ИНФОРМАЦИОННАЯ ВОЙНА - комплексная стратегия достижения информационного превосходства при противоборстве в конфликте путем воздействия на информационную среду противника при одновременном обеспечении безопасности собственной информационной среды. По соотношению "эффективность - себестоимость" И.В. является в настоящее время самым перспективным способом "продолжения политики иными средствами" (см. Война). И.В. правомерно трактовать как составляющую часть информационной борьбы. Особенность информационной борьбы заключается в том, что она ведется постоянно - в мирное и в военное время.

Организация и ведение информационной борьбы подчиняются определенным закономерностям: 1) Информационная борьба является самостоятельной формой конфликта и не может рассматриваться как разновидность его вооруженной составляющей. 2) Информационная борьба всегда бескомпромиссна. 3)

Роль информационной борьбы повышается по мере углубления информатизации общества. Расширение сферы применения новейших информационных технологий повышает их уязвимость и снижает их устойчивость. В ходе информационной борьбы происходит постоянное увеличение числа косвенных участников конфликта, вовлекаемых в него по мере углубления информатизации общества. 4) Информационная борьба ведется непрерывно на протяжении всего конфликта. 5) Следствия ведения информационной борьбы не всегда очевидны для тех, против кого она ведется. 6) Информационная борьба носит упреждающий характер. Только после завоевания информационного превосходства над противником возможно принятие адекватных решений и эффективное разрешение конфликта. 7) Развитие и исход информационной борьбы происходят в пользу стороны, обладающей более высоким информационным и технологическим потенциалом.

Главным инструментарием ведения информационной борьбы и И.В. выступает информационное оружие - совокупность методов и средств разрушения (похищения) информации, запрета доступа к ней законных владельцев, разрушения систем телекоммуникационного обеспечения жизнедеятельности противника. Основными свойствами информационного оружия являются: 1) скрытность (возможность достижения целей войны без ее объявления); 2) масштабность (возможность нанесения противнику невосполнимого ущерба); 3) универсальность (возможность применения военными и невоенными структурами агрессора). Угроза И.В. может исходить от враждебных государств, от террористических групп и от отдельных личностей. В мирное время И.В. имеет целью подрыв безопасности личности, общества и государства противоположной стороны и защиту собственных национальных интересов.

В военное время И.В. сочетается с традиционными способами ведения боевых действий

и направлена на информационно-психологическое обеспечение мероприятий по дезинформации противника и защите собственной информации.

В зависимости от объекта воздействия И.В. подразделяют на информационно-техническую войну и информационно-психологическую войну. Основным военный аспект информационно-технической войны: 1) достижение информационного превосходства над противником в средствах управления и связи; 2) получение опережающей информации о стратегической, оперативной или тактической обстановке для принятия соответствующих решений; 3) дезинформация противника.

Особый интерес для государств и корпораций представляет экономическая информация, научно-технические и государственные тайны. Новейшие информационные технологии позволяют небольшим автономным и рассеянным группам людей координировать собственную деятельность в реальном масштабе времени через любые расстояния. Доминирующее положение на локальном и глобальном уровне занимают субъекты, действующие в сетевой форме.

Эти принципиально новые формы самоорганизации человеческих сообществ нередко возникают внутри уже существующих типов отношений: родоплеменных, иерархических и др. Растет число активных участников неправительственных организаций, владеющих новейшими информационными технологиями: ранее эти группировки были несравнимо слабее субъектов государств и корпоративных структур. Теперь новейшие информационные технологии сняли с групп гражданского общества изоляцию и дали им возможность кооперации, координации, распределения и обмена информацией в планетарном масштабе и в реальном масштабе времени.

Пассивное противодействие И.В. в компьютерных сетях - это законодательное, организационное (выработка политики в области информационной безопасности, анализ угроз и методов их нейтрализации, подбор и обучение персонала, дисциплина информационной безопасности, физическая защита помещений и оборудования и др.) и программно-техническое (защищенные линии связи, управление доступом, технологии "клиент-сервер", криптографическая защита данных, потоковое шифрованное сжатие больших объемов информации, спецификация технологий разработки и независимая сертификация оборудования, программного обеспечения и др.) противодействие.

Активное ведение И.В. в компьютерных сетях - это: 1) кампании дезинформации; 2) техно-программные варианты психологических методик фильтрации информации; 3) "случайные аварии" стратегически важных систем с компьютерным управлением; 4) хакерство; 5) программные вирусы и логические бомбы; 6) создание боевых групп для активной работы в сетях.

В настоящее время в ряде государств разрабатываются меры противодействия сетевым И.В., создавая специальную сеть для отслеживания распространения информации во всем мире.

Возможно автоматически перехватывать любую электронную информацию, распространяемую по мобильным и стационарным телефонам, факсам или электронной почте, непрерывное прослушивание всех коммуникационных каналов с применением словарей ключевых слов, фраз, имен, географических названий, что позволяет повысить эффективность взаимодействия спецслужб различного характера. Телекоммуникационные центры перехвата информации эффективно препятствуют образованию очагов напряженности, с которыми невозможно справиться демократическими методами.

Это широкомасштабное наблюдение, для которого предназначены интеллектуальные компьютерные системы поиска и анализа информации, технологии нейро-агентов, мощные базы данных с обработкой сверхбольших массивов информации и возможностями поиска по нечетким запросам. Сетевой способ ведения информационной борьбы гораздо эффективнее обычного. Живучесть боевой сетевой системы несравнима с традиционными видами иерархически организованных боевых систем "человек - машина".

У сетевой организации наблюдается существенная способность расти более чем в геометрической прогрессии. Здесь имеются в виду принципиально иные формы деятельности и принятия решений в военных и гражданских сообществах, когда происходит трансформация новейших информационных технологий в мегамшины двойного (в том числе и идеологического) назначения. Информация от СМИ воздействует значительно более действенно, чем в прежние годы, на общественное сознание, политические взгляды, моральные ценности и поведение людей.

Информационный прессинг СМИ может создать атмосферу напряженности и политической нестабильности в обществе. Информация оказывает решающее воздействие на процессы формирования личности и может вызвать неадекватное социальное или криминальное поведение групп людей и отдельных лиц, нанести физический, материальный и моральный ущерб гражданам. Последствия информационно-психологического воздействия СМИ - глубокие трансформации индивидуального, группового и массового сознания, изменение социально-психологического климата. Это прежде всего манипуляционные воздействия на личность, на ее представления и эмоционально-волевую сферу; это инструмент психологического давления с целью явного или скрытого побуждения индивидуальных и социальных субъектов к действиям в интересах отдельных лиц, групп, организаций или

ИНФОРМАЦИОННАЯ ВОЙНА

Автор: словарь
19.06.2008 15:18 -

стран, осуществляющих такие воздействия.

С.В. Силков