Дипломатия и защита критической инфраструктуры от киберугроз

Олег Шакиров, консультант ПИР-Центра

09.09.2021

Российско-американский саммит в Женеве, 16 июня 2021

«Ещё одна сфера, которой мы уделили много времени, — это кибербезопасность. **Я говорил о предложении, что определённая критическая инфраструктура не должна подвергаться атакам — никаким — ни киберсредствами, ни какими-либо иными.** Я передал им список [из 16 секторов], которые, согласно политике США, определяются как критическая инфраструктура, от энергетики до систем водоснабжения».

Джо Байден, 16 июня 2021

Начало переговоров по информационной безопасности

1996 непубличные консультации военных экспертов России и США

1998 заявление об общих вызовах безопасности на рубеже XXI века

The New York Times

U.S. and Russia Differ on a Treaty for Cyberspace

In 1996, at the dawn of commercial cyberspace, American and Russian military delegations met secretly in Moscow to discuss the subject. The American delegation was led by an academic military strategist, and the Russian delegation by a four-star admiral. No agreement emerged from the meeting, which has not previously been reported.

Кибердипломатия сегодня

- **Двусторонние** отношения (Россия-США, Китай-США)
- **Региональные и групповые** процессы (ШОС, АСЕАН, НАТО, ОБСЕ)
- **ООН** (Первый комитет Генассамблеи, Третий комитет, Совбез)

В рамках Рабочей группы открытого состав (РГОС) выступили 91 стран + негосударственные организации

Защита КИ в документах ООН (начало)

«Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»

- первая резолюция принята в 1998 по инициативе России в Первом комитете Генассамблеи
  (вопросы разоружения и международной безопасности)
- начиная с **2002** и далее в резолюции выражается «озабоченность тем, что эти технологии и средства потенциально **могут [...] негативно воздействовать на целостность инфраструктуры государств, нарушая их безопасность применительно как к гражданской, так и к военной сферам**»

Защита КИ в документах ООН (начало)

«Создание глобальной культуры кибербезопасности и защита важнейших информационных инфраструктур»

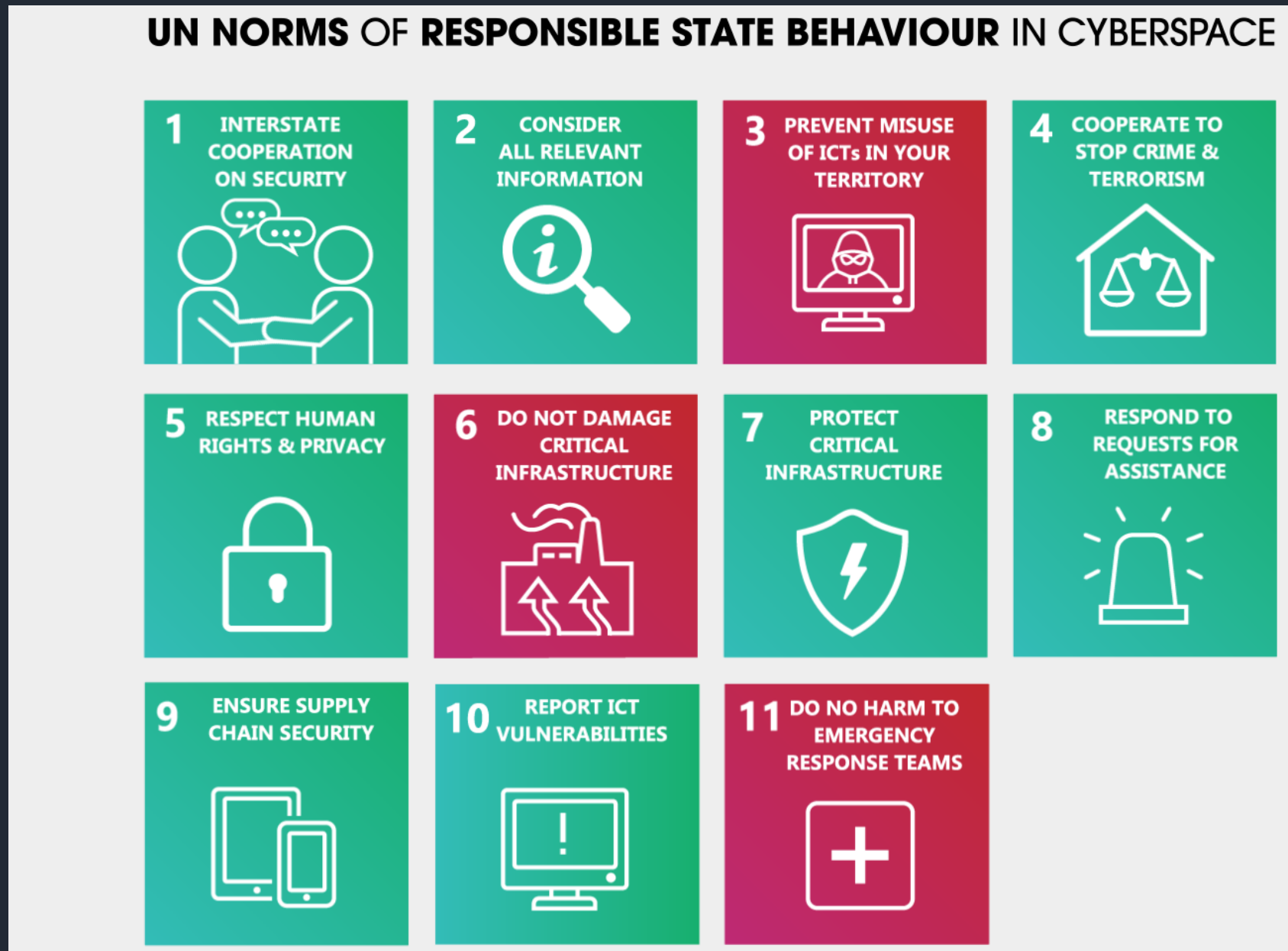
- принята по американской инициативе в **2003** во Втором комитете Генассамблеи
  (экономические и финансовые вопросы)
- перечислены примеры важнейших (критических) информационных инфраструктур
- приложение «Элементы для защиты важнейших информационных инфраструктур»
- **2009**: Инструмент добровольной самооценки национальных усилий по защите КИИ

Как дипломатия помогает защищать КИ?

- **Выработка норм**, касающихся КИ
- **Практическое сотрудничество**, в т.ч. реагирование на инциденты
- Помощь для **наращивания потенциала** в области ИКТ

Логотип Секретариата ООН для переговоров по ИКТ в Первом комитете

Нормы



11 добровольных и необязательных норм, правил или принципов ответственного поведения государств (Доклад ГПЭ ООН 2015)

Визуализация Australian Strategic Policy Institute

Нормы о защите КИ

Норма 13 f)

государства **не должны заведомо осуществлять и поддерживать деятельность** в сфере ИКТ, если такая деятельность противоречит их обязательствам по международному праву, **наносит преднамеренный ущерб критически важной инфраструктуре** (КИ) или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения

Нормы о защите КИ

Норма 13 g)

государства **должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ**, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции

Нормы о защите КИ

Норма 13 h)

государства **должны удовлетворять соответствующие просьбы об оказании помощи**, поступающие от других государств, КИ которых становится объектом злонамеренных действий в сфере ИКТ. Государства должны также удовлетворять соответствующие **просьбы о смягчении последствий злонамеренных действий** в сфере ИКТ, направленных против КИ других государств, если такие действия проистекают **с их территории**, принимая во внимание должным образом концепцию суверенитета

Сектора КИ

Согласно докладу ГПЭ ООН 2021:

- каждая страна сама определяет, что считать КИ
- исключительно важны **санитарно-медицинская инфраструктура и объекты здравоохранения**
- другие примеры КИ:

– **энергетика**
– **производство электроэнергии**
– **водоснабжение и санитария**
– **образование**
– **коммерческие и финансовые услуги**
– **транспорт**
– **телекоммуникации**
– **процесс проведения выборов**

Китай-США, Rose Garden agreement 2015

- В преддверии встречи обсуждался запрет на атаки против КИ в мирное время
- Публично договорились
  - не заниматься и не поддерживать кражу интеллектуальной собственности с помощью киберсредств
  - продвигать международные правила поведения для киберпространства

Россия-Беларусь, соглашение 2013

Статья 4, п. 3

Каждая Сторона имеет равное право на защиту информационных ресурсов и критически важных объектов своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от информационных атак на них.
Каждая Сторона **не осуществляет по отношению к другой Стороне подобных действий** и оказывает содействие другой Стороне в реализации указанного права.

Сотрудничество

Механизмы сотрудничества

- **Меры укрепления доверия**
  - контактные центры на разных уровнях для поддержания контактов между государствами
  - диалог и консультации
  - обмен информацией
- **Помощь в реагировании на инциденты**
- **Выработка общих подходов (ЕС)**

Защита КИ в российских двусторонних соглашениях

Россия подписала соглашения по информационной безопасности **с 10 странами**:

- Беларусь (2013)
- Куба (2014)
- Китай (2015)
- Индия (2016)
- ЮАР (2017)
- Вьетнам (2018)
- Туркменистан (2019)
- Иран (2021)
- Киргизия (2021)
- Никарагуа (2021)

- Во всех соглашения деструктивное воздействия на объекты КИ **указано в числе угроз**
- Соглашения с Индией, Китаем, ЮАС, Беларусью предусматривают **сотрудничество по обеспечению безопасности КИ**
- Соглашение с Беларусью содержит **обязательство не осуществлять атаки на КИ**

Россия-Индия
кибератака на Куданкулам (2019)

Помощь

Наращивание потенциала

Доклад ГПЭ ООН 2015

«Государства несут главную ответственность за обеспечение государственной безопасности и безопасности своих граждан, в том числе в ИКТ-среде, однако некоторые государства могут не обладать достаточным потенциалом для защиты своих ИКТ-сетей. Отсутствие такого потенциала может сделать граждан и критически важную инфраструктуру государства уязвимыми или же превратить такое государство в невольное убежище для злоумышленников».

Наращивание потенциала

- **EU4Digital** — программа ЕС по развитию потенциала в области кибербезопасности в странах восточного партнёрства
- **ENVR** — Национальная школа кибербезопасности с региональной направленностью в Сенегале при поддержке Франции
- **Тренинги** ОАГ при поддержке Великобритании по управление инцидентами, киберпреступления и защита КИ
- **Тренинги MITRE** по запросу Госдепартамента США

Проект USAID Cybersecurity for Critical Infrastructure in Ukraine

- С 2020 по 2024 год, бюджет 38 миллионов
- три компонента
  1) укрепление благоприятной среды для обеспечения кибербезопасности
  2) развитие кадров для кибербезопасности
  3) построение устойчивой индустрии кибербезопасности

Наращивание потенциала

В проекте плана поддержки ИТ-отрасли предлагается (по CNews):

«**обучать работе с отечественными программными средствами обеспечения ИБ руководителей иностранных правительственных структур**. Это также коснется глав профильных ведомств и специалистов по информационной безопасности зарубежных стран. **Помощь в процессе обучения должны оказать российские компании — вендоры ПО, отвечающего за информационную безопасность. Средства на это будут выделяться из федерального бюджета**»

Спасибо

Олег Шакиров, консультант ПИР-Центра
shakirov@pircenter.org