Николас Стэнли,

Президент Stanley Group

КИБЕРБЕЗОПАСНОСТЬ

Безопасность неразрывно связано с понятием «национальные интересы».

Функция национальной безопасности — обеспечение гарантий неуязвимости самых главных интересов национального суверенитета, территориальной целостности государства, защиты населения.

Национальная безопасность — стратегия, необходимая для обеспечения жизненно важных интересов государства.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КИБЕРБЕЗОПАСНОСТЬ

Кибербезопасность и кибертерроризм

Информационная безопасность — состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве

Кибербезопасность — совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Кибербезопасность и кибертерроризм

Информационное пространство – сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.

Киберпространство — сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов интернета и других телекомсетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства).

УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ РОССИИ

- нанесение урона правам, интересам и жизнедеятельности личности, организации, государственных органов;
- проведение кибератак против защищаемых информационных ресурсов со стороны киберпреступников и кибертеррористов;
- использование кибероружия в рамках специальных операций и кибервойн, в том числе сопровождающих традиционные боевые действия.

ПРИНЦИПЫ В ОСНОВЕ КИБЕРБЕЗОПАСНОСТИ РОССИИ

- принцип гарантированности конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;
- принцип максимальной защищенности личности, организаций;
- принцип конструктивного сотрудничества всех субъектов информационного общества;
- принцип баланса между установлением ответственности и введением избыточных ограничений;

Кибербезопасность и кибертерроризм

- принцип приоритезации рисков кибербезопасности в соответствии с вероятностями реализации киберугроз и размерами негативных последствий;
- принцип систематической актуализации средств и методов обеспечения кибербезопасности в целях противостояния изменяющимся киберугрозам.

ЦИФРОВАЯ РАЗВЕДКА

Радиоэлектронная разведка — дисциплина сбора разведывательной информации на основе приёма и анализа электромагнитного излучения. Использует как перехваченные сигналы из каналов связи между людьми и техническими средствами, так и сигналы работающей РЛС, станций РЭБ и тому подобных устройств.

Относится к техническим видам разведки.

ВИДЫ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ

- радиоразведка;
- радиотехническая разведка;
- разведка физических полей;
- радиолокационная разведка;
- разведка инфракрасных устройств;
- разведка лазерных устройств;
- другие.

ОРГАНИЗАЦИИ РАДИОЭЛЕКТРОННОЙ РАЗВЕДКИ

ECHELON («Эшелон») — общепринятое название глобальной системы радиоэлектронной разведки, работающей в рамках соглашения о радиотехнической и разведывательной безопасности Великобритания — США (также известного под названиями UKUSA Agreement, AUSCANNZUKUS или Five Eyes).

СОУД — засекреченная система перехвата информации, созданная СССР и странами Варшавского договора для ведения глобальной радиоэлектронной разведки.

Великобритания: Центр правительственной связи (Government Communications Head Quarters)

- Interception Modernisation Programme — инициатива по расширению возможностей правительства Великобритании на законных основаниях осуществлять перехват коммуникаций и хранить полученные данные.
- Tempora — запущенная в действие осенью 2011 года секретная программа компьютерного слежения, используемая совместно с Агентством национальной безопасности США.

Кибербезопасность и кибертерроризм

- Impact Nominal Index — компьютерная система, предназначенная для полиции и других силовых структур Великобритании, которая позволяет оперативно навести справки об интересующих лицах.
- Karma Police — программа для сбора метаданных пользователей Интернета.
- Squeaky Dolphin — программа, разработанная GCHQ для сбора и анализа данных из социальных сетей.
- MUSCULAR — программа, использовавшаяся GCHQ совместно с АНБ для взлома коммуникаций между дата-центрами Yahoo и Google.

Кибербезопасность и кибертерроризм

Франция: Frenchelon — французский аналог Эшелона. находится в ведении Генерального директората внешней безопасности (DGSE) и Управления военной разведки

Швейцария: Onyx — швейцарский аналог Эшелона. Система радиоэлектронной разведки, контролируемая разведкой Швейцарии, предназначена для перехвата военных и гражданских коммуникаций (электронная почта, факс и телефонные звонки).

Новая Зеландия: Служба безопасности правительственных коммуникаций (GCSB)

Кибербезопасность и кибертерроризм

Канада: Центр безопасности коммуникаций

Австралия: Управление радиотехнической обороны

Швеция: Titan — база данных, созданная Радиотехническим управлением министерства обороны Швеции, где хранятся записи телефонных переговоров, интернет-трафика и данных электронных транзакций, перехваченных в международных коммуникациях.

Кибербезопасность и кибертерроризм

США

— **Разведывательное сообщество США** — система 16 разведслужб, деятельность которых включает в том числе компьютерное слежение и радиоэлектронную разведку.

- Комплексная национальная инициатива по кибербезопасности — доктрина в сфере кибербезопасности США, основные положения которой засекречены.
- Дата-центр АНБ (штат Юта) — строящийся дата-центр АНБ, предназначен для хранения очень больших объёмов данных.

Кибербезопасность и кибертерроризм

— MAINWAY — база данных АНБ, содержащая метаданные о сотнях миллиардов телефонных звонков, совершённых через четыре крупнейших телефонных компании США: AT & T, SBC, BellSouth и Verizon.
  - Stellar Wind — программа слежения за электронными коммуникациями (включая контроль сообщений электронной почты, телефонных разговоров, финансовых операций и интернет-активности)
  - Комната 641A — помещение в здании магистрального провайдера AT&T, использовавшееся для перехвата интернет-телекоммуникаций в интересах АНБ.

Кибербезопасность и кибертерроризм

- Tailored Access Operations (TAO) — подразделение АНБ, занимающееся активным (взломы, установка бэкдоров) и пассивным наблюдением за компьютерами.
- Boundless Informant — система АНБ для анализа глобальных электронных коммуникаций.
- Национальная инициатива контроля подозрительной деятельности.
- PRISM (программа разведки) — программа углубленного наблюдения за интернет-трафиком, формально классифицированная как совершенно секретная, принятая АНБ в 2007 году в качестве замены Terrorist Surveillance Program.

Кибербезопасность и кибертерроризм

- DCSNet — Point-and-click система слежения ФБР, которая может осуществлять прослушивание телефонных разговоров на любых телекоммуникационных устройствах в США.
- Main Core — база данных, хранящую личную и финансовую информацию о миллионах граждан США, которые могут представлять угрозу национальной безопасности.
    - Magic Lantern — программа-кейлогер, рассылаемая ФБР в виде вложений в письма электронной почты. При активации действует как троянец и позволяет ФБР отслеживать действия интернет-пользователя.

Кибербезопасность и кибертерроризм

— NarusInsight — суперкомпьютерная система шпионажа кластерного класса, предназначенная для прослушивания и анализа данных сетевого трафика в интернете. Оператором системы в США является ФБР, пользователями — все федеральные агентства США.

- Carnivore — автоматическая система шпионажа для прослушивания информации, поступающей и уходящей с сайтов, анализа баз данных на сайтах, а также для вскрытия и анализа электронной почты, аналог российского СОРМ-2.

Кибербезопасность и кибертерроризм

- Terrorist Finance Tracking Program — совместная программа ЦРУ и Министерства финансов США по получению доступа к базе транзакций SWIFT.
- X-Keyscore — секретная программа компьютерного слежения, осуществляется совместно Агентством национальной безопасности США, Управлением радиотехнической обороны Австралии и Службой безопасности правительственных коммуникаций Новой Зеландии.

Кибербезопасность и кибертерроризм

Россия

Шестое Управление ГРУ ГШ ВС РФ, войсковые части РЭР, спецсвязь ФСО России, СВР РФ.

СОРМ (сокр. от Система технических средств для обеспечения функций оперативно-розыскных мероприятий) — комплекс технических средств и мер, предназначенных для проведения оперативно-розыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи

Кибербезопасность и кибертерроризм

Следует различать:

- «СОРМ-1» — система прослушивания телефонных переговоров, организованная в 1996 году;
- «СОРМ-2» — система протоколирования обращений к сети Интернет, разработанная рабочей группой представителей Госкомсвязи России, ФСБ России, ЦНИИ Связи и Главсвязьнадзора под руководством Ю. В. Златкиса[12] и организованная в 2000 году (ПТП, КТКС);
- «СОРМ-3» — обеспечивает сбор информации со всех видов связи и её долговременное хранение.

КИБЕРВОЙНА

Кибервойна — противоборство (война) и противостояние в кибернетическом пространстве (киберпространстве), в том числе компьютерное противостояние в Интернете, одна из разновидностей информационной войны.

По целям и задачам военные действия в киберпространстве делятся на две категории: шпионаж и атаки.

Кибербезопасность и кибертерроризм

Кибершпионаж (компьютерный шпионаж, киберразведка) — несанкционированное получение информации с целью получения личного, экономического, политического или военного превосходства, осуществляемый с использованием обхода (взлома) систем компьютерной безопасности, с применением вредоносного программного обеспечения.

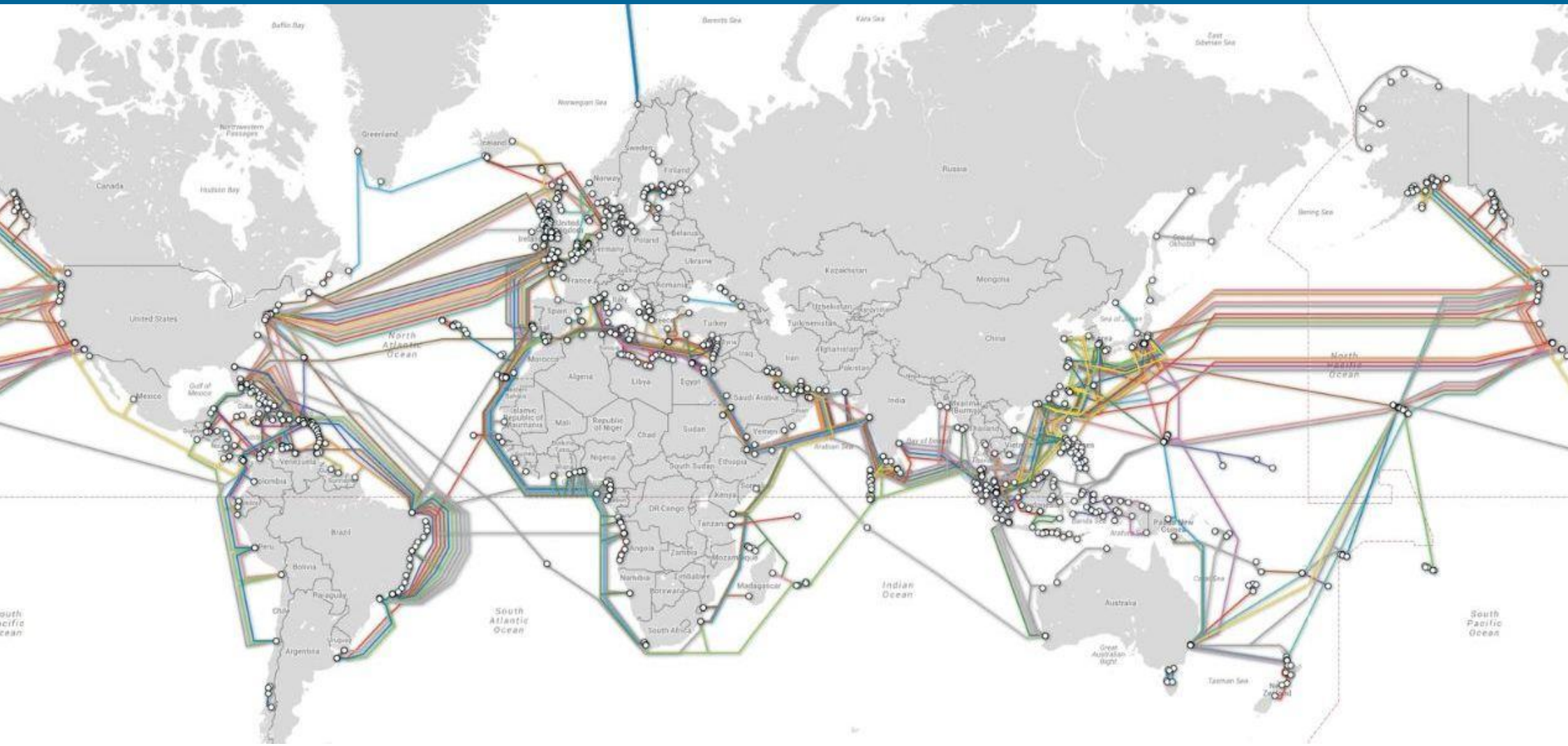
С недавних пор кибершпионаж включает также анализ спецслужбами поведения пользователей социальных сетей с целью выявления экстремистской, террористической или антиправительственной деятельности.

Кибербезопасность и кибертерроризм

Кибер-атаки:

- Вандализм;
- Пропаганда;
- Сбор информации;
- Отказ сервиса;
- Вмешательства в работу оборудования;
- Атаки на пункты инфраструктуры.

Кибербезопасность и кибертерроризм



КИБЕРВОЙСКА

США

Кибернетическое командование США — единое боевое командование вооружённых сил США.

USCYBERCOM планирует, координирует, объединяет, синхронизирует и проводит мероприятия по руководству операциями и защите компьютерных сетей министерства обороны; готовит и осуществляет полный спектр военных операций в киберпространстве, обеспечивает свободу действий США и их союзников в киберпространстве и препятствует аналогичным действиям противника.

Кибербезопасность и кибертерроризм

КНДР

Подразделение 121, или Бюро 121

КНР

Подразделение 61398 (НОАК) — подразделение Народно-освободительной армии Китая, базирующееся в Шанхае, отвечает за проведение военных операций в области компьютерных сетей. Подчинено 3-му управлению Генштаба НОАК, которое считается аналогом американского Агентства национальной безопасности.

Великобритания

Подготовкой к созданию кибервойск в Великобритании занимает британский Центр правительственной связи (Government Communications Headquarters).

Находится в ведении Министра иностранных дел Великобритании, но формально не является частью Форин-офиса. Входит в состав Объединённого разведывательного комитета, совместно с MI5 (внутренняя разведка) и MI6 (внешняя разведка).

Германия

В 2013 году Германия объявила о наличии подразделения кибероперацій в Национальном центре кибербезопасности.

Национальный центр кибербезопасности (нем. Nationales Cyber-Abwehrzentrum, NCAZ) — межведомственное правительственное агентство Федеративной Республики Германии, созданное в 2011 году для защиты от кибератак критически значимых объектов национальной ИТ-инфраструктуры и экономики.

Израиль

Подразделение 8200 — израильское подразделение радиоэлектронной разведки, входящее в Управление военной разведки («АМАН») Армии обороны Израиля, самое крупное подразделение АОИ.

Занимается, в том числе, сбором и декодированием радиоэлектронной информации и другими операциями. Согласно некоторым источникам, является одним из самых крупных таких подразделений в мире.

Первое название: «Разведывательное подразделение № 2».

Кибербезопасность и кибертерроризм

Россия

Войска информационных операций, с 2013 года — формирование Вооружённых сил Российской Федерации, находящееся в подчинении Министерства обороны.

Основными задачами являются централизованное проведение операций кибервойны, управление и защита военных компьютерных сетей России, защита российских военных систем управления и связи от кибертерроризма и надёжное закрытие проходящей в них информации от вероятного противника.

С 2014 года в составе Генерального штаба ВС России есть кибернетическое командование.

Ссылка на эту лекцию:

stnl.ru/121021