ББК 32.97

ПОЛИТИЧЕСКОЕ ХАКЕРСТВО: СУЩНОСТЬ, ТЕНДЕНЦИИ РАЗВИТИЯ

Кирьяков С. А., Соснина Т. Н.

Самарский государственный аэрокосмический университет имени академика С. П. Королёва (национальный исследовательский университет), г. Самара

Использование компьютерных технологий в политическом контексте имеет следствием видоизменение функционального статуса традиционных социальных реалий – диверсий и шпионажа.

Превращение компьютерного кода в оружие обеспечивает нанесение высокоточных ударов по техническим системам противника, не причиняя прямого физического вреда людям-операторам и менеджерам. Через воздействие компьютерных атак возможно похищение данных, трансформация уровней личного и политического риска. Такое развитие цивилизации является свидетельством видоизменения природы политического насилия, необходимости учёта специфики ограничений, касающихся целесообразности проведения кибератак по параметру количество-качество диверсионных операций.

Компьютерный шпионаж, как правило, сопряжён с совершенствованием традиционных методов разведки, использования ресурсов интеллекта человека. В совокупности эти факторы делают проблематичной саму идею о том, что хакерские атаки ассоциируются с приходом эпохи кибервойн.

Любому политическому режиму присуще использование насильственных функций. Государство выживает, в конечном счёте, только сохранив монополию на силу, оформленную в законодательном порядке. Поддерживая доверие к способности государственных органов защитить собственность и обеспечить безопасность граждан, насилие, присущее государственной власти, служит ей опорой, позволяя реализовать верховенство права.

Трудно представить, каким образом кибернетические атаки можно было бы использовать для практической реализации постановлений и законов как внутри государства, так и в международных отношениях.

Более сложное явление – цифровая слежка.

Кибератаки отличаются высокой точностью, они не обязательно огульно подрывают государственную монополию на применение силы. Вместо этого их можно приспособить для нападений на определённые объекты, общественные и политические организации, избирательно подрывая авторитет конкретных социально ориентированных групп.

Существенно, что цифровое насилие связано с этикой и стратегией национальной безопасности. Во многих странах применение компьютеров этически предпочтительнее обычных вооружений: кибератака может быть менее насильственной, менее травматичной и более ограниченной, чем традиционные силовые удары.

Подобные доводы применяются и к этике кибершпионажа. Секретные данные могут быть получены через проникновение в компьютерные системы или перехват цифровых сигналов; путём захвата враждебной территории с риском для субъектов действий.