕРНЕТА, КИБЕР-ОРУЖИЕ ДЕЙСТВИТЕЛЬНО СТАЕТ ВАЖНОЙ СОСТАВЛЯЮЩЕЙ БЕЗОПАСНОСТИ СТРАН.