

Эрик Шмидт, Джаред Коэн

Новый цифровой мир

Как технологии меняют жизни людей, модели бизнеса и понятие государств

Оглавление

Введение	1
Глава 1. Наше будущее «Я»	1
Глава 2. Будущее личности, государства и персональных данных.....	2
Глава 3. Будущее государства	3
Глава 4. Будущее революций	4
Глава 5. Будущее терроризма	5
Глава 6. Будущее конфликтов, войн и иностранного военного вмешательства	7
Глава 7. Будущее возрождения страны.....	9
Заключение	10

Введение

- Интернет относится к тем изобретениям, которые люди создали, но пока не поняли до конца
- По мере расширения интернета, мы будем по-новому на него смотреть
- Коммуникационные технологии очень быстро распространяются по планете
- Растет как область применения электронных устройств, но также их скорость и вычислительная мощь
- Люди станут чаще замечать, что живут в двух мирах – реальном и виртуальном
- ИТ будут влиять на концентрацию власти
- Объединение людей в сети – это и достоинство, и недостаток
- Будут создаваться как реальные личности, так и виртуальные
- ИТ приведет к обострению конкуренции
- ИТ будут помогать восстанавливать страны после катаклизмов
- Эффект масштаба будет использоваться и в ИТ

Глава 1. Наше будущее «Я»

- Цели государств останутся теми же, но средства их достижения изменятся.
- У граждан будет две личности – в физическом мире и в виртуальном.
- С развитием ИТ, человек, который хочет быть продуктивным, будет иметь для этого больше возможностей.
- Изменяется (упрощается) интерфейс взаимодействия с техникой («суррогаты»)

- Всеобщий доступ в сеть должен помочь странам выявить свои конкурентные преимущества
- Бывают нишевые инновации, которые требуются в развивающихся странах, а в развитых просто не бывает таких проблем, которые приводят к изобретению таких нишевых инноваций
- Удаленное образование, предустановленный учебный контент в моб.устройства
- Элементы виртуальной реальности
- ИТ-медицина
- Бедные станут жить чуть лучше, богатые будут жить еще лучше

Глава 2. Будущее личности, государства и персональных данных

- Развитие критического мышления
- Люди и гражданское общество могут влиять на государства
- Способы контроля информации
- Индексация детей с самого рождения
- Сервисы, показывающие всю правду о виртуальной личности человека
- СМИ трансформируются, новостные агентства будут подтверждать те новости, которые будут появляться мгновенно (твиттер и тд)
- Появится куча новых некачественных СМИ от знаменитостей
- Тайна частной жизни
- Защита персональной информации
- Для демократических стран – доступность информации позволит сделать государство еще лучше
- Для авторитарных стран – возможность увеличить цифровые репрессии, контроль за вирт.личостями
- Мобильные устройства позволят распространять новости почти мгновенно по всей территории даже самой большой и закрытой страны
- Мобильные технологии закрывают те прорехи, которые допускают несостоятельные правительства (культурное развитие, сообщества для общения и тд)
- В неразвитых государствах ИТ-преступность будет расти
- Ответственность ИТ-компаний за персональные данные людей
- Репутация компаний (по защите перс.данных) будет важнее их официальных соглашений о защите данных
- Для ИТ-компаний нужно будет нанимать больше юристов, так как исков против авторских прав и тд будет еще больше
- ИТ-компании будут задумываться о человеческой этике и человеческом поведении
- Личную информацию государства будут пытаться защищать с помощью законов
- Каждая страна будет определять, что является секретными личными данными, а что доступно для всех
- НКО будут использовать ИТ в своей деятельности
- Пиринговые сети (связь двух компьютеров без третьей (контролирующей) стороны), связь без интернета
- Дополненная реальность
- Получение данных от органов чувств человека
- По-настоящему безопасных соединений компьютеров не существует
- Возможность блокировать соц.сети в критических ситуациях

- Анонимность в сети имеет как отрицательные, так и положительные стороны (доносы на коррупцию, наркокартели и тд)
- В демократических странах – усиление позиции граждан, появление более честных политиков и укрепление соц.контрактов
- Тоталитарные режимы живут только там, где плохо развито ИТ. Где развита ИТ, там тоталитарные режимы трансформируются (они не запрещают смартфоны, а используют их)
- Тоталитарный режим может создать режим с тотальным контролем виртуальных личностей, но это будет слишком дорого
- Биометрические данные (определение, использование – голос, ДНК, отпечатки, лица)
- Смартфон окажется для спецслужб опаснее пистолета

Глава 3. Будущее государства

- Интернет трансформируется в сеть национальных подсетей
- Фильтрация интернета (например, Китай)
- Три уровня фильтров – агрессивный, умеренный, свободный
- Чтобы заходить в национальные сегменты, нужны будут подопытия электронных виз
- Создание двух уровней интернета: глобальный и национальный (в последнем – жесткая цензура, возможно – даже интранет без выхода в глобальный интернет)

Виртуальные союзы

- Авторитарные государства будут объединяться, чтобы обмениваться технологиями фильтрации интернета
- Демократические государства будут так же объединяться, чтобы противодействовать закрытости и интернета
- Новый вид вооружения – кибервойска и техническая поддержка
- Можно будет экспортировать (как гуманитарную помощь) разворачивание в стране оптоволоконка и строительство вышек связи
- Юридические войны за соблюдение авторских прав

Цифровые провокации и кибервойска

- Худшее – развязывание кибервойн
- Их будут использовать как государства, так и террористы
- Кибервойны уже идут, только обычные люди с ними почти не встречаются
- В виртуальном мире государства будут позволять себе то, что непозволительно в реальном
- Многие вирусы разрабатывают государства, например, Stuxnet специально для ядерного разоружения Ирана
- Большинство кибератак нельзя идентифицировать, никаких реальных доказательств нет
- Государства будут предлагать свои ресурсы за технологическую помощь
- Государства-сверхдержавы будут формировать свои онлайн-сферы влияния

Новая холодная война

- Онлайн-шпионаж, вирусы и тд уже называют новой холодной войной
- Эта новая война будет многополярной
- Сильно разрастутся действия через посредников

- Кибер-шпионаж для коммерческих компаний
- Для устранения DDoS'а предлагается режим карантина – отключать зараженный компьютер от сети
- Навыки кибер-атакующих растут так же, как и защитников
- Кибер-ошибок будет очень много

Глава 4. Будущее революций

- Современные технологии, какими бы они мощными ни были, не могут сотворить чуда, хотя и способны значительно повысить шансы на успех
- Лидерам протеста не хватает политического опыта

Легче начать...

- Многие революционные лидеры будут молоды
- Вспыхнет много протестных движений
- Будут активисты «по совместительству», которые сами выбирают, когда и где протестовать
- Оппозиционные группы будут объединять множество территорий, чаще всего – по религиозному принципу и языку
- Онлайн-платформы для революций, которые позволят быть анонимными их участникам
- Но революции делаются людьми, выходящими на улицу. Онлайн-лидер должен уметь вывести людей
- Будет много «революционеров-туристов», людей, которые прочесывают интернет в поисках революционных движений

...Но труднее закончить

- Если человек не обладает чертами, необходимыми для управления государством, то ему не помогут никакие технологии
- В онлайн-эпоху человек быстро может стать популярным, но завершить революцию не сможет
- У лидеров очень мало времени на «созревание»
- де Голль и Черчилль не могли появиться в онлайн-эпоху
- Революционеры-знаменитости не обладают «толстой» политической кожей
- ИТ помогут искать лидеров
- Создание виртуальных фронтов, но никакой реальной пользы они могут и не принести
- Из-за этого и из-за всеобщей гласности, жители стран будут критически относиться как к правительству, так и к оппозиции
- В дальнейшем, от революционных лидеров потребуют плана жизни страны после революции
- После «успешной» революции, нередко к власти приходят люди, которые не могут управлять страной, поэтому революции возникают снова
- Реализация правительством открытости и доступности информации о своей деятельности, чтобы снизить интерес к революциям

Виртуальные репрессии и виртуальное сдерживание

- Репрессивные режимы будут отключать связь

- Но это будет приводить к разжиганию конфликтов, так как конфликт – важен каким-то конкретным людям, а интернет важен всем
- Возможно, будет сообщество операторов сотовой связи под эгидой ООН
- Государства будут использовать превосходство над гражданами в ИТ (будут следить за всеми), и сумеют предотвращать восстания
- Авторитарные правительства уже не будут проводить жесткие репрессии в цифровую эпоху, так как вся информация сохраняется
- Они будут применять «виртуальное сдерживание» - давать гражданам возможность «сбросить пар» в интернете, то есть, оппозиционное движение под крылом государства
- Авторитарные государства будут следить за этой онлайн-активностью, а потом арестовывать активистов тогда, когда до восстания будет оставаться несколько дней
- Будут показательные процессы за коррупцию, с наказанием некоторых политиков, но само государство будет двигаться дальше
- Никто точно не сможет спрогнозировать, к чему могут привести виртуальные восстания

Последняя «весна»

- Чем больше стран получают интернет, тем более вероятно восстание в них
- Информационные технологии не создали связи между людьми, а только усилили их
- Религиозные сообщества так же будут использовать ИТ
- За счет доступности информации, страны (где могут произойти восстания), будут учиться на чужих ошибках и предотвращать свои
- Государства будут разрабатывать эффективные ИТ-инструменты онлайн-сдерживания
- Например, нынешний Китай. Интернет приведет к какой-то форме революции там, но какой она будет – никто не знает
- Революции будущего смогут привести к смене режима, но не обязательно смогут привести государство к демократии
- Революцию сделать можно довольно быстро, но отсутствие сильных, самостоятельных лидеров приведет к тому, что будет много государств со склонным к авторитаризму правительством
- Революция – это стремление групп людей изменить нынешний мир, но найдутся люди, которые хотят это сделать в одиночку и более агрессивными методами – революционеры.

Глава 5. Будущее терроризма

- ИТ – это средство мощное, а порой и разрушительное
- Террористы будут и в мире реальном, и в виртуальном
- Благодаря соц.сетям, атаки террористов получают большой резонанс
- Но развитие ИТ сделает жизнь террористов хуже

Новые рубежи, новые риски

- С помощью интернета можно найти технологию создания взрывных устройств
- Развитие дронов делает возможным доставку взрывчатки по воздуху
- Также будет развиваться кибертерроризм
- Мишенью кибератак могут стать транспортная система, полиция, фондовая биржа, электрические сети и т.д.

- Будущие похитители людей будут красть не физических людей, а их «виртуальные личности»
- Террористы будут использовать онлайн-платформы для поиска исполнителей
- Террористы будут пиариться в интернете
- Они будут проникать в телекоммуникационные компании, будут создавать приложения для своей популяризации
- Руководители террористических организаций смогут отдавать команды через телефоны, даже из тюрьмы
- Глушить связь не получится, все-равно будут находить способы обхода
- Полицейские будут использовать «зараженные» смартфоны для сбора информации
- Власти будут делать всё, чтобы «виртуальная личность» человека, попадавшего в тюрьму – изымалась из интернета, чтобы человек исчезал

Активизация террористов-хакеров

- Буду организовываться группы людей, которые будут атаковать кого-то определенного, например, как это делает WikiLeaks
- Но будут и такие, кто захочет выступать не за свободу слова, а за убийства
- А за счет анонимности в интернете, будет очень сложно понять – кто вообще всё это делает
- В начале эпохи ИТ, чтобы стать кибертеррористом – нужны были технические навыки. Сейчас этот барьер сглаживается
- Будут создавать специальные инженерные лагеря террористов, где будут стоять компьютеры и где будут учиться программировать
- Будут государства, которые поспособствуют росту кибертерроризма
- Но набор молодых «хакеров» приведет к тому, что сама террористическая организация будет на краю гибели, так как молодые легче срываются и могут всех сдать
- Многие страны станут взаимодействовать в области противодействия кибертерроризма
- Государства будут еще больше привлекать на свою сторону бывших хакеров

Ахиллесова пята террористов

- Развитие ИТ приведет к тому, что, поймав одного террориста со смартфоном – можно будет найти всю сеть
- Но и использование телефонов сделает теракты еще более кровавыми
- Террористов можно будет вычислять по звонкам их родственникам и друзьям
- Люди ошибаются, террористы тоже, так что будет легче найти сеть террористов до теракта
- Незнание навыков ИТ приведет к тому, что террористы будут пользоваться собственными аккаунтами в соц.сетях – полиция их будет быстро хватать

Никаких людей-невидимок

- С течением времени, власти будут вести список людей, которых нет ни в одной соц.сети – скорее всего, таким людям есть что скрывать
- В дальнейшем будут созданы единые базы данных информации на человека (сейчас эта информация разрозненная)
- Создадут алгоритмы, которая будет эту информацию анализировать и принимать решения, террорист человек или нет
- Но люди будут бороться за сохранение тайны частной жизни
- Скорее всего, алгоритмы победят. Правительства будут собирать и анализировать огромные массивы данных о людях, и будут это использовать

- Следующий шаг – верифицировать данные, чтобы не захлебнуться в этом массиве информации
- Будут ставиться цифровые водяные знаки и тд
- С помощью ИТ не защитить людей от влияния терроризма, нужно общаться с людьми
- Победить терроризм смогут две вещи: власть закона и возможности в жизни
- Область ИТ может создать возможности для угнетенных молодых людей, которые часто становятся исполнителями террористических актов
- Благодаря интернету будут появляться новые рабочие места
- Будет создавать контент для таких «групп риска», сами люди смогут это делать, реализовывать себя, забудут постепенно про терроризм
- ИТ-продуктами будут пользоваться не только обычные люди, но и террористы, так что ИТ-конторам придется разрабатывать средства противодействия
- Разница между безопасностью и цензурой очень тонкая, но люди будут понимать, что это нужно
- Терроризм был и будет всегда, но в эпоху интернета за террористами намного больше «глаз» наблюдает, и им будет намного сложнее
- За счет интернета, отдельные террористические акты могут вылиться в большие конфликты

Глава 6. Будущее конфликтов, войн и иностранного военного вмешательства

- Настоящие новости - плохие новости
- Нам кажется, что насилия сейчас очень много (из-за фоток и видео в интернете), но сейчас очень мирное время
- Хоть ИТ и помогает сократить кол-во насилия, оно все-равно останется частью нашей жизни

Меньше геноцида, больше дискриминации

- Есть важная причина конфликтов (но не единственная) - систематическая дискриминация и преследование меньшинств
- Например, можно удалить всю информацию о меньшинствах
- Увеличится мощь виртуальных гонений, могут им блокировать доступ в сеть
- Государство может давать преференции тем меньшинствам, которые будут с ним сотрудничать
- Виртуальную дискриминацию смогут делать не только государства, но и все остальные, даже частные лица

Конфликт с участием нескольких сторон

- Отношение к конфликту будет определяться исходом информационных войн между сторонами
- Равенство пропагандистских возможностей будет сильно влиять на отношение к конфликту мирного населения
- Данные информационного конфликта не то же самое, что данные разведки. Нужно их разделять и выделять главное
- Если есть гос.ресурс - то проводить информационную войну проще
- Но это приведет к всплеску дезинформации
- Способ решения - цифровая верификация контента

- Могут быть созданы международные группы мониторинга и проверки информации
- Эти группы будут изучать данные, а не политику. Но, и здесь тоже будет коррупция
- Участники конфликтов будут атаковать и виртуальные активы сторон
- Возможно, скоро атаки будут настолько сильны, что смогут отключать электростанции, блокировать поезда, линии электропередач и тд
- Коллективная мудрость
- Невозможность удаление информации
- Ответственность за контент перед обществом
- Международный суд будет иметь возможность получить всю необходимую информацию
- Виртуальные свидетельства для суда (верифицированные)
- Программы онлайн-защиты свидетелей
- Облачное хранение данных (свидетельских показаний) поможет свидетелям, например, после того, как видео залили в облако - телефон можно уничтожить

Автоматическое оружие

- Появится виртуальный фронт
- Робототехника, искусственный интеллект, БПЛА
- Интеграция ИТ в военные технологии
- Роботы не боятся пуль
- Они будут использоваться как для разведки, так и для нападения
- Но от солдат-людей не откажутся, так как люди могут использовать интуицию, братство и тд
- Солдаты будут больше и чаще использовать ИТ в войне
- Создание новых вооружений тормозится долгой процедурой гос.закупок
- Можно использовать коммерчески готовые продукты
- Уже нет однополярного ИТ-мира
- Легкие и недорогие БПЛА можно будет легко купить и использовать для терроризма
- Так что полеты БПЛА будут лицензироваться
- В дальнейшем, противники уже не будут уничтожать технику противника, а будут ее взламывать и забирать себе, или направлять против бывших хозяев
- Распространение БПЛА и роботов приведет к увеличению количества конфликтов в мире, поэтому будет разработан договор по сокращению их количества
- Снизится смертность солдат
- Но в роботах и БПЛА будут и ошибки, которые могут приводить к фатальным последствиям
- Солдаты будут находить способы бороться с технологиями, и так будет всегда
- Остается открытый вопрос - кто будет нести ответственность за робота, который убьет ребенка/не солдата?

Новые способы вмешательства

- В конфликты могут вмешиваться не только государства, но и физические лица
- Скорее всего, ООН не сможет быстро измениться под новый мир
- При конфликтах, страны, которые помогают, могут организовывать гуманитарную техническую помощь по восстановлению интернета
- Маленькие страны будут создавать мощные технологичные военные органы, которые можно «виртуально» отправлять в точки конфликта, а не физически
- Технологические компании тоже будут участвовать в конфликтах, естественно, виртуально

- После завершения конфликта – в этой стране открываются огромные возможности для использования ИТ.

Глава 7. Будущее возрождения страны

- ИТ не способно предотвратить стихийное бедствие и остановить гражданскую войну
- Но ИТ могут сделать менее болезненным процесс восстановления страны
- При восстановлении будут стараться, в первую очередь, восстанавливать связь
- С помощью восстановленной связи, люди смогут связываться друг с другом, искать потерявшихся и тд
- Первая компания, восстановившая связь после конфликта, может стать чуть ли не монополистом в этой стране
- Даже в бедных странах связь очень и очень важна
- Лидерами процесса возрождения стран будут телекоммуникационные компании
- Начинают появляться (или развиваться) «цифровые олигархи»
- Мир становится все более взаимосвязанным
- За счет соц.сетей можно очень быстро узнать что происходит в локальных странах
- Если нет регуляции со стороны правительства – можно построить телекоммуникационную сеть с очень низкими тарифами (Ирак, Сомали и тд)
- Информационные технологии помогут защитить частную собственность, ведь вся инфа хранится онлайн, а не на бумаге
- Будут создавать «бекап» правительства – будут создаваться копии институтов в онлайн, без офисов, в облаке
- Правительства, отправленные в изгнание, смогут работать из других стран

Предприимчивость и эксплуатация

- В результате глобального доступа к сети, появится больше волонтеров, которые готовы помогать в развитии страны
- В цифровую эру маркетинг будет играть заметную роль, даже для НКО
- Благотворительные организации-стартапы будут вести более агрессивный характер, получают деньги – но потеряют их из-за отсутствия опыта
- В результате этого процесс оказания помощи будет замедляться
- Помощь эффективнее всего будет оказываться специалистами из самой страны. На специально разработанных сайтах будут размещаться призывы о помощи, специалисты, находящиеся рядом, будут читать эти призывы и помогать
- Такие сайты будут строить партнерские отношения с крупными НКО
- Но распределение помощи будет менее равномерным
- В будущем должны будут исчезнуть неповоротливые традиционные благотворительные организации, которые создают дистанцию между получателями помощи и теми, кто ее оказывает

Пространство для инноваций

- Оно существует всегда, даже в разваленной стране
- Возможно, кризисы будут инициировать правительства стран, чтобы подстегнуть инновации
- Современные технологии позволят повышать уровень безопасности граждан
- Будут привлекать к процессу восстановления страны и жителей этой страны
- ИТ позволяет доказать владение недвижимостью даже если подделаны документы; позволяет найти редкие драгоценности и тд

- Например, крупные страны-производители оружия могли бы договориться вставлять чипы в каждый ствол. Тогда поиск тайников с оружием стал бы намного проще
- Можно менять оружие на мобильные устройства, в кризисных странах связь очень важна, а оружия очень много, есть что менять
- Если не решить проблему перевооружения – может получиться новый конфликт
- ИТ повлияет и на суды, они будут работать быстрее
- В судах будут использоваться электронные доказательства, но они должны быть верифицированы

Заключение

- За короткий срок произойдет столько изменений, сколько не знало ни одно поколение людей
- Каждые два дня появляется столько цифрового контента, сколько было создано за весь период с момента возникновения цивилизации до 2003 года
- ИТ будут столь же повсеместны, как электричество
- Сдерживать развитие ИТ (интернета) не получится
- ИТ не спасут от всех проблем
- Виртуальное пространство не изменит и не улучшит существующий мировой порядок
- Государствам придется проводить по две внешних и по две внутренних политик – виртуальная и реальная
- Благодаря ИТ люди получают очень большую власть. Но пользователи не должны забывать о защите своих персональных данных
- Будут созданы новые возможности шифрования данных
- Произойдет взаимовлияние виртуальной и материальной цивилизации, а баланс между ними определит, каким станет наш мир
- Развитие технологий и доступ в интернет помогают бороться со злоупотреблениями, страданием и насилием
- Мы не можем уничтожить неравенство и ненависть, однако, давая людям технологии, мы в состоянии изменить баланс сил в их пользу в надежде, что люди найдут им применение.