Муниа Бен Айсса

Кибервойна. Она происходит в виртуальном пространстве, но ее последствия вполне реальны. Чтобы разрушить страну, уже не нужны пушки и бомбы – кибератака не менее эффективна, хотя шума значительно меньше. Как же ведутся новые войны?

Сентябрь 2007 года. Таллинн, столица Эстонии, столкнулся с войной нового типа. Менее кровавое, чем обычное, но столь же эффективное и губительное нападение произошло на новом поле сражения – в Интернете. На четыре недели были парализованы сайты средств массой информации, банков и правительства. Тысячи компьютеров со всего мира затопили эстонские сайты запросами, создавая «пробку», в которой остановилась система.

Кто несет ответственность за это? Точно узнать невозможно, но некоторые подозревают могущественного соседа Эстонии – Россию, раздраженную переносом памятника в честь победы Советского Союза.

Как бы то ни было, нападение послужило уроком, и НАТО создал в Таллинне центр кибернетической безопасности. Однако, по признанию полковника Ильмара Тамма, центр создан, скорее, для организации исследований, а не обороны (и уж тем более не для нападения). «Киберсолдаты проводят исследования и анализ (…) того, что происходило в прошлом, чтобы прогнозировать будущее». Президент Эстонии Тоомас Хендрик Ильвес считает, что единственный способ эффективно бороться с новой угрозой, это прогнозировать завтрашние кибератаки и применять «масштабный подход с использованием международных организаций».

Франция тоже подвергается кибератакам. Находящееся в Париже новое Государственное агентство по безопасности информационных систем контролирует критически-важную инфраструктуру страны. В прошлом году киберсолдаты изучили, проанализировали или отбили 200 крупных нападений. Генеральный директор Патрик

Пайло так описывает разные виды нападений: «одни нападения совершаются с целью заблокировать систему, это так называемые атаки типа «отказ в обслуживании». Задача других – взять компьютеры под свой контроль, чтобы украсть информацию или использовать компьютер для очередных нападений».

Такие атаки угрожают и безопасности, и экономической устойчивости. Правительствам нужно понять масштаб происходящего и принять соответствующие меры – им еще предстоит сформировать доктрину кибервойны, чтобы лучше организовать сопротивление гражданскими и военными средствами.

Смотреть видео: *www.france24.com* .