

О войнах будущего, в которых стороны будут "сражаться битами и байтами", пишет немецкая Die Welt, рассказывая, как опасны хакерские атаки для химических заводов, самолетов и систем энергоснабжения.

Израильская армия опробовала эту форму ведения войны уже три года назад, при нападении на секретный строительный объект в Сирии, сообщает автор статьи Мальте Хервиг. 6 сентября 2007 года на экранах сирийских радаров было все спокойно, но в то же самое время израильские самолеты наносили удары по атомной энергетической установке, которую Сирия строила при помощи Северной Кореи.

В код программного обеспечения сети сирийской противовоздушной обороны израильские военные хакеры тайком внедрили "троянцев", и израильтяне смогли управлять системой противовоздушной обороны противника, сообщает издание.

С сентября 2009 года в армии США существует киберкоманда - U.S. Cyber Command. Киберподразделение есть и у Китайской народной армии. Два года назад аналогичный отдел был создан в бундесвере. Тем более, как показала в феврале 2009 года атака червя Conficker, который заразил несколько сотен компьютеров германской армии, "враг в сети не дремлет".

Онлайн-армии имеют еще 20 или 30 государств, в их числе Россия, Южная Корея, Индия, Пакистан, Франция и Израиль, сообщает Хервиг со ссылкой на Ричарда Кларка, советника Белого дома по кибербезопасности. В своей новой книге "Cyber War: The Next Threat to National Security and What to Do About it" Кларк пишет, что глобальная война в сети уже началась и многочисленные хакеры, находящиеся на службе у различных государств, готовят поля для будущих сражений.

США, Россия и Китай, говорится далее в статье, "наступательно используют возможности кибершпионажа". Они не только создают военные киберподразделения, но и сотрудничают с гражданскими хакерами.

Китайская армия, технически проигрывая американцам в вооружении, сократила численность своих войск и стала вкладывать деньги в новые технологии. При этом

китайцы с самого начала сделали ставку на наступательную войну в киберпространстве.

Во времена кибершпионажа разведчик из плоти и крови уходит в прошлое, говорится в статье. Новые копировальные аппараты могут содержать микрочипы, сохраняющие каждую копию и отправляющую ее заказчику. Специальные программы способны отслеживать все изменения на жестких дисках и регистрировать ввод любых данных с клавиатуры зараженного компьютера.

На Западе, напоминает Хервиг, в сети интегрирована не только вся экономика, но и системы электроснабжения, а также транспорта. Вражеская кибератака может нанести им ущерб больший, чем ядерный удар, полагает Кларк. "После такой атаки следующая война, пожалуй, снова будет рукопашной - безо всякого интернета", - заключает издание.

Мальте Хервиг
Die Welt
По материалам: InoPressa.ru