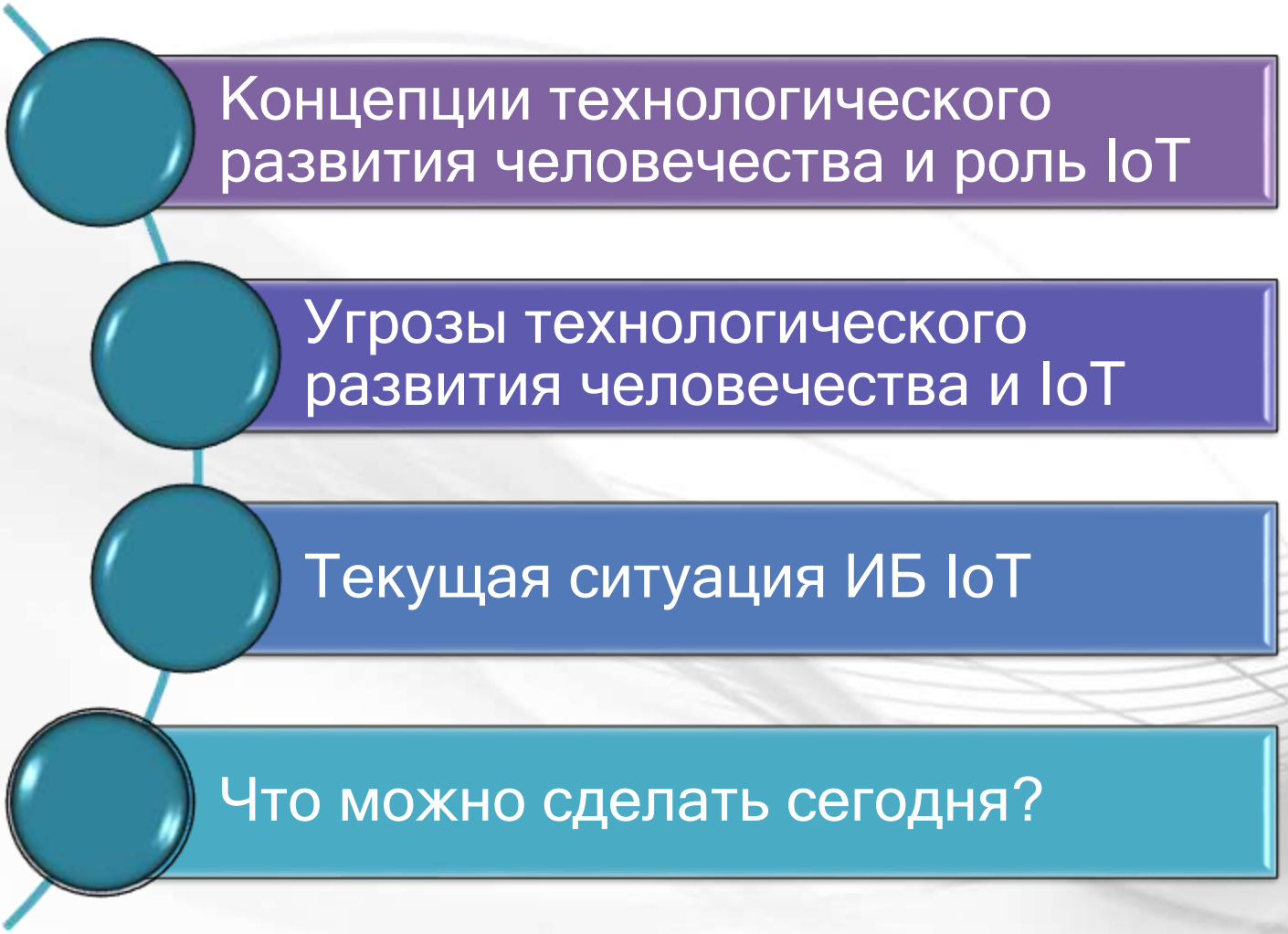
Кибербезопасность. Каких угроз нам ждать от ждать от Интернета вещей и Промышленного Интернета?

Алексей МАЛЬНЕВ,

Заместитель директора департамента ИБ АМТ-ГРУП amalnev@amt.ru

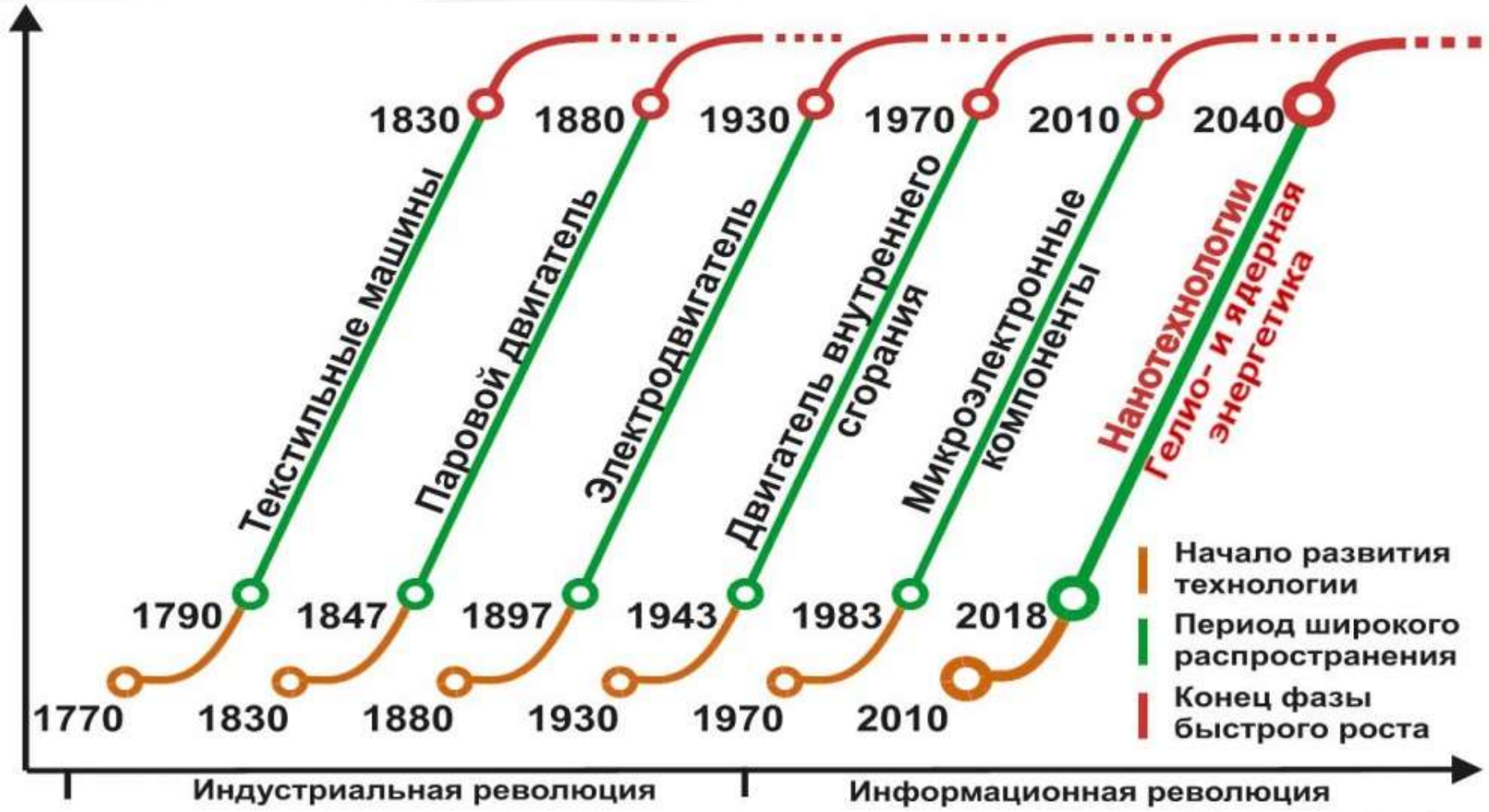
Содержание



AMT GROUP

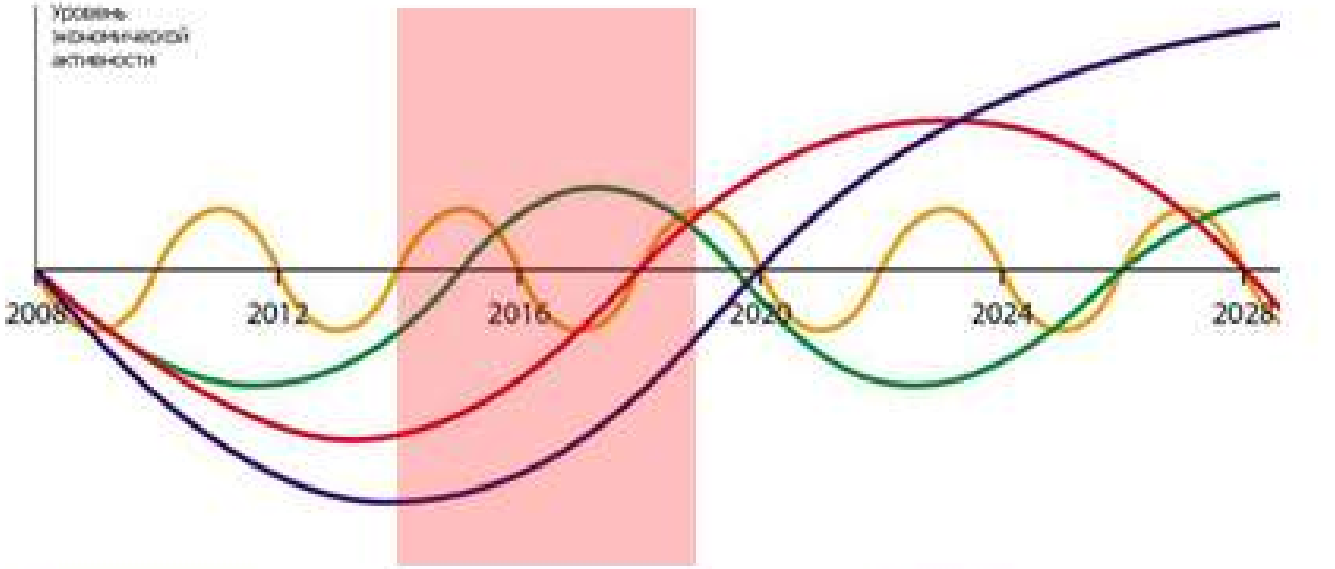
Концепции технологического развития и роль IoT

Технологическое развитие человечества
Концепция технологических укладов



Технологическое развитие человечества
Концепция технологических укладов

Глобальный кризис как сочетание циклических кризисов



цикл Китчина

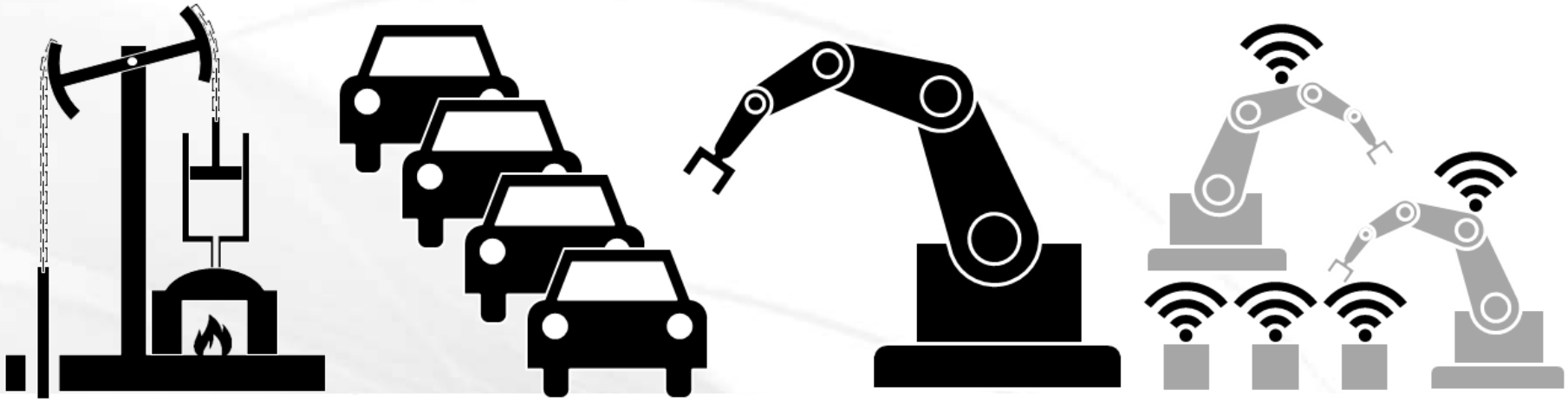
цикл Жугляра

цикл Кузнеца

цикл Кондратьева

– война за технологическое лидерство и доминирование в мировой экономике

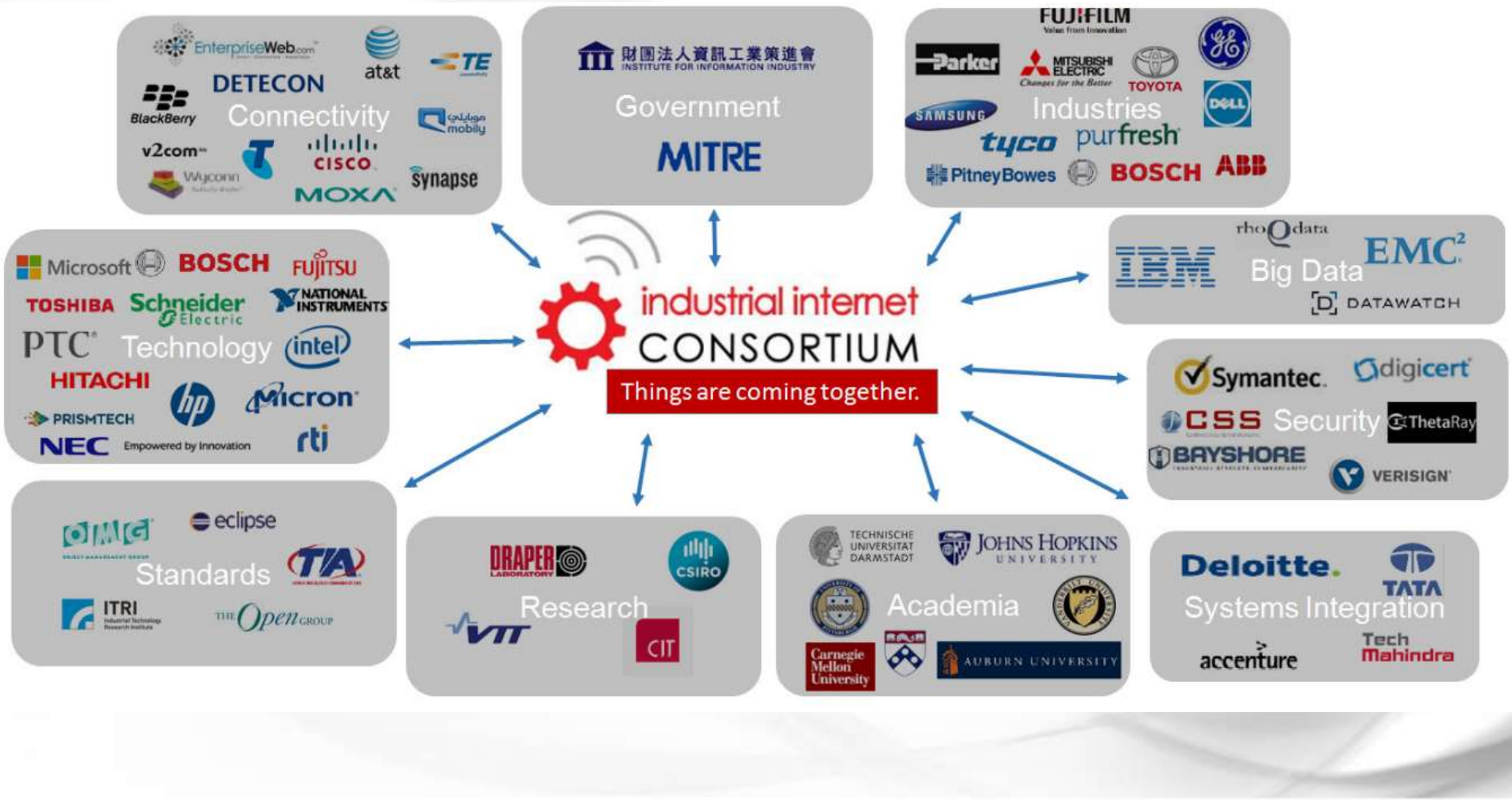
Технологическое развитие человечества
Концепция Industry 4.0



1st	2nd	3rd	4th
Механизация, Использование силы воды и пара	Массовое производство, конвейеры, электричество	Компьютеры и автоматизация	Киберфизические системы и персонализированное производство

AMT GROUP

Технологическое развитие человечества
Консорциум Промышленного Интернета



Технологическое развитие человечества Консорциум промышленного интернета

Программа	Индустрия 4.0	Консорциум промышленного интернета
Идеологи	Правительство Германии	Транснациональные корпорации
Ключевые организаторы	Правительство, бизнес, ученые	Бизнес, ученые, правительство
Этап развития	Четвертая революция	Третья революция
Платформа	Правительственная промышленная политика	Некоммерческий консорциум с открытым участием
Фокус	Промышленность	Производство, энергетика, медицина, транспорт, сельское хозяйство, коммунальные услуги
География	Германия и немецкие компании	Все компании

AMT GROUP

Технологическое развитие человечества
Internet of Things

Технологическое развитие человечества
Умные города

AMT GROUP

Технологическое развитие человечества
Умные города

Поколение умных городов	Умная городская среда	Умная мобильность	Умная экономика	Умное управление	Умные жители	Умная экология	Умная модель жизни (умное проживание)
первое поколение							
второе поколение							
третье поколение							
четвертое поколение							
пятое поколение							

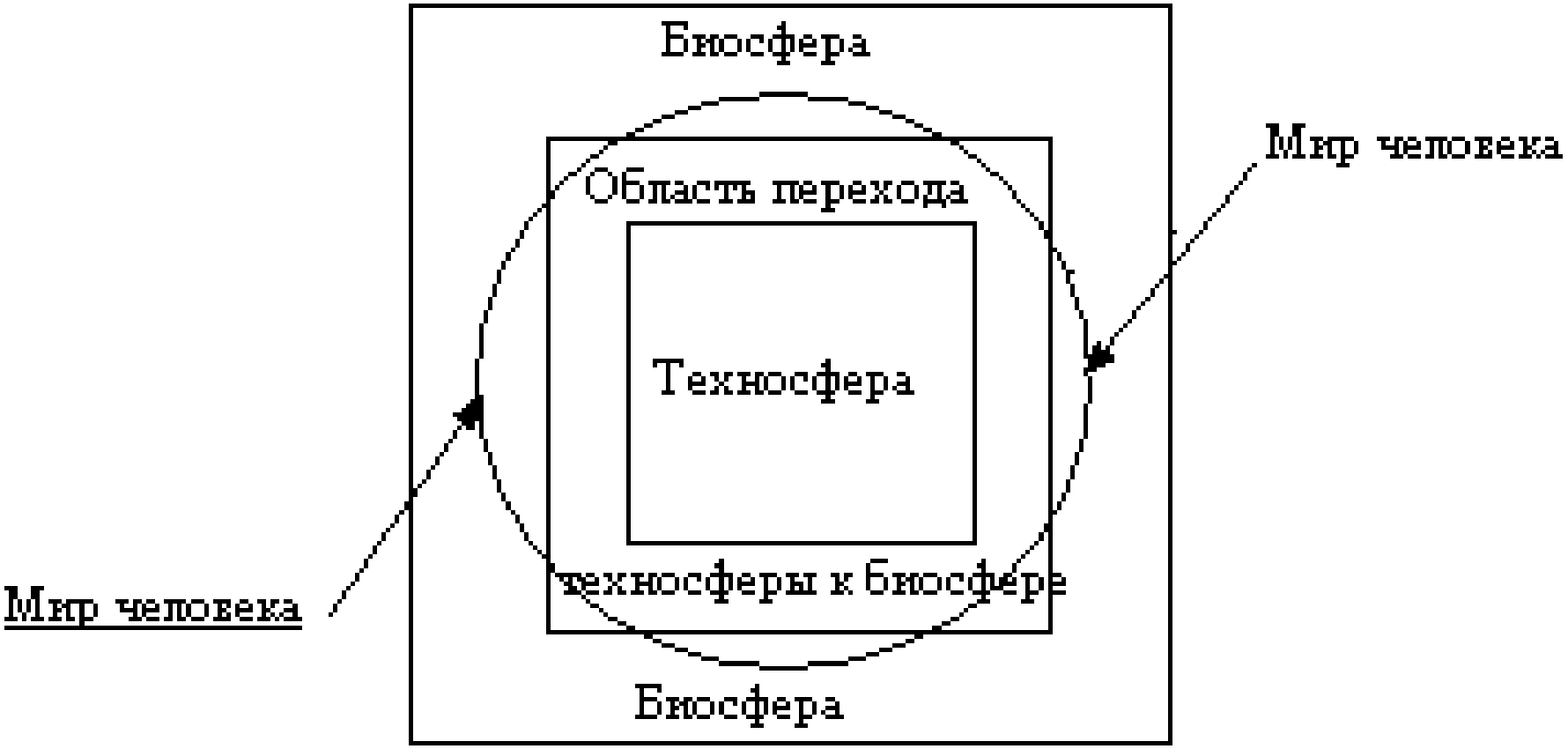
Угрозы технологического развития человечества

Технологическое развитие человечества
Угрозы и вызовы

- Социальные;
- Экономические;
- Политические;
- Военные;
- Техногенные;
- Информационные;

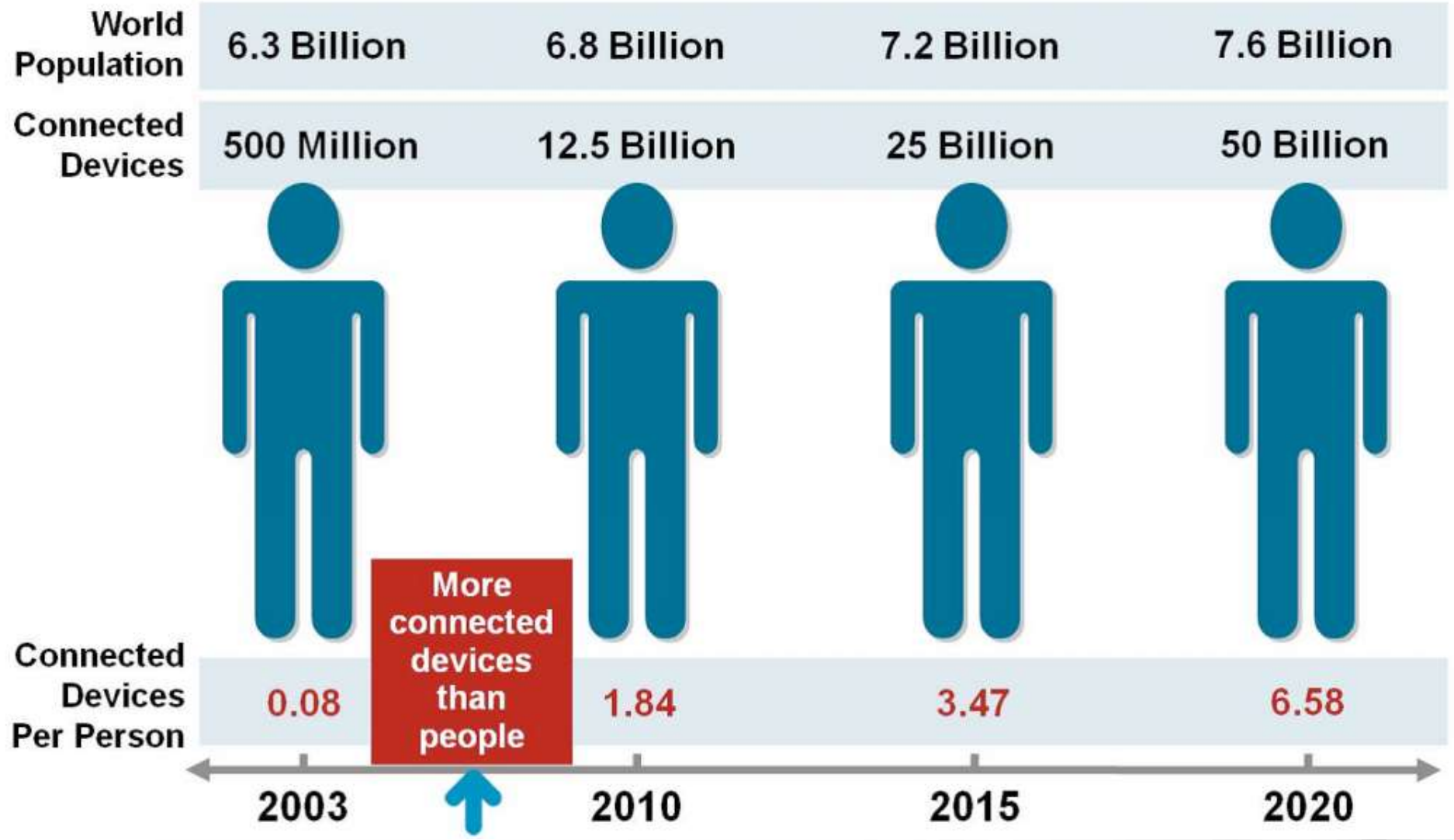
AMT GROUP

Технологическое развитие человечества
Влияние техносферы на человека



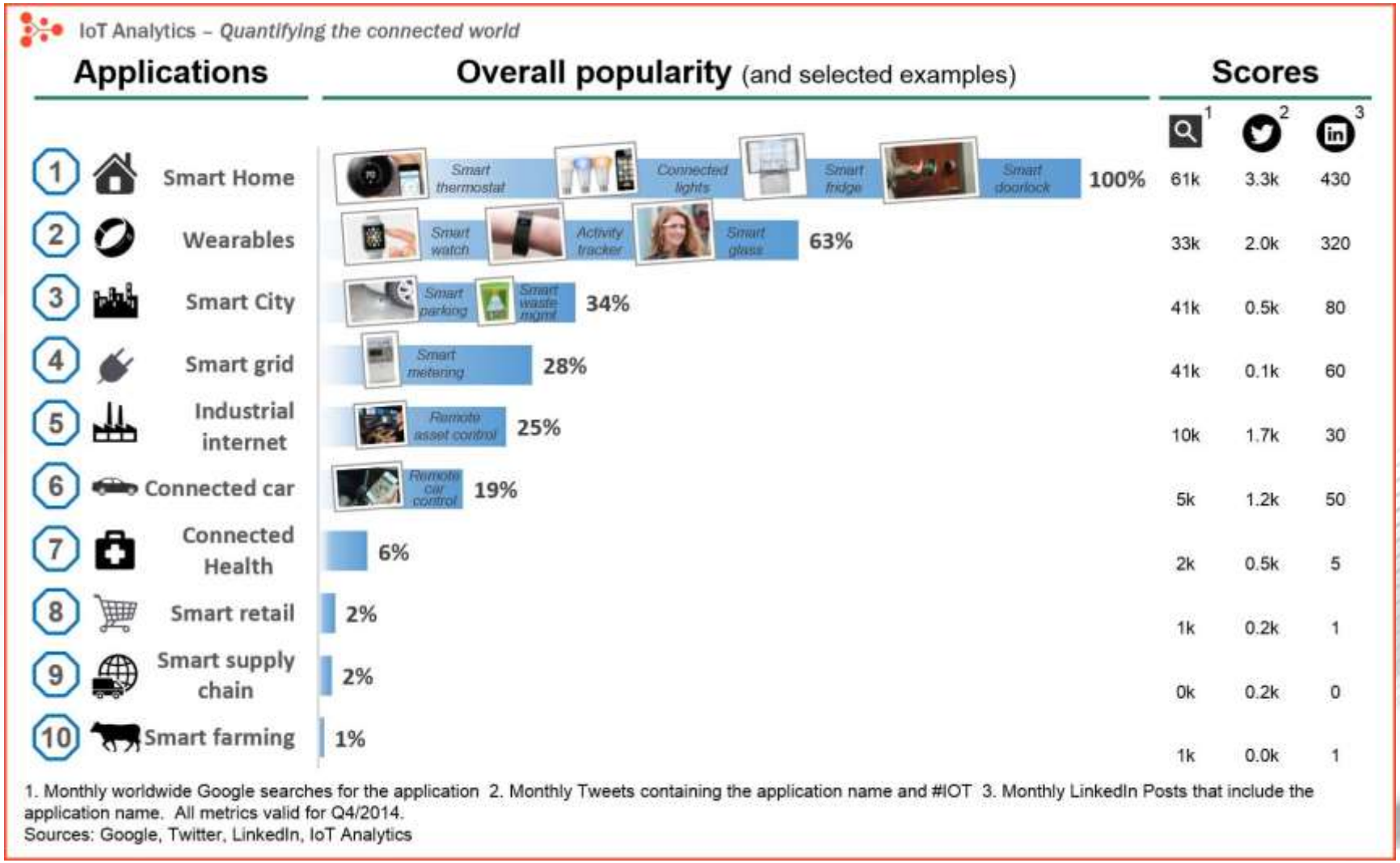
AMT GROUP

Технологическое развитие человечества
Рост количества устройств IoT

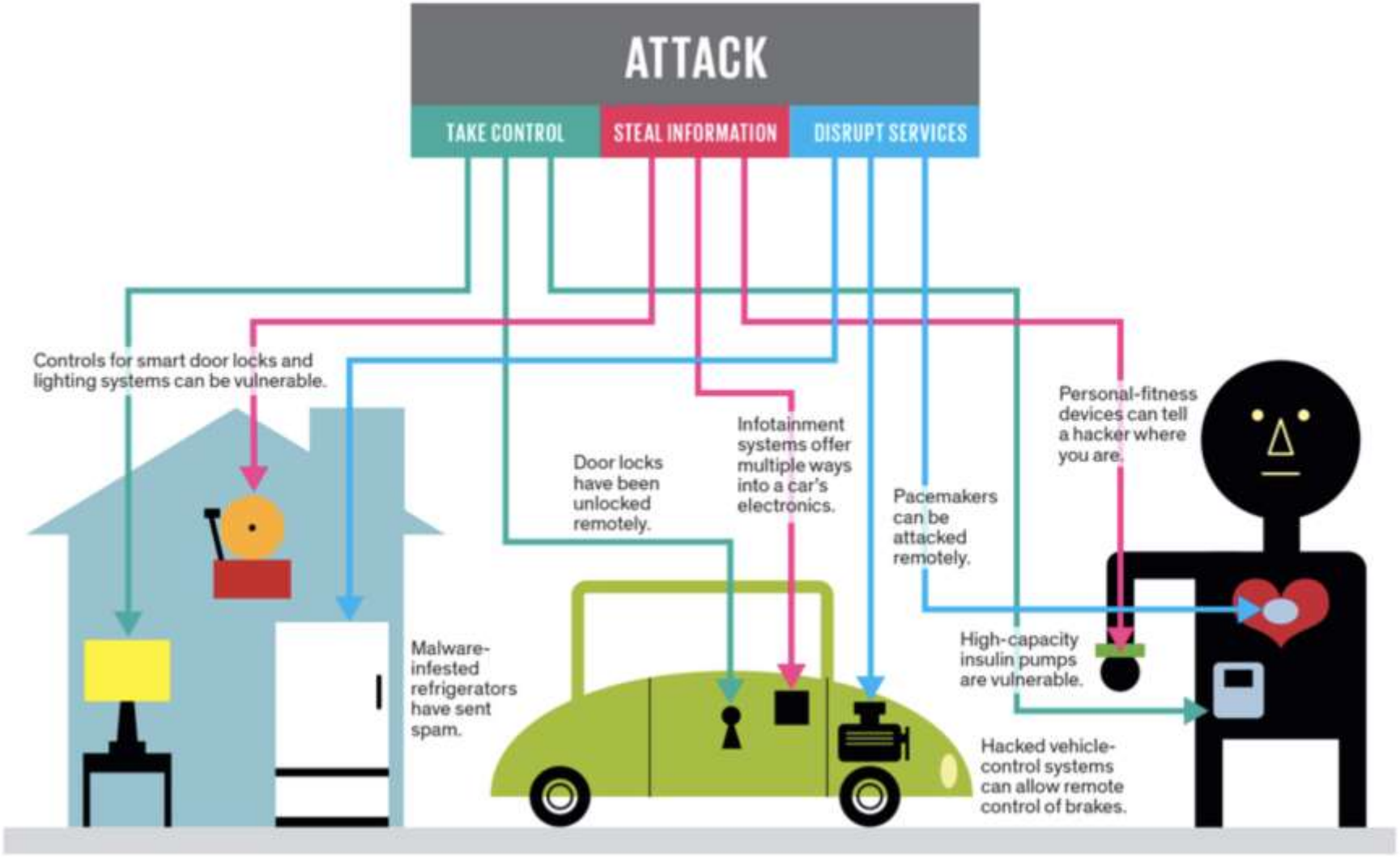


AMT GROUP

Технологическое развитие человечества
Рост количества устройств IoT



Киберугрозы Интернета вещей

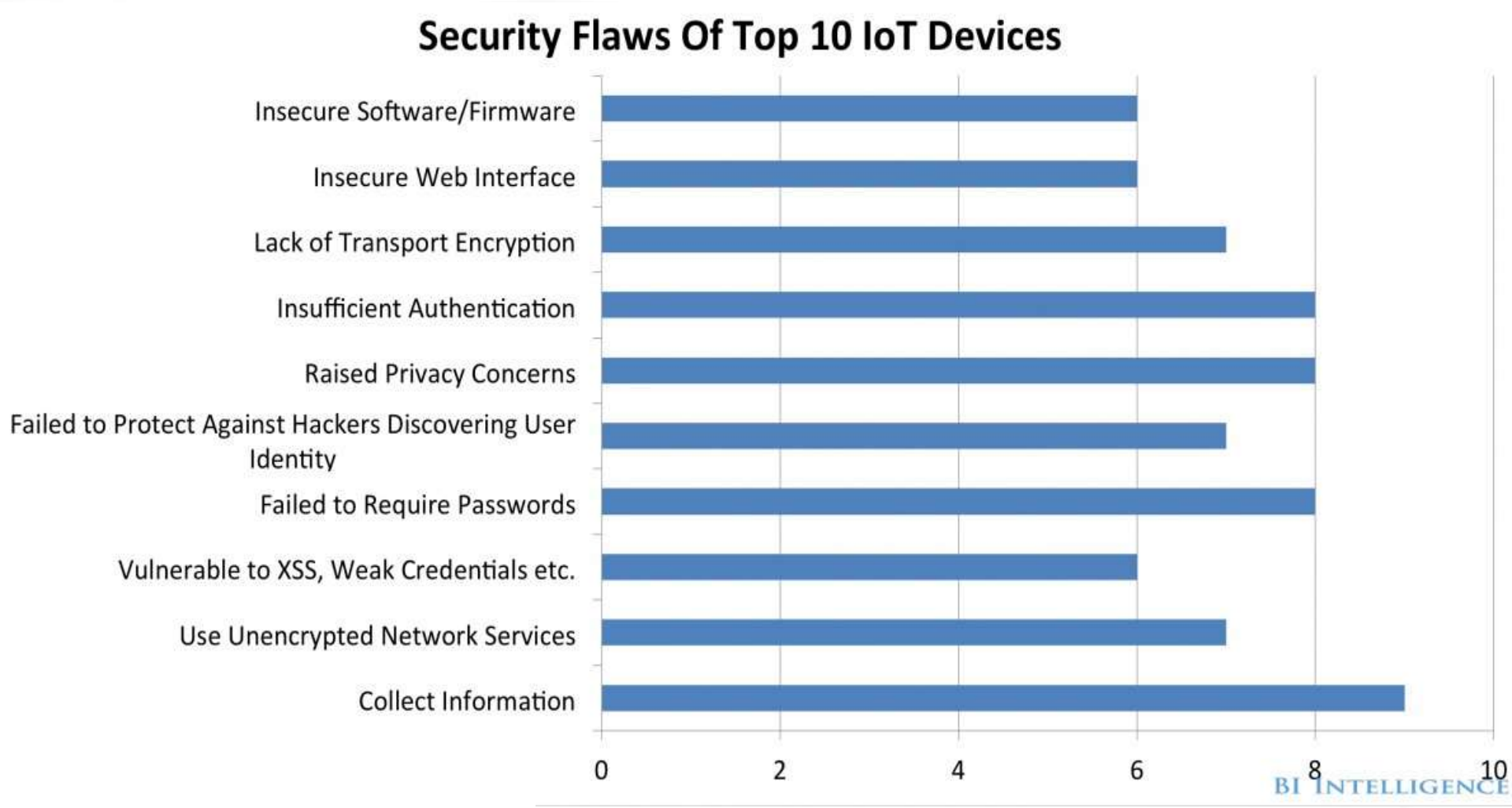


AMT GROUP

Основные угрозы IOT

- Конфиденциальность: ПДн и КТ в IoT в 90% случаев;
- Слабая аутентификация: в 80% случаев;
- Нет шифрования в 70% случаев;
- Угрозы Web интерфейса в 60% случаев;
- Отсутствие Path Management в 60% случаев;

Основные угрозы IOT



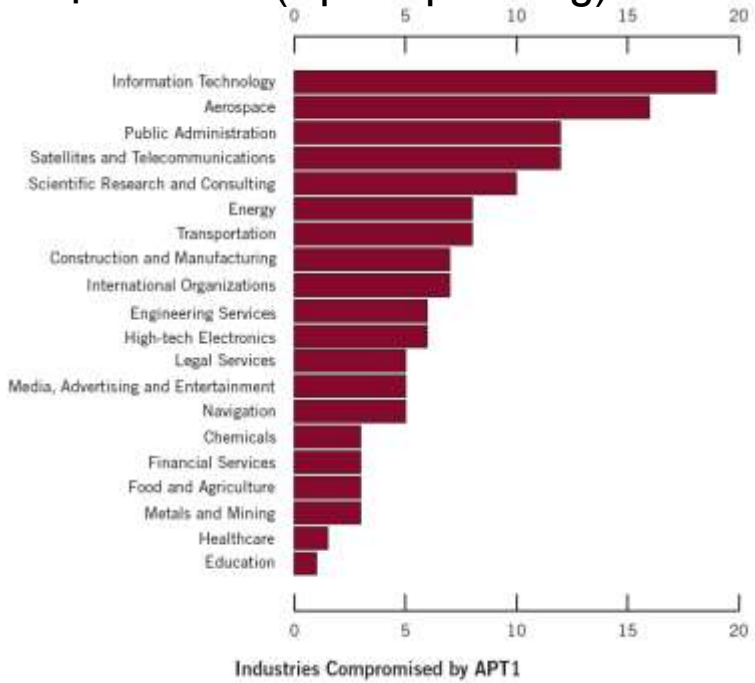
AMT GROUP

Как сегодня обстоят дела с ИБ критичной техносферы?

Актуальные угрозы ИБ: Advanced Persistent Threat

- Февраль 2013: отчет Mandiant об APT1
- APT1 - одна из более 20 зафиксированных APT-группировок в Китае и одна из крупнейших
- Базируется в Шанхае
- Подразделение №61398 НОАК

- С 2006 года скомпрометирована 141 компания, из них более 30% заняты в отраслях, относящихся к АСУ ТП
- Более 1000 серверов присутствия по всему миру
- Несколько сотен участников
- Векторы атак: как технологические, так и социальные (Spear-phishing)

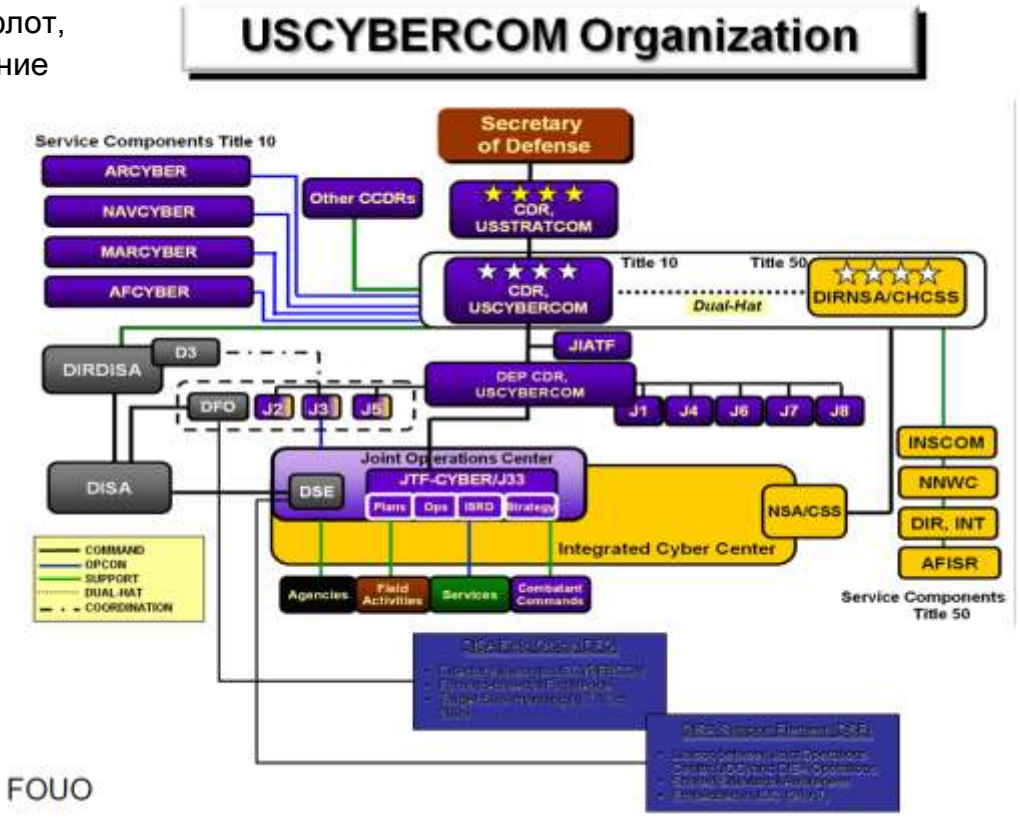


Industries Compromised by APT1

AMT GROUP

Актуальные угрозы ИБ: Advanced Persistent Threat

- Расположено на территории военной базы Форт-Мид, штат Мэриленд
- Функционирует с 21 мая 2010 года
- Объединило ранее созданные организации (Соединение глобальных сетевых операций JTF-GNO и командование сетевой войны JFCC-NW и тд)
- Включает: 9-е армейское командование связи, 10 флот, 24 воздушная армия и кибернетическое командование корпуса морской пехоты
- 6 апреля 2016 года: МО Эштон Картер дал первое задание военного времени: атаковать ИГ с целью нарушения руководства ИГ



Что делать?

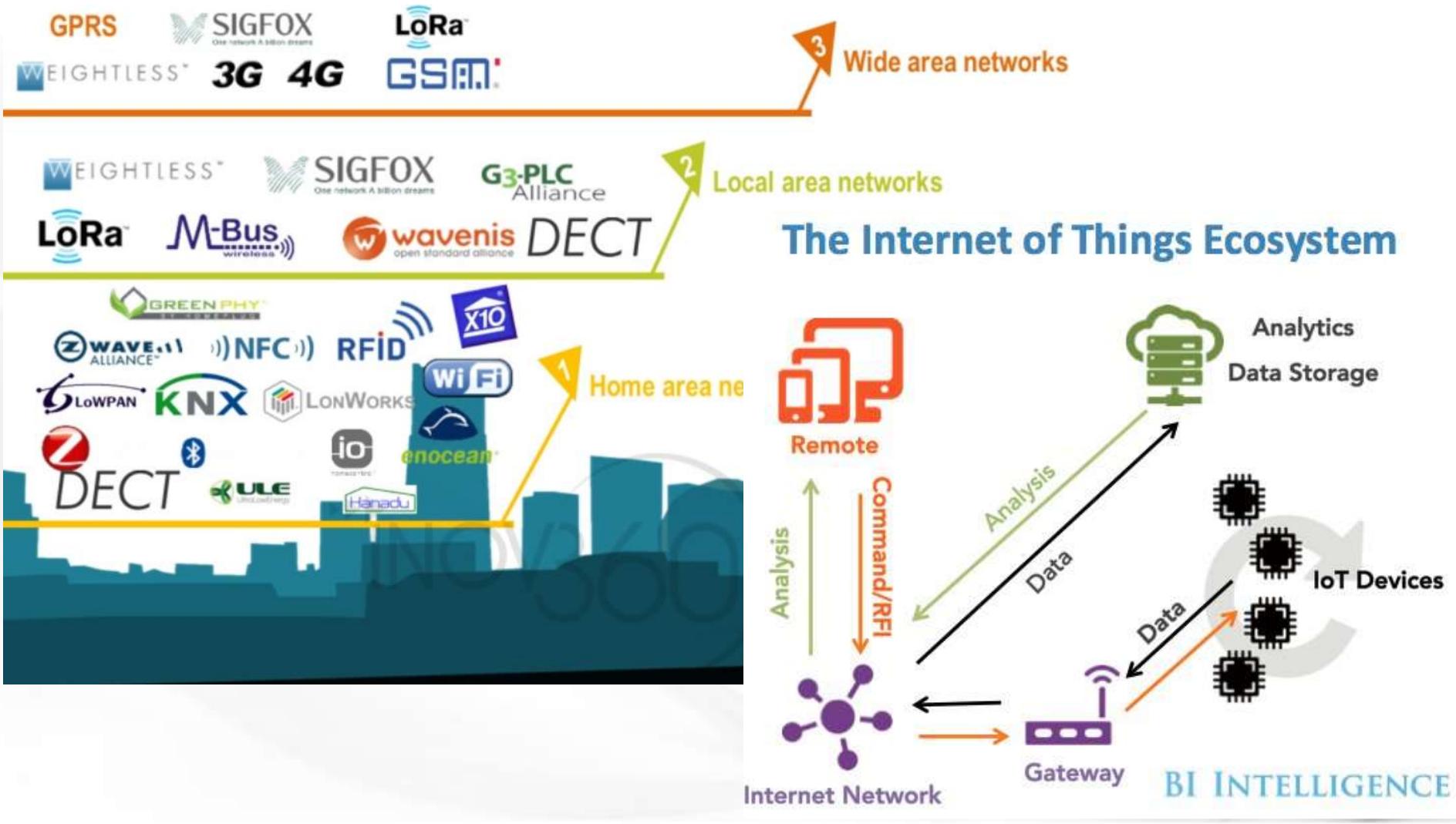
Разработка Compliance, стандартизация IOT Security

AMT GROUP

Безопасность IoT. Развитие специализированных коммерческих стандартов IoT с учетом требований ИБ

AMT GROUP

Безопасность IoT. Развитие специализированных коммерческих стандартов IoT с учетом требований ИБ



Безопасность IoT. Развитие специализированных коммерческих стандартов IoT с учетом требований ИБ

The AllSeen Alliance	Была основана некоммерческой организацией Linux Foundation. На данный момент в нее входят больше 50-ти организаций, включай таких тяжеловесов как Microsoft, Qualcomm, LG, Sharp и Panasonic. AllSeen ищет способ создать универсальные фреймворки для приложений.
The Open Interconnect Consortium (OIC)	Поддерживается Intel, Atmel, Broadcom, Dell. Главной задачей видят разработку общих требований для совместимости умных устройств.
The Thread Group	Сформирована подразделением Google Nest Labs. Включает больше восьмидесяти участников Samsung, ARM Holdings, Silicon Labs и другие. Умные дома
HomeKit	Поддерживается Apple и дает возможность производителям устройств ставить лейбл "Совместимо с iPhone". Умные дома
Industrial Internet Consortium	Основан Intel, Cisco, AT&T, GE и IBM. Включает более 150 участников, которые занимаются совместной разработкой стандартов связи между устройствами. **Определение стандартов безопасности и конфиденциальности IIC возложило на компанию CyberX и софтварного гиганта SAP**

AMT GROUP

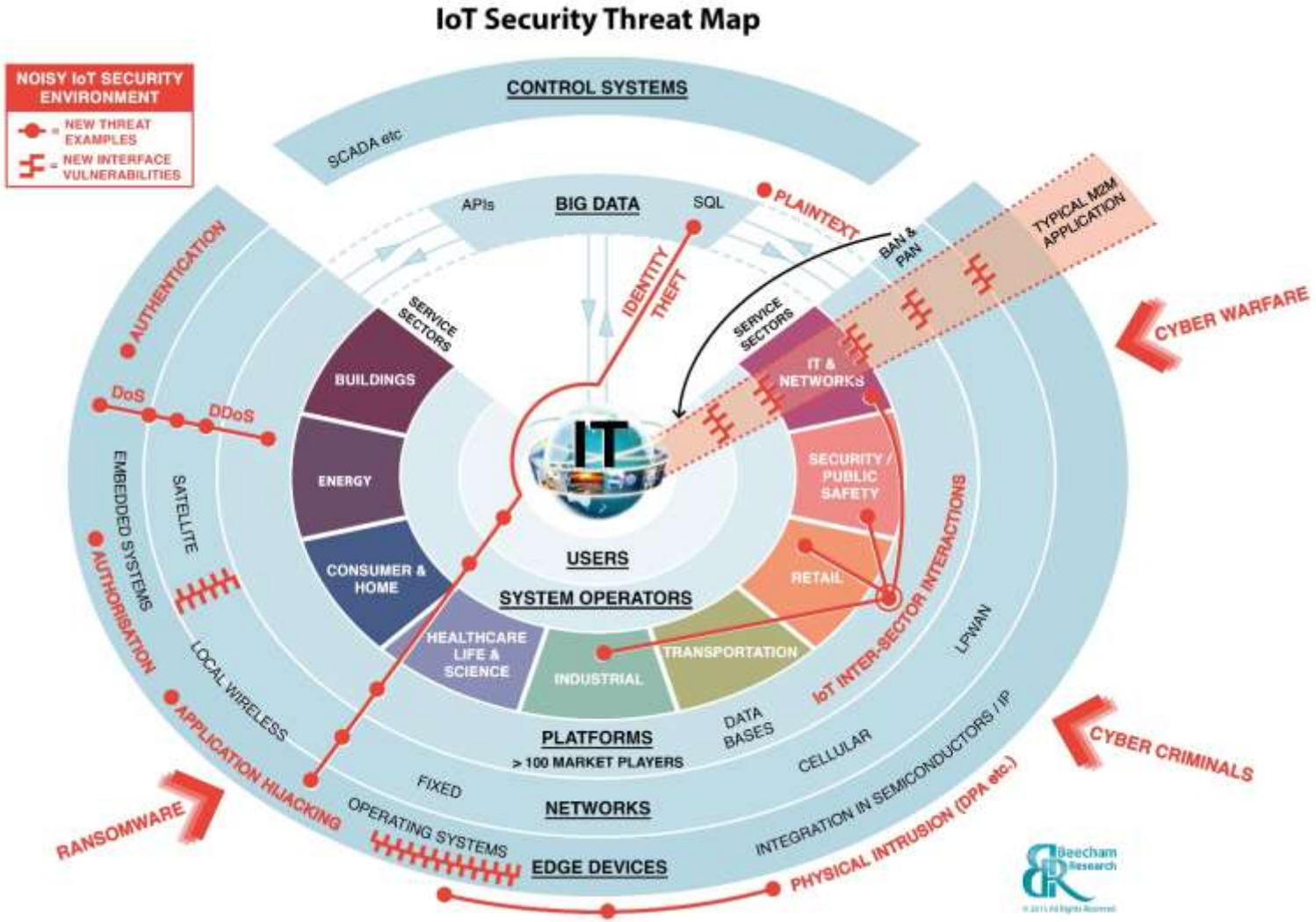
Безопасность IoT. Развитие традиционной нормативной базы ИБ

- ISO 27001
- NERC
- ISA 99 (62443)
- ФСТЭК
- HIPAA
- PCI DSS
- NIST

AMT GROUP

Практическая реализация IOT Security

Практическая реализация ИБ IOT



Практическая реализация ИБ IOT

1.Определение типа IoT, способа взаимодействия IoT
2. Исключить незащищенные устройства;
3. Шифрование передачи данных IoT;
4. Единая модель безопасности IoT;
5. Контроль доступа к IoT;
6. Контроль состояния устройств IoT;
7. Контроль подключения IoT;
8. Управление обновлениями IoT;
9. Соблюдение Compliance;
10. Применять новые и уникальные подходы ☺

AMT GROUP

СПАСИБО ЗА ВНИМАНИЕ!

AMT GROUP