НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Е.А. Мартынова, аспирант Аспирантской школы по праву, преподаватель департамента международного права, факультет права НИУ «Высшая школа экономики»

СЕМИНАР ПРОЕКТНОЙ ГРУППЫ «ОТ НАУЧНОЙ ФАНТАСТИКИ К ПРАВОВОЙ НАУКЕ: ОТВЕТСТВЕННОСТЬ ГОСУДАРСТВ В «КИБЕРПРОСТРАНСТВЕ»

11 ноября 2022 года

«От научной фантастики к правовой науке: ответственность государств в «киберпространстве»

- Проектная группа аспирантов и студентов факультета права и факультета мировой экономики и мировой политики

  Куратор: профессор В.Н. Русинова

- **междисциплинарное исследование** вопросов ответственности государств за совершение враждебных действий в «киберпространстве»

- Четыре научных семинара и круглый стол с презентацией результатов исследования

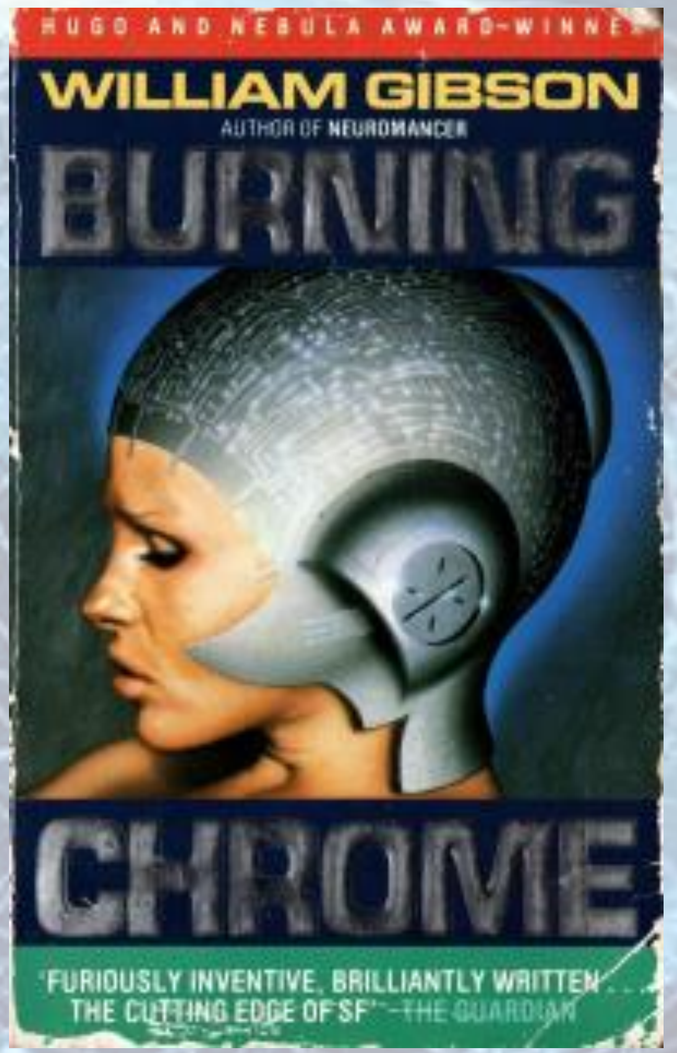
«NotPetya» и не только:
предположительно спонсированные государствами «кибероперации», 2005-2021

Источник: https://www.cfr.org/cyber-operations/

«Киберпространство»: из киберпанка в международное право

Уильям Гибсон, «**Сожжение Хром**» (1982):

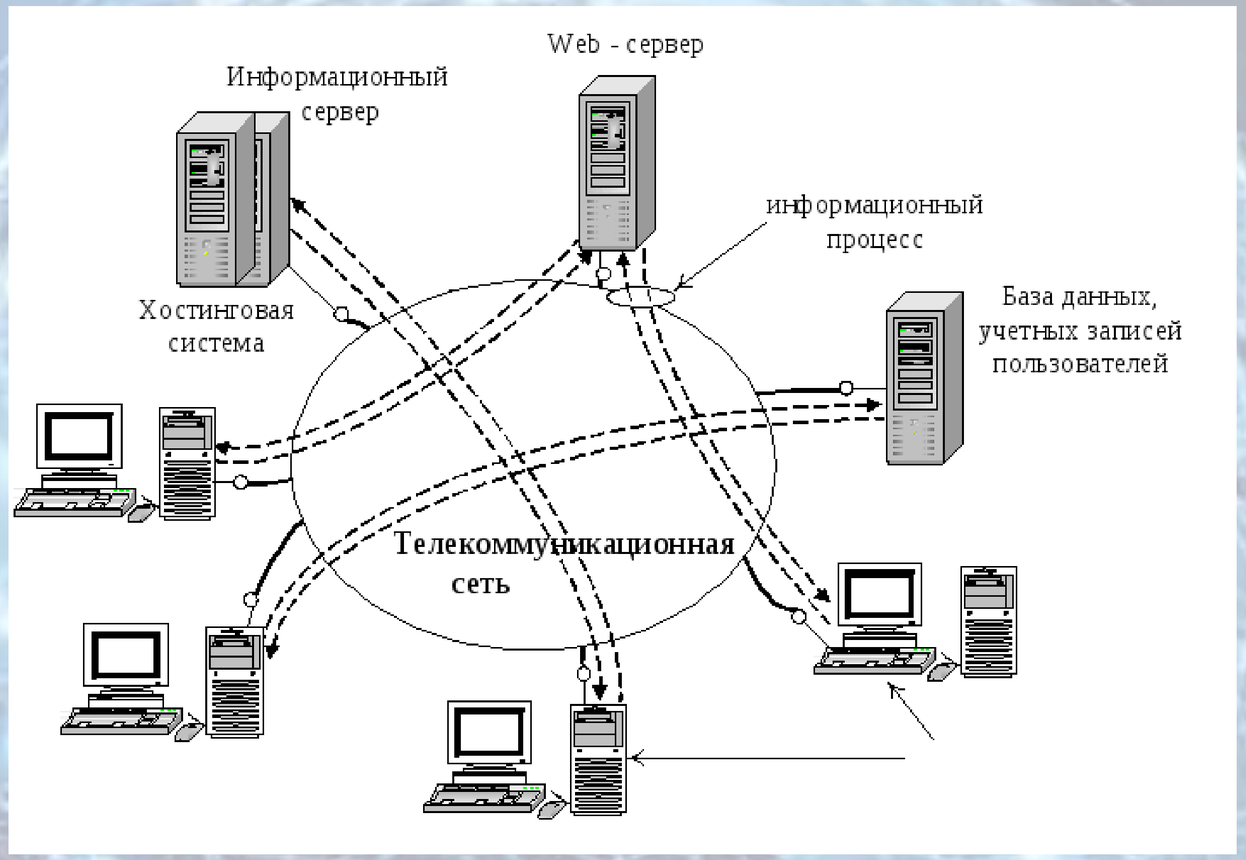
Киберпространство - «*монохромное псевдопространство, где, как редкие звезды во тьме, светились плотные сгустки данных, мерцали галактики корпораций и отсвечивали холодным блеском спирали военных систем*».



«Киберпространство»: из киберпанка в международное право

«**Киберпространство**» как «пространство»:

- отличается от физического пространства: внетерриториальный, безграничный, всепроницающий характер
- множество стейкхолдеров, концепция открытого, децентрализованного пространства
- 4 взаимосвязанных элемента: «железо», софт, информация, «кибер-персоны»



«Киберпространство»: из киберпанка в международное право

«Киберпространство» с точки зрения международного права:

- Консенсусный доклад ГПЭ 2013 года (§19-20): **международное право** и, в частности, Устав ООН, а также суверенитет и международные нормы и принципы, проистекающие из него, **применимы** в киберпространстве
- Консенсусный доклад ГПЭ 2015 года 11 «добровольных, необязательных норм, правил или принципов ответственного поведения государств» в киберпространстве
- Концепция суверенитета: пределы применения в киберпространстве

  Русинова В., Ассаф А., Мошников Д. Спор о суверенитете в киберпространстве: содержание, пределы и перспективы развития позитивистского дискурса // Международное правосудие. 2020. № 3 (35). С. 55–66

Ответственность государств в «киберпространстве»: элементы

- **Квалификация** кибератаки/кибероперации как нарушение международно-правового обязательства
- **Вменение** деяния государству
- **Применение** вторичных норм международного права об ответственности государств
- *Ответственность за нарушение обязательства due diligence?*

«Кибератака»: из киберпанка в международное право

Уильям Гибсон, «**Сожжение Хром**» (1982):

Русская программа, прокладывает себе дорогу наверх, пронзая насквозь башни данных и окрашивая все, что вокруг, в цвета игровой комнаты. Я ввожу пакет подготовленных Бобби команд прямо в центр холодного сердца Хром. В него врезается струя передачи — импульс сконцентрированной информации, и выстреливается прямо вверх, мимо сгущающейся стены тьмы, мимо русской программы, в то время, как Бобби силится удержать под контролем ту единственную секунду, которая для нас сейчас важнее, чем жизнь. Не до конца оформившееся щупальце тьмы делает судорожную попытку наброситься с высоты мрака, но слишком поздно.
Мы сделали это.
Матрица складывается вокруг меня сама по себе с волшебной легкостью оригами.

«Кибератаки»: квалификация государствами

США, Указ № 13694 2015 года	Регламент ЕС от 17 мая 2019 года	Регламент Великобритании 2020 года	Регламент Австралии 2021 года
(a) серьезное вмешательство в функционирование компьютера или сети компьютеров, которые поддерживают один или несколько объектов КВИ; (b) существенное вмешательство в работу одного или нескольких субъектов в секторе КВИ; (c) существенное нарушение доступности компьютера или сети компьютеров; (d) незаконное присвоение значительных средств или экономических ресурсов, коммерческой тайны, ПД или финансовой информации для коммерческого или конкурентного преимущества или личной финансовой выгоды.	(a) доступ к информационным системам; (b) вмешательство в информационную систему; (c) интерференция данных; (d) перехват данных.	(a) получение доступа или попытка доступа к информационной системе; (b) осуществление или попытка вмешательства в работу информационной системы; (c) осуществление или попытка вмешательства в данные, за исключением разрешенных случаев.	(a) действия, которые уничтожили или сделали недоступными основные услуги или КВИ; (b) действия, которые привели к гибели человека или вызвали серьезный риск таких последствий; (c) нарушение прав ИС, коммерческой тайны или конфиденциальной деловой информации с целью получения конкурентного преимущества; (d) вмешательство в политический или правительственный процесс.

Ответственность государств в «киберпространстве»: элемент нарушения

Ст. 2 Проектов статей об ответственности государств за международно-противоправные деяния

Международно-противоправное деяние государства имеет место, когда какое-либо поведение, состоящее в действии или бездействии:

a) присваивается государству по международному праву; и

b) представляет собой нарушение международно-правового обязательства этого государства.

Нарушение:

- вытекает из существующей нормы обычного или договорного права
- может быть мгновенным или длящимся
- может состоять из серии действий или бездействий (составное деяние)
- может возникать в отношении действий другого государства (помощь или содействие, руководство и контроль, принуждение)

Ответственность государств в «киберпространстве»: квалификация

Кибероперации потенциально могут квалифицироваться как действия, нарушающие:

- обязательство уважать суверенитет других государств
- принцип невмешательства во внутренние дела другого государства
- запрет на применение силы или угрозы силой
- международное право прав человека
- международное гуманитарное право в случае совершения кибероперациий в контексте вооруженного конфликта

НО! отсутствие консенсуса государств по многим аспектам нарушений вне контекста кибероперациий + расхождение позиций о применимости норм МП в киберпространстве + политизация дискурса => ограниченный потенциал квалификации кибероперациий с позиции *lex lata.*

От научной фантастики к правовой науке…

Целеполагание на проект:

- **рассмотреть** более подробно отдельные аспекты применения положений ***lex lata*** в отношении:
  - квалификации кибератак на персональные данные в контексте вооруженных конфликтов
  - применения международного права прав человека в киберпространстве, в том числе экстратерриториальное применение международных договоров о правах человека
- рассмотреть **особенности вменения** кибероперациий государству как необходимого условия применения вторичных норм международного права
- описать индивидуальные и коллективные **меры принуждения**, доступные государствам, пострадавшим от враждебной деятельности в киберпространстве (и, потенциально, третьим государствам)
- **case study** и анализ нескольких киберинцидентов и ответных мер государств с политологической и экономической точек зрения

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Департамент международного права
факультета права
НИУ «Высшая школа экономики»

www. https://pravo.hse.ru/intlaw/

eamartynova@hse.ru