Информационный суверенитет - новая реальность

Игорь Ашманов

24.04.2013

Ашманов
и партнеры

Ашманов
и партнеры

24.04.2013

Традиционный суверенитет

В независимом государстве должны быть:

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

А также менее обязательные элементы:

- язык
- гражданство
- транспорт

….

Ашманов
и партнеры

06.05.13

Составляющие суверенитета

Традиционные составляющие:

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

В последние годы появился новый ключевой компонент суверенитета: цифровой суверенитет

Ашманов
и партнеры

06.05.13

Мы живём в эпоху слома суверенитетов

- Экономическая глобализация
- Идеологическая глобализация
- Военная и политическая глобализация
- Слом Вестфальской системы суверенитетов
- Взлом суверенитетов через идеологию
- Замена идеологии через дыры в информационном суверенитете

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

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

06.05.13

Цифровой суверенитет: назначение

А. Электронный суверенитет: устойчивость к кибервойнам

- Защищённость от вирусов, атак, взломов, утечек, закладок, кражи данных, спама, выключения инфраструктуры и ПО
- Устойчивость к электронным атакам (мониторинг, обнаружение, предупреждение, блокирование, контратаки)

Б. Информационный суверенитет: устойчивость в информационной войне

- Самостоятельное управление информацией (фильтрация, выключение, распространение);
- Устойчивость к информационным атакам (обнаружение, предупреждение, блокирование, контратака).

Ашманов
и партнеры

06.05.13

Составляющие идеального цифрового суверенитета

Электронный щит:

- Собственная аппаратная платформа (сетевая 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 и средства пропаганды и ведения информационных войн
- Развитая идеология, законы, рынок идеологических услуг

Ашманов
и партнеры

06.05.13

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» показывают, что информационными средствами можно **сменить режим**, обосновать военное **вторжение**;

Информационное доминирование – аналог господства в воздухе в прошлых войнах.

Ашманов
и партнеры

06.05.13

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

Ашманов
и партнеры

06.05.13

Средства пропаганды и информационных войн

- **Анализ медийной среды**, мониторинг трафика и социальных медиа
- **Средства фильтрации** трафика
- **Законодательство** об ответственности за контент (хостеров, провайдеров доступа и медийных провайдеров)
- **Средства распространения контента**: СМИ, блоги, социальные сети)
- **Силы для распространения контента**: специальные подразделения и средства для информационных войн в сети
- **Рынок идеологических услуг**

Ашманов
и партнеры

06.05.13

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 8М аккаунтов русского Твиттера живых – 1,5М, из них 700К – спамеры и боты.
  - **Технологичные системы «отмывки» новостей и вбросов.** Вброс в Твиттер отмывается в СМИ, снова обсуждается в Твиттере и т.п.

Ашманов
и партнеры

06.05.13

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
- Большинство популярных соцсетей, видеохостингов и блогохостингов
- Средства ведения электронных и информационных войн (мировые СМИ, специальные подразделения мониторинга и управления мнениями, боевые вирусы последних лет)

Энергичные усилия 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»;
- Спецподразделения для войн в соцсетях;
- Информационные пушки: Wikileaks и аналоги, отвязка публикации от ответственности;
- Активные информационные операции на «интернет-территориях» других стран

Ашманов
и партнеры

06.05.13

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.).
- **ЮВА и арабский мир** испытывают нехватку человеческих и технологических ресурсов для самостоятельного построения необходимых компонент цифрового суверенитета.

Ашманов
и партнеры

06.05.13

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

06.05.13

Что делать?

1. Региональный игрок не сможет сам построить полный периметр информационного суверенитета.
2. Становиться в кильватер США – ведёт к крушению/прозябанию, что показывает судьба лояльных к ним светских арабских режимов и республик бывшего СССР.
3. Нужно объединять усилия (очевидно, с Китаем или Россией, странами СНГ).
4. Концентрироваться в первую очередь на информационной войне.
5. Строить не только системы контроля, но и системы влияния (распространения информации, управления мнениями).
6. Строить хотя бы «малый информационный щит»

Ашманов
и партнеры

06.05.13

Строить как минимум «малый щит»

1. Средства контроля:

- Мониторинг информационного пространства
- Законодательство об ответственности за контент разных категорий операторов (хостер, провайдер доступа, медийный провайдер, СМИ).
- Законодательство о фильтрации, публичное правоприменение
- Страновой фильтр на всех уровнях (школы, университеты, магистрали). Хотя бы как возможность «военного времени».

Средств контроля недостаточно, нужны средства влияния

Ашманов
и партнеры

06.05.13

Малый информационный щит

2. Средства влияния:

- **Рынок идеологических услуг** и технологий, работа над собственной идеологией
- **Система влияния** и ведения информационных войн (кадры и инструменты).
- **Информационная инфраструктура**: своя или заимствованная у союзников (поисковики, контентные проекты, блоги, соцсети).

СПАСИБО!

Игорь Ашманов

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

17.05.2010

Ашманов
и партнеры