18й НАЦИОНАЛЬНЫЙ ФОРУМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНФОФОРУМ 2016

НАЦИОНАЛЬНЫЙ ИНСТИТУТ ИССЛЕДОВАНИЙ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

НИИГлоБ

NATIONAL INSTITUTE FOR RESEARCH OF GLOBAL SECURITY

IV ПРОМЫШЛЕННАЯ РЕВОЛЮЦИЯ (INDUSTRY 4.0): ИНФОРМАЦИОННЫЕ РИСКИ ДЛЯ РОССИИ

АНАТОЛИЙ ИВАНОВИЧ СМИРНОВ

Президент НИИГЛОБ,

Член Экспертного совета Комитета Госдумы РФ по безопасности и противодействию коррупции,

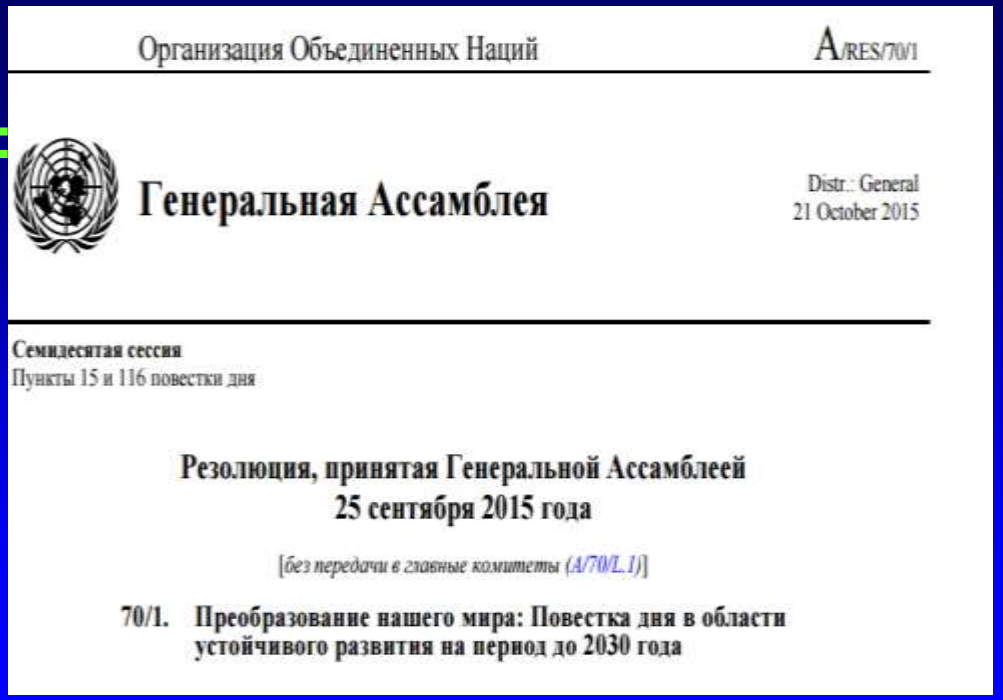
Чрезвычайный и Полномочный Посланник РФ в отставке,

Член бюро президиума РАЕН, д.и.н, профессор МГИМО(У)

http://niiglob.ru aismirnov@niiglob.ru

Резолюция ГА ООН 70/1 Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 г.

п.35. Обеспечение устойчивого развития невозможно без мира и безопасности, а без устойчивого развития мир и безопасность окажутся под угрозой…



Организация Объединенных Наций A/RES/70/1

Генеральная Ассамблея

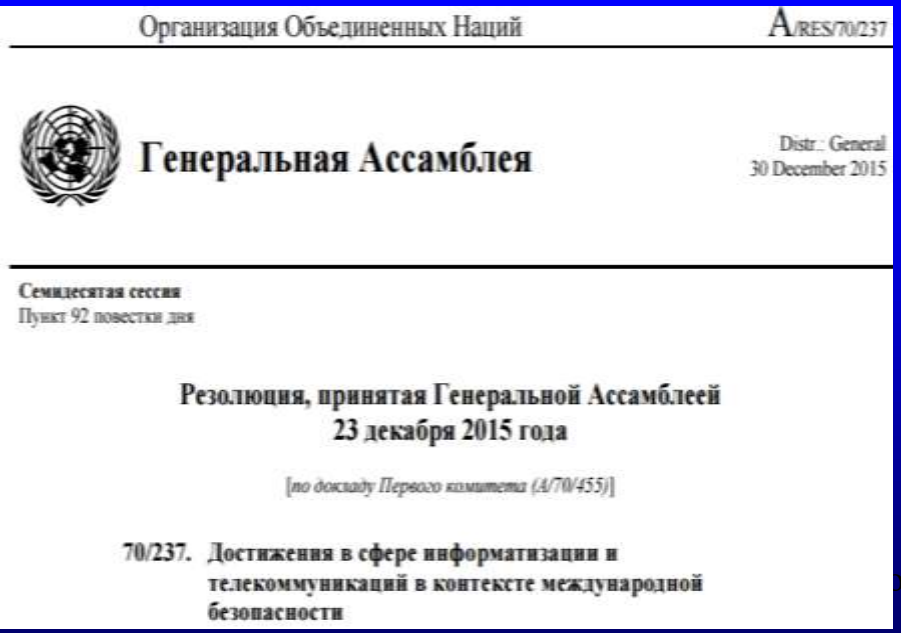
Distr.: General
21 October 2015

Семидесятая сессия
Пункты 15 и 116 повестки дня

Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года

[без передачи в главные комитеты (A/70/L.1)]

70/1. Преобразование нашего мира: Повестка дня в области устойчивого развития на период до 2030 года



Организация Объединенных Наций A/RES/70/237

Генеральная Ассамблея

Distr.: General
30 December 2015

Семидесятая сессия
Пункт 92 повестки дня

Резолюция, принятая Генеральной Ассамблеей 23 декабря 2015 года

[по докладу Первого комитета (A/70/455)]

70/237. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Резолюция ГА A/RES/70/237 (23.12 2015 по докладу Первого комитета (A/70/455)

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента России 31 декабря 2015 г. № 683)

п.21.«Все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории.»

п.70. Для решения задач национальной безопасности в области науки, технологий и образования необходимы:

- развитие перспективных высоких технологий (генная инженерия, робототехника, биологические, информационные и коммуникационные, когнитивные технологии, нанотехнологии, природоподобные конвергентные технологии);

Посыл о том, что инфогенные риски приобрели стратегическое значение в матрице национальной безопасности, подтверждается, в частности, тем, что в Стратегии содержится 36 обращений к понятию «информационная» (в Стратегии 2009 г. было 23).

Из заявления Секретаря Совбеза РФ Н.П.Патрушева «О четвертой международной встрече высоких представителей, курирующих вопросы безопасности» (Владивосток, 2-4.07.13)

- «С интересом заслушано сообщение делегации РФ о современном этапе конвергенции наук и технологий как альтернативного ответа на новые вызовы и угрозы глобального характера. Подчеркивалась необходимость формирования нового эффективного международного механизма обеспечения безопасного развития и использования конвергентных технологий».
- Четвертая промышленная революция, более известная как «Индустрия 4.0», получила свое название от инициативы 2011 г., возглавляемой бизнесменами, политиками и учеными, которые определили ее как средство повышения конкурентоспособности промышленности ФРГ через интеграцию «киберфизических систем» (CPS) в заводские процессы
- «Данные для «Индустрии 4.0», собираются не национальными компаниями, а четырьмя фирмами из Кремниевой долины, — заявил министр экономики ФРГ З. Габриэль. — В этом наши опасения».
- Другая проблема: создание безопасных сетей. Интеграция физических систем с Интернетом делает их уязвимыми к кибератакам.

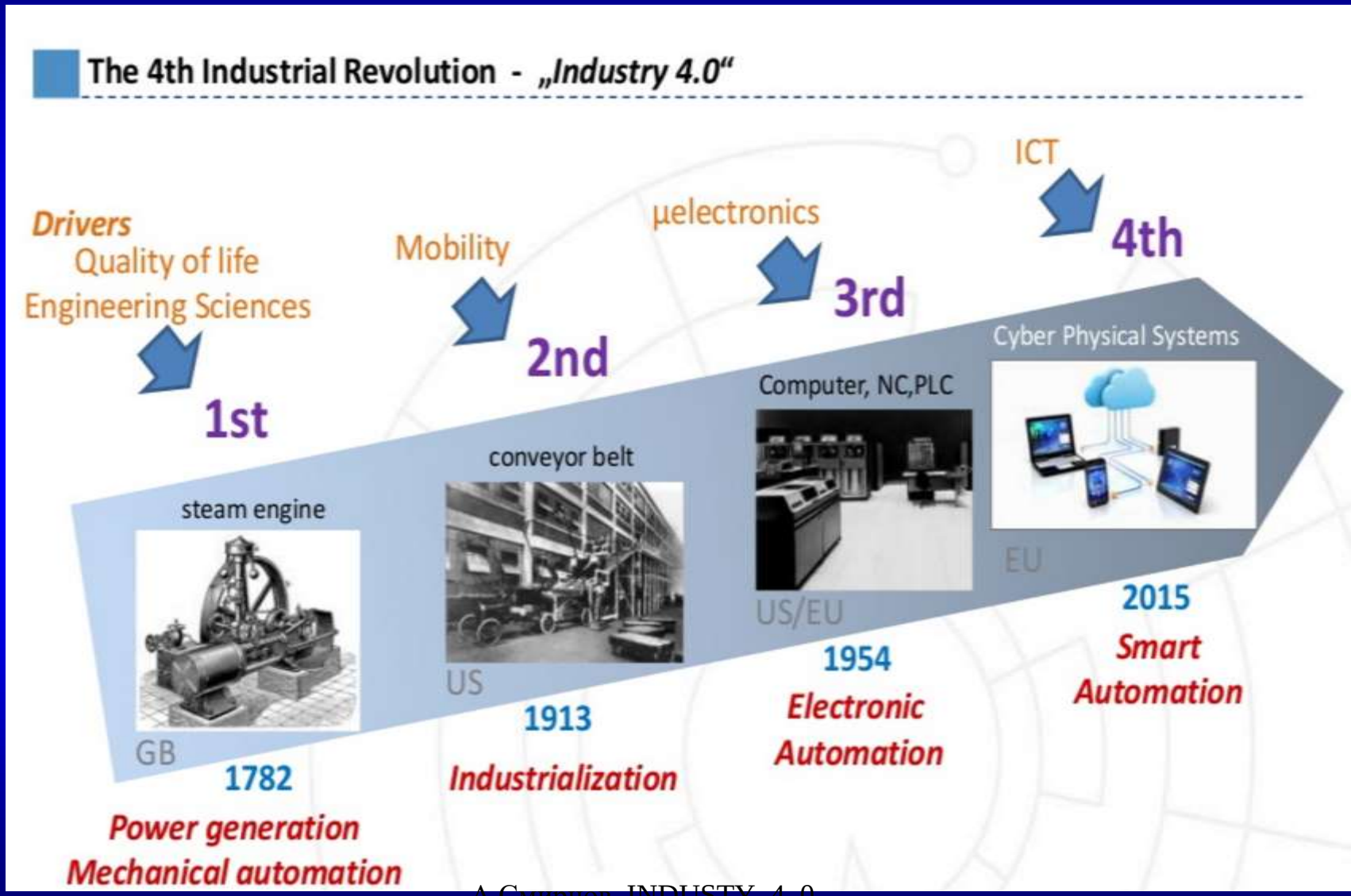
Титульная тема Всемирного экономического форума в Давосе: “IV промышленная революция» (20-23.01. 2016 г.)

На открытии Форума его президент Клаус Шваб подчеркнул:

- Человечество стоит перед новой промышленной революцией, которая кардинально изменит нашу жизнь, работу и отношение друг к другу
- В **первой** промышленной революции сила воды и пара позволила механизировать производство
- Во **второй** электроэнергия использовалась для организации массового производства
- В **третьей** ИКТ автоматизировали производство
- **Четвертая** промышленная революция:

сочетание технологий, стирающих границы между физической, цифровой и биологической сферами (Интернет вещей (IoT), смарт-ткани, киберфизические системы (CPS) и др).

ЭВОЛЮЦИЯ ПРОМЫШЛЕННЫХ РЕВОЛЮЦИЙ



Мегатренды: ИКТ – локомотив пятого технологического уклада и основа - шестого (НБИК – технологий)

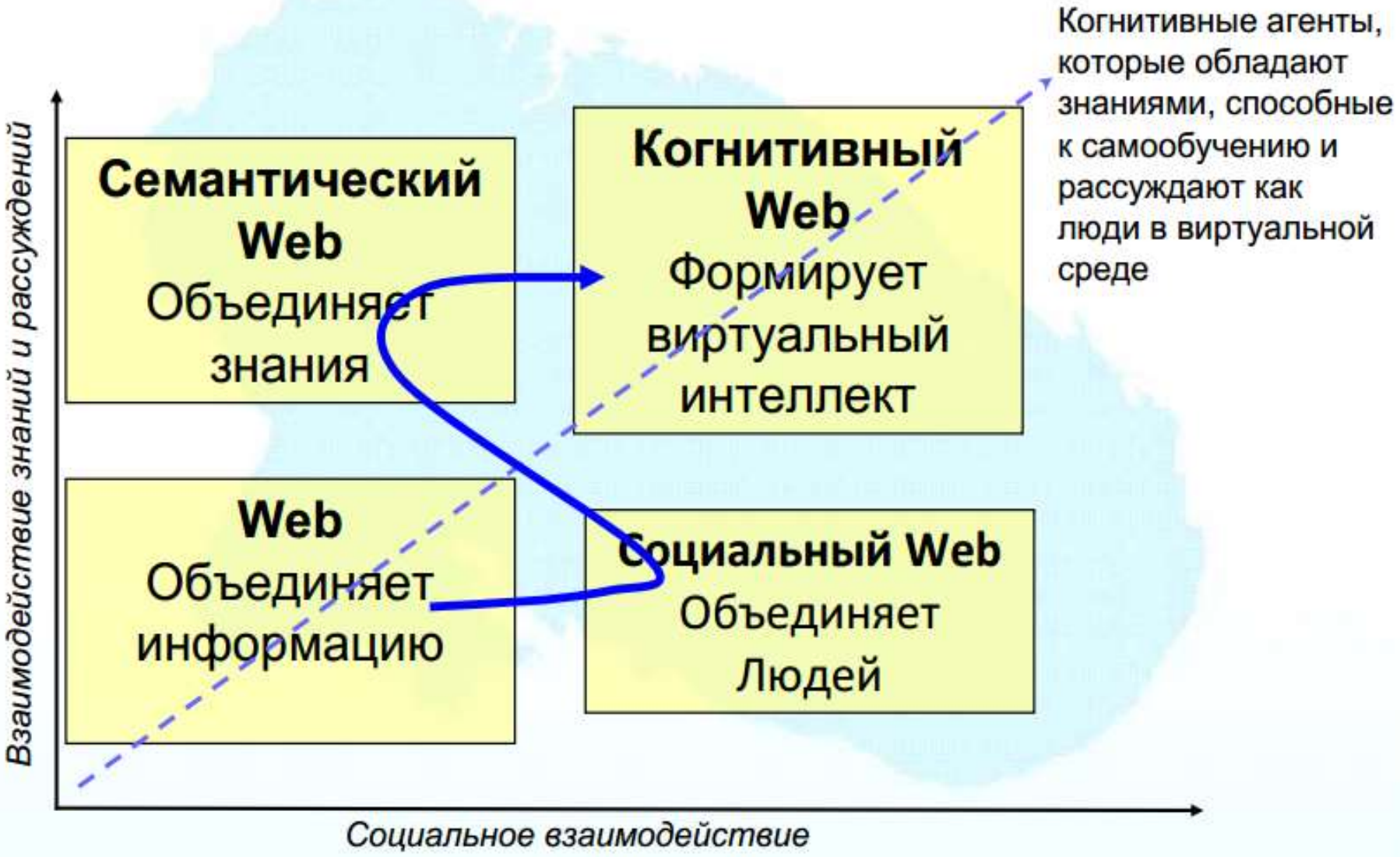
В России принято понятие «технологический уклад» - комплекс технологий инноваций, лежащих в основе количественного и качественного скачка в развитии производительных сил общества (акад. С.Глазьев)

2014-2019 гг. - глобальный кризис, война за технологическое лидерство и доминирование в мировой экономике

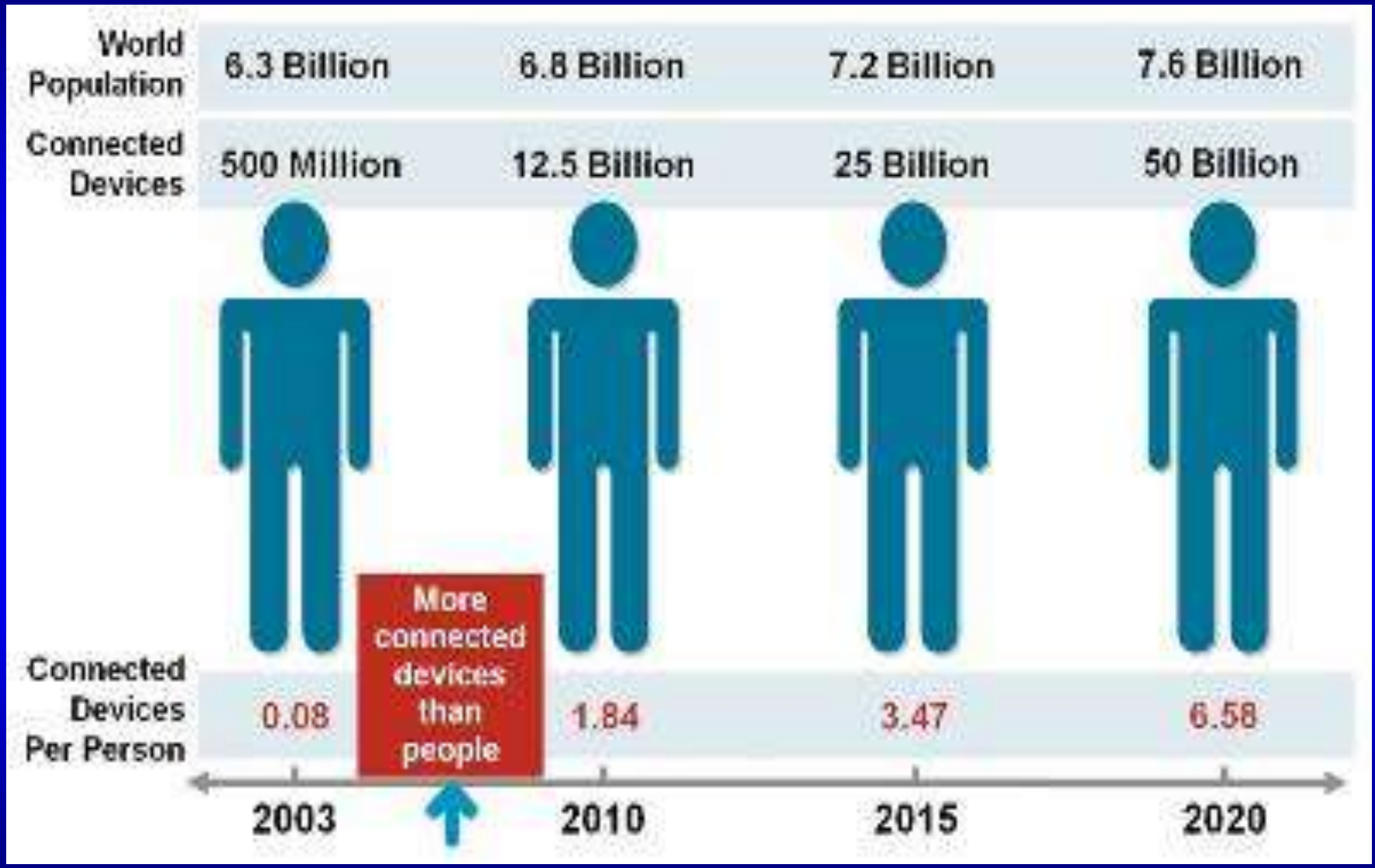
Анализ циклов накопления капитала, циклов Кондратьева, циклов накопления Кузнеца и деловых циклов показывает:
мир проходит крайне опасный момент совпадения нижних поворотных точек всех этих циклов, что создает опасный резонанс для потрясений

В контексте Industry 4.0 и НБИК – технологий

Конвергенция когнитивных и web-технологий

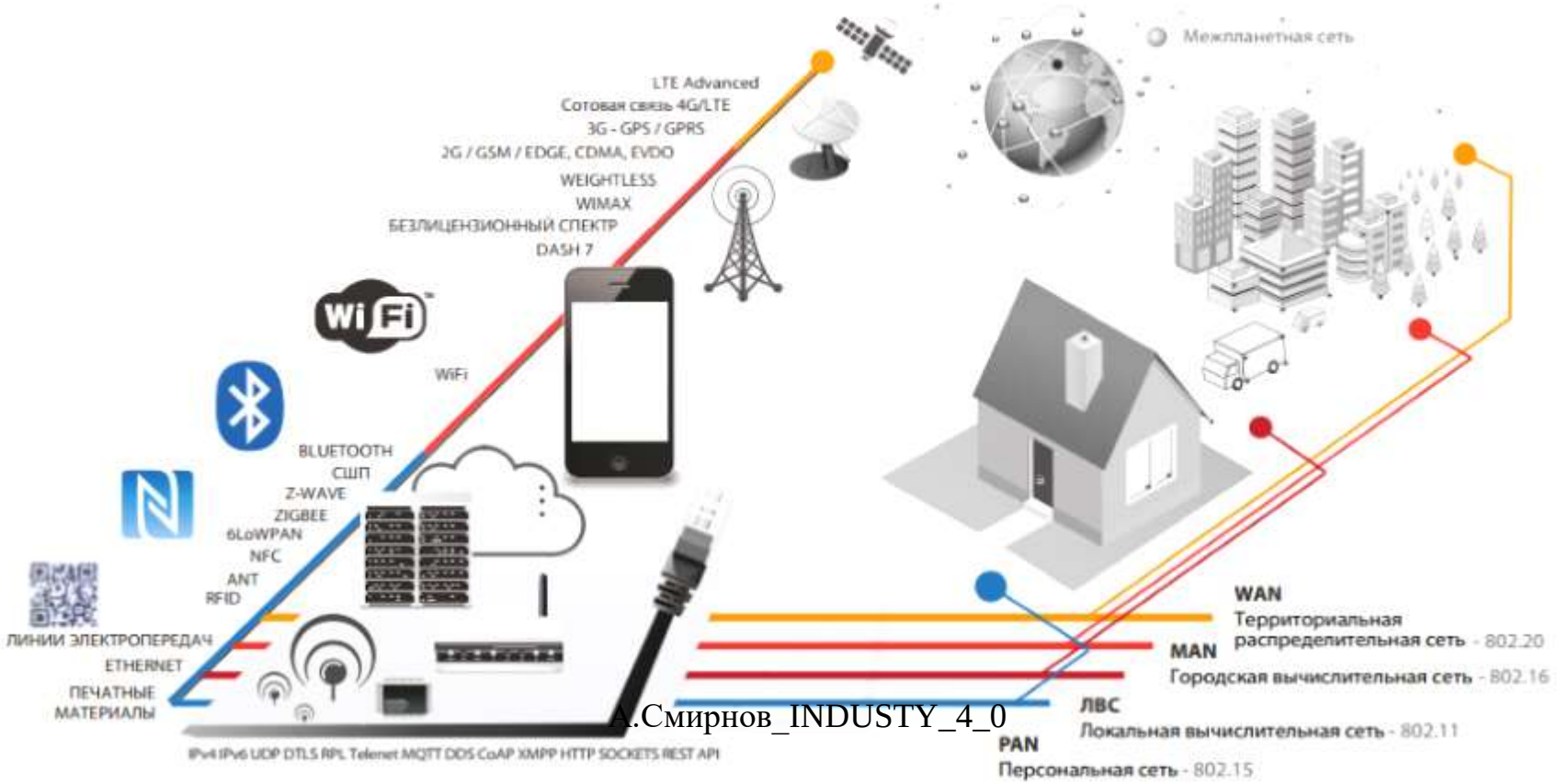


Переход от Интернета людей к Интернету вещей (2008)

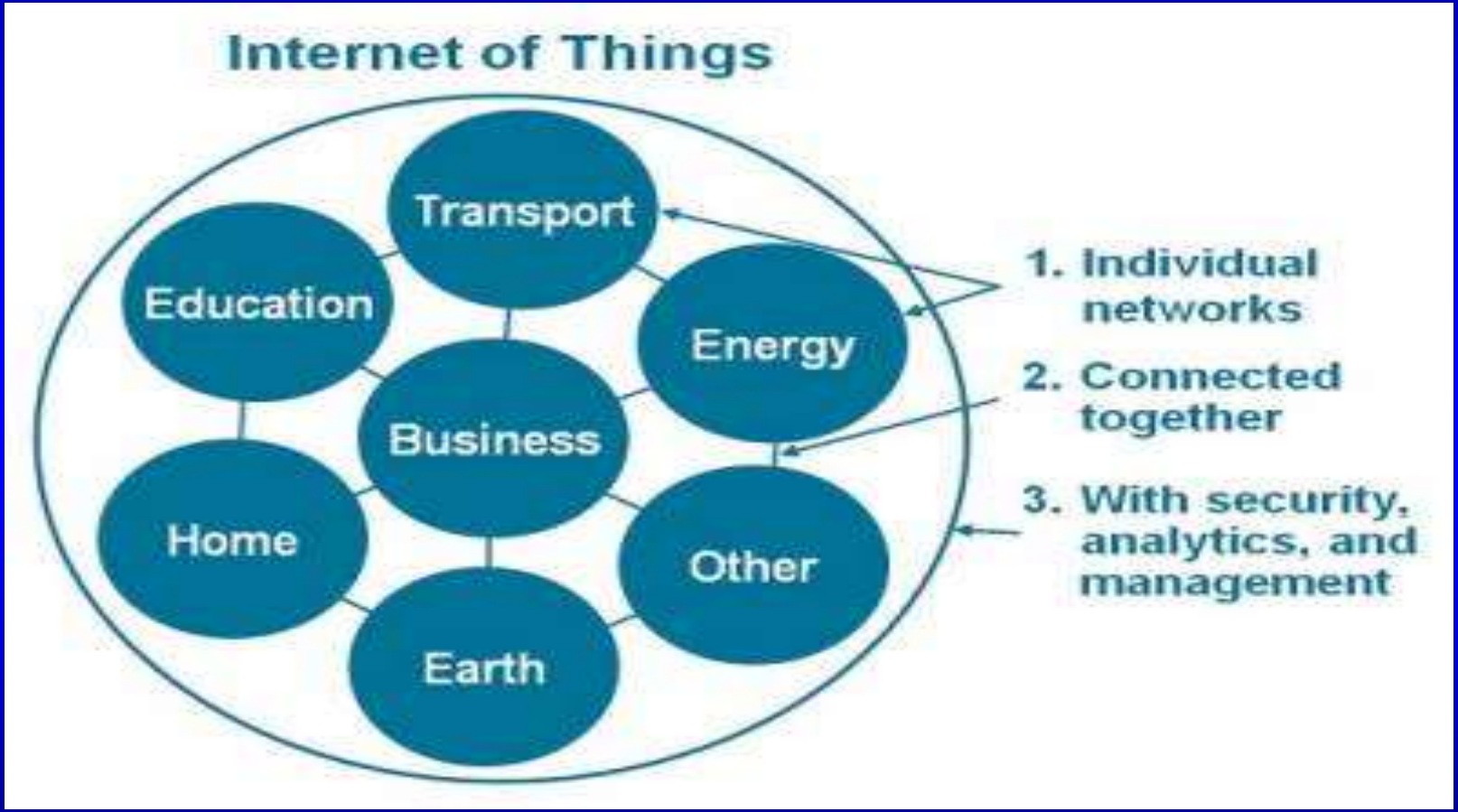


Интернет вещей (Internet of Things, IoT) –драйвер Industry 4.0

IoT расширяет возможности платформ и устройств, обеспечивает взаимодействие между человеком и машиной, а также межмашинное взаимодействие (M2M) без вмешательства человека. Среди устройств будут и ныне "глупые" (тостер, холодильник и т.д.), которые «поумнеют» благодаря встроенным сенсорам реального времени для взаимодействия



Интернет вещей можно рассматривать в качестве "сети сетей"



Интернет вещей и информационная безопасность

Проблемы безопасности IoT возникают из-за растущего объема данных, оконечных устройств и роста ценности данных:

- агрегация и анализ больших объемов даже некритичных данных позволяет сгенерировать информацию, утечка которой может привести к весьма болезненным результатам
- К 2020 г. связь "машина-машина" (M2M) будет осуществляться с помощью 24 млрд. интеллектуальных датчиков и подключенных устройств, а объем рынка M2M составит $1,2 триллиона

Непредсказуемые техногенные катастрофы, стандарты и нормативные правила

- В "Интернете вещей" всегда есть вероятность того, что полезные элементы могут вдруг вызвать либо ускорить катастрофический сбой. Предугадать такой сбой практически невозможно, например, отключение сети электропередачи.
- для защиты критически важной инфраструктуры, такой как сеть электропередачи, нужно найти правильное соотношение между открытостью, встроенной избыточностью и механизмами аварийного подхвата.
- Невозможно выработать и единый стандарт для безопасности Интернета вещей, а также создать адекватную законодательную базу

http://www.cisco.com/web/RU/news/releases/txt/2013/03/032813c.html

INDUSTRY 4.0 и проекты НАТО

История войн - это история технологических прорывов

-П.24….Партнерства также важны для работы с новыми и существующими транснациональными вызовами, такими как распространение оружия массового уничтожения, терроризм, безопасность на море, кибербезопасность и энергетическая безопасность. Т.Е. в стратегическую концепцию НАТО впервые включено положение о киберпространстве как новой сфере военной деятельности

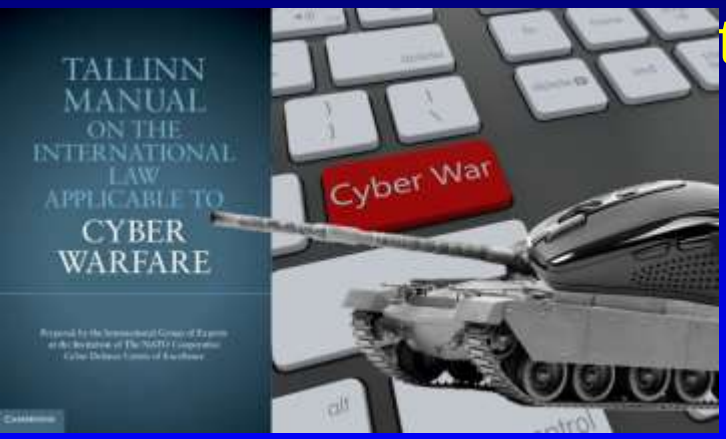
-На саммите НАТО в Уэльсе (4-5.09.2014), кибербезопасность стала ключевой проблемой – 21 упоминание!

-В Военной доктрине РФ (24.12.2014) – 20 упоминаний ИКТ

США приняли стратегию наступательной кибервойны

- Эштон Картер: в новой стратегии (2015 г.) МО США в сфере кибербезопасности предусмотрены атаки на военные сети и инфраструктуру противника (Стратегия 2011 носила оборон. характер)
- Решение о кибератаке принимают президент США и министр обороны (например, вывести из строя командно-контрольные сети противника и лишить его способности применять оружие)
- За кибероперации с 2010 г. отвечает Киберкомандование США (US Cybercom) Минобороны. (6,2 тыс. чел), киберподразделения есть у сухопутных войск, ВМС и ВВС, Лидер - АНБ, а её директор М. Рождерс руководит и US Cybercom. В его ведении ок 40 тыс. чел
- Новую Стратегию представил министр обороны и назвал 4 государства - угрозы, — это Китай, Россия, Иран и Северная Корея.
- Проект бюджета США на 2016 г включает $14 млрд на кибербезопасность, что на $1 млрд больше, чем в 2015 г
- Э. Картер призвал (сентябрь 2015) к кибервойне с РФ и КНР
- В 2015 г создано агентство - Cyber Threat Intelligence Integration Center, как часть Управления Нацразведки США (координация СЦВ, гибридной войны с киборгами, дронами, боевыми экзоскелетами и т.д.)

"Таллинское руководство" НАТО о кибервойнах - это их легализация «Tallinn Manual on the International Law Applicable to Cyber Warfare»



Центр НАТО разработал (2013) руководство о применении положений международного права к кибервойнам (ЦРУ: 130 стран создают информоружие)

Разработано 95 правил, в т.ч.:

- отвечая на атаку государство может либо привлекая агрессора к ответственности, либо "пропорциональными контрмерами"
- Считая атаку "вооруженным нападением", правомерна самооборона , в т.ч. и с использованием традиционного оружия
- кибератаки следует приравнять к применению химического, биологического и радиологического оружия
- вооруженным нападением не признаются кибершпионаж, киберкражи и атаки на сайты (кроме ущерба в гос. масштабе)
- государство-агрессор должно нести ответственность, даже если оно атакует при помощи посредников из других стран…

Проект «Таллинн 2.0»

«Таллинн 2.0» направлен на решение следующей задачи :

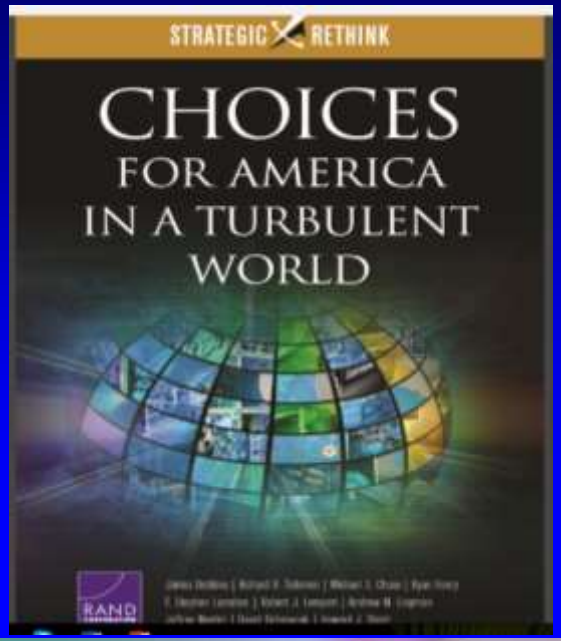
- международное право и враждебные операции меньшего калибра, но наносящие значительный ущерб (финансы, закрытие доступа к важным Интернет-услугам и т.д).

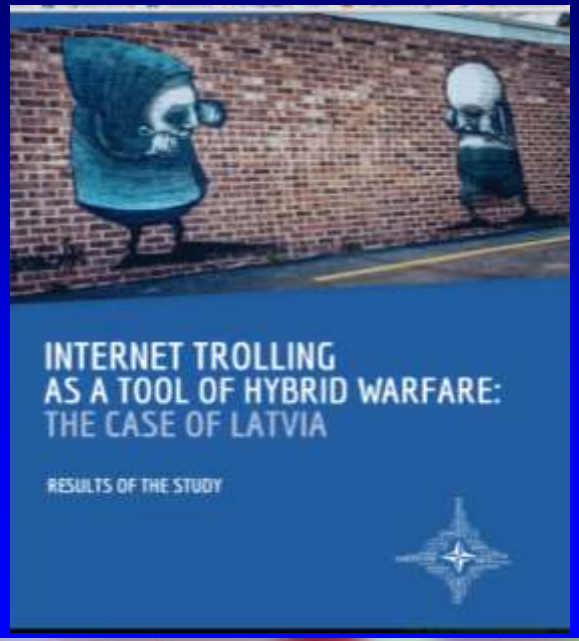
Второе издание «Таллиннского руководства» - выйдет в середине 2016 г. В нем будут рассмотрены нормы международного права, применимые к кибероперациям государств с использованием INDUSTRY 4.0 в мирное и военное время.

НАТО формирует стратегию противостояния России **на новой технологической базе**

НАТО и ЕС не смогут противостоять России методами простой пропаганды заявил 20.02.2015 на заседании Подкомитета Европарламента по безопасности и обороне Директор созданного в январе 2014 г. в Риге Центра стратегических коммуникаций НАТО (NATO StratCom COE) Я.Карклиньш http://www.stratcomcoe.org/Organisation/Structure.aspx

Новые труды и мероприятия НАТО





CyCon 2016: 'Cyber Power'

The 8th International Conference on Cyber Conflict will take place **1-3 June 2016** in Tallinn, Estonia. **31 May** is dedicated as the CyCon workshops day. Focusing on the theme of *Cyber Power*, CyCon 2016 will ask how the traditional concept of power applies to cyberspace. The issues to be covered include international cooperation, technical challenges and requirements, conflict in cyberspace, legal framework, regulations and standards.

CyCon is organised by the NATO Cooperative Cyber Defence Centre of Excellence. Every year, over 500 decision-makers and experts from government, military and industry from all over the world approach the conference's key theme from legal, technology and strategy perspectives, often in an interdisciplinary manner.

Заседание СБ РФ «О противодействии угрозам национальной безопасности РФ в информационной сфере» 1.10.2014г.

- Надёжная работа информресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России.

Коллегия ФСБ РФ 26.03.2015

- Пресечено более 70 млн кибер-атак
- Закрыты 1,5 тыс. экстремистских сайтов

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

От 22.05.2015 № 260

О некоторых вопросах информационной безопасности Российской Федерации

В целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации п о с т а н о в л я ю:

1. Преобразовать сегмент международной компьютерной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны Российской Федерации, в российский государственный сегмент информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), являющийся элементом российской части сети "Интернет" и обеспечивающий:

ВЫВОД:

- Всемерно укреплять технологический суверенитет, внедрять Industry 4.0 и информационную безопасность России, в т.ч. ускорение разработки и принятия новой Доктрины ИБ;
- С партнерами по ОДКБ, ШОС и БРИКС договариваться, в т.ч. в формате ГПЭ ООН по МИБ и Акту об Электронном ненападению

Альтернатива иррациональна:

Авторский коллектив

СМИРНОВ Анатолий Иванович - Президент Национального института исследований глобальной безопасности (НИИГлоБ), член Президиума Российской академии естественных наук, доктор исторических наук, профессор, Чрезвычайный и Полномочный Посланник Российской Федерации в отставке, член Экспертного совета Комитета Государственной Думы Федерального Собрания Российской Федерации по безопасности и противодействию коррупции, советник РКСС

ГРИГОРЬЕВ Виталий Робертович - Главный научный советник ЗАО "РНТ", доцент Московского государственного технического университета, радиотехники, электроники и автоматики (МИРЭА), кандидат технических наук, Почетный работник профессионального образования Российской Федерации

КОХТЮЛИНА Ирина Николаевна - Ответственный секретарь Научного совета Национального института исследований глобальной безопасности (НИИГлоБ), член-корреспондент Российской академии естественных наук, кандидат политических наук

КУРОЕДОВ Борис Витальевич - Директор Центра моделирования Института экономических стратегий (ИНЭС), член-корреспондент Российской академии естественных наук, кандидат военных наук

САНДАРОВ Олег Владимирович - Руководитель группы программирования Института экономических стратегий (ИНЭС)

www.niiglob.ru

Глобальная безопасность в цифровую эпоху: стратагемы для России

НИИГлоБ
НАЦИОНАЛЬНЫЙ ИНСТИТУТ ИССЛЕДОВАНИЙ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

ГЛОБАЛЬНАЯ БЕЗОПАСНОСТЬ В ЦИФРОВУЮ ЭПОХУ:

СТРАТАГЕМЫ ДЛЯ РОССИИ

Под общей редакцией А.И.СМИРНОВА

НАЦИОНАЛЬНЫЙ ИНСТИТУТ ИССЛЕДОВАНИЙ ГЛОБАЛЬНОЙ БЕЗОПАСНОСТИ

NATIONAL INSTITUTE FOR RESEARCH OF GLOBAL SECURITY

СПАСИБО ЗА ВНИМАНИЕ!

http://niiglob.ru aismirnov@niiglob.ru

18 мая 2015 г. коллегия МИД России «Глобальные вызовы в области информтехнологий. Задачи МИД по обеспечению международной информационной безопасности»

- Участвовали: зам. Секретаря Совбеза России Буравлев С.М., представители компетентных ведомств
- Отмечено, что современная обстановка характеризуется нарастанием угрозы использования ИКТ в противоправных целях и в нарушение общепризнанных норм международного права.
- Современные военно-политические, террористические и криминальные угрозы в информационной сфере носят глобальный характер, и борьба с ними требует принятия адекватных мер в самом широком масштабе.
- Приоритетом РФ остается выработка универсальных правил ответственного поведения государств в информпространстве, которые бы препятствовали попыткам совершения актов агрессии, закрепляли бы принципы уважения госсуверенитета, невмешательства во внутренние дела других государств, основных прав и свобод человека.
- Взаимодействие со всеми государствами, проявляющими готовность противостоять попыткам милитаризации информсферы, содействовать выработке международных норм по мирному использованию ИКТ

Концепция внешней политики Российской Федерации (утверждена Президентом РФ В.В.Путиным 12.02.2013)

20. Неотъемлемой составляющей современной международной политики становится «мягкая сила» - комплексный инструментарий решения внешнеполитических задач с опорой на возможности гражданского общества, информационно-коммуникационные, гуманитарные и другие альтернативные классической дипломатии методы и технологии.

Вместе с тем усиление глобальной конкуренции и накопление кризисного потенциала ведут к рискам подчас деструктивного и противоправного использования «мягкой силы» и правозащитных концепций в целях оказания политического давления на суверенные государства, вмешательства в их внутренние дела, дестабилизации там обстановки, манипулирования общественным мнением и сознанием, в т.ч. в рамках финансирования гуманитарных проектов и проектов, связанных с защитой прав человека, за рубежом.

Авторитетный справочник «Military Balance 2015» характеризует понимание Западом «гибридной войны» как:

«Использование военных и невоенных инструментов в интегрированной кампании, направленной на достижение внезапности, захват инициативы и получение психологических и физических преимуществ, с использованием дипломатических возможностей, оперативных дезинформационных операций, а также электронных и кибернетических операций, военных и разведывательных действий под прикрытием, а иногда и без прикрытия, и экономического давления».

В связи с событиями на Украине редакторы преподносят сомнительный «комплимент» России «и потенциально другим государствам за применение инновационных методов поддержки верных им сил [proxies] и ниспровержения правительств».

Но редакторы зря скромничают - честь первооткрывателя «инновационных» методов свержения зарубежных правительств Запад давно закрепил за собой.

В марте 2015 г. В Брюсселе председ Комитета СФ К.И.Косачев задал вопрос генсеку НАТО Й.Столтенбергу, будет ли НАТО бомбить государство в ответ на кибератаку с его территории. Тот ушел от ответа, т.к. в НАТО нет общего понимания о «пропорциональном» ответе на кибератаку как элемента «гибридной войны».

Соглашение между Правительством РФ и Правительством КНР о сотрудничестве в области обеспечения МИБ

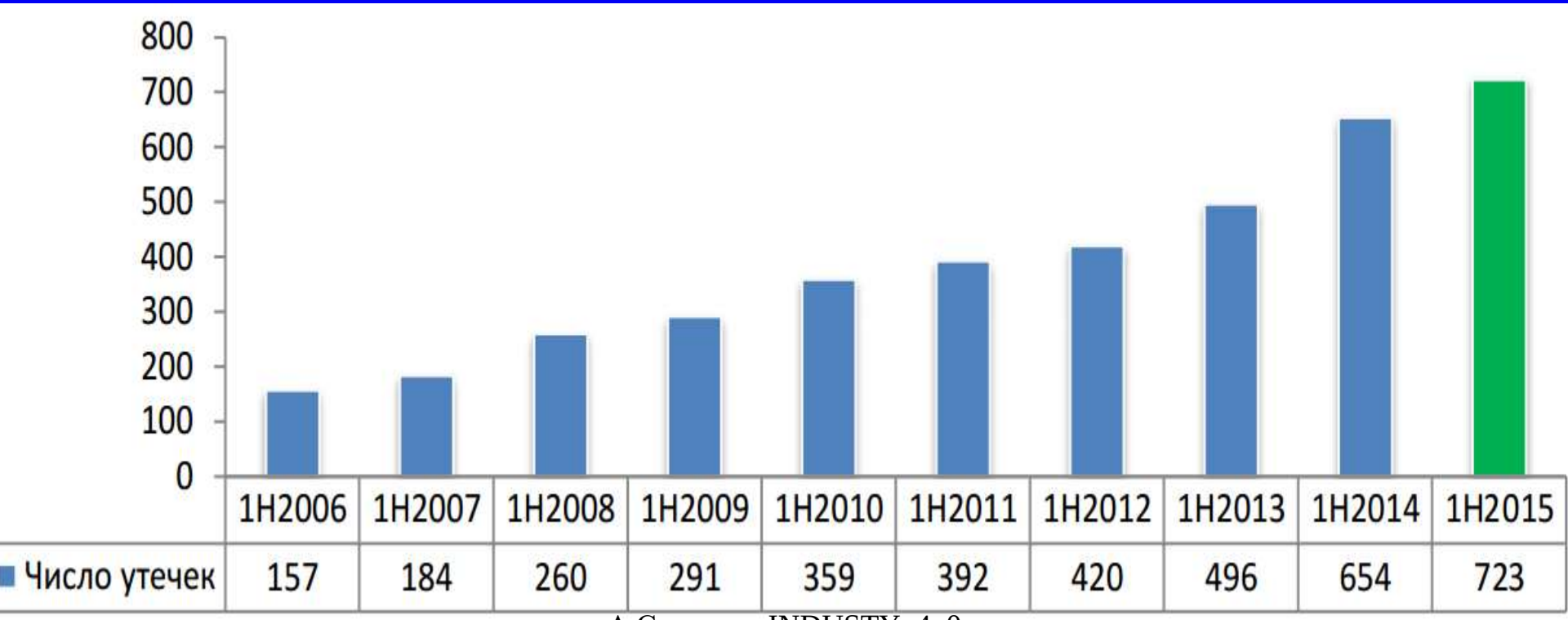
8 мая с.г. в ходе визита Председателя КНР в РФ мининдел дел РФ и КНР подписали межправсоглашение о сотрудничестве в области МИБ.

Документ выводит взаимодействие на новый уровень и предполагает:

- прикладной характер (совместное решение конкретных задач по обеспечению национальной и международной ИБ)
- диалог заинтересованных ведомств по вопросам МИБ.
- совместное реагирование на острые угрозы, включая противодействие использованию ИКТ в нарушение принципов международного права, в т.ч. для вмешательства во внутренние дела государств, подрыва суверенитета, политической и экономической стабильности, разжигания межнациональной и межконфессиональной вражды.
- борьбу с использованием ИКТ в террор-их и иных противоправных целях
- обмен информацией о рисках и угрозах,
- взаимодействие по совершенствованию международно-правовой базы
- совместные меры укрепления доверия, научные исследования, подготовку и обмен студентами, аспирантами, преподавателями
- суверенное право государств проводить госполитику по вопросам Интернет, в т.ч. его интернационализации
- углубление сотрудничества в рамках ООН, МСЭ, ШОС, БРИКС и форума АСЕАН по безопасности

Число зарегистрированных в мире утечек конфиденциальной информации 2006 – 2015 гг

За I полугодие 2015 г. Аналитическим центром InfoWatch зарегистрировано 723 случая утечки конфиденциальной информации Это на 10% больше, чем за аналогичный период 2014 года (654 утечки).



	1H2006	1H2007	1H2008	1H2009	1H2010	1H2011	1H2012	1H2013	1H2014	1H2015
Число утечек	157	184	260	291	359	392	420	496	654	723

Об итогах заключительного заседания ГПЭ ООН по МИБ

22-26.06 2015 г. в Нью-Йорке состоялось заключительное заседание ГПЭ по МИБ (20 стран)

Консенсусом принят доклад Генсеку ООН для представления на 70-й сессии ГА ООН.

Итоговый доклад Группы - это политико-правовой документ, закладывающий общие рамки взаимодействия государств в информпространстве. Подтверждена заинтересованность стран в мирном использовании ИКТ и важность усилий международного сообщества на предотвращение конфликтов в информпространстве. Подтверждено суверенное право государств распоряжаться своей инфраструктурой и определять политику в сфере МИБ

Документ, опирается на доклады ГПЭ 2010 и 2013 гг., развивает их в соответствии с современными реалиями. Новым элементом доклада стало положение о том, что любые обвинения государств в организации и совершении противоправных деяний с использованием ИКТ должны быть доказаны. Это исключает возможность «огульного» привлечения государств к ответственности за атаки, якобы совершенные ими.

Признано, что международное право применимо к сфере использования ИКТ, однако оно может быть развито. В этом контексте особое внимание уделено выработке норм, правил и принципов ответственного поведения государств в информпространстве. Отдельный пункт доклада посвящен инициативе ШОС «Правила поведения в области обеспечения МИБ», (обновленный проект Генсеку ООН в январе 2015 г).

Сохраняется последовательность и непрерывность обсуждения проблематики МИБ на площадке ООН. В рамках ООН должен продолжаться институциональный диалог по МИБ. ГПЭ выступила за созыв новой группы уже в 2016 г., для выработки общего понимания и исследования угроз в сфере МИБ и совместных мерах по их устранению.

Включены рекомендации по наращиванию международного сотрудничества в области МИБ укреплению доверия, преодолению «цифрового разрыва». Предусмотрено увеличение объемов техпомощи, реагирования на инциденты с использованием ИКТ, ускорение передачи знаний и технологий, прежде всего развивающимся странам.

В День дипломатического работника….

Резолюция ГА ООН от 19.11.2014 «Право на неприкосновенность личной жизни в цифровой век» – реакция на разоблачения Сноудена о тотальной слежке , в т.ч. мобильных устройств АНБ США и их союзниками

United Nations A/C.3/69/L.26/Rev.1

General Assembly

Distr.: Limited
19 November 2014

Original: English

Sixty-ninth session
Third Committee
Agenda item 68 (b)
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Argentina, Austria, Belgium, Bolivia (Plurinational State of), Brazil, Bulgaria, Chile, Costa Rica, Croatia, Cyprus, Denmark, Dominican Republic, Ecuador, El Salvador, Finland, France, Germany, Greece, Guatemala, Hungary, Iceland, Indonesia, Ireland, Liechtenstein, Luxembourg, Malta, Mexico, Netherlands, Nicaragua, Norway, Paraguay, Peru, Poland, Portugal, Russian Federation, Slovenia, Spain, Switzerland and Uruguay: revised draft resolution

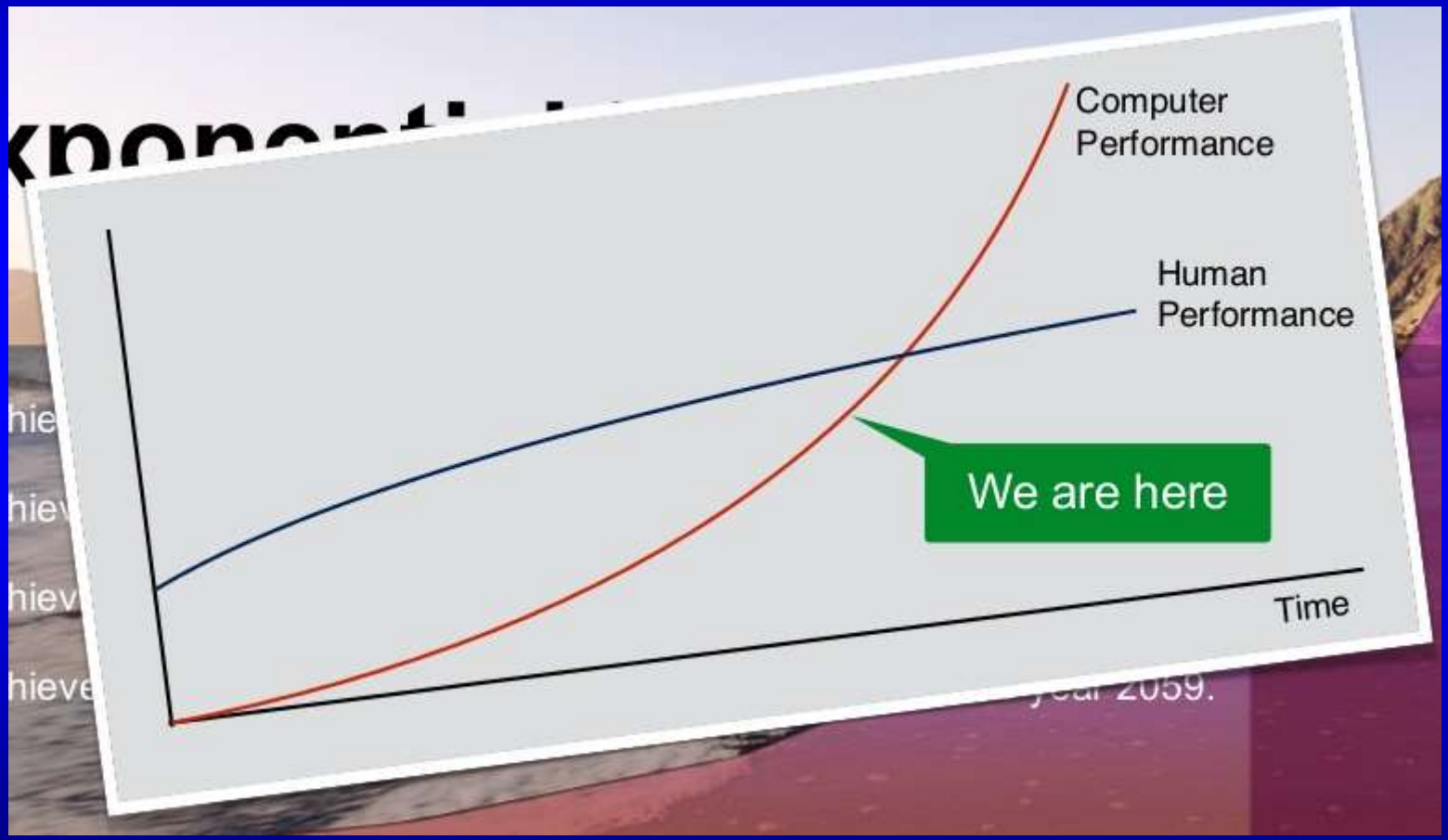
The right to privacy in the digital age

Секретные программы слежки АНБ за устройствами под управлением ОС Android, iOS и BlackBerry:

CO-TRAVELER — за передвижением владельцев и выявлением их скрытых контактов,

Fairview — за пользователями на территории иностранных государств (особенно за SMS)

JUGGERNAUT — для перехвата разговоров, факсов, и текстов по сетям мобильной связи

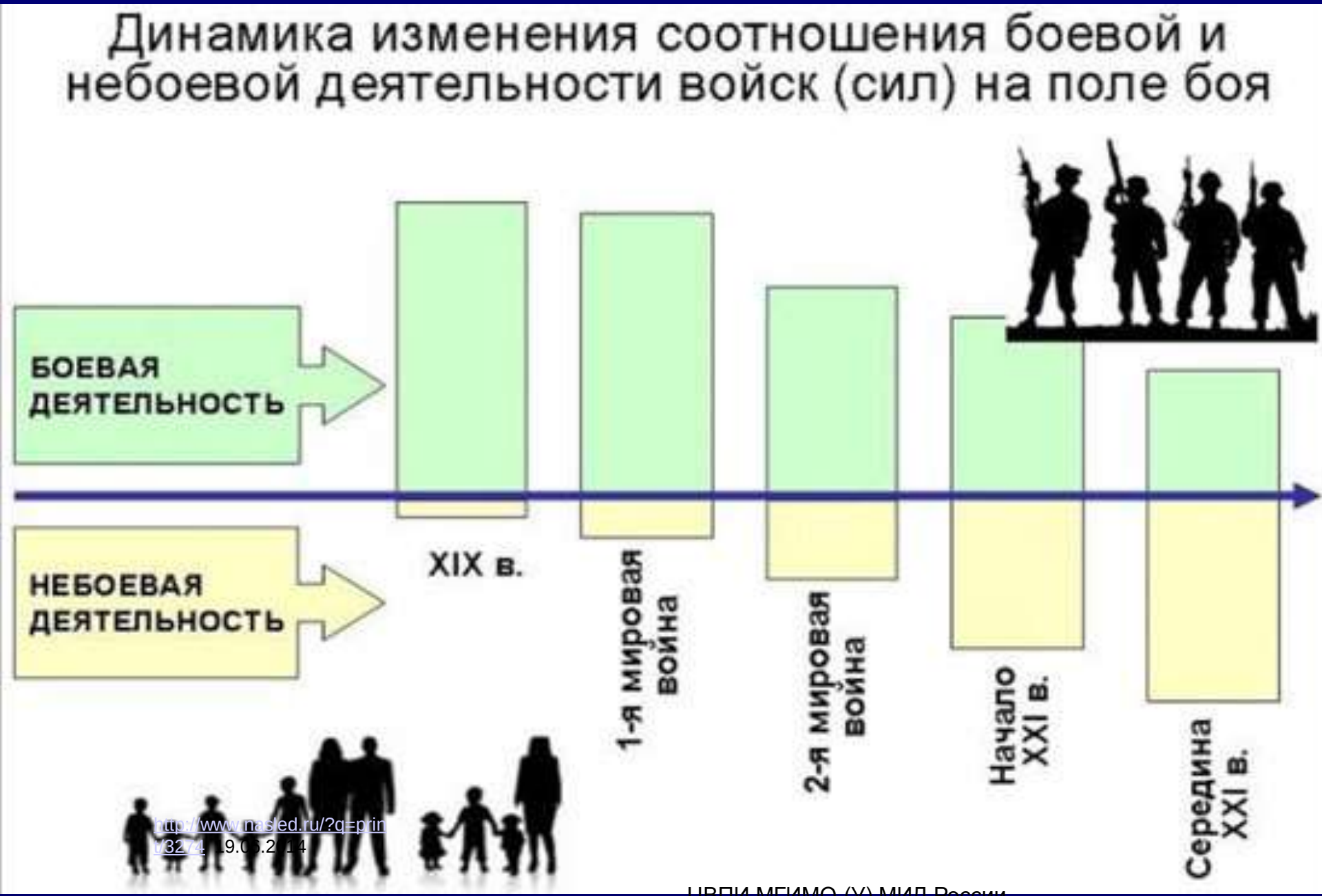

Computer
Performance
Human
Performance
We are here
Time

Глобальная безопасность: госдолг США $18,8 трлн. – 109,9% к ВВП Общий долг:1 квадрил! -не покрыть без крупной войны (кибер?) Акт "О поддержке свободы на Украине" нацелен против РФ (вместо «Акта о предотвращении российской агрессии» №2277,- курса на смену режима в РФ) https://beta.congress.gov/bill/113th-congress/senate-bill/2277

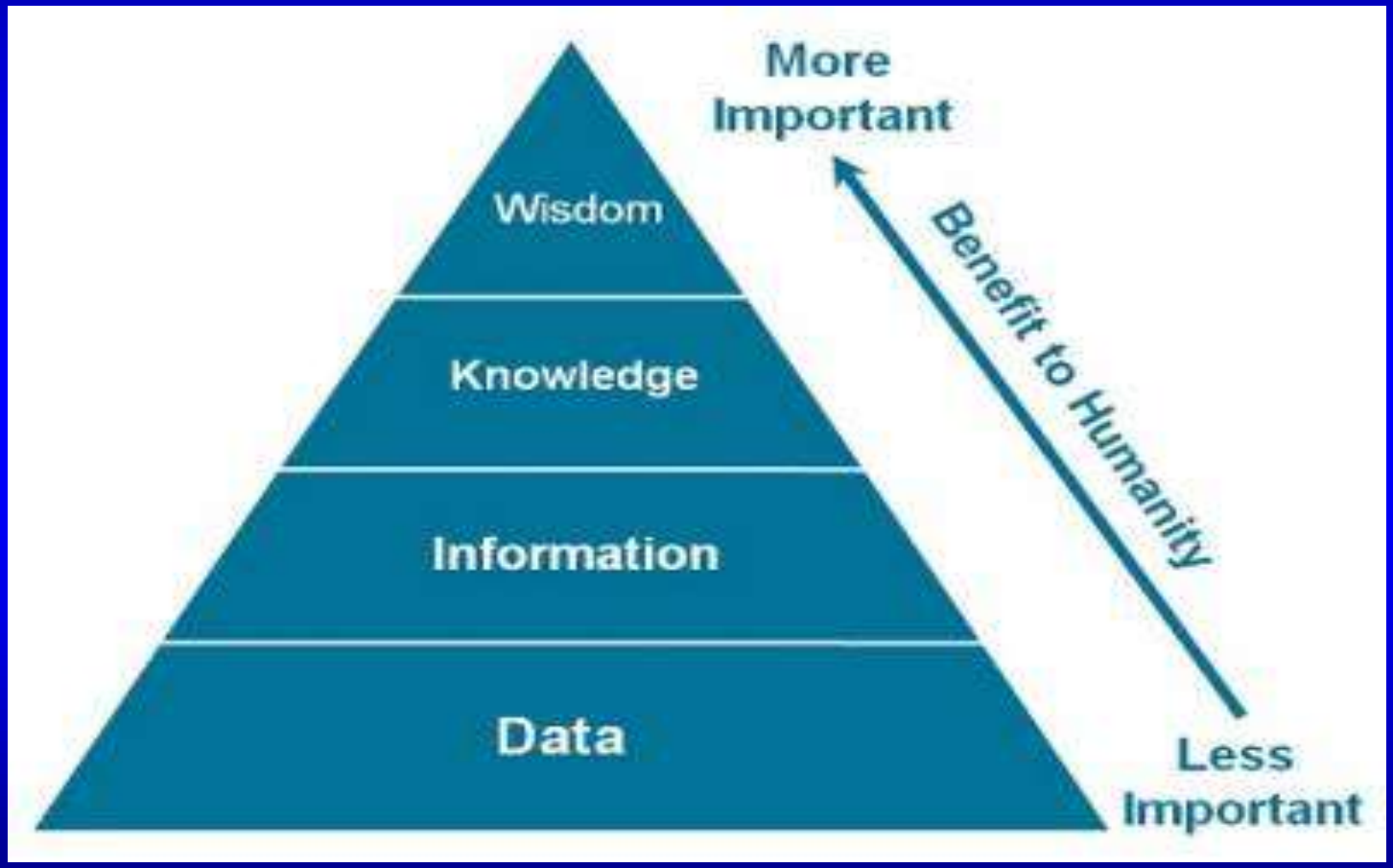
http://www.usdebtclock.org/

ВОЕННО-ПОЛИТИЧЕСКИЕ СОСТАВЛЯЮЩИЕ МИБ

Человечество идет к гиьрмдным войнам…



'Человек превращает данные в "мудрость"



Восемь способов использования Интернета террористами («террор сознания»)

(согласно классификации американского терроролога Габриэля Веймана):

1) проведение психологической войны,
2) поиск информации,
3) обучение террористов,
4) сбор и перевод денежных средств,
5) пропаганда,
6) вербовка,
7) организация террористических сетей,
8) планирование и координирование террористических действий.

«Гибридная война» на Украине и международное право

«Войной» в традиционном смысле называются масштабные боевые действия между вооруженными силами государств.

Вспышка интереса к «гибридной войне» на Украине спровоцирована лидерами и СМИ стран НАТО о её развязывании РФ и является частью информационной кампании. Запад: Россия, мол, «аннексировала Крым», «сбила» лайнер и то ли совершила «агрессию», то ли ведет «гибридную войну» в Донбассе (путаются).

Международно-правовой анализ должен дать ответ на вопрос, применимы ли нормы международного права?:

- принципов территор. целос-ти гос-в и самоопределения народов

- незаконного использования силы государствами в межд-х отношениях

«теневой» бюллетень ЦРУ «Stratfor» 23.06.2015 поправил лидеров Запада, отметив, что именно НАТО и ЕС первыми нарушили в Косово межд.право, а не РФ на Украине в 2014-15 гг.

РФ внесла в ООН предложение о принятии декларации о недопустимости вмешательства во внутренние дела и суверенитет гос-в, и неприемлемости госпереворотов как метода смены власти - этот принцип, уже стал нормой межд-го права в Африке и Лат. Америке.

Но Запад ответил новой попыткой переворота - в Македонии.

Практические действия США по управлению ресурсами Интернет в геополитических целях (Сирия)