Информационный суверенитет - новая реальность

Игорь Ашманов

14.07.2015

Ашманов
и партнеры

Традиционный суверенитет

В независимом государстве должны быть:

- правительство
- законодательство
- вооружённые силы, полиция
- деньги, банки, налоги
- границы

А также менее обязательные элементы:

- язык, культура
- гражданство

….

Ашманов
и партнеры

20.07.2015

Составляющие суверенитета

Традиционные составляющие:

- Государственный
- Военный
- Дипломатический
- Экономический
- Политический
- Культурный/идеологический

В последние годы появилась новая, ключевая компонента суверенитета: цифровой суверенитет

Ашманов
и партнеры

17.05.2010

Новый, цифровой суверенитет

Право и возможность национального правительства:

- Самостоятельно и независимо определять и внутренние и геополитические **национальные интересы в цифровой сфере**;
- Вести самостоятельную внутреннюю и внешнюю **информационную политику**;
- Распоряжаться собственными информационными ресурсами, формировать **инфраструктуру** национального информационного пространства;
- Гарантировать электронную и информационную **безопасность** государства.

Ашманов
и партнеры

20.07.2015

Мы живём в эпоху слома суверенитетов

- Экономическая глобализация
- Идеологическая глобализация
- Военная и политическая глобализация
- Попытка установления мирового господства одной страной
- Слом Вестфальской системы суверенитетов
- Взлом суверенитетов через идеологию
  - Замена идеологии через дыры в информационном суверенитете
  - Организация «майдана» и смены власти на внешнее управление
  - Разрушение и разграбление страны, превращение её в Ливию/Ирак, вычёркивание с геополитической карты

В настоящее время отсутствие цифрового суверенитета может привести и к потере суверенитета вообще

Ашманов
и партнеры

20.07.2015

Цифровая защищённость: две компоненты

- **А. Электронный суверенитет:**
  - Защищённость от выключения извне
  - Защищённость от кибер-угроз: вирусов, троянов, закладок, утечек, атак
  - Стабильность критической инфраструктуры
  - Работа инфраструктуры для обычных пользователей

- **Б. Информационный суверенитет:**
  - Защищённость от информационных вирусов, информационных атак и кампаний
  - Контроль над своим информационным пространством, определение политики в нём
  - Защита самой критической инфраструктуры – умов

Составляющие идеального цифрового суверенитета

Электронный щит:

- Собственная аппаратная платформа (сетевая, мобильная и ПК)
- Собственная или контролируемая программная платформа (сетевая и ПК)
- Собственная/контролируемая мобильная платформа

Информационный щит:

- Собственная интернет-инфраструктура
- Собственная медийная структура СМИ, ТВ и Интернета
- Собственная система пропаганды и ведения информационных войн
- Развитая идеология, законы, рынок идеологических услуг

Полноценный цифровой суверенитет есть только у США

- Большинство процессоров и микросхем
- Сетевое оборудование и ПО
- Система GPS
- Большинство мировых ОС (десктопы и мобильные)
- Офис, браузеры, антивирусы, управление предприятием, игры
- Большинство популярных соцсетей, видеохостингов и блогохостингов
- Средства ведения электронных и информационных войн (мировые СМИ, специальные подразделения мониторинга и управления мнениями, боевые вирусы последних лет)

Остальные догоняют или смирились

- **Китай** энергично строит цифровой суверенитет (свои ОС, процессор, поисковики, почта, мессенджеры, социальные сети, антивирусы, сетевое оборудование и ПО, страновой фильтр Golden Shield, …)
- **Россия** имеет элементы суверенитета, начинает движение (ГЛОНАСС, свои поисковики, почта, социальные сети, СМИ, антивирусы, …)
- **Европа и Япония** по сути - в кильватере США (нет своих поисковиков, социальные сети – Фейсбук/Твиттер и т.п., американское ПО для B2C и B2B).
- **ЮВА и арабский мир** испытывают нехватку человеческих и технологических ресурсов для самостоятельного построения необходимых компонент цифрового суверенитета.

Энергичные усилия США по разрушению чужих информационных суверенитетов

- Быстрый переход на шифрованное соединение HTTPS в большинстве популярных сервисов (Facebook, Google, Twitter etc.) – уже > 80-90%;
- Возможность обращаться к населению напрямую, не обращая внимания на национальное правительство
- Разработка «независимого интернет-доступа» и «независимого GSM»;
- Глобальная прослушка по всем каналам
- Спецподразделения Пентагона и АНБ для войн в соцсетях;
- Информационные пушки: Wikileaks и аналоги, отвязка публикации от ответственности;
- Активные информационные операции на «интернет-территориях» других стран

Безопасность Интернета в РФ – недостаточна для суверенитета

- **Обычно трактуют, как наличие сигнала в сети:**
  - Бесперебойное функционирование **связи**
  - **Критическая инфраструктура:** банки, госуслуги, расписания, образование, прочее
  - **Довольные граждане:** развлечения, новости, поиск, электронная коммерция, прочие потребности

- **Увы, при наличии сигнала риски могут быть ещё выше:**
  - **Информационный шум:** заполнение инфопространства фейками, ложью
  - **Информационные атаки** на организации, инфраструктуру, персон
  - **Выход атак в офлайн:** организация волнений, восстаний и т.п.

Пример: атака на Сбербанк 18.12.2014

- Пиковый рост курса доллара, общее возбуждение и тревожность аудитории
- Внезапная активность около 1000 аккаунтов на темы:
  - Visa прекращает операции по картам Сбербанка
  - Сбербанк скоро прекратит выдачу депозитов
  - Нельзя вынуть деньги из банкомата, у Сбера нет денег
- Больше половины аккаунтов – украинские
- Массовая SMS-рассылка о том же
- СМИ подхватили атаку, помогли создать панику
- Паника, деньги завозили фурами и самолётами
- Граждане сняли более 300 миллиардов рублей

Фактически, была проведена атака на критическую инфраструктуру при отлично работающем Интернете, за которую никто не ответил

Ашманов
и партнеры

20.07.2015

Наиболее опасны информационные войны

- **Кибервойна** – часть обычной «горячей» войны, причиняет материальный ущерб; её нужно решиться начать, это недружественный акт, противоречит международному праву;
- **«Холодная» информационная война** идёт постоянно, прямо сейчас, не запрещена никакими законами и актами;
- Войны в Югославии, Ираке, Сирии, «Арабская весна», украинская майданная «революция» показывают, что информационными средствами можно **сменить режим**, обосновать **военное вторжение**;

Информационное доминирование – аналог господства в воздухе в прошлых войнах.

Ашманов
и партнеры

20.07.2015

Информационная война уже идёт

- Информационная война не объявляется
- Информационная война идёт всегда, она всегда «горячая»
- Её непросто доказать, она не признаётся противником
- и за неё невозможно наказать противника
- Информационная война не регулируется никаким правом, ни национальным, ни международным
- Информационную войну можно только выиграть или проиграть
- Значительная часть боевых действий происходит в цифровом пространстве, Интернете и соцсетях

Противник в информационной войне

- В информационной войне нет «вероятного» противника, противник всегда реальный, который воюет прямо сейчас
- Этот противник – США и Канада (и немного Англия и ЕС)
- Пентагон начал открыто создавать **кибервойска** для информационной войны 4 года назад
- Мы, увы, как обычно, готовимся к войнам прошлого; у нас кибервойск пока нет
- Сейчас мы только начинаем совершать перелом в ходе тяжёлой информационной войны на нашей территории
- Олимпиада, Крым, Донбасс – это наши Сталинграды и Прохоровки

Ашманов
и партнеры

20.07.2015

Современные инструменты информационных войн

- **Ангажированные СМИ,** система «отмывки» вбросов (цикл соцсети-СМИ-снова соцсети-снова СМИ)
- **Автоматы:** боты, тролли, спам
- **Системы управления виртуалами:** один инфобоец управляет 30-50 аккаунтами разных жанров
- **Многослойные человеческие структуры** в соцсетях («Стадо Навального» на 40-50 тысяч пользователей)
- **Ангажированные массовые сервисы** (Твиттер, Youtube, поисковики, агрегаторы новостей)
- **«Пятая колонна»:** ангажированные деятели культуры, ангажированные чиновники, журналисты
- **Ложная и навязанная идеология:** структура права, система понятий о хорошем и правильном (концепция «свободы слова» в том числе)

Свойства информационной среды

- **Пользователи стремительно глупеют:**
  - **Беспамятность:** в Твиттере, Фейсбуке нет памяти, контент тонет. Среднее время жизни поста в ФБ, Твиттере – не более 6 часов. Это позволяет применять одни и те же сценарии и вбросы по многу раз.
  - **Клиповое мышление.** Средний пост в ЖЖ – 3800 знаков, в ФБ – 630 знаков (вместе со сниппетами ссылок).
  - **Ожесточение и поляризация.** Градус дискуссий повышается, никто никого не слышит.
  - **Стало всё можно.** Вбросы, обман, пропаганда, спам перестали быть постыдным делом. Лозунг эпохи: «вы не рефлексируйте, вы распространяйте»!
- **В соцсетях активно оперируют профессионалы:**
  - **Активные сообщества спамеров.** Из 20М аккаунтов русского Твиттера живых – 1,5М, из них 700К – спамеры и боты.
  - **Технологичные системы «отмывки» новостей и вбросов.** Вброс в Твиттер или ФБ отмывается в СМИ, снова обсуждается в Твиттере и т.п.

Информационные атаки

- **Тактические, быстрые, актуальные:**
  - На персоны (Якунин, Сечин)
  - На институты, организации (Сбербанк 18.12.2014)
  - Привязанные к событиям (9 Мая, «Бессмертный полк»)
- **Среднесрочные кампании:**
  - Атаки на институты и организации (милиция, армия – длиной в полтора-два года)
  - Атака на РПЦ (9 месяцев с 03.2012 по 12.2012)
- **Стратегические, постоянно действующие:**
  - Создание долгоиграющих мифов, мемов (армия насильников, одна винтовка на троих, нефтяная игла) – с 80-х годов
  - Фальсификация истории, искажение источников (с 70-х годов)
  - Постоянная атака на Путина и его окружение (14 лет)

Ашманов
и партнеры

20.07.2015

Риски для построения информационного суверенитета

- Уход общения в мобильные чаты
- Переход массовых сервисов на шифрованные соединения с пользователем
- Попытки построения «независимого» Интернета
- Переход информационной войны в горячую фазу
- Возникновение огромного разнообразия «сетевых автоматов», производящих и внедряющих контент
- Появление информационных армий
- Включение фейков и вбросов в «метаболизм» СМИ
- Доминирование «продавцов заблуждений»

Что нужно для построения информационного суверенитета

- **Доступ к контенту**
  - Сертификаты
  - Прозрачность основных сервисов (API, готовность сотрудничать)
- **Ответственность массовых сервисов за контент**
  - Законы (139-ФЗ, закон об информационных посредниках, закон о размещении западных сервисов, пр.)
  - Постоянный мониторинг СМИ, социальных сетей
  - Процедуры проверки и доказывания, правоприменительная практика, ИТ-образованность адвокатов, следователей и судей
- **Возможность блокировки информационных атак и плохого контента**
  - Мониторинг, общие экраны и «выключатели»
  - Выборочная и быстрая блокировка атак и вбросов
- **Своя информационная стратегия, своя идеология, своя медийная экосистема сервисов и контента**

Свобода слова тут ни при чём, это вопрос суверенитета

- Во всех «развитых» странах Интернет **уже** контролируется.
  - В США, Британском Содружестве – постоянный мониторинг, реальные сроки за посты в соцсетях;
  - в Европе законы против анонимности;
  - Япония хочет запретить Tor и прочий анонимный трафик.
  - Китай мониторит и фильтрует. ЮВА идёт туда же.
- Системы законодательного ограничения, фильтрации и мониторинга Интернета, кибервойска строятся и **будут построены** всеми самостоятельными игроками.
- **Борьбу** с попытками государств построить информационный суверенитет будут вести в основном США/Запад. Главным инструментом и аргументом будет «свобода слова».

Ашманов
и партнеры

20.07.2015

Информационный суверенитет: медийная инфраструктура

- Поисковые машины, справочные ресурсы
- Социальные сети, мессенджеры
- Блоги, форумы, рассылки
- Интернет-СМИ, традиционные СМИ и ТВ
- Видеохостинги и фотохостинги
- Контентные ресурсы (рейтинги/аналитика, история, наука, автомобили, спорт, кино, книги…)
- Приложения для социальных сетей и мобильных устройств
- Детский Интернет, игры

СПАСИБО!

Игорь Ашманов

Информация о компании,
услугах и технологиях
www.ashmanov.com

14.07.2015

Ашманов
и партнеры