ПИР-Центр
Центр политических исследований России

Совместные операции в киберпространстве система кибероборонны: подход Киберкомандования ВС США

Координатор программы ПИР-Центра
Олег Демидов

РусКрипто-2013
Московская область,
28.03.2013

конференция
РусКрипто'2013

http://www.ruscrypto.ru/conference/

ПИР-ЦЕНТР
Центр политических исследований России

Институционализация стратегической кибероборонны: выборочные примеры

Олег Демидов
РусКрипто-2013
28.03.2013

США

- 1991 г.: «Буря в пустыне»: триумф *Smart Weapons*
- 1993 г.: Центр информационных боевых действий ВВС США
- 1998 г.: «Объединенная доктрина информационных операций»
- 2007 г.: Киберкомандование ВВС США (*Air Force Cyber Command*)
  «Оборона означает поражение!»
  2009 г.: Киберкомандование США (U.S. Cybercommand)
- 2014-2015 гг.: Объединенное Киберкомандование США (?)

НАТО

2007 г.: Кибератаки на Эстонию – первая дискуссия о возможности применения Статьи V Устава НАТО
2008 г.: Учреждение CCD COE в Таллинне
2010 г.: Приоритет киберугроз в новой Стратегической концепции НАТО
2013 г.: Таллиннский мануал: попытка системной норм МГП к киберпространству

Операции в кибер-пространстве

Китай

1991 г.: «Буря в пустыне»: шок от потенциала *Smart Weapons* США
1999 г.: концепция информационной войны
2011 г.: *Blue Team* и другие подразделения
2013 г.: Белый дом прямо обвиняет Пекин в массированных кибератаках (Unit 61398)

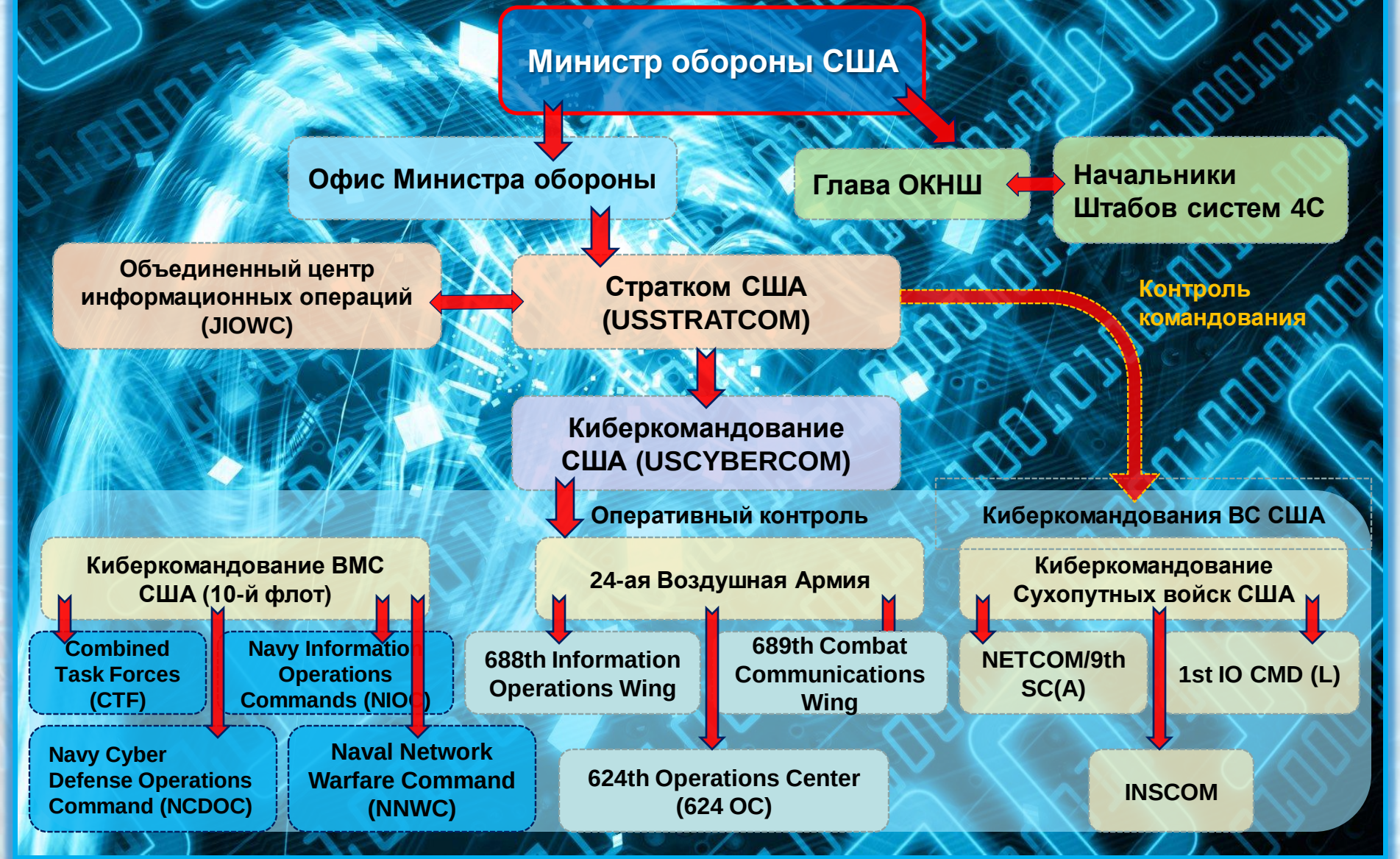
Россия

- Январь 2012 г.: «Концептуальные взгляды…» Минобороны РФ
- 15 января 2013 г.: Указ 31с - создание системы предупреждения и защиты от кибератак возложено на ФСБ РФ
- 2013 г.: Создание аналога Киберкомандования ВС США
- Конкуренция между Минобороны и спецслужбами (ФСТЭК, ФСБ) (?)

ПИР-ЦЕНТР
Центр политических исследований России

Структура Киберкомандования ВС США

Олег Демидов
РусКрипто-2013
28.03.2013



ПИР-ЦЕНТР
Центр политических исследований России

Роль и функции Киберкомандования ВС США

Олег Демидов
РусКрипто-2013
28.03.2013

Киберкомандование США (US CYBERCOM)

Рабочая структура в составе Стратегического командования США по осуществлению операций в киберпространстве, включая наступательные операции. Подчиняется Страткому в качестве координационного центра операций ВС США в киберпространстве, осуществляет делегированный Страткомом оперативный и тактический контроль над отведенными в его подчинение силами

Объединённый оперативный центр (Joint Operations Center, JOC)

Координирует, синхронизирует и осуществляет операции в киберпространстве, включая: (а) отслеживание состояния и статуса сетей, (б) поиск уязвимостей и выявления враждебной активности, (в) распространение приказов, (г) выработку ответных контрмер, (д) координирует взаимодействия с внешними структурами и организациями

Объединенный Центр кибероперaций (Joint Cyber Center, JCC)

Служит связующим звеном для структур и деятельности Боевых командований. При поддержке Киберкомандования обеспечивает персонал/либо компонент планирования и контроля над оборонительными операциями в киберпространстве (DCO), операциям в GIG Минобороны, а также наступательным операциям в киберпространстве (OCO)

ПИР-ЦЕНТР
Центр политических исследований России

Концептуальное видение киберпространства: определения

Олег Демидов
РусКрипто-2013
28.03.2013

Ключевые понятия

Cyberspace

«Глобальное пространство в пределах информационной среды, состоящее из взаимозависимой сети инфраструктур информационных технологий, в том числе Интернета, сетей связи, компьютерных систем, встроенных процессоров и контроллеров» (CJCS CM-0363-08)

Cyberspace Operations

«Использование киберпотенциала, в первую очередь для достижения целей в киберпространстве либо посредством киберпространства. К таким операциям относятся операции в компьютерных сетях, а также деятельность по управлению и обеспечению безопасности GIG» (JP03)

Situational Awareness

«Полная ситуационная осведомленность в отношении GIG достигается за единства процессов, стандартов и технического оборудования, делая возможным управление практически в режиме реального времени любым активом с целью оптимизации сетецентричных Сервисов»
(The Joint CONOPS for GIG NetOps)

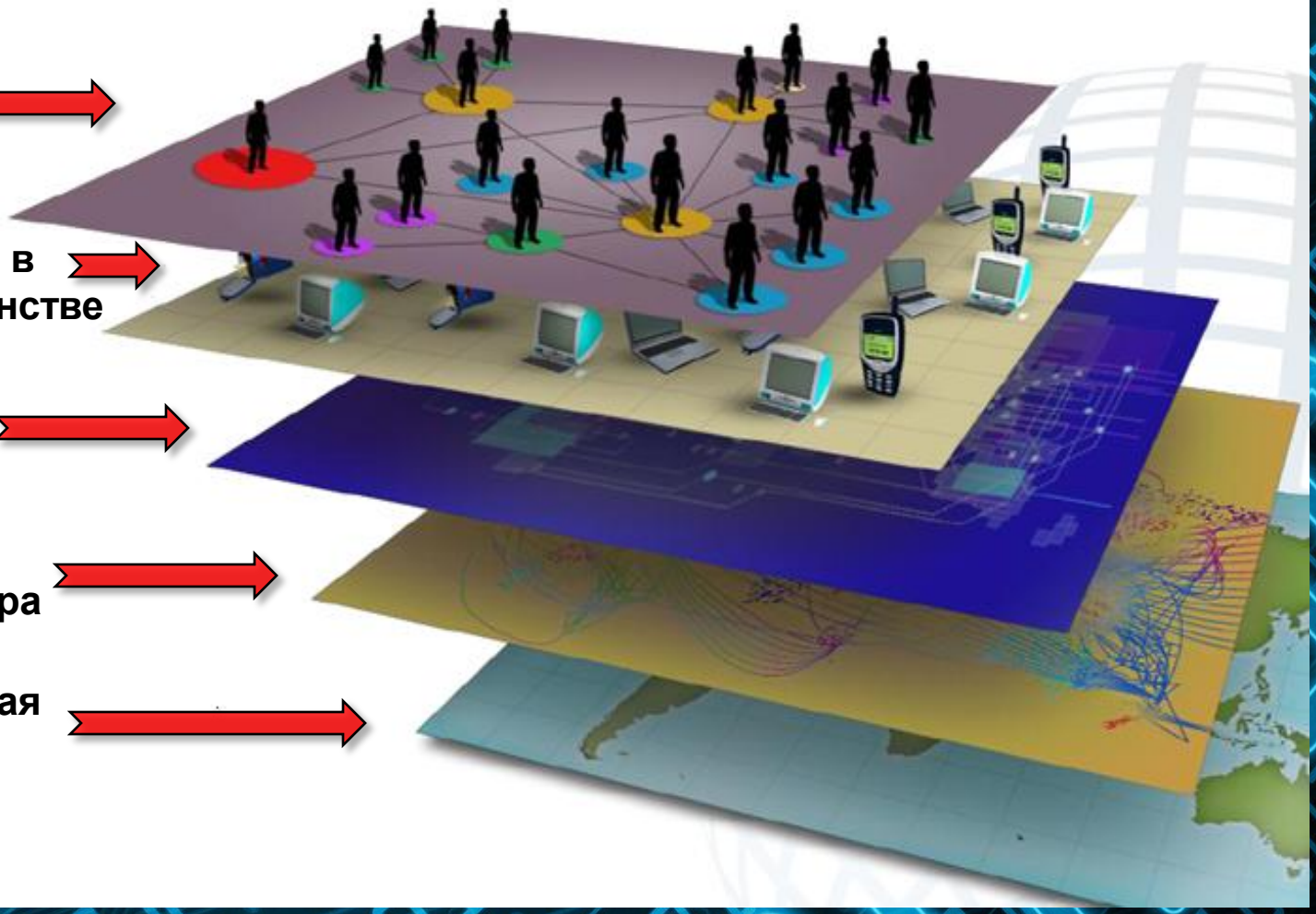
Situational Awareness

«Первичная цель ситуационной осведомленности состоит в повышении качества и своевременности принятия решений в отношении использования, обеспечения безопасности и обороны Глобальной Информационной Сетки»
(The Joint CONOPS for GIG NetOps)

ПИР-ЦЕНТР
Центр политических исследований России

Пространство совместных кибероперацій ВС США

Олег Демидов
РусКрипто-2013
28.03.2013



ПИР-ЦЕНТР
Центр политических исследований России

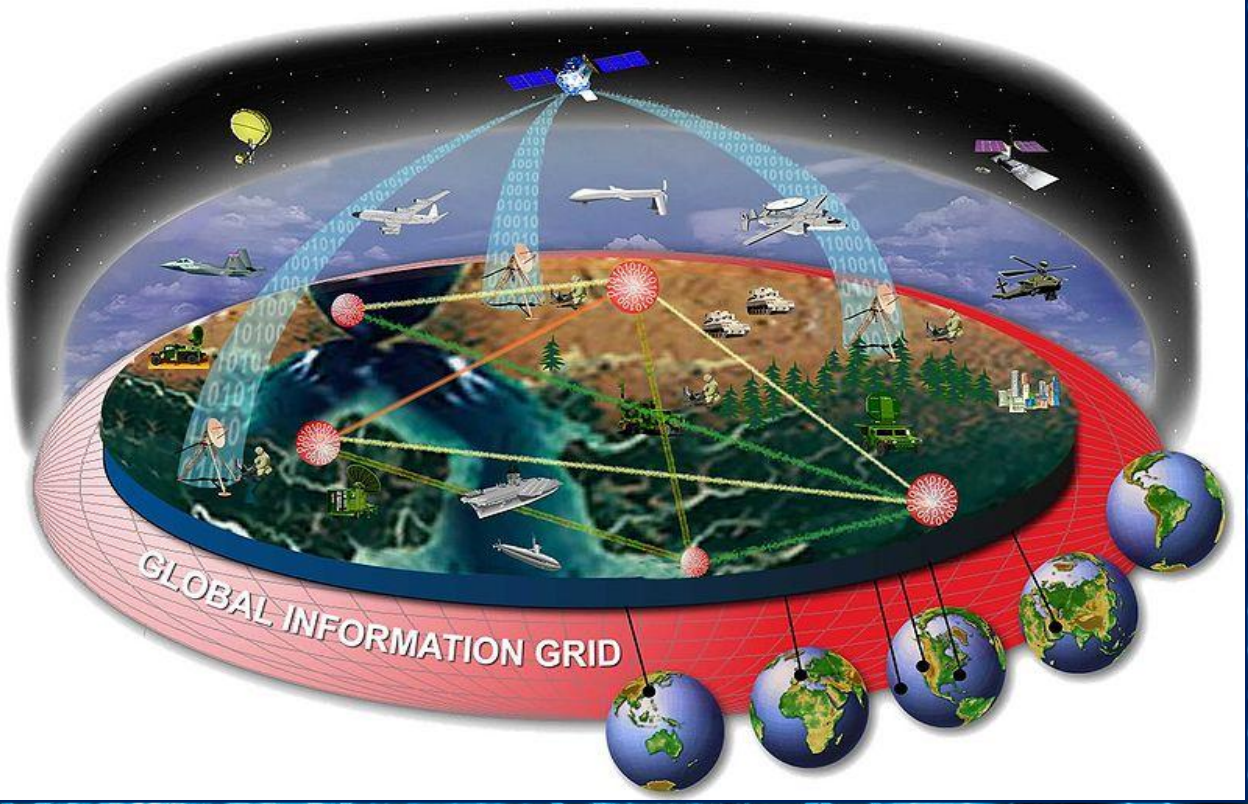
Глобальная информационная сетка (GIG): опыт Минобороны США (1)

Олег Демидов
РусКрипто-2013
28.03.2013

Future Combat Systems (FCS) программа 2000-2008 гг.

Изначальная цель: интеграция всех видов действий ВС США в едином информационно-временном пространстве (in real time) Создание единого интегрированного пространства управления (C4ISR)

2009 г.: сокращение по причине невыполнения основных целей, включая GIG



- Являлся одним из ключевых продуктов доктрины сетецентричной войны (*NetCentric Warfare*)
- GIG: «глобально взаимосвязанная сквозная совокупность информационных средств, предназначенная для сбора, обработки, хранения, распространения и управления информацией по запросу войск США, политического руководства и вспомогательного персонала»
- Включает все системы, оборудование, ПО и сервисы Минобороны, а также связанные с ними сервисы, необходимые для достижения и удержания информационного превосходства

ПИР-ЦЕНТР
Центр политических исследований России

Глобальная информационная сетка (GIG): опыт Минобороны США (2)

Олег Демидов
РусКрипто-2013
28.03.2013

Цели и задачи

- Высокий уровень интеграции вооружений, разведки и военного персонала, достаточный для ведения войны сетевого типа
- Резкое повышение качества и оперативности военных коммуникаций
- Создание инфраструктурной и технической среды для мгновенного доступа бойцов и командования к необходимым данным, независимо от подчиненности и местонахождения

Техническая концепция

- Сеть, объединяющая закрытыми высокопроизводительными каналами связи разнородные источники информации
- Сенсоры, средства наблюдения и перехвата данных космического и мобильного (авиационного) базирования
- Акцент на спутниковые наблюдающие и радиокоммуникационные системы следующего поколения
- GIG как «военный аналог интернета»

Ключевые функции GIG

- Предоставление информации о потенциале рассредоточенных по миру операционных сил и средств (баз, лагерей, станций и т.д.)
- Предоставление интерфейса оперативной связи с коалиционными силами, союзниками, другими авторизованными невоенными пользователями системы

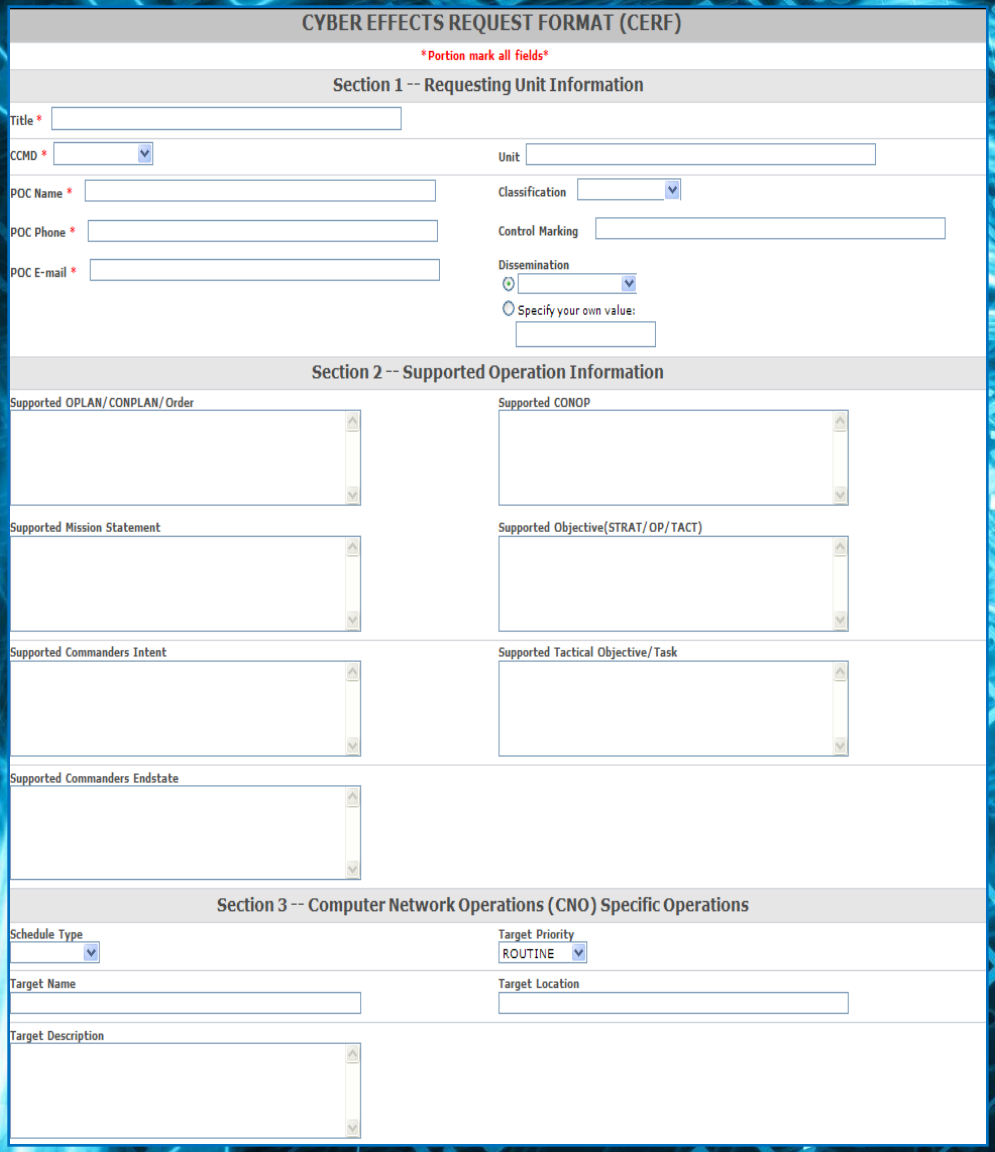
Основные составляющие GIG

- Новые коммуникационные спутники
- Радиотехнологии нового поколения, взаимодействующие с различными сетями
- Новая коммуникационная сеть наземного базирования, с расширенной рабочей полосой частот
- Службы защиты сети
- Системы содействия пользователю в поиске информации, ее пересылке и обмену

ПИР-ЦЕНТР
Центр политических исследований России

Портал CERF: формат запроса действий

Олег Демидов
РусКрипто-2013
28.03.2013



CYBER EFFECTS REQUEST FORMAT (CERF)

Portion mark all fields

Section 1 -- Requesting Unit Information

Title *

CCMD *

Unit

POC Name *

Classification

POC Phone *

Control Marking

POC E-mail *

Dissemination

Specify your own value:

Section 2 -- Supported Operation Information

Supported OPLAN/CONPLAN/Order

Supported CONOP

Supported Mission Statement

Supported Objective(STRAT/OP/TACT)

Supported Commanders Intent

Supported Tactical Objective/Task

Supported Commanders Endstate

Section 3 -- Computer Network Operations (CNO) Specific Operations

Schedule Type

Target Priority

ROUTINE

Target Name

Target Location

Target Description

Cyber Effects Request Format (CERF) – с 2012 г.

- **Обеспечивает увязку желаемого эффекта с тактической задачей, оперативной целью и конечной целью**
- **Запросы на осуществление записи, слежения и управления (*Records, Tracks, and Manages*)**
- **Режим 24/7, последовательное распределение задач в соответствии с временным горизонтом и функциям**
- **Обеспечивает возможность диалоговой коммуникации и прямой субординации, а также транспарентности в ходе операции**
- **Обеспечивает приоритезацию запросов и поддержки, отражает приоритезацию Объединенных командований, которым обеспечивается поддержка**

<u>Цель:</u> обеспечивать проактивную поддержку в киберпространстве всем подразделениям ВС США по запросу в режиме реального времени

ПИР-ЦЕНТР
Центр политических исследований России

Функциональные составляющие операций в киберпространстве

Олег Демидов
РусКрипто-2013
28.03.2013

Операции в киберпространстве

Информированность о ситуации

Информированность о состоянии сетей

- ❑ Учет сетевых ресурсов
- ❑ Идентификация (уникальных) активов
- ❑ Управление конфигурированием
- ❑ Управление уязвимостями
- ❑ Отказ в авторизованном обслуживании
- ❑ Сетевой и системный мониторинг
- ❑ Прочее

Информированность об угрозах

- ❑ Информация разведки из открытых источников
- ❑ Тактика, технологии и действия противника (TTPs)
- ❑ Информация об обнаружении вторжения
- ❑ Информация о выявлении несанкционированного доступа
- ❑ Внутрисистемная угроза
- ❑ Атрибуция атаки
- ❑ Правила боя

Управление ситуацией

Информированность о целях миссии

- ❑ Типы миссий
- ❑ Модель процессов миссии
- ❑ Степень зависимости миссии от инфраструктуры
- ❑ Анализ воздействий в рамках миссии
  - ✓ Реактивные
  - ✓ Проактивные
- ❑ Статус активных миссий
- ❑ Оценка боевых возможностей и качеств

Оценка ситуации

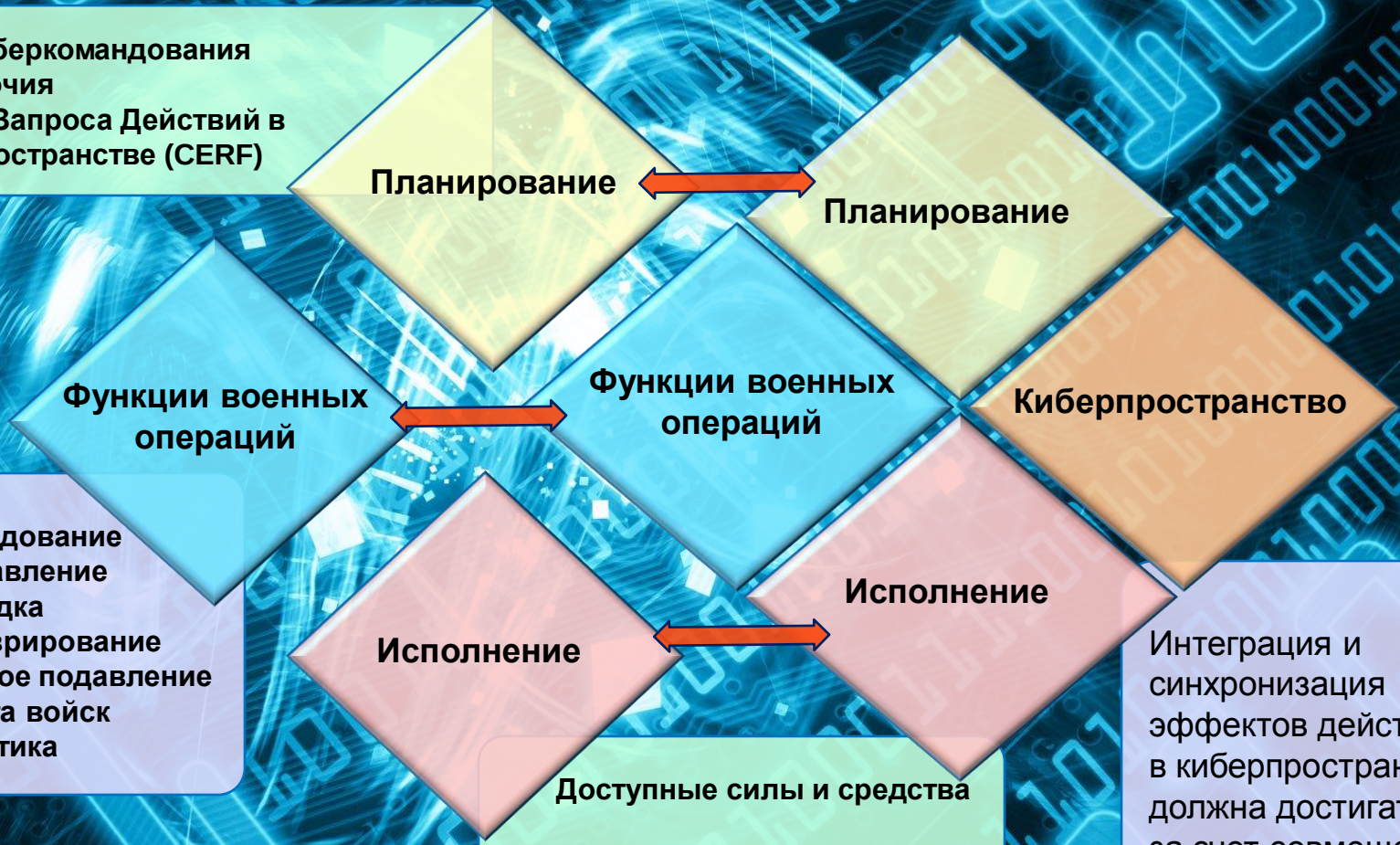
- ❑ Управление сбором данных
- ❑ Авто-ассоциация информации
- ❑ Управляемая ассоциация информации
- ❑ Выявление «шаблонов данных»
- ❑ Выявление исключений
- ❑ Индикаторы и предупреждения (I&W)
- ❑ Идентификация и отслеживание ситуации
- ❑ Анализ, выявление корреляций и обобщение (ACF)

ПИР-ЦЕНТР
Центр политических исследований России

Функции совместных военных операций в киберпространстве

Олег Демидов
РусКрипто-2013
28.03.2013

Цели Киберкомандования
Полномочия
Формат Запроса Действий в киберпространстве (CERF)



- Командование и управление
- Разведка
- Маневрирование
- Огневое подавление
- Защита войск
- Логистика

Доступные силы и средства

- Средства обнаружения
- Дружественные силы кибероборонны
- Боевые подразделения
- Оперативная картина

Интеграция и синхронизация эффектов действий в киберпространстве должна достигаться за счет совмещения планирования и исполнения военных операций со средой киберпространства

ПИР-ЦЕНТР
Центр политических исследований России

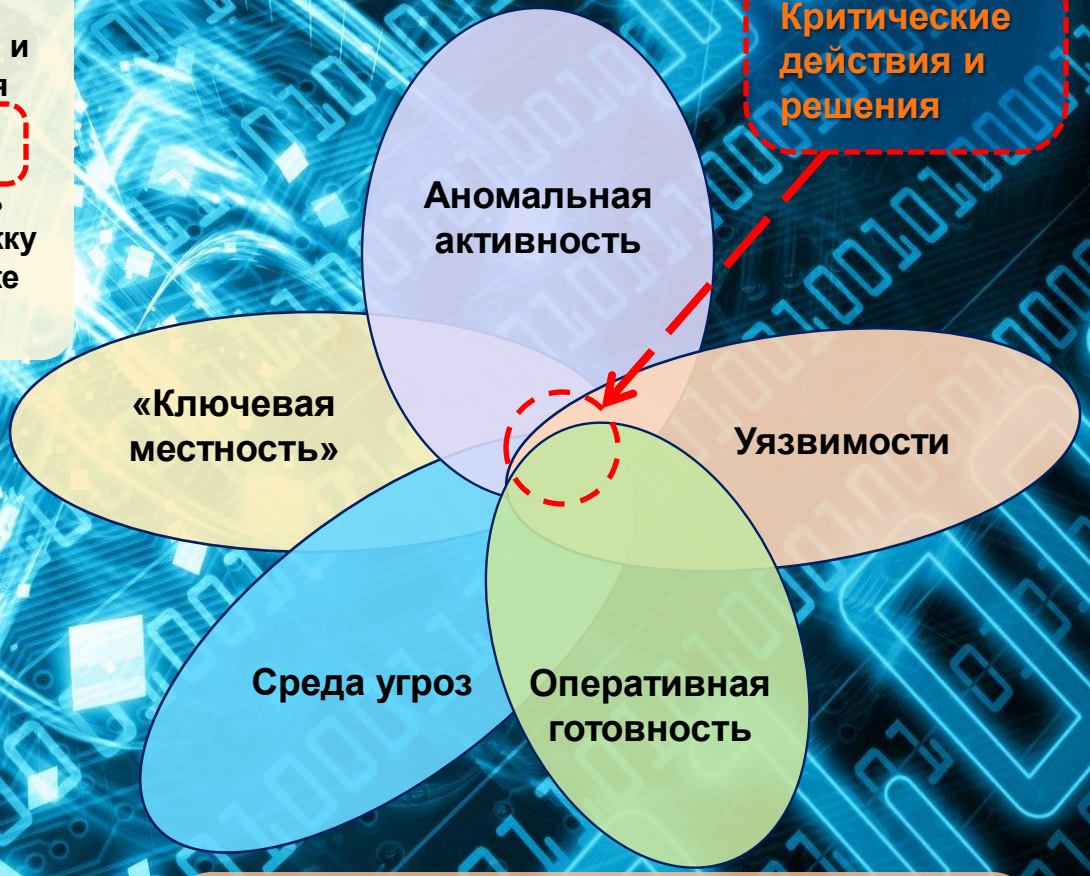
Конечные цели операций в киберпространстве

Олег Демидов
РусКрипто-2013
28.03.2013

Конечной целью *Ситуационной осведомленности* (Situational Awareness, SA) и *Выявления и предупреждения* (I&W) является обеспечение стратегического и тактического понимания среды военных операций в киберпространстве, что позволяет оценивать операционные риски, обеспечивать поддержку текущих действий и не вмешиваться в ход уже ведущихся операций в киберпространстве

Достижению цели служит комплексная оценка пяти факторов:

1. Среда угроз в данный момент и в кратчайшей перспективе
2. Наличие выявленных глобальных угроз и существенных аномалий
3.Уязвимости систем Минобороны, а также базовой инфраструктуры
4.Приоритетная «***ключевая местность»,*** которая обеспечивает понимание операционных и технических рисков операций и сетей
5.Текущая готовность к операциям и располагаемые средства киберподразделений и разведки



Непрерывное обеспечение SA/IW обеспечивает возможность активных и обеспеченных информацией действий

ПИР-ЦЕНТР
Центр политических исследований России

Кибервойна США с КНР: Сценария Белого Дома

Олег Демидов
РусКрипто-2013
28.03.2013

Сценарий составлен по материалам книги: *Clarke R., Knake R.* Cyberwar. Ecco: 2009

- 2016 г.: китайско-вьетнамский кризис вокруг Южно-китайского моря
- В рамках морских учений США-АСЕАН в Южно-китайское море направлены 2 авианосных группировки (20 кораблей, 150 самолетов, подлодки)

США: Шаг 1

- Взлом военной сети КНР, рассылка деморализующих материалов
- Отключение энергоснабжения базы флота КНР в Чжаньцзяне на сутки

КНР: Шаг 2

- Уничтожение баз данных крупнейших американских банков и транспортных операторов, а также военных сетей
- Остановка грузового ЖД сообщения, закрытие аэропортов, Нью-Йоркской биржи, ущерб в $10-100 млрд.

США: Шаг 3

- Поражение спутника связи КНР
- Вывод из строя компьютерных систем на базе китайского ВМФ
- Разрушение электрогенераторов в ряде регионов КНР, до 50 млн чел. остаются без энергоснабжения

КНР: Шаг 4 (финал)

- В периметре авианосной группы США всплывает китайская субмарина: американский флот под ударом
- Вашингтон отзывает группировки и отменяет военно-морские учения. Конфликт урегулирован в пользу КНР

ПИР-ЦЕНТР
Центр политических исследований России

Выводы

Олег Демидов
РусКрипто-2013
28.03.2013

1. Институциональная и стратегическая интеграция является магистральным путем с точки зрения национальной кибероборонны

2. Одна из самых серьезных трудностей на примере Net Centric Warfare в США связана с отсутствием универсальных решений на программном уровне

3. Опыт Киберкомандования США является специфичным в силу выраженного акцента на проактивную и превентивную компоненты стратегии действий в киберпространстве

4. Несмотря на неудачу в реализации GIG до настоящего времени, стратегическим ориентиром ВС США остается создание системы, обеспечивающей глобальное и мгновенное превосходство в киберпространстве в военном отношении

5. РФ целесообразно ориентироваться на единый подход , более сбалансированный на вопросах обороны и национальном охвате

ПИР-Центр
Центр политических исследований России

Олег Демидов
РусКрипто-2013
28.03.2013

Спасибо за внимание!

- Информация о программе ПИР-Центра «Международная информационная безопасность и глобальное управление интернетом»: net.pircenter.org
- Электронная почта координатора программы: demidov@pircenter.org