Симанов Егор

ЛЕТНЯЯ ШКОЛА
по управлению интернетом

«I hear there's rumors on the, uh, Internets…»
George W. Bush

Киберпространство, как объект анализа в контексте безопасности.

Что такое «кибербезопасность», «кибервойна», «гибридная война», «информационная война»? В чем отличие между «войной» и «противоборством»? Какую роль играют государства в «киберпространстве»? Кто еще есть в «интернетах» и как этот феномен можно исследовать в строгих рамках современной науки? В рамках каких дисциплин это можно сделать?

Данные вопросы в 2022 году стоят как никогда остро, во-первых, из-за практически всемирной вовлеченности в «интернеты», во-вторых, из-за серьезной конфронтации между разными частями мира. Два этих аспекта поднимают множество сложных проблем и затрагивают многие сферы жизни общества. Например, как можно при единой инфраструктуре и технологической составляющей «всемирной паутины» оставить её всемирной, отрезав кого-то от неё? Или как можно наказать кого-то за противоправные действия (в самом широком понимании - от фишинга, до атак на критическую инфраструктуру), если неизвестно откуда он и чью юрисдикцию применять при поимке? Как идентифицировать персональные данные нарушителя и сохранить персональные данные порядочных граждан? Решить их – значит в очередной раз «закончить историю», отсюда вывод о нерешаемом характере данных проблем и необходимости иначе и уже формулировать вопросы, чтобы понимать, как на них можно ответить.

В данном эссе предлагаю сосредоточиться на узком аспекте безопасности и постараться прояснить часть вопросов из введения. Для этого необходимо описать интернет как систему (в рамках системного анализа в гуманитарных науках), отметить его эволюцию, проследить какая безопасность может быть в данной системе и дать прогноз развития ситуации.

Что такое «интернет»?

В российском законодательстве есть ряд определений так или иначе затрагивающих этот вопрос:

«информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники»[5]

«информационная сфера - совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений».

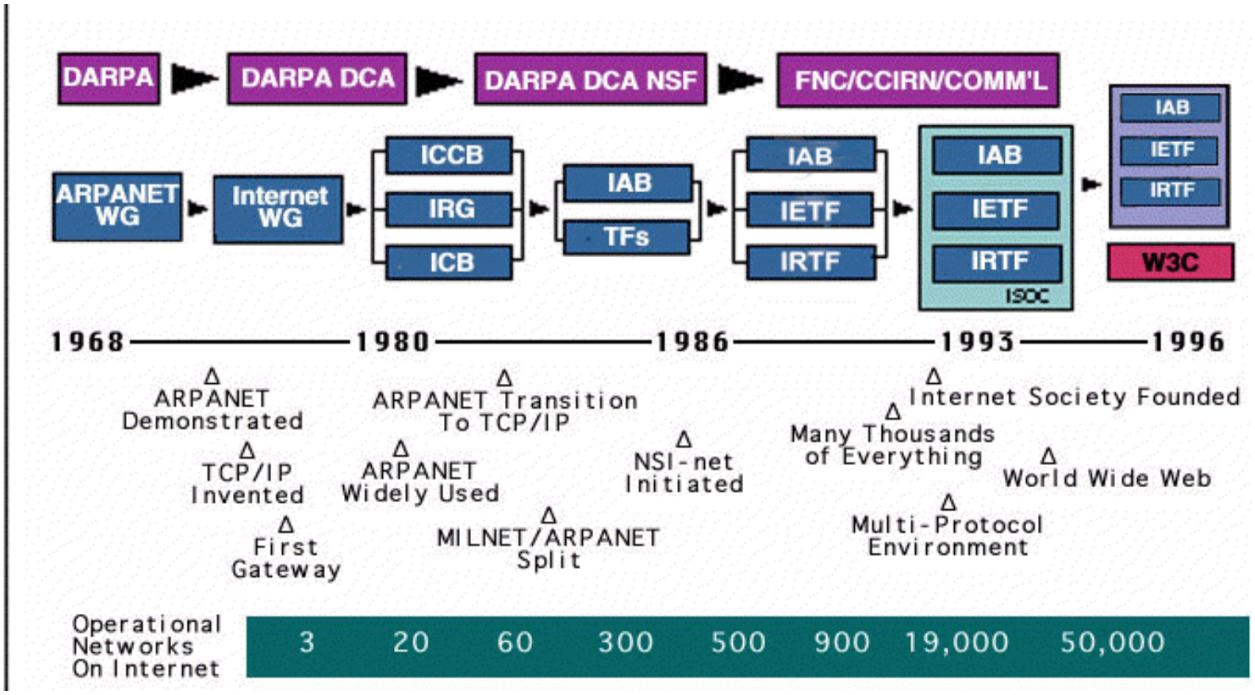
В учебнике по управлению интернетом за авторством Курбалийи [3], в самом предисловии отмечается наличие самых разных трактовок «интернета» и связанных с ним вопросов в зависимости от профессиональной сферы исследователя.

В качестве базового допущения можно сказать что 1) интернет это сеть сетей и 2) интернет это медиум, т.е. информационное наполнение, содержание, контент. От этого универсального определения будем отталкиваться в нашей краткой исторической справке.

Эволюция интернета.

Большинство имеющейся литературы по истории интернета и управления интернетом в делении на исторические эпохи делают акцент на технологических решениях. Например, курс Internet Society "Internet governance"[4] в Модуле 1.История Интернета “сосредотачивается на истории Интернета с точки зрения его технологической истории, его управления, его ранней коммерциализации и управления Интернетом”.

“A Brief History of the Internet” [8] за авторством отцов-основателей интернета выделяет следующие вехи, на основании новых технологических решений и технологий:



Однако, еще никто не делал акцент на истории взаимоотношений между ключевыми игроками создающими, обслуживающими и использующими сам Интернет, что является непосредственным полем для исследования в гуманитарных науках и вопросах безопасности. Для создания адекватного нашему исследованию поля данных следует обратиться к хронологиям и таймлайнам Интернета, например Hobbes' Internet Timeline [9].

1) 1957 год - Создание Управления перспективных исследовательских проектов (ARPA) под эгидой Министерства обороны США, в ответ на запуск СССР первого искусственного спутника земли.

2) 1966-1969 дискуссии специалистов об ARPANET и запуск проекта в рамках научных центров ARPA

3) 1970 - 1978 - техническая обкатка тестирование и налаживание международных связей в рамках исследовательских проектов в США, Великобритании и Франции.

4) 1978 год - разделение протокола TCP на TCP/IP, первая коммерческая спам рассылка

5) 1983 год разделение APARNET на гражданский APARNET и MILNET для нужд военных

6) 1980-е - “война протоколов” (можно проинтерпретировать как борьбу за финансирование в разработке технологических решений для обеспечения работы сетей и как следствие подрядов на них). Поглощение всех участников NSFNET. Вывод сетей и исследовательских центров из под “опеки” военных в гражданское исследовательское русло под “опекой” государства.

7) 1990-1991 годы - создание World Wide Web специалистами CERN

8) 1991 год - US High Performance Computing Act - заложил основы для коммерциализации интернета, объединив разросшиеся исследовательские сети и центры в National Research and Education Network (NREN).

9) 1993 год - Бизнес и медиа начинают обращать внимание на интернет

10) 1995 год - приватизация NSFNET

11) 1996 год - первые ограничения в Интернете:

a) Китай: требует от пользователей и интернет-провайдеров регистрации в полиции

b) Германия: закрывает доступ к некоторым группам новостей на CompuServe.

c) Саудовская Аравия: ограничивает доступ в Интернет университетами и больницами

d) Сингапур: требует от поставщиков политического и религиозного контента государственной регистрации

e) Новая Зеландия: классифицирует компьютерные диски как «публикации», которые могут быть подвергнуты цензуре и конфискованы.

12) 2001 год - Европейский совет завершает работу над международным договором о киберпреступности 22 июня и принимает его 9 ноября. Это первый договор, касающийся уголовных преступлений, совершенных через Интернет.

13) 2003 год - Регистрация домена ogrish.com удалена (11 января) немецким регистратором Joker.com по запросу немецких органов, заявивших о спорном/нарушающим правила контенте; однако был сайт размещен (hosted) в США и соответствовал законам США.

14) 2007 год - Эстония проводит первые общенациональные парламентские выборы онлайн 26-28 февраля

15) 2010 год - 22 января Google заявляет, что вместе с более чем 20 другими американскими компаниями она стала целью кибератаки из Китая, а 22 марта прекращает подвергать цензуре свои услуги в Китае.

16) 2012 год - доменное имя .com канадской компании Bodog, занимающейся спортивными азартными онлайн-играми, было заблокировано Министерством внутренней безопасности США, что вызвало опасения у международных компаний, которые могут нарушать законы США и чьи TLD (Top level domain - домен верхнего уровня) зарегистрированы в реестрах США.

17) 2016 год - Судья окружного суда Калифорнии удовлетворил ходатайство о том, что считается первой разрешенной подачей иска через Twitter

18) 2017 год - Предполагается, что Facebook и другие социальные сети использовались иностранными правительствами для оказания влияния на выборы в США и других странах.

Без сомнения, предложенный найми таймлайн “гуманитарного” поля исследований интернета нуждается в уточнениях и более фундированном выделении дат и эпох, но уже, на собранном нами материале, можно сделать обобщения и выводы. Выделим этапы в истории Интернета:

1. 1950-1980 – технологическое становление Интернета

2. 1980-1990 – закладывание основ для широкого использования разработок и технологий Интернета

3. 1990-2000 – Всемирная паутина, управление, приватизация и коммерциализация Интернета, первые ограничения.

4. 2000- настоящее время – Интернет и Информационное общество

На первом этапе основными пользователями Интернета было профессиональное сообщество, оно было ключевым стейкхолдером и использовало Интернет в своих узких целях. Государство играло роль «ночного сторожа» не вмешиваясь во внутренние дела профессионального сообщества ни на техническом треке (сеть сетей), ни в информационном, финансирование и опека разработок велись под эгидой военных программ.

На втором и третьем этапах, начала происходить постепенная приватизация различных «технических» составляющих интернета и его коммерциализация. Бизнес апробировал различные финансовые стратегии в рамках технического трека и, особенно, медиума. Скорее всего отсюда идет широкое использование технологий маркетинга и пиара, для информационного наполнения. Вовлеченность государства в использование интернета в политических целях можно описать фразой Джорджа Буша младшего «I hear there’s rumors on the, uh, Internets…[10]», но уже встают вопросы регуляции интернет ресурсов и информации.

Четвертый этап скорее всего необходимо разбивать на промежуточные этапы, так как за 22 года практика использования Интернета государством и обществом отошла от «слухов в интернетах», к использованию ресурсов медиума для победы в президентских выборах и обвинений во вмешательстве в них, проведению информационно-психологических операций, слежки за отдельными гражданами и правительствами и т.д. Отдельная периодизация этого этапа достойна собственного исследования, мы же отметим вовлечение государства в вопросы медиума и в вопросы регулирования технической составляющей, с использованием при этом наработок бизнеса и достижений технического прогресса Интернета.

Необходимо обобщить собранный материал по ключевым игрокам и их ролям на каждом из этапов развития Интернета.

Таблица 1. Матрица акторов и эпох

Эпоха\ Игрок	Профессиональное сообщество[1]	Бизнес[2]	Государства
1950-1980	Ключевой стейкхолдер	-	«Ночной сторож». Разработки идут под “присмотром” и при финансировании военных.
1980-1990	Ключевой стейкхолдер	Различные исследовательские технические коллективы боролись за финансирование	Разделение военной и гражданской “опеки”. Перевод исследовательских сетей на государственное гражданское финансирование.
1990-2000	Потеря монополии на интернет	«Атлант расправляет плечи»	«Ночной сторож», но в ряде вопросов – уже регулятор (приватизация)
2000-настоящее время	Один из многих стейкхолдеров	Различная финансовая структура и положение в финансовых моделях «освоенного» интернета	Вмешательство в уже освоенный бизнесом и построенный техническим сообществом мир. “Влиятельный гость” с претензией на то, чтобы стать хозяином в клиенто-патерналистских отношениях с остальными “сожителями”.

Отметим важную роль технологических корпораций и платформ, так как они являются на определенных ступенях иерархии (финансовой и медиума) монополистами или, как минимум, законодателями мод. В ряде случаев они же выступают регуляторами

[1] В рамках профессиональных сообществ мы рассматриваем, как формальные организации, занимающиеся вопросами обеспечения работоспособности протоколов, сетей и соединений, так и неформальные объединения и мнения технических специалистов

[2] Сюда мы включаем технологические корпорации, а так же игроков занимающихся преимущественно коммерческой деятельностью

информационного наполнения интернета, используя отработанные маркетингом и PR-ом стратегии для достижения экономических целей.

В качестве краткого вывода по эволюции интернета подчеркнем, что по мере развития Интернета как всемирной сети именно бизнес начал создавать ряд правил игры в «медиуме» и коммерциализировать его, что происходило лишь на 3 этапе, то есть в 1990-2000 годы. Отсюда особый характер угроз и проблем, связанных с безопасностью данных, прав человека и киберпреступностью, когда Интернет из узкой сферы деятельности специалистов “взорвался” подобно большому взрыву и создал колоссальное пространство медиума. Государства входили в уже функционирующую, наполненную контентом среду со своими правилами игры, в неформальной разработке которых государство не принимало участия, но предоставляло ресурсы в надежде воспользоваться плодами работы специалистов и бизнеса. Интернет используется в самых разных аспектах повседневной жизни, порождая множество «измерений» (финансового, экономического, потребительского, развлекательного, на уровне государств, граждан, отдельных пользователей, международных организаций и т.д.), что затрудняет выработку универсального подхода к регуляции, как на международном уровне, так и на государственном.

Безопасность и интернет.

Безопасность – всегда была, есть и скорее всего будет проклятым вопросом международных отношений. Современные наработки теории международных отношений выделяют самые разные её виды, типологии и категории, зависящие от объекта, подвергающегося угрозам, функционального типа угроз и т.д[2]. Определение безопасности может иметь две трактовки:

1) позитивная - состояние защищенности (угрозы могут существовать, но есть инструменты, институты, которые способны им противостоять).

2) негативное - отсутствие угрозы, то есть отсутствие вызовов и угроз.

Традиционное понимание безопасности в теории международных отношений затрагивает конвенциональную военную и ядерную безопасность. В свою очередь это приводит нас к необходимости обратиться к военным специалистам за особенностями понятия «война». Военная терминология применительно к международным отношениям заставляет нас обратиться к международному праву, чтобы выяснить границы регулирования и нормы применимые к «войнам». Отсюда и термины «warfare» или «противоборство», что оставляет военным и государствам «лазейку» по воздействию на оппонента, выводя действия из юридического и публичного фокуса внимания.

Кроме этого военные специалисты выделяют различные измерения войны[1], которые накладываются на два измерения Интернета (сеть сетей и медиум) и на различные измерения и уровни самого медиума. Что в финальном варианте рождает феномены, имеющие такие газетные заголовки как «гибридная война/противоборство» и «кибервойна», которые уже перекочевали в научную литературу и в доктринальные документы.

Выводы.

Не углубляясь в дискуссию о различных взглядах на безопасность в Интернете можно отметить, что она фокусировалась на негативном аспекте – попытке устранить все угрозы в технической составляющей (например, полное исключение перехвата

информации при передачи пакетов), вызовы правам человека (устранение неправомерного сбора персональных данных), проблемы общественного спокойствия (прекращение информационно-психологического воздействия на население, создание обособленного национального сегмента интернета) и угрозы объектам критической инфраструктуры (пример кибератаки на трубопроводах в США [7] или на завод по обогащения урана в Иране [6]) и проч. Однако с вовлечением государства и переносом межгосударственной борьбы в медиум можно прогнозировать, что все больше в определение угроз в киберсреде/медиуме/Интернете будет входить позитивная трактовка и необходимость разработки решений по противодействию угрозам.

Для обеспечения своих интересов государства будут все больше опекать имеющихся игроков (таких как крупные технологические корпорации, профессиональное сообщества различные сросшиеся с интернетом бизнес структуры) в интернете, а тех, кто опеке противится или не признает, государства будут запрещать. Характер отношений (государство - опекаемый) скорее всего будет различаться в зависимости от глобальных противоборствующих блоков, имеющих свои технические, технологические, экономические и юридические особенности и традиции.

Государства (военные в гос-вах) еще не осознали до конца всю мощь и потенциал Интернета (как новинки техники наподобие танка и самолета или нового способа коммуникации как изобретение телеграфа) для своих целей и их участие на данный момент ограничено отсутствием опыта и непривычным для них характером среды (господство бизнеса и детерминированная научным и профессиональным сообществом децентрализованная физическая структура интернета как сети сетей).

Список источников и литературы:

1. Кокошин А.А. Несколько измерений войны // Вопросы философии. 2016. № 8.
2. Кулагин В.М. Современная международная безопасность : учебное пособие / В.М. Кулагин. — М. : КНОРУС, 2012. — 432 с. — (Для бакалавров).
3. Курбалийя Й., Управление интернетом, 2016.
4. Онлайн курс “Internet governance” разработки Internet Society. URL: https://www.internetsociety.org/issues/past-categories/internet-governance/
5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
6. Федуненко Е., Чернышева Е. Кибератаки на ядерные объекты., Коммерсантъ, 20.01.2017., URL: https://www.kommersant.ru/doc/3196397
7. Шакиров О. Зашифрованные отношения: как атака на трубопровод Colonial Pipeline может помочь России и США наладить диалог., Forbes., 15.05.2021., URL: https://www.forbes.ru/obshchestvo/429281-zashifrovannye-otnosheniya-kak-ataka-na-truboprovod-colonial-pipeline-mozhet
8. “A brief history of the Internet”, ACM SIGCOMM Computer Communication Review. Volume 39, Number 5, October 2009
9. Hobbes' Internet Timeline by Robert H'obbes' Zakon. URL: https://www.zakon.org/robert/internet/timeline/
10. "Transcript of the third Gore-Bush presidential debate". Commission on Presidential Debates. 2000-10-17. Retrieved 2010-03-15