«Мягкая сила» и «управляемый хаос» - инструменты современной мировой политики

Общеуниверситетский факультатив Института проблем безопасности
Национального исследовательского университета «Высшая школа экономики»

Профессор Бондаренко А.В.

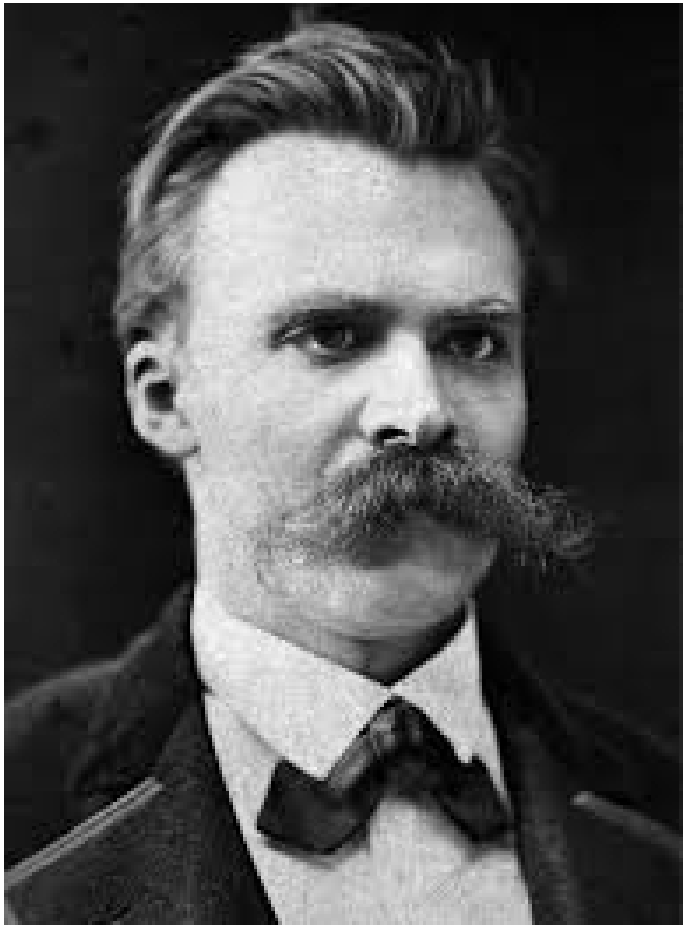
Информационные войны

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 возможной теоретическую возможность — прямое манипулирование информацией противника.

Информационная эра



В каком диковинном упрощении и фальши живет человек! Невозможно вдосталь надивиться, если когда-нибудь откроются глаза, на это чудо! каким светлым, и свободным и легким, и простым сделали мы все вокруг себя! - как сумели мы дать своим чувствам свободный доступ ко всему поверхностному, своему мышлению - божественную страсть к резвым скачкам и ложным заключениям! - Как ухитрились мы с самого начала сохранить свое неведение, чтобы наслаждаться едва постижимой свободой, несомненностью, неосторожностью, неустрашимостью, веселостью жизни, - чтобы наслаждаться жизнью!

Фридрих Ницше

Любой конфликт между людьми в первую очередь информационный. Информация необходима людям для принятия любых решений. Она не только позволяет совершать оптимальные действия в конфликте, но и управляет самой целенаправленной деятельностью, смыслом существования и гибели систем. Информация – необходимый ресурс деятельности человека, отделяющий его от остального мира. Выделить его как специфический «ресурс» нападения и защиты пытались давно, но только сравнительно недавно начали появляться теории, которые могут быть положены в основу методологии (технологий?) ведения информационных войн.

Каковы 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.

Информационная война: определение

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.

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: определение

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

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

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.

Информационная война: определение

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.

Информационно-психологическая война

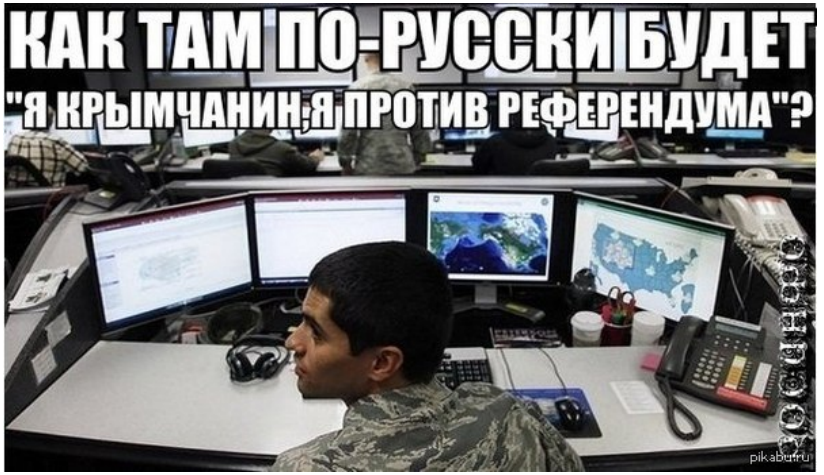
Информационная война (англ. Information war) — термин, имеющий два значения: Воздействие на гражданское население и (или) военнослужащих другого государства путём распространения определённой информации.
Термин «информационно-психологическая война» был заимствован в русский язык из словаря военных кругов США.

Перевод этого термина («information and psychological warfare») с английского языка может звучать и как «информационное противоборство», и как «информационная, психологическая война», в зависимости от контекста конкретного официального документа или научной публикации (Манойло А.В.).

В этом смысле также используется термин психологическая война — психологическое воздействие на гражданское население и (или) военнослужащих другого государства с целью достижения политических или чисто военных целей.

Целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем.

Элементы 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 аэродром и считать его настоящим. Только тогда эта информация станет той, которую должен иметь противник по нашему мнению.

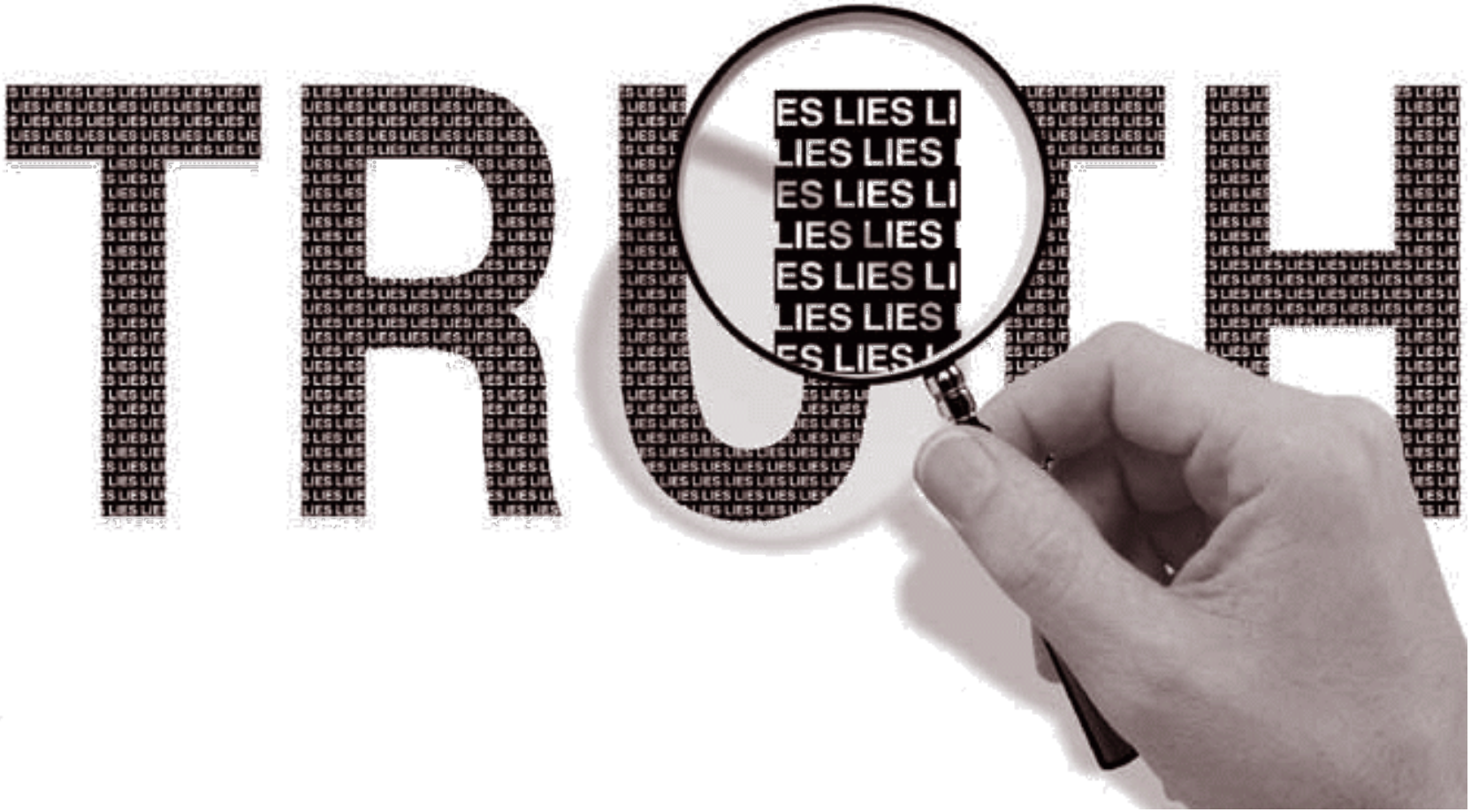
Прямая информационная атака: если мы создаем информацию о ложном авиаполке в хранилище информации у противника, то результат будет точно такой же. Но средства, задействованные для получения этого результата, будут разительно отличаться.

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

Основные черты информационных войн

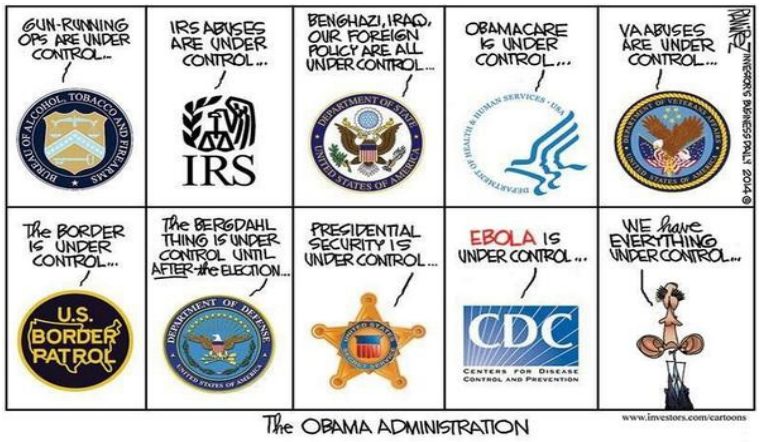
ИНСТРУМЕНТЫ: В информационной войне не задействуются психоактивные вещества, прямой шантаж и запугивание (это характерно для терроризма), подкуп, физическое воздействие и т. п. Хотя указанные воздействия могут применяться параллельно с информационной войной, они не являются обязательным элементом.
ОБЪЕКТЫ: Объектом является как массовое сознание, так и индивидуальное. Индивидуального воздействия «удостаиваются» лица, от решения которых зависит принятие решений по интересующим противоборствующую сторону вопросам (президент, премьер-министр, глава МИД, диппредставители, главы воинских формирований и т. п.).
МЕТОДЫ: Можно сказать, что методы информационной войны воздействуют на массовое сознание аналогично тому, как методы психотерапии воздействуют на сознание индивидуальное.
АНТУРАЖ: Информационное воздействие может осуществляться как на фоне информационного шума, так и в условиях информационного вакуума.
СПЕЦИФИКА: Навязывание чуждых целей — это то, что делает информационную войну войной и отличает её от обычной рекламы.
СРЕДСТВА: Средствами ведения информационной войны являются любые средства передачи информации — от СМИ до почты и сплетен.
СУЩНОСТЬ: Информационное воздействие содержит искажение фактов или навязывает подвергающимся ему эмоциональное восприятие, выгодное воздействующей стороне.

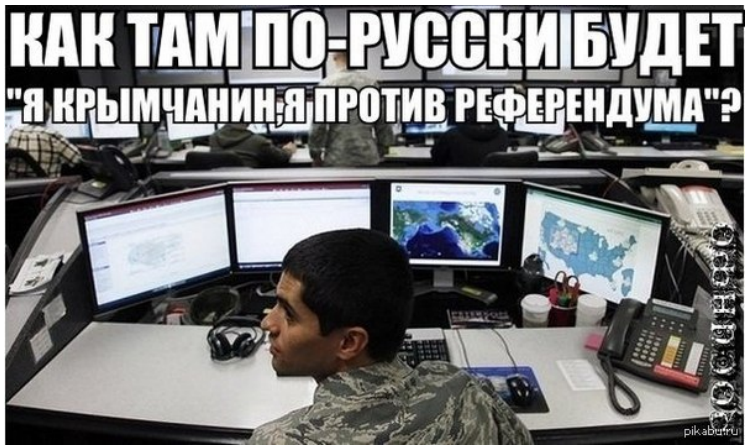
Информационная война, *или* Похвальное слово *Лжи*



Информационная война, *или* Похвальное слово *Лжи*

Информационная война, *или* Похвальное слово *Лжи*

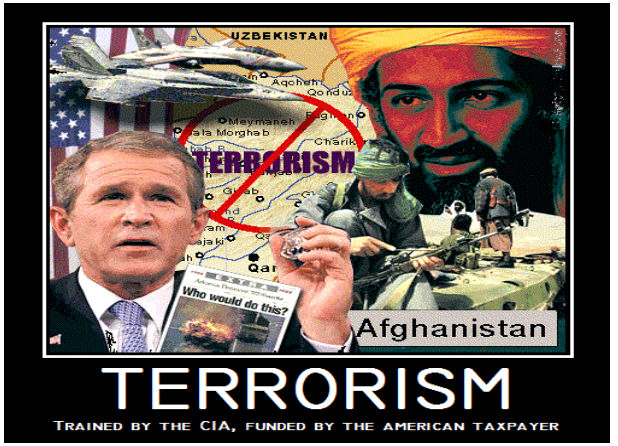




Информационная война, *или* Похвальное слово *Лжи*

Информационная война, *или* Похвальное слово *Лжи*

Информационная война, *или* Похвальное слово Лжи



Евромайдан и Украинский кризис 2014: Война в эфире

Проукраинская сторона использовала в СМИ «лексику ненависти» — «колорады», «ватники», «титушки», «террористы» — для очернения своих пророссийских оппонентов. Россия парировала акцентом на бандеровской символике евромайдановцев и «нацистской сути» новой власти в Киеве, а также на олигархическом характере новой власти. В отношении сторонников майдана, независимо от их этнической принадлежности, стали употребляться слова «укры», «укропы», «майдауны», «каратели» и другие.

Вторым моментом информационной войны стали «фейки» или ложные заявления («утки», «вбросы») о причастности оппонентов к тому или иному инциденту. Ярким фейком считается заявление украинских СМИ о причастности сепаратистов к ракетному обстрелу Луганска 2 июня 2014 года. Более ранним примером фейка считается информация о снайперах, которые расстреливали протестующих якобы по приказу Януковича. Отличием фейка от вброса является наличие визуального материала в виде фотографии или видеоролика, снятого по другому поводу.

Также украинские СМИ подчеркивали миф об успехах украинской армии и безоговорочной поддержке новых властей на востоке Украины.

Украинские СМИ в свою очередь обвиняют российские СМИ в тенденциозности, лжи и подтасовках фактах во время выпусков новостей, в ходе которых сообщается непроверенная информация с ссылкой на неназванные источники в государственных органах (вброс) или на пристрастных очевидцев событий (слух). В результате вещание ряда каналов было запрещено на территории Украины. В России в аналогичной практике обвинили западные СМИ за их преждевременные обвинения до завершения следствия по делу о сбитом малазийском Боинге. Часто в информационных вбросах с украинской стороны обвинялся Дмитрий Тымчук. Его российским аналогом (по версии украинской стороны) стал Дмитрий Киселев. В информационной войне за Украину участвовала и британская газета Independent (журналист Margareta Pagano), сообщив 31 июля с ссылкой на "источники" (sources) о планах по свержению Путина и возвращения Крыма Украине. Также в августе британские журналисты (Guardian, Telegraph) сообщали о вторжениях русских войск на территорию Украины.

Российские СМИ также обвиняли своих оппонентов в постановочных фото (Глеб Гаранич), рассчитанных на максимальный эмоциональный ответ аудитории

СРАВНИТЕЛЬНЫЕ ХАРАКТЕРИСТИКИ ТРАДИЦИОННЫХ И ИНФОРМАЦИОННЫХ ВОЙН

Информационные войны

Обычные войны

Методологический
(мировоззрение, методология, культура мышления, концепция и полнота управленческой деятельности)

Хронологический
(история и хронология, направленность течения процессов)

Фактологический
(описание частных процессов и их взаимосвязей, вероучения, идеологии, технологии, фактология наук)

Экономический
(деньги и все экономические процессы)

Генное оружие
(алкоголь, табак, другие наркотики, некоторые виды пищи и медикаментов, экологические загрязнители)
сюда же можно отнести терроризм и угрозу применения ядерного оружия

Военное оружие
(оружие в традиционном понимании этого слова, уничтожающее и калечащее людей, объекты техносферы, памятники культуры)

Быстродействие

Мощность (в смысле необратимости результатов)

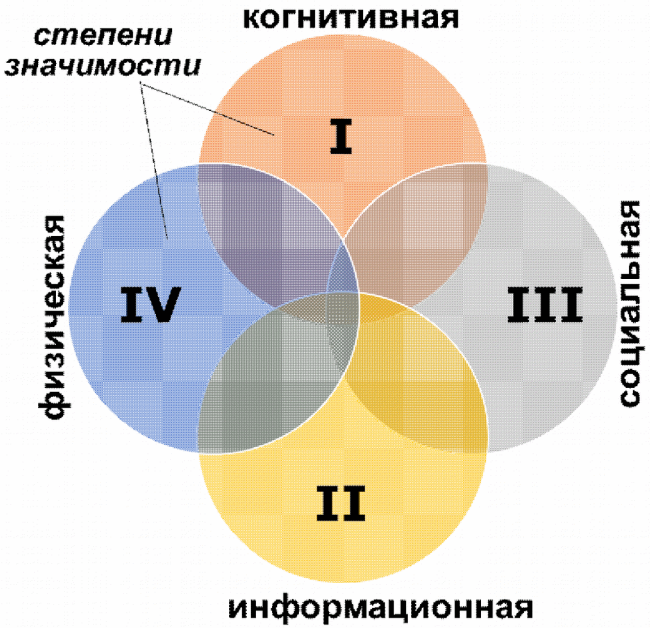
СЕТЕЦЕНТРИЧЕСКИЕ ВОЙНЫ

СЕТЕЦЕНТРИЧЕСКИЕ ВОЙНЫ

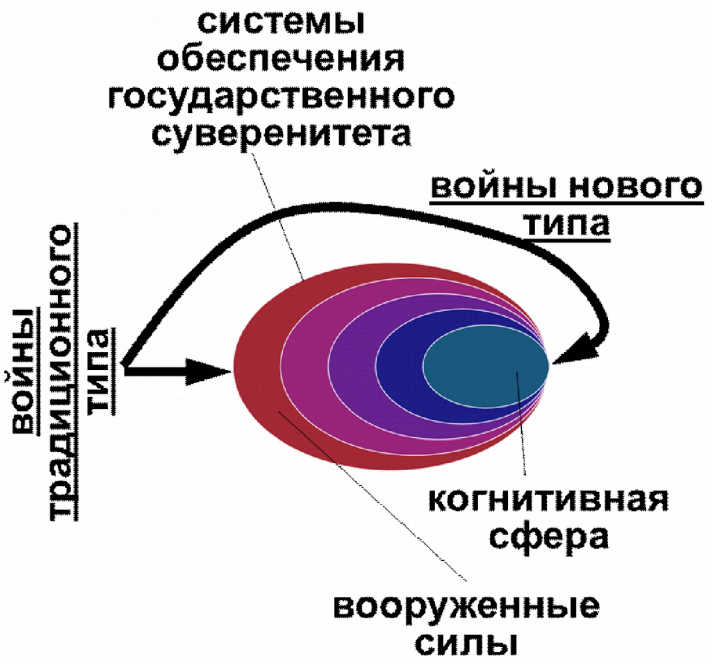
СЕТЕЦЕНТРИЧЕСКИЕ ВОЙНЫ

СЕТЕЦЕНТРИЧЕСКИЕ ВОЙНЫ

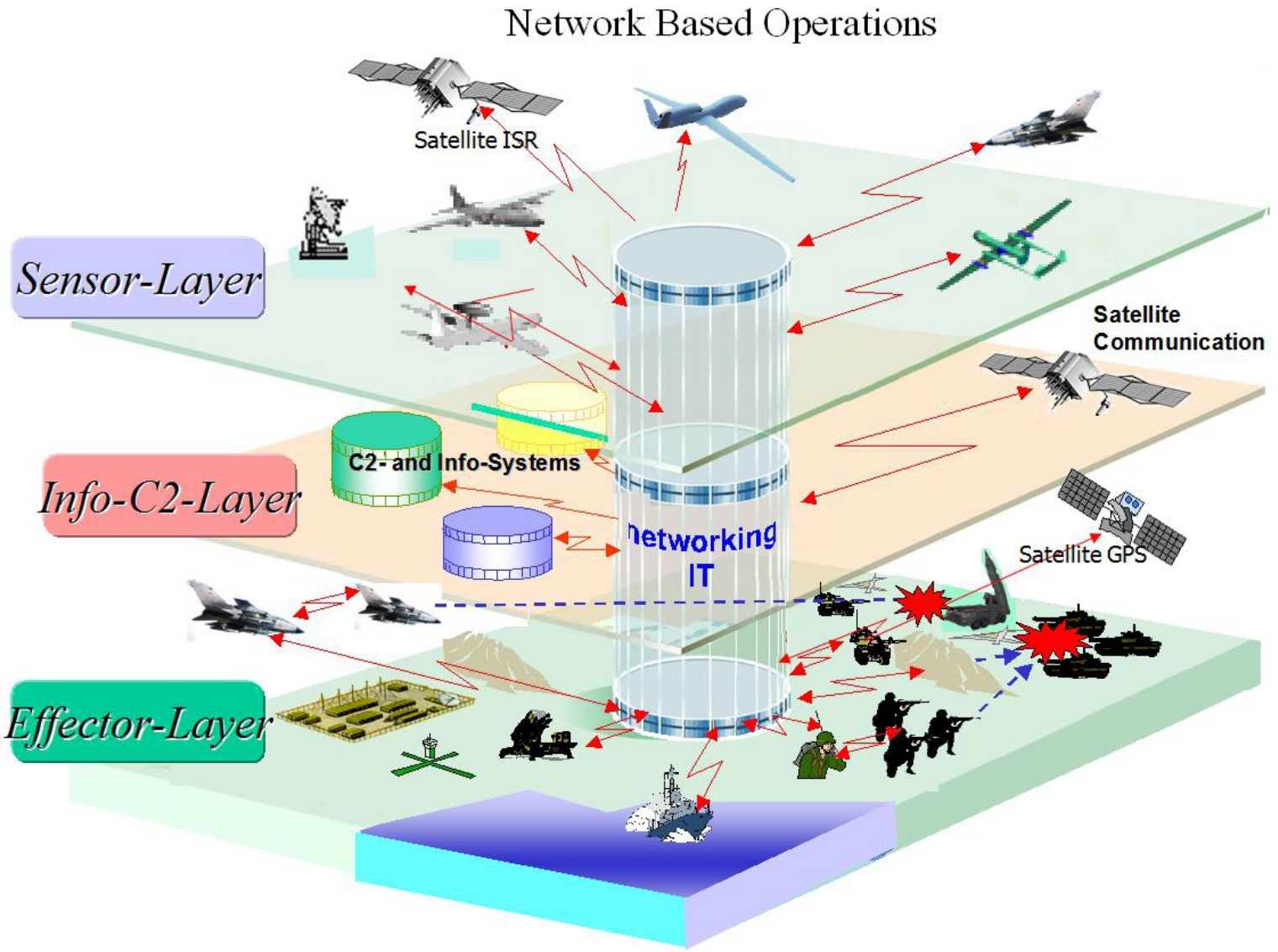
Области сетецентричной войны



Системы обеспечения государственного суверенитета и войны нового типа



СЕТЕЦЕНТРИЧЕСКИЕ ВОЙНЫ



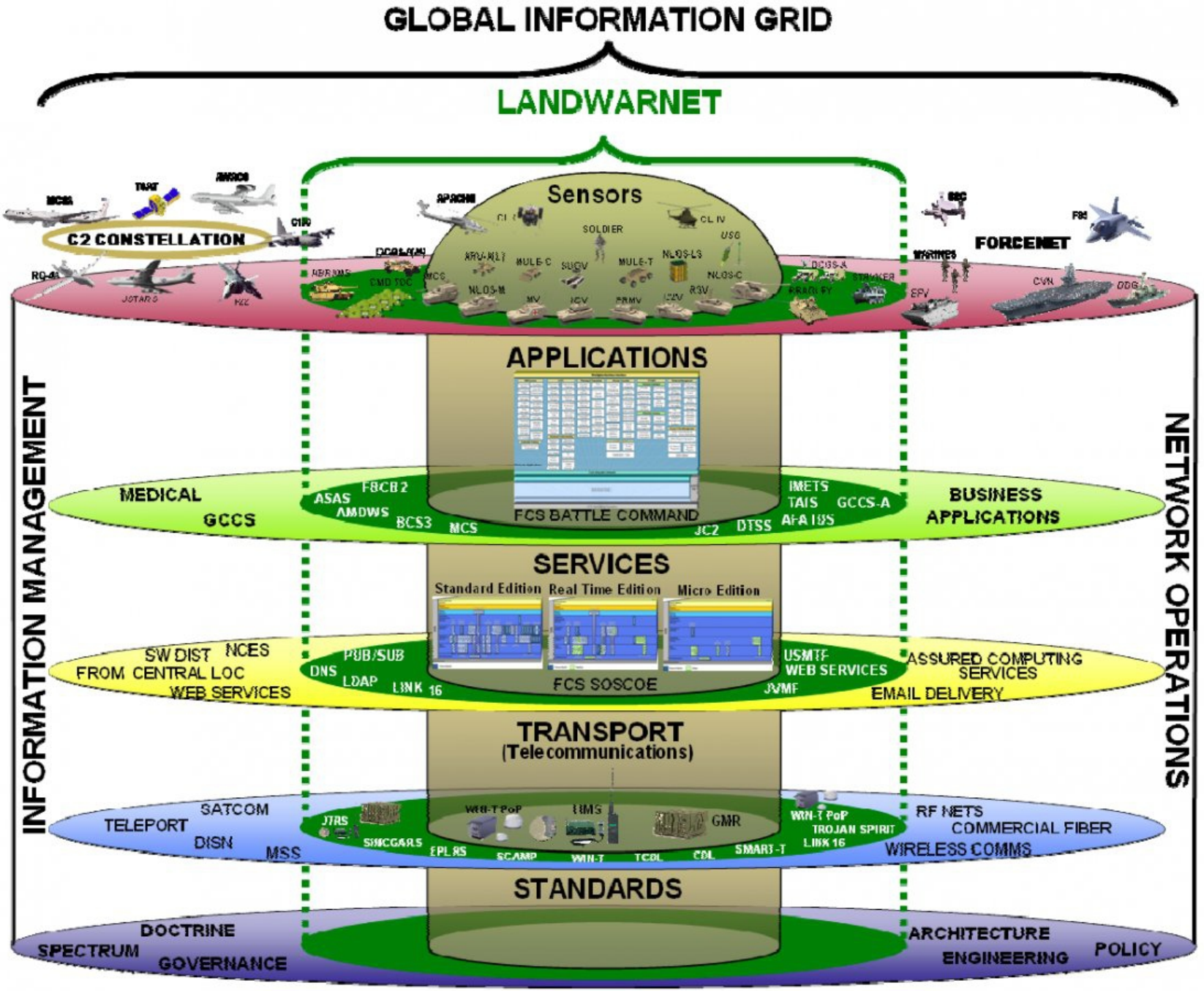
Кибернетическая война

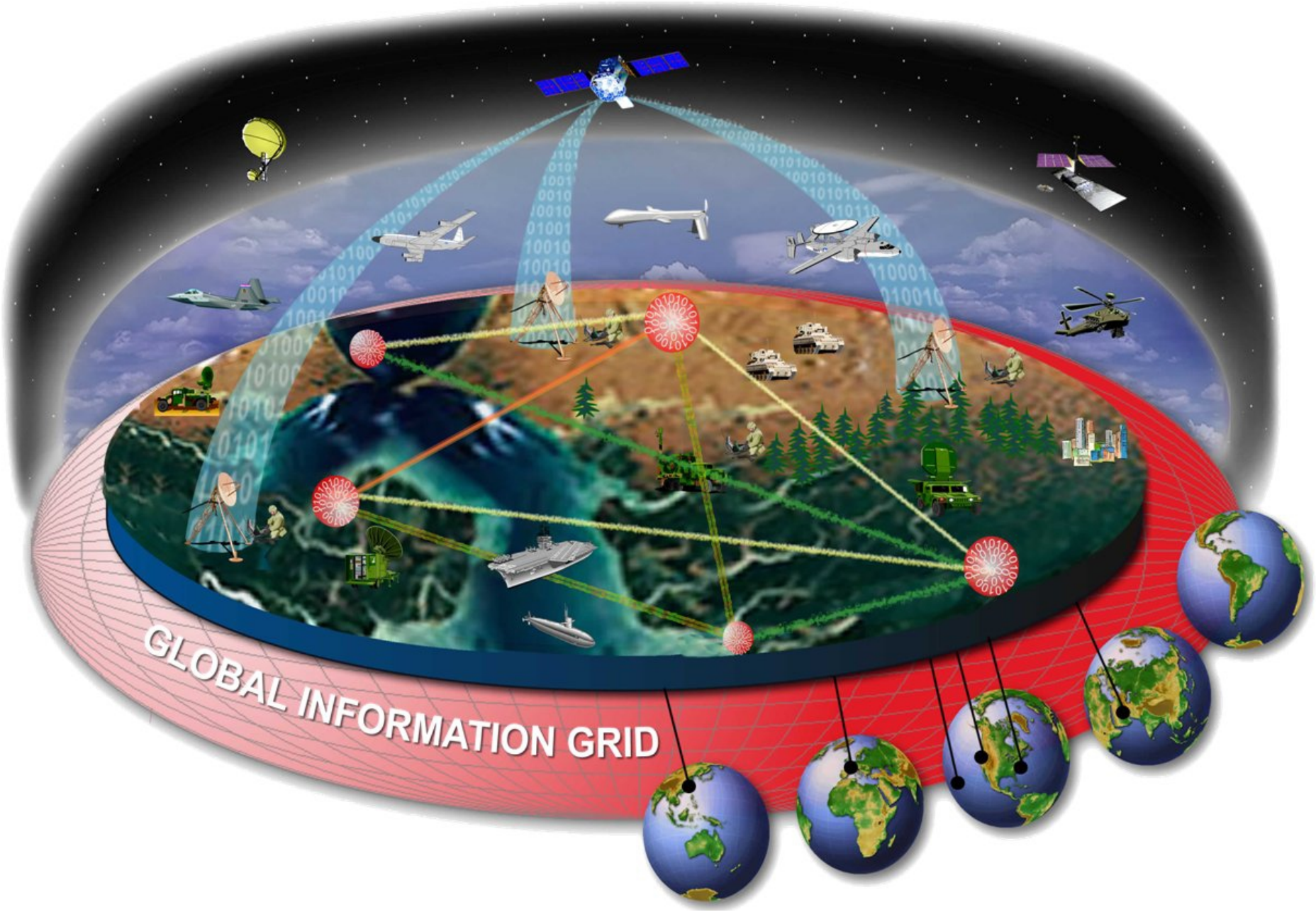
Кибервойна (англ. Cyber-warfare) — компьютерное противостояние в пространстве Интернета. Направлена прежде всего на дестабилизацию компьютерных систем и доступа к интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран, которые полагаются на интернет в повседневной жизни. Межгосударственные отношения и политическое противостояние часто находит продолжение в интернете в виде кибервойны: вандализме, пропаганде, шпионаже и непосредственных атаках на компьютерные системы и серверы.

Одно из определений термина звучит так: «„кибервойна“ — использование Интернета и связанных с ним технологических и информационных средств одним государством с целью причинения вреда военной, технологической, экономической, политической и информационной безопасности и суверенитету другого государства». Как писал эксперт по безопасности правительства США Ричард Кларк в своей книге «Кибервойна» (англ. CyberWarfare) (вышла в мае 2010 года) «кибервойна — действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения».

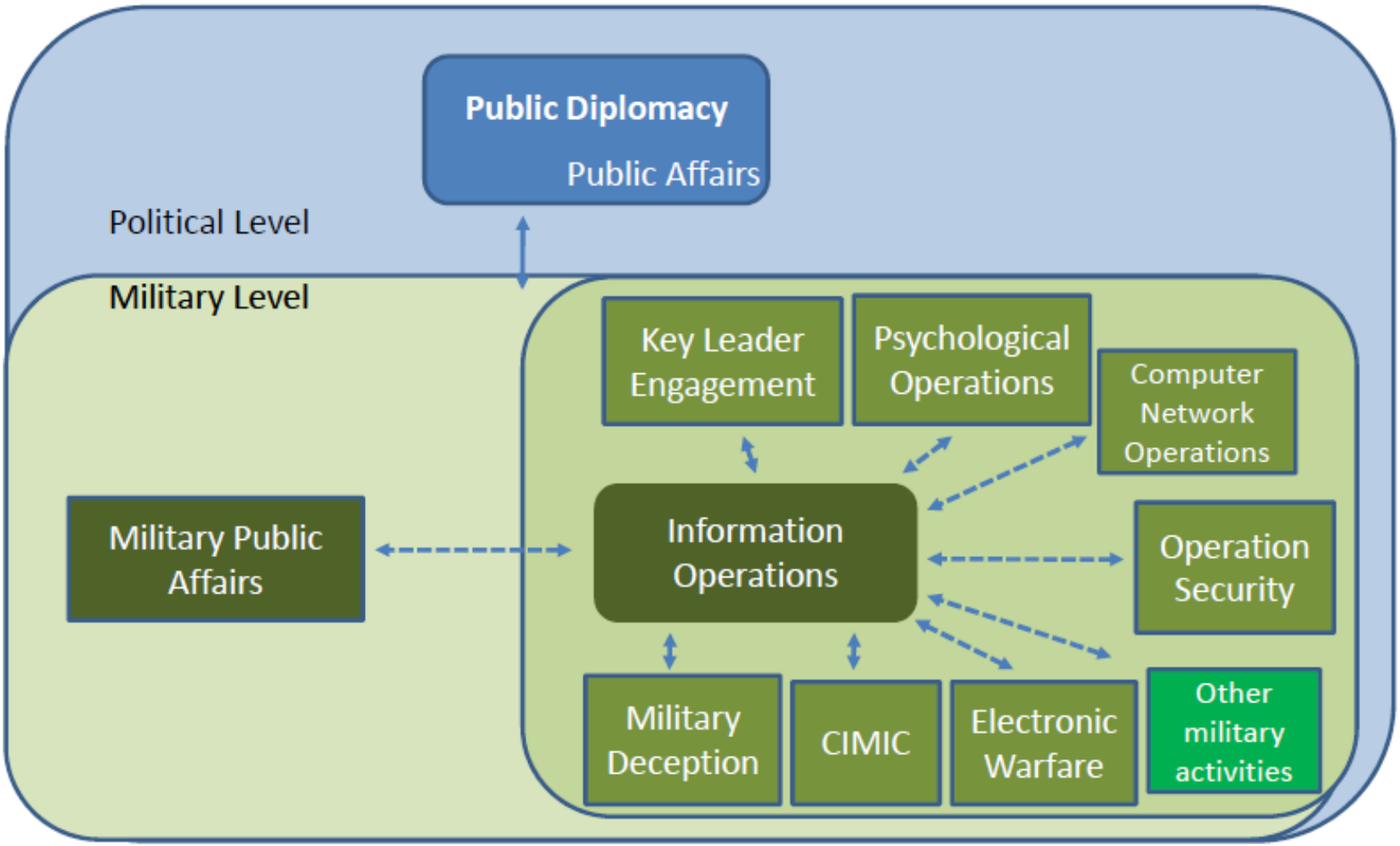
Американский журнал The Economist описывает кибервойну как «пятую область войны, после земли, моря, воздуха и космоса». О важности готовности к ведению военных действий в киберпространстве свидетельствует факт создания в США целого воинского подразделения — киберкомандования США.

КИБЕРВОЙСКА

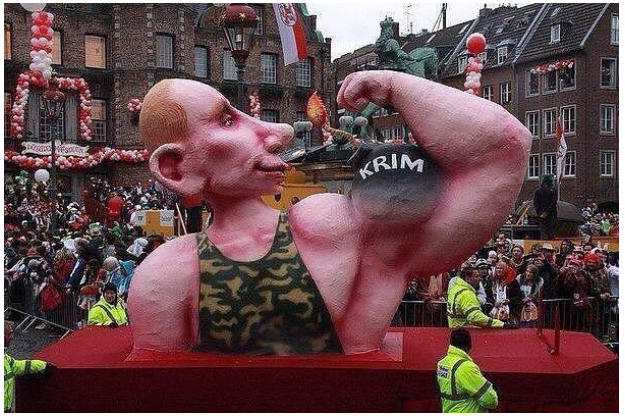

GLOBAL INFORMATION GRID
LANDWARNET
C2 CONSTELLATION
Sensors
FORCENET
APPLICATIONS
FCS BATTLE COMMAND
MEDICAL
GCCS
F6CB2
ASAS
AMDWS
BCS3
MCS
IMETS
TAIS
GCCS-A
AFATDS
JC2
DTSS
BUSINESS APPLICATIONS
SERVICES
Standard Edition
Real Time Edition
Micro Edition
FCS SOSCOE
SW DIST
NCES
FROM CENTRAL LOC
WEB SERVICES
PUB/SUB
DNS
LDAP
LINK 16
USMTF
WEB SERVICES
JMMF
ASSURED COMPUTING SERVICES
EMAIL DELIVERY
TRANSPORT
(Telecommunications)
SATCOM
TELEPORT
DISN
MSS
JTRS
SINCGARS
EPLRS
WIN-T PoP
SCAMP
WIN-T
TCDL
UMS
GMR
CDL
SMART-T
WIN-T PoP
TROJAN SPIRIT
LINK 16
RF NETS
COMMERCIAL FIBER
WIRELESS COMMS
STANDARDS
DOCTRINE
SPECTRUM
GOVERNANCE
ARCHITECTURE
ENGINEERING
POLICY
INFORMATION MANAGEMENT
NETWORK OPERATIONS


GLOBAL INFORMATION GRID

How StratCom Interacts



ИМИДЖЕВЫЕ ВОЙНЫ



ИМИДЖЕВЫЕ ВОЙНЫ

ИМИДЖЕВЫЕ ВОЙНЫ

ИНФОРМАЦИОННАЯ ВОЙНА: ЦИВИЛИЗАЦИОННЫЙ ВЫБОР

Методы ведения информационных войн

Как правило, методами информационной войны является вброс дезинформации, или представление информации в выгодном для себя ключе. Данные методы позволяют изменять оценку происходящего населением территории противника, развивать пораженческое настроение, и, в перспективе, обеспечить переход на сторону ведущего информационное воздействие. В качестве примера можно привести «прелестные письма», в которых Степан Разин призывал всех ищущих воли на свою сторону, выдавая себя за восстановителя справедливости, борца с предавшей царя местной властью. С появлением средств массовой информации и общим повышением уровня грамотности в XX веке ведение информационной войны стало более эффективным. Ярким примером изменения общественного сознания является деятельность Йозефа Геббельса, рейхсминистра народного просвещения и пропаганды.

Методы ведения информационных войн

Колорадский Жук - Своё название жук получил в 1859 году после того, как опустошил картофельные поля в штате Колорадо США.

Продвигаясь на восток по ходу преобладающих в летние месяцы ветров, к концу 1940-х годов жук достиг границ СССР. Первые его очаги на территории СССР были обнаружены во Львовской области Украины в 1949 году

Кто после этого колорады ?
http://ru.wikipedia.org/wiki/Колорадский_жук

Методы ведения информационных войн

Информационная война также шла во время грузино-осетинского конфликта в августе 2008 года.

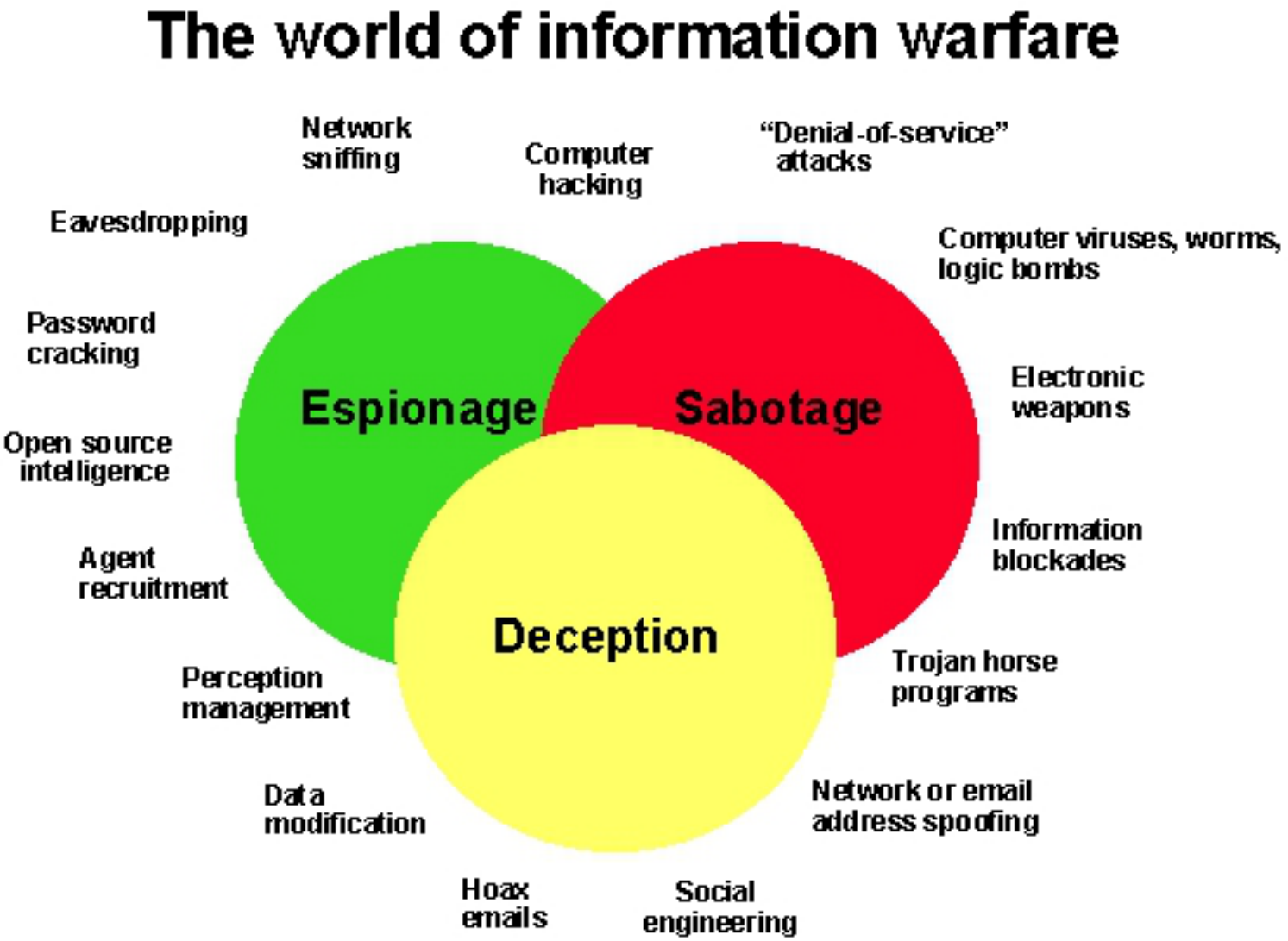
Так Михаил Саакашвили поначалу заявлял:

«На нашу территорию вторглись более 80 тысяч солдат, было введено более трех тысяч единиц бронетехники и ещё около тысячи бронемашин стояло у наших границ. Наши территории бомбили несколько десятков, а может, и сотен самолетов, которые совершили более 200 боевых вылетов. Реально это была попытка искоренения и уничтожения нашего народа».

— Михаил Саакашвили

Это не соответствовало действительности: Южная Осетия — 3 тыс. личного состава и не меньше 20 танков и 25 САУ, Абхазия — 5 тыс. личного состава, контингент России — 15 тыс. личного состава.

Методы ведения информационных войн



Методология войн нового типа

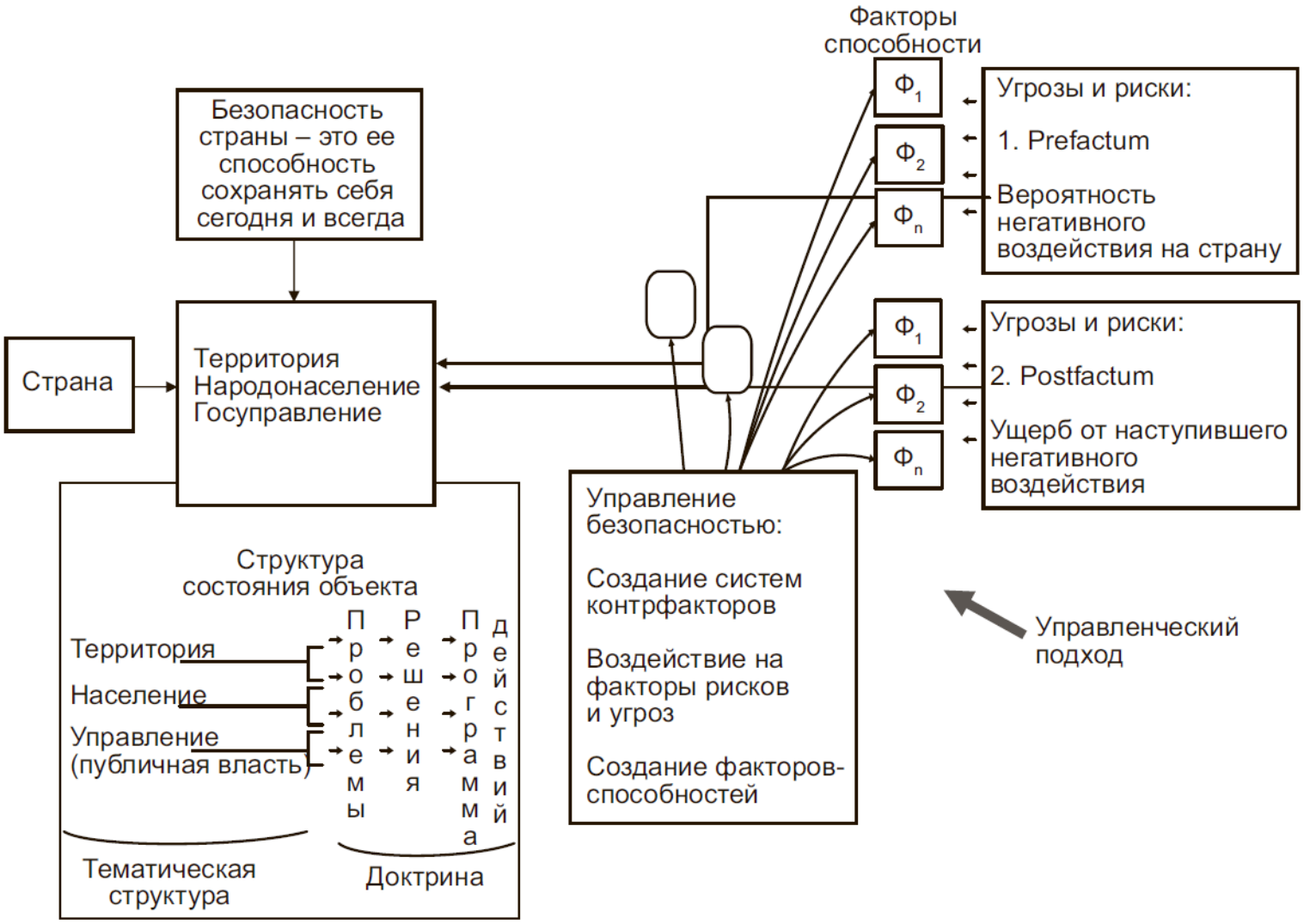


Рис. 1. Функциональное и системообразующее пространство безопасности страны

Методология войн нового типа

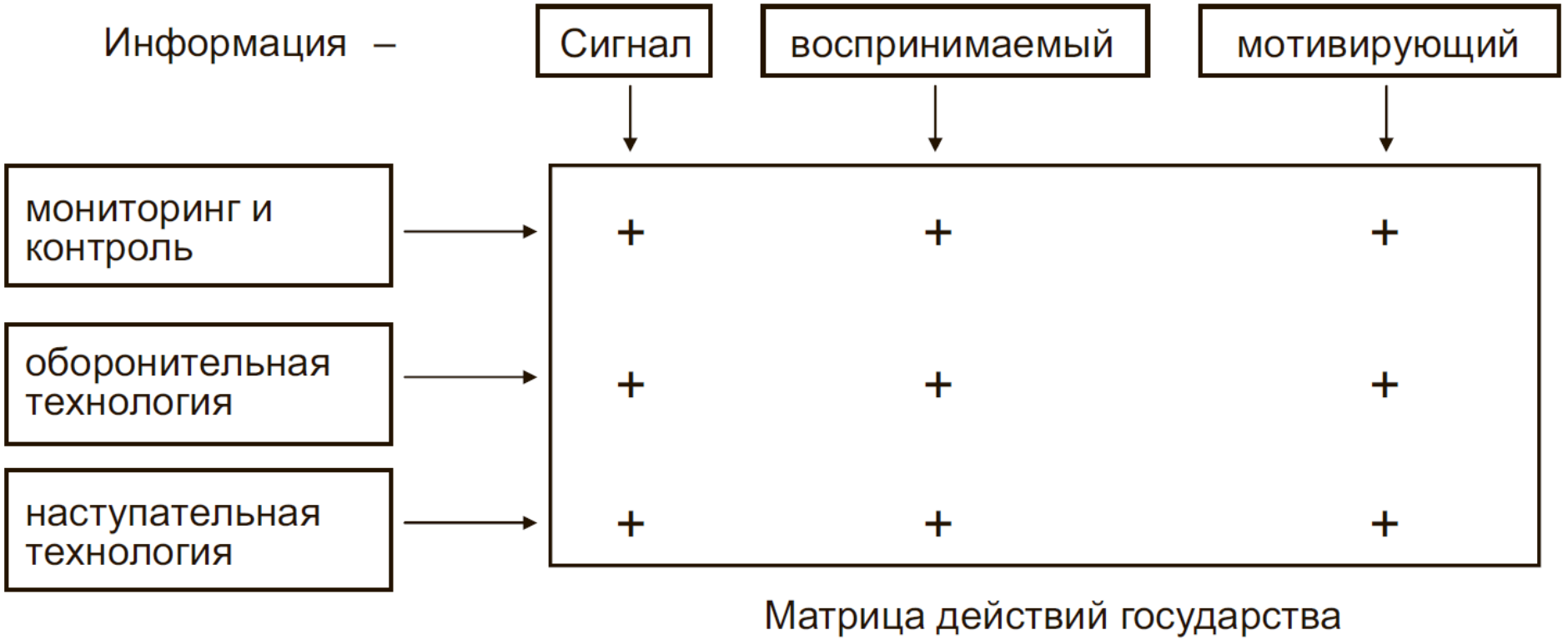


Рис. 2. Структура информационного воздействия

Методология войн нового типа

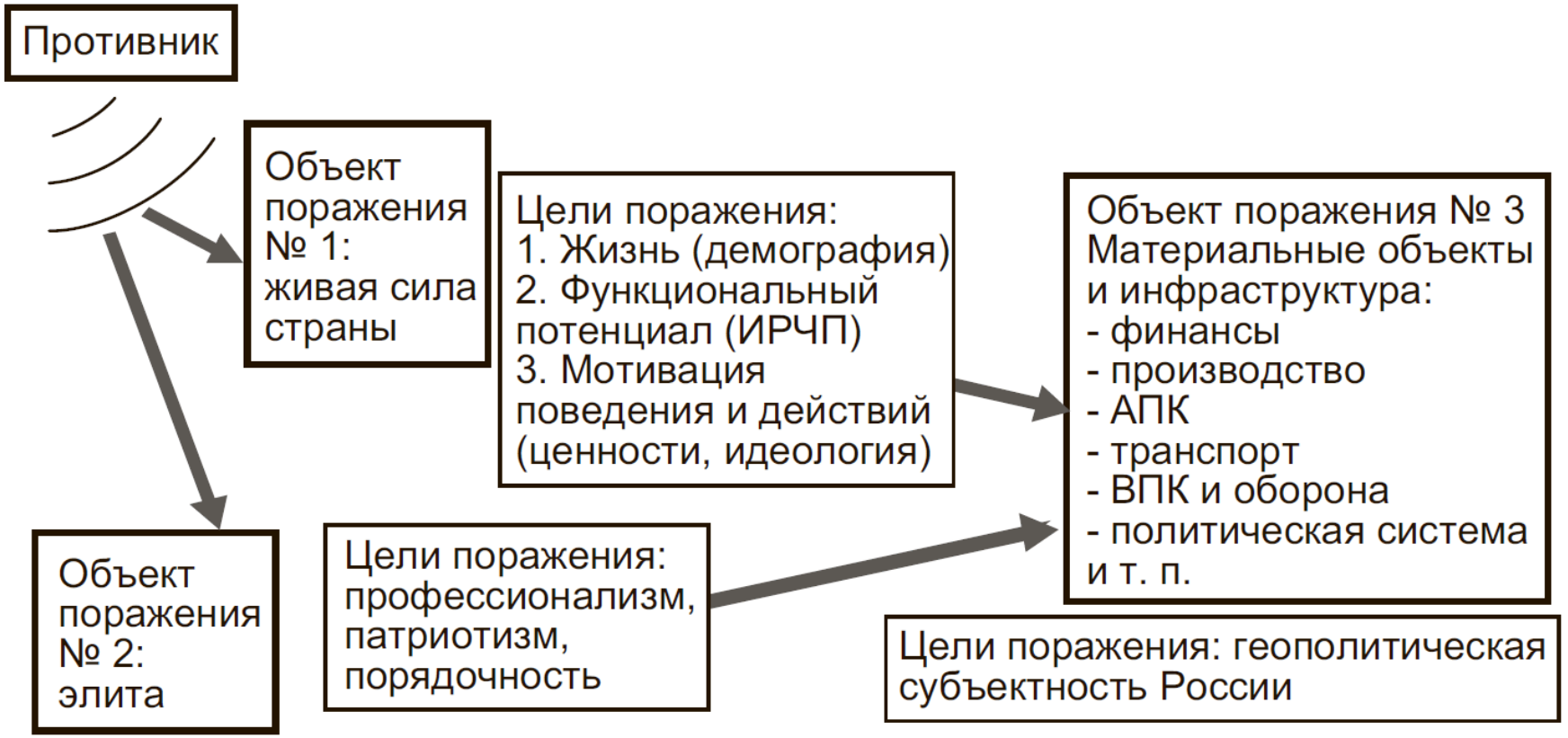


Рис. 3. Объекты информационного поражения

АКТОРЫ ИНФОРМАЦИОННЫХ ВОЙН

Место и роль средств массовой информации в войне нового типа

Место и роль средств массовой информации в войне нового типа

ИНФОРМАЦИОННЫЕ ВОЙНЫ: ГЕОЭКОНОМИКА (РЕЛИЗ – 2.0.)

АКТИВНАЯ КОНТРПРОПАГАНДА

АКТИВНАЯ КОНТРПРОПАГАНДА

АКТИВНАЯ КОНТРПРОПАГАНДА

АКТИВНАЯ КОНТРПРОПАГАНДА

АКТИВНАЯ КОНТРПРОПАГАНДА

АКТИВНАЯ КОНТРПРОПАГАНДА

Как не стать жертвой информационной войны?

- **ЕСТЬ ТОЛЬКО ОДНО ИДЕАЛЬНОЕ ПРОТИВОЯДИЕ — почти полностью изолировать себя от СМИ. Но в постиндустриальном обществе это возможно только в том случае, если вы станете отшельником. Тем, кто не готов к такой радикальной мере, пригодятся несколько советов, которые позволят сгладить влияние дезинформации и пропаганды до минимума:**

- **Старайтесь читать, а не слушать или смотреть. Когда человек читает, он мыслит критичнее, и его не так просто ввести в заблуждение.**

- **Помните приёмы манипулирования и подмечайте их в жизни. Как говорилось выше, если вы обнаружили манипулирование, то оно уже не сработало на вас.**

- **Не доверяйте безусловно ни одному источнику. Если вы избежали пропаганды одной стороны, это не значит, что вы не станете жертвой пропаганды другой стороны: во время войны врут все.**

- **ТАКЖЕ ПОМНИТЕ, ЧТО ИНФОРМАЦИОННЫЕ ВОЙНЫ ВЕДУТСЯ ПОЭТАПНО. Поддерживать высокий градус напряжения долго не получается, а потому в самые напряжённые моменты войн разумно устраивать себе информационную диету. Например, уехать в отпуск или засесть за какой-нибудь сериал или книгу.**

Рекомендуемая литература

- Манойло А.В. Информационно-психологическая война: факторы, определяющие формат современного вооружённого конфликта http://psyfactor.org/lib/psywar35.htm.
- Манойло А.В., Петренко А.И., Фролов Д.Б. Государственная информационная политика в условиях информационно-психологической войны. 3-е изд. М.: Горячая линия - Телеком, 2012.
- Расторгуев С.П. Информационная война http://evartist.narod.ru/text4/54.htm.
- Волкогонов Д.А. Психологическая война: Подрывные действия империализма в области общественного сознания. М. Воениздат, 1983.
- Завадский И.И. «Информационная война – что это такое?»//Защита информации. «Конфидент». №4, 1996.
- Власенко И.С., Кирьянов М.В. Информационная война: искажение реальности. М.: ИД «Канцлер», 2011.
- Воронцова Л.В., Фролов Д.Б. История и современность информационного противоборства. М.: Горячая линия - Телеком, 2006.
- Гриняев С.Н. Поле битвы — киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. Мн.: Харвест, 2004.
- Лисичкин В. А., Шелепин Л. А. Третья мировая информационно-психологическая война. М.: Академия социальных наук, 1999.
- Панарин И. Н. Информационная война, PR и мировая политика. М.: Горячая линия - Телеком, 2006.
- Панарин И. Н. Технология информационной войны. М.: Издательство «КСП+», 2003.