Интернет, как фактор безопасности в Центральной Азии: за и против

Артем Горяйнов
ОФ «Гражданская инициатива Интернет политики»

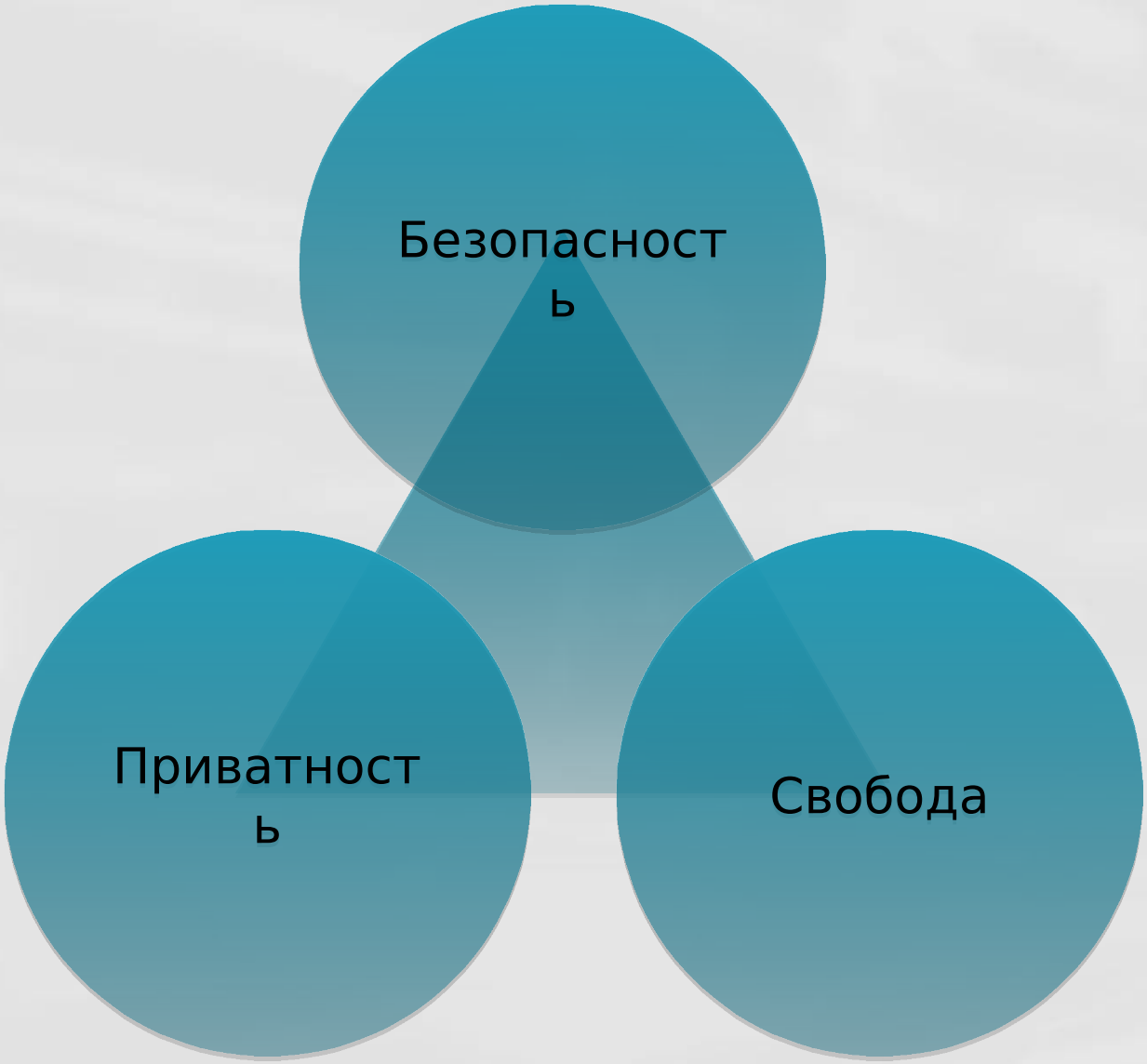
Угрозы в Интернет

Слабость или сила

?

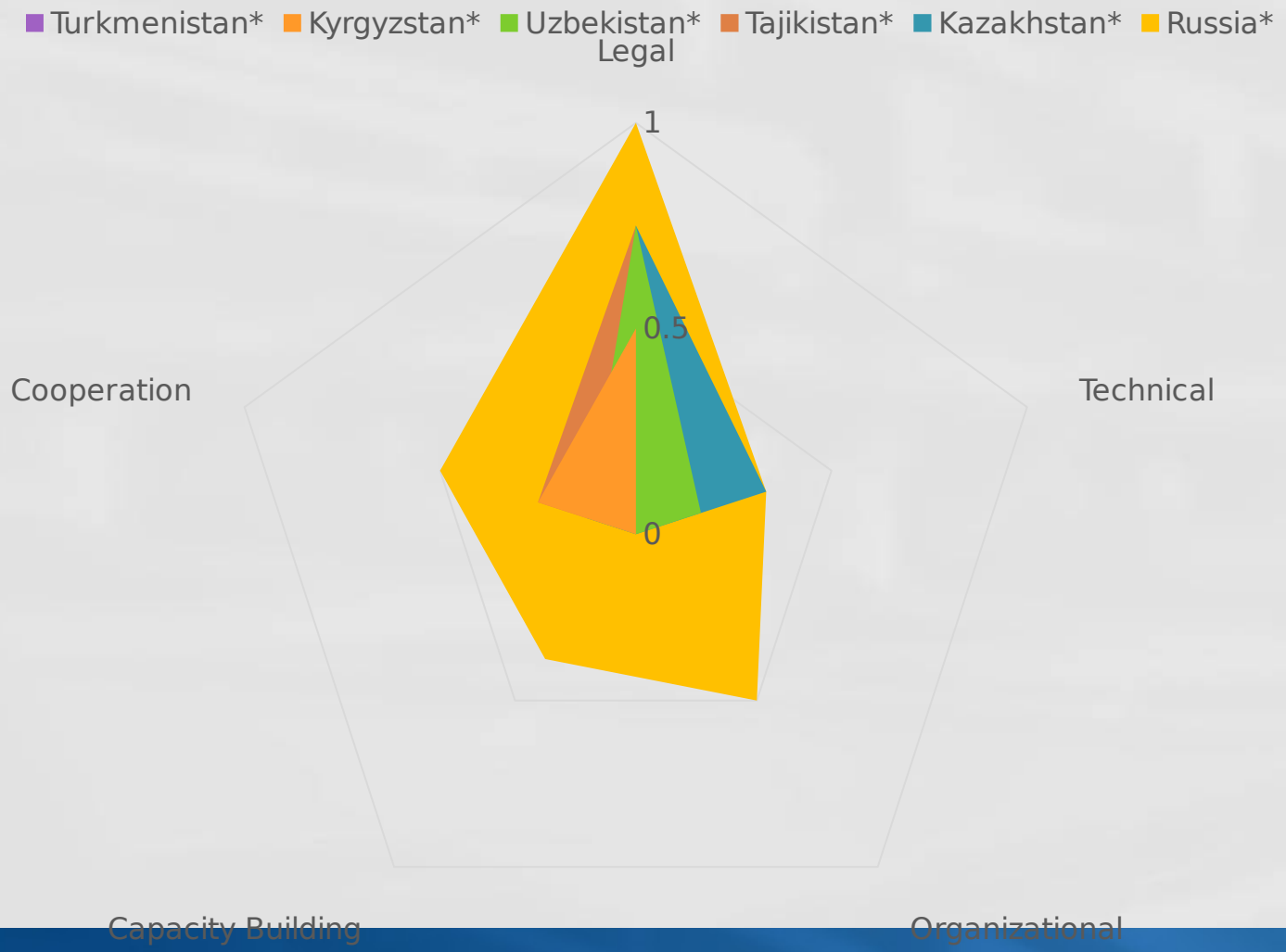
Угрозы экстремизма в Интернет

- Вербовка через Интернет
- Распространение идеологии и устрашение
- Использование для коммуникаций
- Сбор(хищение) и отмывание денег
- Сбор информации и совершение атак.


Безопасность
Приватность
Свобода


Безопасность
Приватность
Свобода

Индекс кибербезопасности МСЭ для России и стран ЦА



Источник: ITU-ABIresearch, Global Cybersecurity Index (GCI) 2014

Ограничение доступа к информации

- Блокирование и фильтрация со стороны государства
  - + Ограничивает доступ к материалу некоторой аудитории.
  - - Без специального дорогостоящего оборудования (DPI, контент-фильтры) отсутствует фокусная блокировка.
  - - Не работает с шифрованными протоколами (https), сетями доставки контента (CDN)
  - - Легко обходится
  - - Создает «иллюзию» работы правоохранительных органов.

Ограничение доступа к информации

- Блокирование и фильтрация со стороны контент провайдеров
  - + Точечно ограничивает контент для страны.
  - + Не требует приобретения специального дорогостоящего оборудования (DPI, контент-фильтры).
  - + Работает для всех видов доступа, включая шифрованные
  - + Публикуются отчеты прозрачности (для некоторых контент провайдеров)
  - +- Требует как минимум судебного решения или обращения правоохранительных органов
  - +- Удовлетворяется не всегда
  - - Легко обходится

Ограничение доступа к информации

- Удаление контента
  - + Удаляет контент без возможности доступа.
  - + Публикуются отчеты прозрачности (для некоторых контент провайдеров)
  - +- Требует как минимум судебного решения или обращения правоохранительных органов
  - +- Удовлетворяется не всегда
  - - Сам контент может появиться в другом месте

Ограничение доступа к информации

- Ужесточение наказания за размещение противоправного контента в сети.
  - + Количество противоправного контента может уменьшиться
  - - Расплывчатость формулировок ведет серьезным злоупотреблениям
  - - настоящие злоумышленники находят трудноотслеживаеые способы размещения контента

Перехват информации

- Использование СОРМ
  - + Необходимость в век технологий
  - - Не работает с шифрованными протоколами
  - - Возможны серьезные злоупотребления при бесконтрольном использовании (-- при использовании malware или национального сертификата безопасности)

Мониторинг интернет ресурсов

- Автоматический или ручной сбор информации
  - + Позволяет оперативно получать информацию о появлении определенного контента
  - + Позволяет получить базу данных для анализа
  - - Может использоваться не по назначению

Контроль публичных точек интернет

- Контроль публичного WiFi, интернет кафе
  - + Позволяет снизить вероятность использования публичных точек для противоправной деятельности
  - - Сложен в исполнении
  - - Открывает простор для коррупции
  - - Малоэффективен

Централизация каналов связи

- Монополия международного трафика
  - +- Единая точка контроля
  - - Единая точка отказа
  - - Убийство рынка связи

Online vs Offline

За каждым противоправным онлайн действием стоят реальные люди,

Каждое противоправное онлайн действие направлено на реальных людей

Спасибо
за внимание!