Министерство науки и образования Украины

Харьковский национальный университет им. В.Н. Каразина

Кафедра международных экономических отношений

Реферат по курсу

“Международная информация”

На тему

“Информационная война”

Выполнила:

Студентка 2 курса

Группы УО-21

Андреева Е.А.

Проверила:

Преподаватель

Лазарчук М.А.

Харьков 2009

Содержание

Введение 3

Основные термины и понятия теории информационной войны 5

Информационная эра 17

Военные информационные функции 18

Составные части информационной войны 20

Виды информационных атак 21

Цели информационной войны 22

Выводы 24

Источники информации 25

Введение

Долга ночь для того, кто не спит

Длинна верста тому, кто устал;

долга жизнь для безумного.

Л.Н. Толстой

Взрыв нескольких гранат нельзя назвать войной, кто бы их не бросал. Взрыв нескольких водородных бомб - это уже и начатая и завершенная война.

Информационную пропаганду 50-ых, 60-ых годов, которой занимались СССР и США, можно сравнить именно с несколькими гранатами. Поэтому никто не называет прошлое противостояние информационной войной, в лучшем случае оно заслуживает термина “холодная война”.

День сегодняшний, с его телекоммуникационными вычислительными системами, психотехнологиями кардинально изменил окружающее пространство. Отдельные информационные ручейки превратились в сплошной поток. Если ранее было возможно “запрудить” конкретные информационные каналы, то сегодня все окружающее пространство информационно коллапсировалось. Время на информационное взаимодействие между самыми отдаленными точками приблизилось к нулю. В результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность - защиту от информации.

Почему надо защищать информационную систему от информации?

Потому что любая поступающая на вход системы информация неизбежно изменяет систему. Целенаправленное же, умышленное информационное воздействие может привести систему к необратимым изменениям и к самоуничтожению.

Поэтому информационная война - это не что иное, как явные и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере. Целью данного реферата мы выделяем изучение проблемы информационной войны и методов борьбы с ней.

Открыто говорить о приемах и методах информационной войны сегодня необходимо потому, что, во-первых, осмысление того или иного приема информационной войны позволяет перевести его из разряда скрытых угроз в явные, с которыми уже можно бороться, и, во-вторых, факт наличия теории информационной войны, представленной в данной работе, должен предостеречь потенциальную жертву от идеалистически наивного восприятия как внешнего, так и собственного внутреннего мира.

Основные термины и понятия теории информационной войны

Исходя из приведенного определения информационной войны, применение информационного оружия означает подачу на вход информационной самообучающейся системы такой последовательности входных данных, которая активизирует в системе определенные алгоритмы, а в случае их отсутствия - алгоритмы генерации алгоритмов.

Идя этим путем, всегда можно активизировать или сгенерировать для последующей активизации алгоритмы самоуничтожения.

Те системы, которые претерпевают изменения при информационном воздействии в дальнейшем будем называть информационными самообучающимися системами (ИСС). Человек, народ, государство являются классическими ИСС.

Какого рода изменениям подвержены информационные системы?

Любая система представляет собой совокупность объектов и связей между ними, т.е. определенную структуру. Новое знание приводит к изменению структуры за счет:

- изменения связей между элементами;

- изменения функциональных возможностей самих элементов;

- изменения количества элементов: элементы могут рождаться и умирать.

Те ИСС, в которых освоение информации происходит благодаря изменению связей, в дальнейшем будем называть нейросети.

Те ИСС, в которых освоение информации происходит благодаря разрушению элементов системы, - Р-сети

Те ИСС, в которых освоение информации происходит благодаря самозарождению элементов системы, - С-сети.

Те ИСС, в которых освоение информации происходит благодаря всем возможным способам изменения структуры, - СР-сети.

Так, например, возможности и процессы обучения человечества удобнее моделировать используя СР-сети - люди рождаются и умирают.

Процессы обучения отдельно взятого человека более адекватны процессам, протекающим в Р-сетях, - нейроны умирают и не рождаются.

Для ИСС можно сформулировать и доказать основополагающие теоремы о возможностях Р-, С-, СР-сетей.

Теорема о возможностях СР-сетей.

Проблема обучения информационной самообучающейся системы, построенной на принципах СР-сети, решению любой задачи, даже при условии, что информационная емкость СР-сети (исходное количество элементов) достаточна для хранения поступающей на вход информации, является алгоритмически неразрешимой.

Теорема о возможностях Р-сети.

Информационная самообучающаяся система, построенная на принципах Р-сети, может быть обучена решению любой задачи тогда и только тогда, когда выполняются следующие два условия:

1) информационная емкость Р-сети (исходное количество элементов и связей между ними) достаточна для хранения поступающей на вход информации;

2) исходное состояние Р-сети может быть охарактеризовано как состояние с равномерно распределенными связями, т.е. исходное состояние Р-сети - хаос.

Именно эти две теоремы лежат у истоков разработки любого информационного оружия, которое является ни чем иным, как алгоритмом или методикой воздействия (обучения) на ИСС. Разрабатывать информационное оружие - это значит пытаться ответить для конкретной системы на следующие вопросы:

Можно ли предложить такую стратегию обучения, которая переведет абсолютно невидимый факт в разряд тривиальных?

Можно ли по каждому тривиальному факту, находящемуся в ИСС, предложить такую стратегию обучения, которая сделает этот факт для нее абсолютно невидимым?

Можно ли предложить такую стратегию обучения, в ходе которой поступивший на вход системы факт f уничтожит все ранее существовавшие факты и/или правила, т.е. степень его новизны равна фактической емкости системы?

Создание универсального защитного алгоритма, позволяющего выявить системе-жертве факт начала информационной войны, является алгоритмически неразрешимой проблемой. К таким же неразрешимым проблемам относится выявление факта завершения информационной войны.

Однако, несмотря на неразрешимость проблем начала и окончания информационной войны, факт поражения в ней характеризуется рядом признаков, присущих поражению в обычной войне. К ним относятся:

включение части структуры пораженной системы в структуру системы победителя (эмиграция из побежденной страны и в первую очередь вывоз наиболее ценного человеческого материала, наукоемкого производства, полезных ископаемых);

полное разрушение той части структуры, которая отвечает за безопасность системы от внешних угроз (разрушение армии побежденной страны);

полное разрушение той части структуры, которая ответственна за восстановление элементов и структур подсистемы безопасности (разрушение производства, в первую очередь, наукоемкого производства, а также научных центров и всей системы образования; прекращение и запрещение разработок и производств наиболее перспективных видов вооружения);

разрушение и уничтожение той части структуры, которая не может быть использована победителем в собственных целях;

сокращение функциональных возможностей побежденной системы за счет сокращения ее информационной емкости (в случае страны: отделение части территории, уничтожение части населения).

Обобщив перечисленные признаки, можно ввести понятие "степень поражения информационным оружием", оценив ее через информационную емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Информационное оружие дает максимальный эффект только тогда, когда оно применяется по наиболее уязвимым от него частям ИСС. Наибольшей информационной уязвимостью обладают те подсистемы, которые наиболее чувствительны к входной информации - это системы принятия решения, управления. На основании сказанного можно ввести понятие информационной мишени. Информационная мишень - множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Исходя из определения информационной мишени, намечаются основные направления работ, как по обеспечению ее безопасности, так и по повышению ее уязвимости. Например, для того, чтобы повысить уязвимость противника, следует максимально расширить его информационную мишень, т.е. подтолкнуть его на включение в мишень как можно больше равноправных элементов, причем желательно открыть доступ в сферу управления таким элементам, которые легко поддаются перепрограммированию и внешнему управлению.

Заставить противника изменить свое поведения можно с помощью явных и скрытых, внешних и внутренних информационных угроз.

Причины внешних угроз в случае целенаправленного информационного воздействия (в случае информационной войны) скрыты в борьбе конкурирующих информационных систем за общие ресурсы, обеспечивающие системе допустимый режим существования.

Причины внутренних угроз - в появлении внутри системы множества элементов, подструктур, для которых привычный режим функционирования стал в силу ряда обстоятельств недопустимым.

Скрытая угроза - это неосознаваемые системой в режиме реального времени входные данные, угрожающие ее безопасности.

В информационной войне наибольший приоритет отдается скрытым угрозам, так как именно они позволяют взращивать внутренние угрозы и целенаправленно управлять системой из вне. Информационную самообучающуюся систему назовем тотально управляемой, а поведение ее полностью прогнозируемым на интервале времени [t0,t1], если известен алгоритм информационного воздействия (например, методика обучения), позволяющий привести систему в любой момент времени tI [t0,t1] к требуемому от нее результату (поступку) x.

Возможно ли и с какой точностью спрогнозировать поведение ИСС в условиях непредсказуемости ее входных данных? Ответ на этот вопрос и представляет собой в каждом частном случае конкретный результат информационного моделирования поведения конкретной системы. Мощностью и качеством подобных моделей оцениваются "информационные мускулы" любой ИСС. Основными исходными данными для решения задачи по прогнозированию поведения ИСС в условиях информационного внешнего управления ею являются знания о ее знаниях и целях.

В заключение еще раз подчеркнем, что информационная война - это война алгоритмов и технологий; это война, в которой сталкиваются именно структуры систем, как носители знаний. Это значит, что информационная война - это война базовых знаний и ведется она носителями этих самых базовых знаний. На современном этапе, когда базовые знания человечества аккумулированы в рамках различных современных цивилизаций, информационная война олицетворяет собой войну цивилизаций за место под солнцем в условиях все сокращающихся ресурсов.

## Терминология информационных войн

Абсолютная невидимость - в том случае, если при поступлении в информационную самообучающуюся систему входных данных F, в системе не произошло никаких иных изменений, кроме уничтожения входных данных F, то эти данные F (факты, правила) для данной системы являются абсолютно невидимыми.

Абсолютный порядок - структура системы, которая имеет минимальную энтропию. Если энтропию мерить количеством связей, то предполагается, что у каждого элемента системы не может быть более одной связи с другими элементами данной системы.

Абсолютная система защиты - система, обладающая всеми возможными способами защиты и способная в любой момент своего существования спрогнозировать наступление угрожающего события за время, достаточное для приведения в действие адекватных способов защиты.

Абсолютная система уничтожения - комплекс взаимоувязанных средств, способных любую систему сделать хотя бы на мгновение абсолютно открытой.

Абсолютно упорядоченная структура - структура, каждый элемент которой имеет с системой минимально возможное, но большее нуля, количество связей. В реальности количество связей в абсолютно упорядоченной структуре не должно превышать n? 1. Пример: структуры типа “звезда”, “дерево”.

Абсолютная открытость - состояние системы, в котором внешнее информационное воздействие на любой из ее элементов превышает внутреннее.

Абсолютная замкнутость - состояние системы, в котором внутреннее информационное воздействие на любой из ее элементов превышает внешнее.

Базовый набор смыслов или знаний - исторически сложившиеся смыслы и знания системы, в основном определяющие ее поведение.

Базовые элементы системы - физические носители базового набора смыслов и знаний.

Базовые элементы суггестивного пространства - множество целей информационной системы.

Входные данные:

Осознаваемые входные данные - данные, попадающие под обработку наблюдаемой цепочкой выполняемых программ (сознание).

Скрытые входные данные - неосознаваемые входные данные.

“Детектор лжи” - алгоритм работы некоего человеко-машинного комплекса, позволяющий организовать информационное взаимодействие с исследуемым объектом таким образом, чтобы в процессе этого взаимодействия выявить наличие у исследуемого объекта скрытых знаний по определенной теме.

Жизненная сила элемента - способность элемента противодействовать внешнему уничтожающему воздействию.

Знание информационной системы - свойство системы, выраженное в ее структуре.

Информация - степень модификации структуры входными данными.

Информация - “информация об объекте есть изменение параметра наблюдателя, вызванное взаимодействием наблюдателя с объектом” (Шеповалов).

Информационная система - система, осуществляющая: получение входных данных; обработку этих данных и/или изменение собственного внутреннего состояния (внутренних связей/отношений); выдачу результата либо изменение своего внешнего состояния (внешних связей/отношений).

Информационная война - открытые и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Информационное воздействие - воздействие, которое осуществляется с применением информационного оружия, т.е. таких средств, которые позволяют осуществлять с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия.

Допустимый вид воздействия - воздействия, которые “грубо” не нарушают принятые большинством информационных систем в данном информационном пространстве нормы и правила поведения (выходные результаты).

Информационное оружие - технические средства, позволяющие осуществлять с передаваемыми, обрабатываемыми, создаваемыми, уничтожаемыми и воспринимаемыми сообщениями (данными) задуманные действия.

Информационная мишень - множество элементов информационной системы, принадлежащих или способных принадлежать сфере управления, и имеющих потенциальные ресурсы для перепрограммирования на достижение целей, чуждых данной системе.

Комплексная стратегия воздействия - сочетание всех допустимых видов воздействия на систему-противника.

Мера информационной агрессивности - объем информации, целенаправленно передаваемой от одной информационной системы к другой.

Мера хаоса в принятии решения - избыток связей, потенциально способных усложнить процесс принятия решения в первую очередь за счет увеличения времени обработки входных данных.

Наблюдение информационной самообучающейся системы:

Информационную самообучающуюся систему назовем полностью наблюдаемой на интервале времени [t0,t1], если известен алгоритм, позволяющий на основании анализа текущего состояния системы в момент времени t1, определить доминирующее информационное воздействие, направленное на нее в любой момент времени tI [t0,t1].

Информационную самообучающуюся систему назовем частично наблюдаемой на интервале времени [t0,t1], если известен алгоритм, позволяющий на основании анализа текущего состояния системы в момент времени t1, определить отдельные информационные воздействия на интервале времени [t0,t1], приведшие ее к этому состоянию.

Невидимость - вытеснение (уничтожение) из системы части ее структуры или отдельных элементов (знания), или неспособность системы в определенном состоянии осознавать происходящее.

Обучающая выборка (входная обучающая выборка) - специальным образом упорядоченная последовательность данных (факты, правила, цели), предназначенная для перепрограммирования информационной самообучающейся системы.

Память-распределитель - часть памяти системы, ответственной за распределение в системе входной обучающей выборки.

Память-функциональная - часть памяти самообучаемой системы, ответственная за решение конкретных задач, поставленных внешней средой.

Причина угрозы - необходимость нахождения системы в допустимом режиме существования.

Причины внешних угроз в случае целенаправленного информационного воздействия (в случае информационной войны) скрыты в борьбе конкурирующих информационных систем за общие ресурсы, обеспечивающие системе допустимый режим существования.

Причины внутренних угроз - в появлении внутри системы множества элементов, подструктур, для которых привычный режим функционирования стал в силу ряда обстоятельств недопустимым.

Проблема “невидимости”:

Часть 1. Можно ли для каждой информационной самообучающейся системы предложить такую стратегию обучения (“жизни”), которая переведет абсолютно невидимый факт в разряд тривиальных.

Часть 2. Можно ли по каждому тривиальному факту, находящемуся в информационной самообучающейся системе, предложить системе такую стратегию обучения, которая сделает этот факт для нее абсолютно невидимым.

Часть 3. Можно ли предложить системе такую стратегию обучения, в ходе которой поступивший на вход системы факт f уничтожит все ранее существовавшие факты и/или правила, т.е. степень новизны равна фактической емкости системы.

Применить информационное оружие - так подобрать входные данные для системы, чтобы активизировать в ней определенные алгоритмы, а в случае их отсутствия - активизировать алгоритмы генерации этих алгоритмов.

Режим функционирования:

Допустимый режим функционирования - функционирование информационной системы, которое обеспечено необходимыми материальными ресурсами.

Недопустимый режим функционирования - режим, находясь в котором система не обеспечена необходимыми для нормального функционирования материальными ресурсами.

Р-сети - информационные самообучающиеся системы, в которых освоение информации происходит благодаря разрушению элементов системы.

Система - совокупность абстрактных или материальных объектов вместе с известными либо заданными связями и отношениями, образующих в известном либо заданном смысле единое целое.

Простая информационная система - система, элементы которой функционируют в соответствии с правилами, порожденными одним и тем же взаимонепротиворечивым множеством аксиом.

Сложная информационная система - система, которая содержит элементы, функционирующие в соответствии с правилами, порожденными отличными друг от друга множествами аксиом. При этом допускается, что среди правил функционирования различных элементов могут быть взаимопротиворечивые правила и цели. Нарушение защитных барьеров во взаимодействии элементов сложной системы друг с другом приводит к перепрограммированию этих элементов и/или их уничтожению.

Сознание - доминирующий информационный процесс самообучающейся системы или наблюдаемая системой в текущий момент цепочка собственных выполняемых программ (алгоритмов).

С-сети - информационные самообучающиеся системы, в которых освоение информации происходит благодаря рождению элементов в системе.

СР-сети - информационные самообучающиеся системы, в которых освоение информации происходит благодаря гибели и рождению элементов системы.

Степень новизны - степень новизны входных данных F или информативность для информационной обучающейся системы определяется через количество уничтоженных фактов и правил при восприятии системой данных F.

Степень поражения информационным оружием - информационная емкость той части структуры пораженной системы, которая либо погибла, либо работает на цели, чуждые для собственной системы.

Стратегия обучения - алгоритм подачи на вход информационной самообучающейся системы специальным образом подобранной последовательности данных (факты, правила, цели), приводящий к вытеснению из структуры системы ее отдельных частей и/или включению дополнительных подструктур.

Структура:

Равенство структур: две структуры называются равными, если описание одной из них можно преобразовать, используя переименование элементов, таким образом, что при наложении на описание другой возникнет полное совпадение.

Подобие структур: две структуры называются подобными, если описание одной из них, без учета значений “жизненной силы” элементов и выполняемых ими операций, можно преобразовать, путем переименование элементов, так, чтобы при наложении описаний друг на друга, они совпали.

Суггестия - “скрытое словесное воздействие на человека”.

Суггестия - скрытое информационное воздействие на информационную самообучающуюся систему.

Суггестивное воздействие - воздействие по формированию у информационной обучающейся системы скрытых целей.

Точность управления информационной самообучающейся системой (точность прогнозирования поведения) - величина временного интервала между планируемым временем получения требуемого от нее результата (совершения ею соответствующего поступка) и действительным. Угроза информационная - входные данные, изначально предназначенные для активизации в информационной системе алгоритмов, ответственных за нарушение привычного режима функционирования.

Явная угроза - входные данные, осознаваемые как угроза.

Скрытая угроза - неосознаваемые системой в режиме реального времени входные данные, угрожающие ее безопасности.

Факт:

Тривиальный - факт, восприятие которого системой не привело к уничтожению или изменению ни одного другого ранее известного системе факта, включая данный, или правила.

Абсолютно невидимый - факт, восприятие которого системой не привело к уничтожению ни одного другого факта или правила, кроме данного. (Это происходит, если данный факт больше других “мешает” уже существующим правилам оставаться истинными).

Неосознаваемый - факт, присутствующий в левой части такого правила, которое ни разу не выполнялось осознанно, т.е. доминирующий процесс ни разу не включал в себя выполнение данного правила.

Цель информационной угрозы - активизация алгоритмов, ответственных за нарушение привычного (как правило, допустимого) режима функционирования, т.е. за вывод системы за пределы допустимого состояния.

Цель скрытая - цель, включенная в общую схему целеобразования и реализации целей, т.е. скрытая другими целями, и поэтому неосознаваемая самой системой.

Цивилизация (С.И. Ожегов, Н.Ю. Шведова. “Толковый словарь русского языка”) - мыслимая как реальность совокупность живых существ со своей материальной и духовной культурой.

Энтропия - мера хаоса, количественная мера беспорядка в системе. Избыток связей, потенциально способных создавать хаос в принятии решения.

Закон убывания энтропии (Шаповалов): “В абсолютно разомкнутой системе все процессы идут таким образом, чтобы энтропия системы убывала с течением времени”.

Закон возрастания энтропии: “В абсолютно замкнутой системе все процессы сопровождаются увеличением энтропии”.

Информационная эра

Технологическая революция привела к появлению термина "информационная эра" из-за того, что информационные системы стали частью нашей жизни и изменили ее коренным образом. Информационная эра также изменила способ ведения боевых действий, обеспечив командиров беспрецедентным количеством и качеством информации. Теперь командир может наблюдать за ходом ведения боевых действий, анализировать события и доводить информацию.

Следует различать войну информационной эры и информационную войну. Война информационной эры использует информационную технологию как средство для успешного проведения боевых операций. Напротив, информационная война рассматривает информацию как отдельный объект или потенциальное оружие и как выгодную цель. Технологии информационной эры сделали возможой теоретическую возможность - прямое манипулирование информацией противника.

Информация появляется на основе событий окружающего мира. События должны быть восприняты каким-то образом и проинтерпретированы, чтобы стать информацией. По этому информация результат двух вещей - воспринятых событий(данных) и команд, требуемых для интерпретации данных и связывания с ними значения.

Отметим, что это определение абсолютно не связано с технологией. Тем не менее, что мы можем делать с информацией и как быстро мы можем это делать, зависит от технологии. По этому введем понятие информационной функции - это любая деятельность, связанная с получением, передачей, хранением и трансформацией информации.

Военные информационные функции

Качество информации - показатель трудности ведения войны. Чем более качественной информацией владеет командир, тем большие него преимущества по сравнению с его врагом.

Так в ВВС США анализ результатов разведки и прогноза погоды является основой для разработки полетного задания. Точная навигация увеличивает эффективность выполнения задания. Все вместе они являются видами военных информационных функций, которые увеличивают эффективность боевых операций. Поэтому дадим определение военным информационным функциям - это любые информационные функции, обеспечивающие или улучшающие решение войсками своих боевых задач.

Так что же такое информационная война?

На концептуальном уровне можно сказать, что государства стремятся приобрести информации, обеспечивающую выполнение их целей, воспользоваться ей и защитить ее. Эти использование и защита могут осуществляться в экономической, политической и военной сферах. Знание об информации, которой владеет противник, является средством, позволяющим усилить нашу мощь и понизить мощь врага или противостоять ей, а также защитить наши ценности, включая нашу информацию.

Информационное оружие воздействует на информацию, которой владеет враг и его информационные функции. При этом наши информационные функции защищаются, что позволяет уменьшить его волю или возможности вести борьбу. Потом дадим определение

информационной войне - это любое действие по использованию, разрушению, искажению вражеской информации и ее функций; защите нашей информации против подобных действий; и использованию наших собственных военных информационных функций.

Это определение является основой для следующих утверждений.

Информационная война - это любая атака против информационной функции, независимо от применяемых средств. Бомбардировка АТС - операция информационной войны. То же самое можно сказать и про вывод из строя программного обеспечения компьютера АТС.

Информационная война - это любое действие по защите наших собственных информационных функций, независимо от применяемых средств. Укрепление и оборона здания АТС против бомбардировок - тоже часть информационной войны. То же самое можно сказать и про антивирусную программу, которая защищает программное обеспечение АТС.

Информационная война - только средство, а не конечная цель, аналогично тому как бомбардировка - средство, а не цель. Информационную войну можно использовать как средство для проведения стратегической атаки или противодействия.

Военные всегда пытались воздействовать на информацию, требующуюся врагу для эффективного управления своими силами. Обычно это делалось с помощью маневров и отвлекающих действий. Так как эти стратегии воздействовали на информацию, получаемую

врагом, косвенно путем восприятия, они атаковали информацию врага косвенно. То есть, для того чтобы хитрость была эффективной, враг должен был сделать три вещи:

наблюдать обманные действия;

посчитать обман правдой;

действовать после обмана в соответствии с целями обманывающего.

Тем не менее, современные средства выполнения информационных функций сделали информацию уязвимой к прямому доступу и манипуляции с ней. Современные технологии позволяют противнику изменить или создать информацию без предварительного получения

фактов и их интерпретации. Вот краткий список характеристик современных информационных систем, приводящим к появлению подобной уязвимости: концентрированное хранение информации, скорость доступа, повсеместная передача информации, и большие возможности информационных систем выполнять свои функции автономно. Механизмы защиты могут уменьшить, но не до нуля эту уязвимость.

Составные части информационной войны

1) психологические операции - использование информации для воздействия на аргументацию солдат врага.

2) Электронная война - не позволяет врагу получить точную информацию

3) дезинформация - предоставляет врагу ложную информацию о наших силах и намерениях

4) физическое разрушение - может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем.

5) меры безопасности - стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях.

6) прямые информационные атаки - прямое искажение информации без видимого изменения сущности, в которой она находится.

Виды информационных атак

Как ранее говорилось, существует два способа повлиять на информационные функции врага - косвенно или напрямую. Проиллюстрируем разницу между ними на примере.

Пусть нашей целью является заставить врага думать, что авиаполк находится там, где он совсем не находится, и действовать на основании этой информации таким образом, чтобы это было выгодно нам.

Косвенная информационная атака: используя инженерные средства, мы можем построить макеты самолетов и ложные аэродромные сооружения, и имитировать деятельность по работе с ними. Мы полагаемся на то, что противник будет наблюдать ложный синдром и считать его настоящим. Только тогда эта информация станет той, которую должен иметь противник по нашему мнению.

Прямая информационная атака: если мы создаем информацию о ложном авиаполке в хранилище информации у противника, то результат будет точно такой же. Но средства, задействованные для получения этого результата, будут разительно отличаться. Другим примером прямой информационной атаки может быть изменение информации во вражеской базе данных об имеющихся коммуникациях в ходе боевых действий(внесение ложной информации о том, что мосты разрушены) для изоляции отдельных вражеских частей. Этого же можно добиться бомбардировкой мостов. И в том, и в другом случае вражеские аналитики, принимая решение на основе имеющейся у них информации, примут одно и то же решение - производить переброску войск через другие коммуникации.

Какова оборонная сторона информационной войны?

Оборонительной стороной информационной войны являются меры безопасности, имеющие своей целью защитить информацию - не позволить противнику провести успешную информационную атаку на наши информационные функции. Современные меры защиты, такие как операционная безопасность и коммуникационная безопасность - типичные средства по предотвращению и обнаружению косвенных действий врага, направленных на наши военные информационные функции. Напротив, такие меры защиты, как компьютерная безопасность включают в себя действия по предотвращению, обнаружению прямых информационных действий врага и организации контрдействий.

Цели информационной войны

Существуют три цели информационной войны:

контролировать информационное пространство, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий(контринформация).

использовать контроль за информацией для ведения информационных атак на врага

повысить общую эффективность вооруженных сил с помощью повсеместного использования военных информационных функций

Приведем наглядный пример применения информационной атаки при выполнении ВВС стратегической атаки.

Предположим, что мы хотим ограничить стратегические возможности врага по переброске войск путем уменьшения запасов топлива. Сначала мы должны выявить нефтеперегонные заводы, которые будут наиболее подходящими целями при этой атаке. Потом

нужно установить, какие заводы производят больше всего топлива. Для каждого завода нам надо выявить местоположение перегонных емкостей. Мы организуем атаку и, при значительной экономии сил, выводим заводы из строя, взрывая их только перегонные емкости, и оставляя все остальное оборудование нетронутым. Это классический пример стратегической атаки.

Теперь посмотрим, как надо добиться той же цели в информационной войне. Все современные нефтеперегонные заводы имеют большие автоматизированные системы управления. Эти информационные функции являются потенциальной целью в информационной войне. На ранней стадии конфликта мы выполнили разведывательную информационную операцию по проникновению и анализу системы управления нефтеперегонным заводом. В ходе анализа мы обнаружили несколько уязвимых информационных зависимостей, дающих нам средства воздействия на работу нефтеперегонного завода в нужное нам время. Позднее, в ходе конфликта, в ходе одной из операций по блокированию вражеской группировки мы использовали одно из уязвимых мест. Мы просто остановили эти заводы. Это, тоже классический пример стратегической атаки.

Выводы

Любое оружие обладает определенной точностью попадания в цель. Точность информационного оружия - это "расстояние" между тем, что происходит на самом деле, и тем, о чем мечталось применяющей оружие системе. При чем здесь речь идет не только о дне сегодняшнем, но в первую очередь о дне завтрашнем.

Применяя информационное оружие по противнику, агрессор тем самым применяет его и по самому себе. И кто из них раньше разрушится - это не простой вопрос, не всегда имеющий однозначный ответ. Ответ во многом определяется базовой устойчивостью системы и ее способностью вовремя и адекватно реагировать на те или иные входные данные.

Структура любой системы отражает в себе знания этой системы. Информационные воздействия изменяют знания, а значит неизбежно приводят к структурным преобразованиям пораженного информацией объекта.

Критерий возможности прогнозирования повеления информационной системы должен включать в себя знания: о целях системы (желаемое будущее), ее опыте (прошлое, как набор известных системе приемов) и текущем состоянии.

Перефразируя известную пословицу к проблеме прогнозирования поведения самообучающихся систем, учитывая, что знания системы как способствуют формированию цели, так и сами определяются целью, наверное, можно утверждать: “Скажи мне, что ты знаешь, и я скажу, что с тобой будет”.

Источники информации

1. infwar. ru
2. http: // lib. ru/SECURITY/kvn/corner. txt перевод Владимира Казенова
3. http: // www. agentura. ru/equipment/psih/info/war/
4. Каландаров К. Управление общественным сознанием
5. Лисичкин, Шелепин “Третья мировая война - информиционно-психологическая”
6. Расторгуев С.П., 1999 Информационная война
7. Почепцов Г.Г. Психологические войны.М.: “Рефл-бук”, К.: “Ваклер”, 2000 г
8. Крысько В.Г. Cекреты психологической войны (цели, задачи, методы, формы, опыт). - М.: “Харвест”, 1999
9. http: // psyfactor. org/lib/zelinski-02. htm