Security Directions and Trends

Eric Hibbard, CISSP, CISA
CTO Security & Privacy
Hitachi Data Systems

Securing the Critical Infrastructure and Social Infrastructure of Tomorrow

Center for European Policy Studies

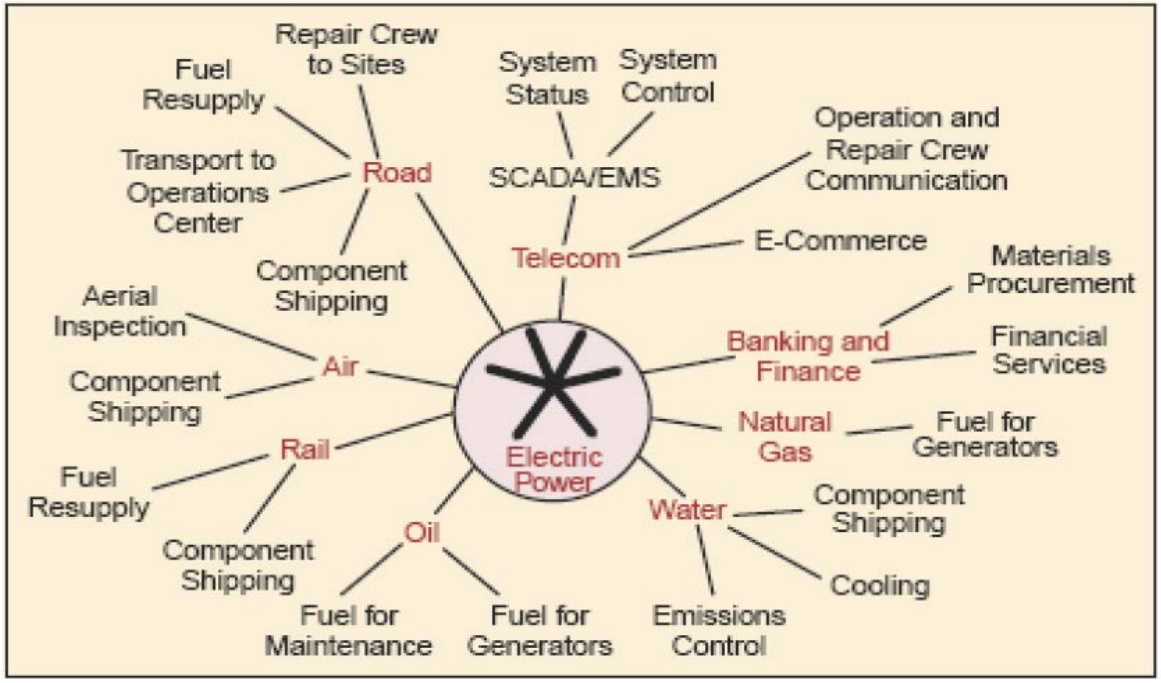
- CEPS Task Force Report, *Protecting Critical Infrastructure in the EU*
  - *"…several governments around the world have concluded that infrastructures that are considered to be 'critical' are increasingly vulnerable and interdependent with other critical infrastructures.*"
  - *"…the continuity of government, for business operations and for the supply of basic services to citizens has become so high that a disruption of any of these fundamental assets can cause considerable damage."*

Critical Infrastructure Sectors

- Identifying the elements of critical infrastructure is fraught with difficulties; globally inconsistent
- Differ from country to country, but generally include:
  - transportation systems (air, rail, road, sea);
  - energy production and shipping;
  - government facilities and services, including, in particular, defense, law enforcement and emergency services ;
  - information and communication technology;
  - food and water;
  - public health and health care;
  - financial institutions.
- US=16 sectors; CA=10 sectors; EU=12 sectors; UK=9 sectors; JP=10 sectors.

U.S. Critical Infrastructure

- Less than 20% controlled by government
- Significant vulnerabilities exist
- Cybersecurity a major focus
- Interdependencies can result in cascading failures

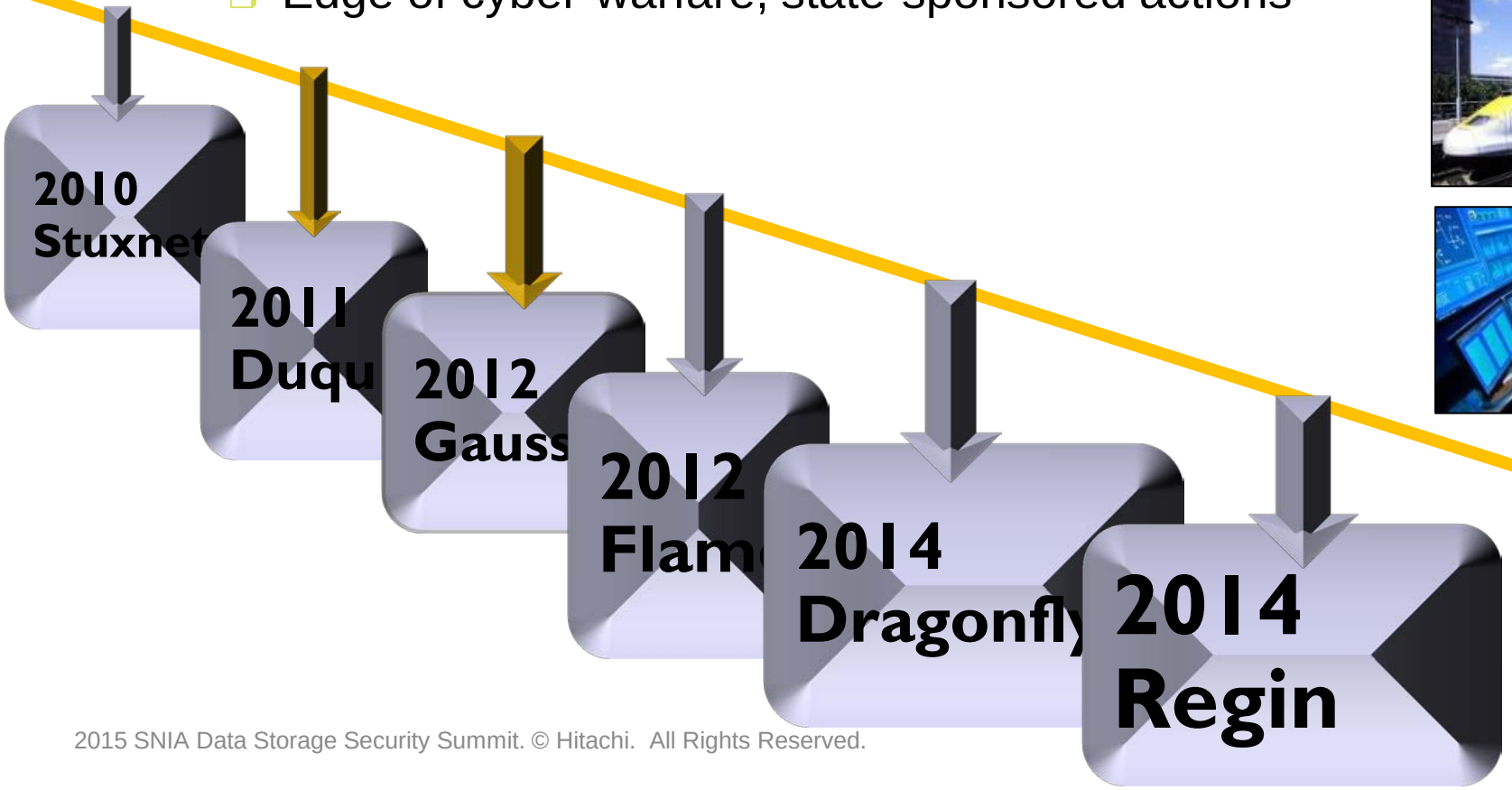


Threat Landscape for Critical Infrastructure (CI)

U.S. Department of Homeland Security, *Strategic National Risk Assessment*, December 2011, http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf. The full results of the SNRA are classified.

CI Protection

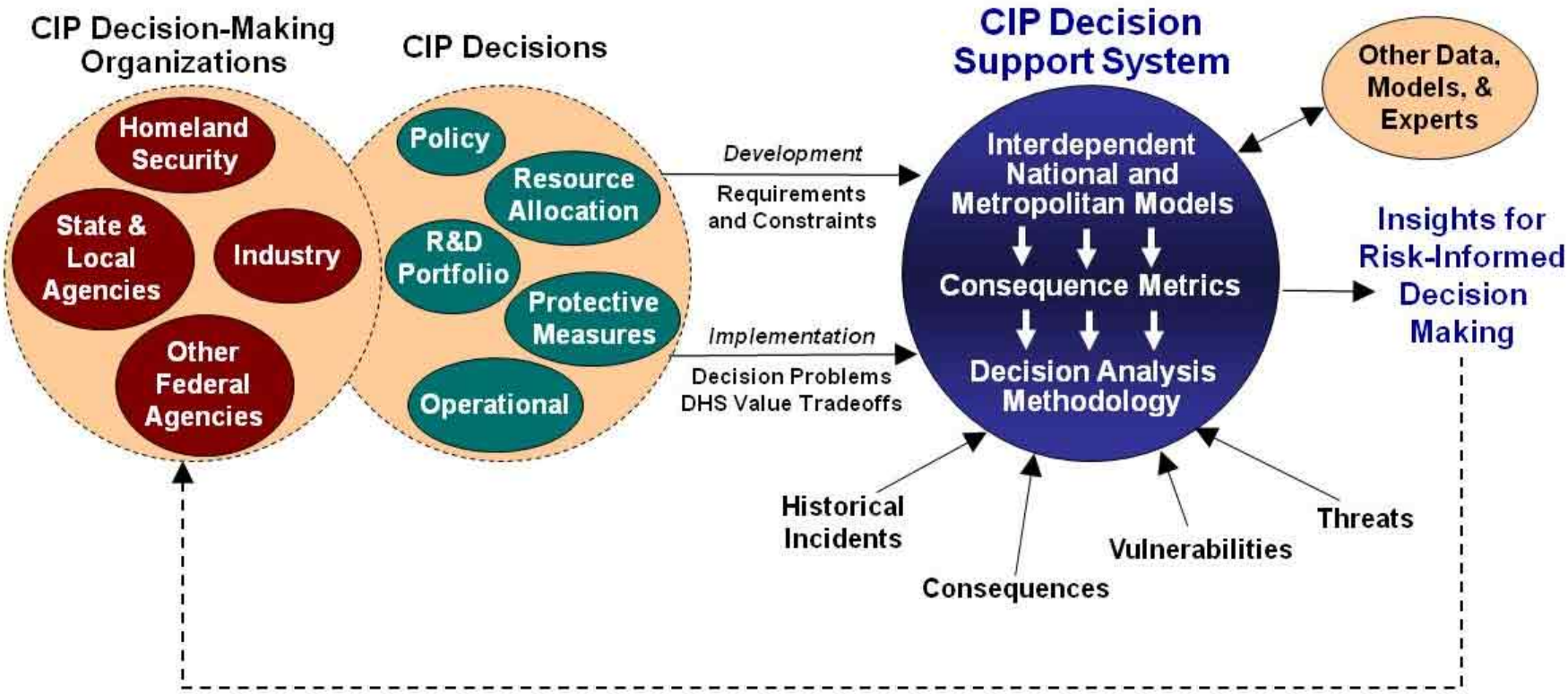
- **Catapulted to the forefront**
  - Several incidents of various nature
  - Widespread concern
  - Edge of cyber-warfare, state-sponsored actions



“National Emergency”

President Obama declared on April 1, 2015 that the rising number of cyberattacks against the United States is a national emergency and issued an executive order that would sanction those behind the attacks.

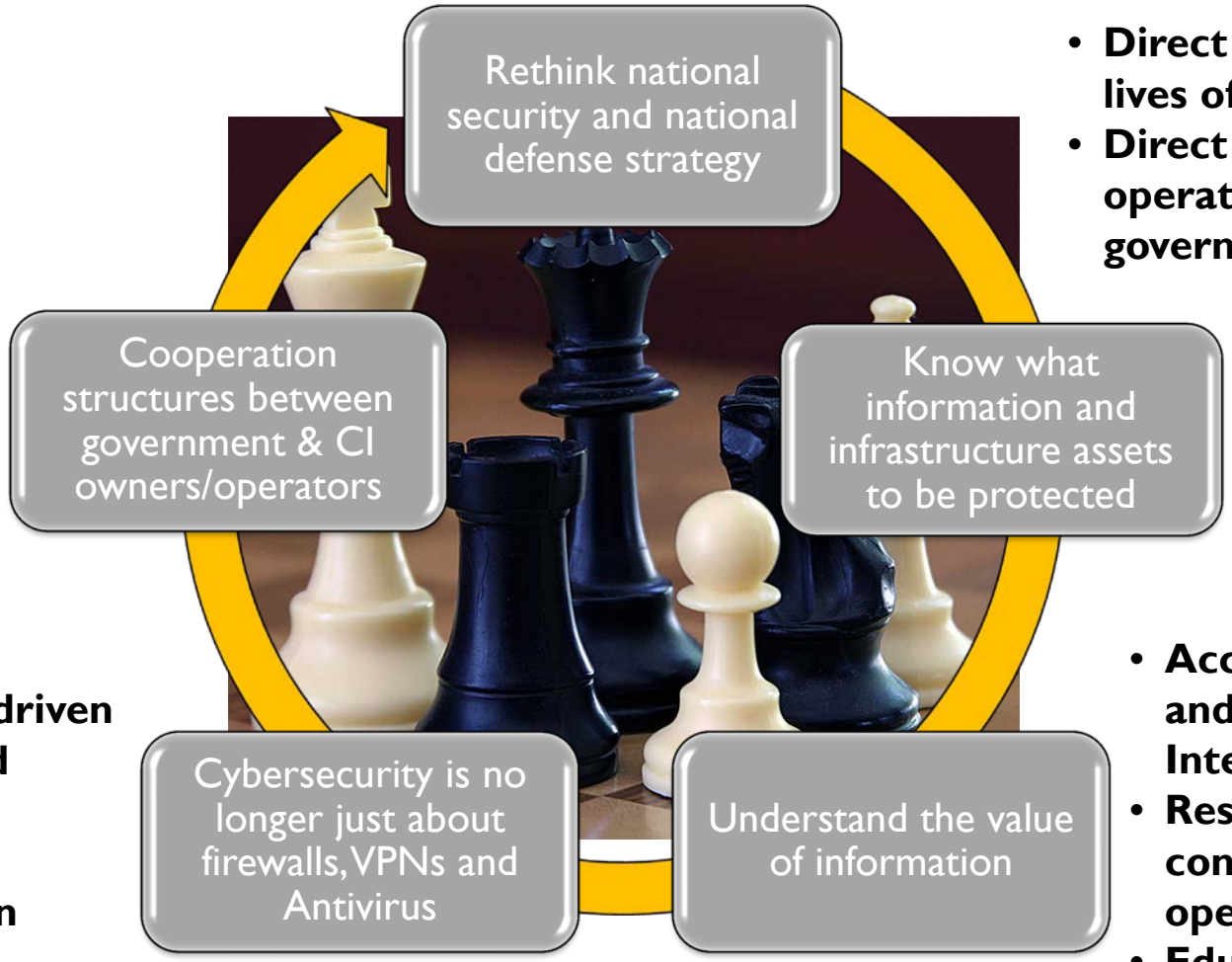
CI Protection Initiatives



http://www.lanl.gov/programs/nisac/cipdss.shtml

Where is the U.S. public sector going?

- **Info-sharing**
- **Threat mitigation**
- **Incident response**



- **Direct impact on the lives of citizens**
- **Direct impact on the operations of government**

- **Intelligence driven**
- **Dynamic and mobile**
- **Process and people driven**

- **Accidental loss and Open Source Intelligence**
- **Resilience and continuity of operations**
- **Educate the users**

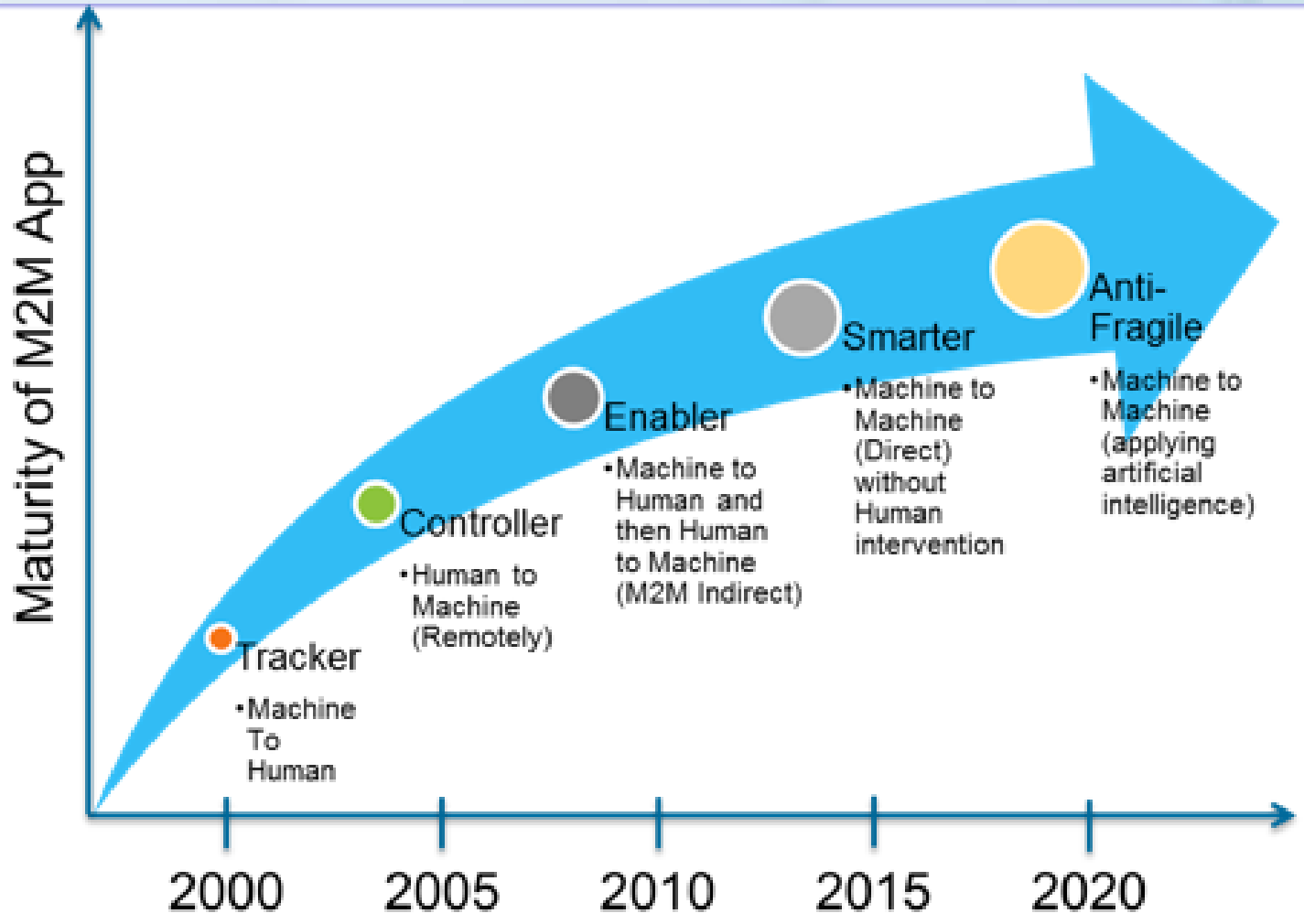
Changing ICT Landscape …

Disruptive Technologies

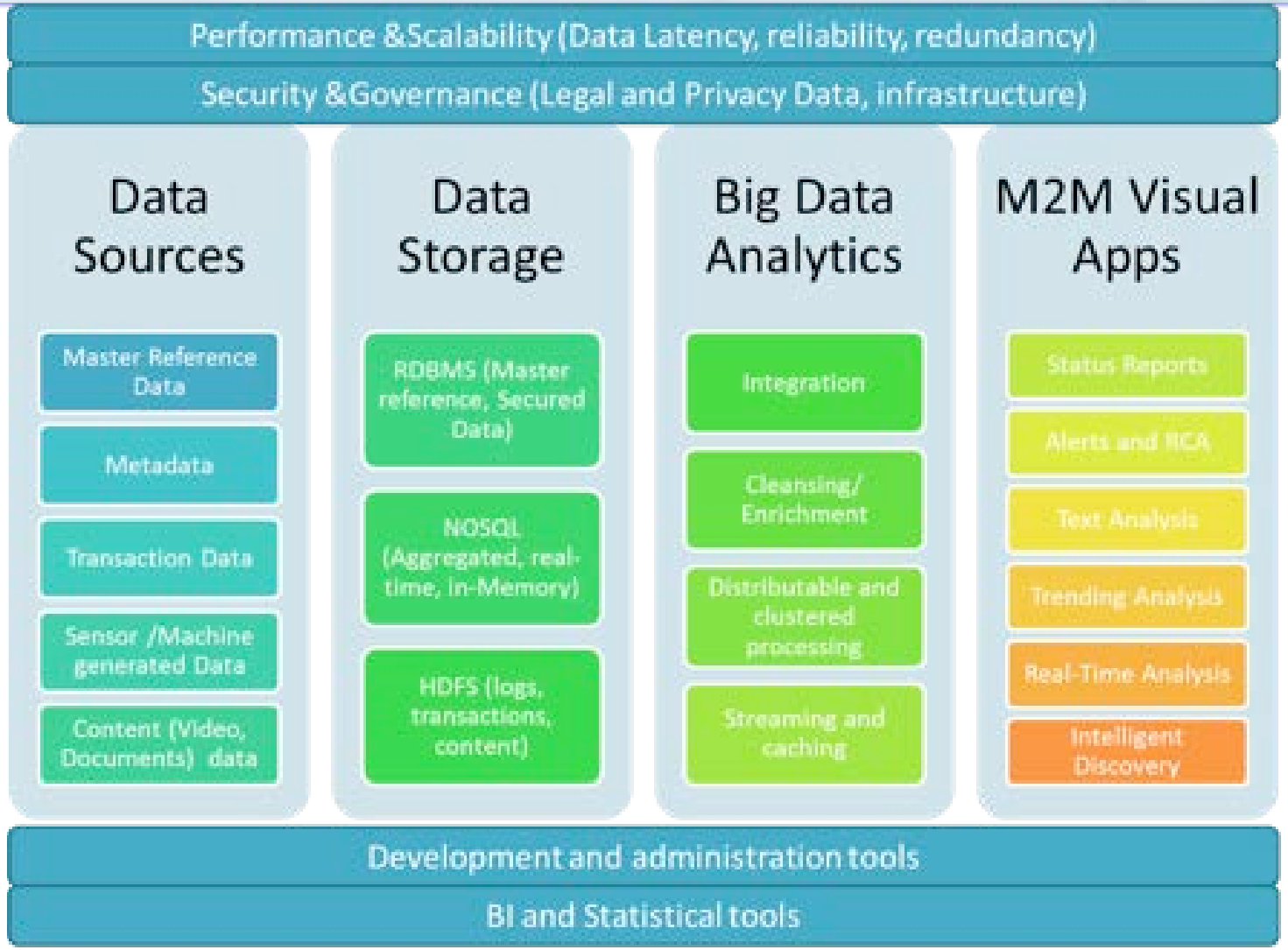
- Mobile computing
- Cloud computing
- Machine-to-machine (M2M)
- Big Data & Analytics
- Industrial Internet
- Internet of Things (IoT)
- Industry 4.0
- Software Defined “Anything”

- There are security & privacy issues for each
  - Complexity is compounded when they are used together

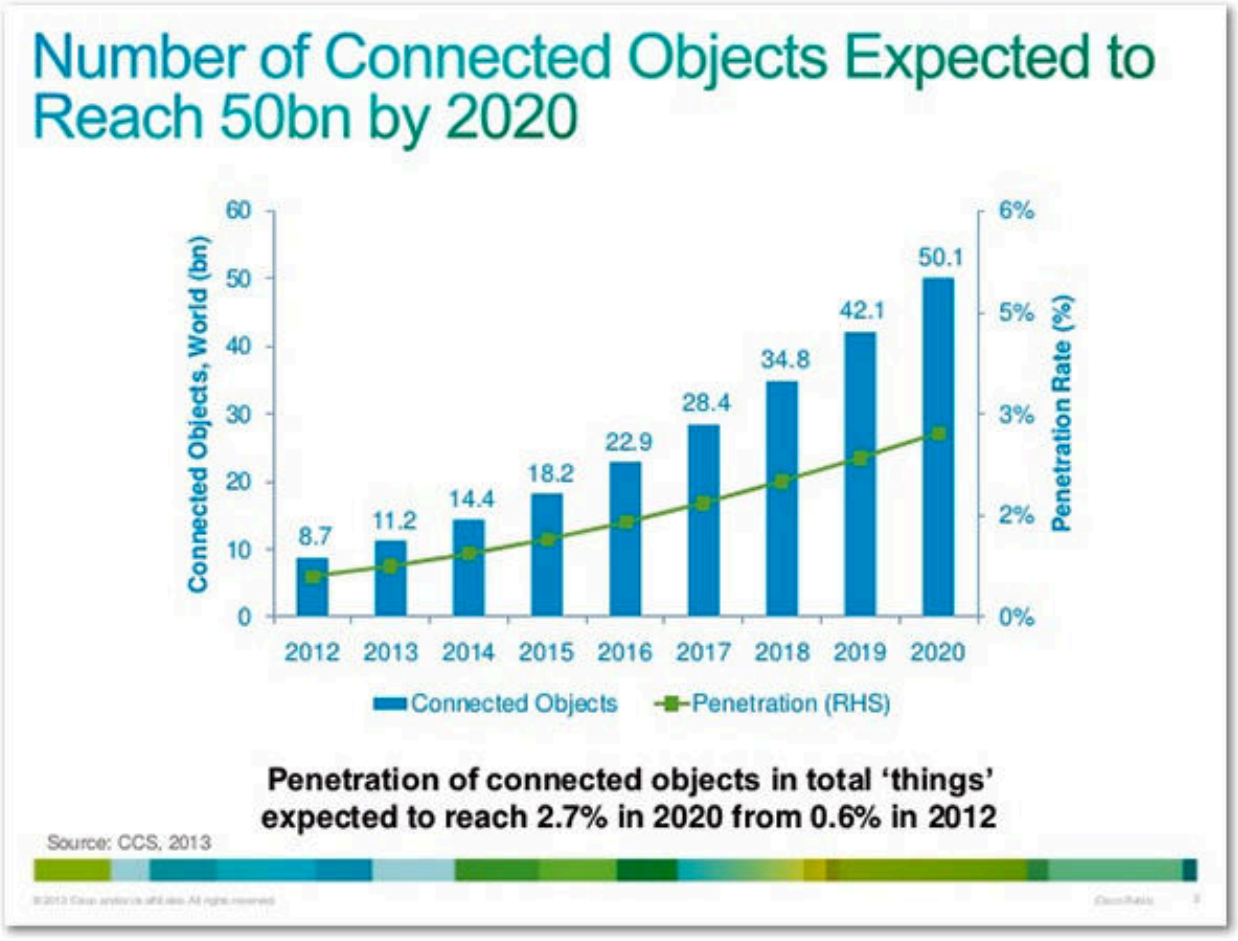
M2M Maturity



M2M analytics building blocks



How many IoT *things*?



NOTE: EMC and IDC are somewhat more conservative, putting the 2020 IoT population at 32 billion, while Gartner comes in with 26 billion.

IoT Will Drive Big Data Adoption

- IoT technologies will allow for real-time and accurate data sensing and transmission of that data to Internet-based systems (Web, cloud, etc.)
- IoT will lead to an exponential increase in the data that an enterprise is required to manage
  - from appliances, from machinery, from train tracks, from shipping containers, from power stations
- Without the proper data-gathering in place (big data and analytics), it will be impossible for businesses to sort through all the information flowing in from IoT systems
  - without big data, the Internet of Things can offer an enterprise little more than noise

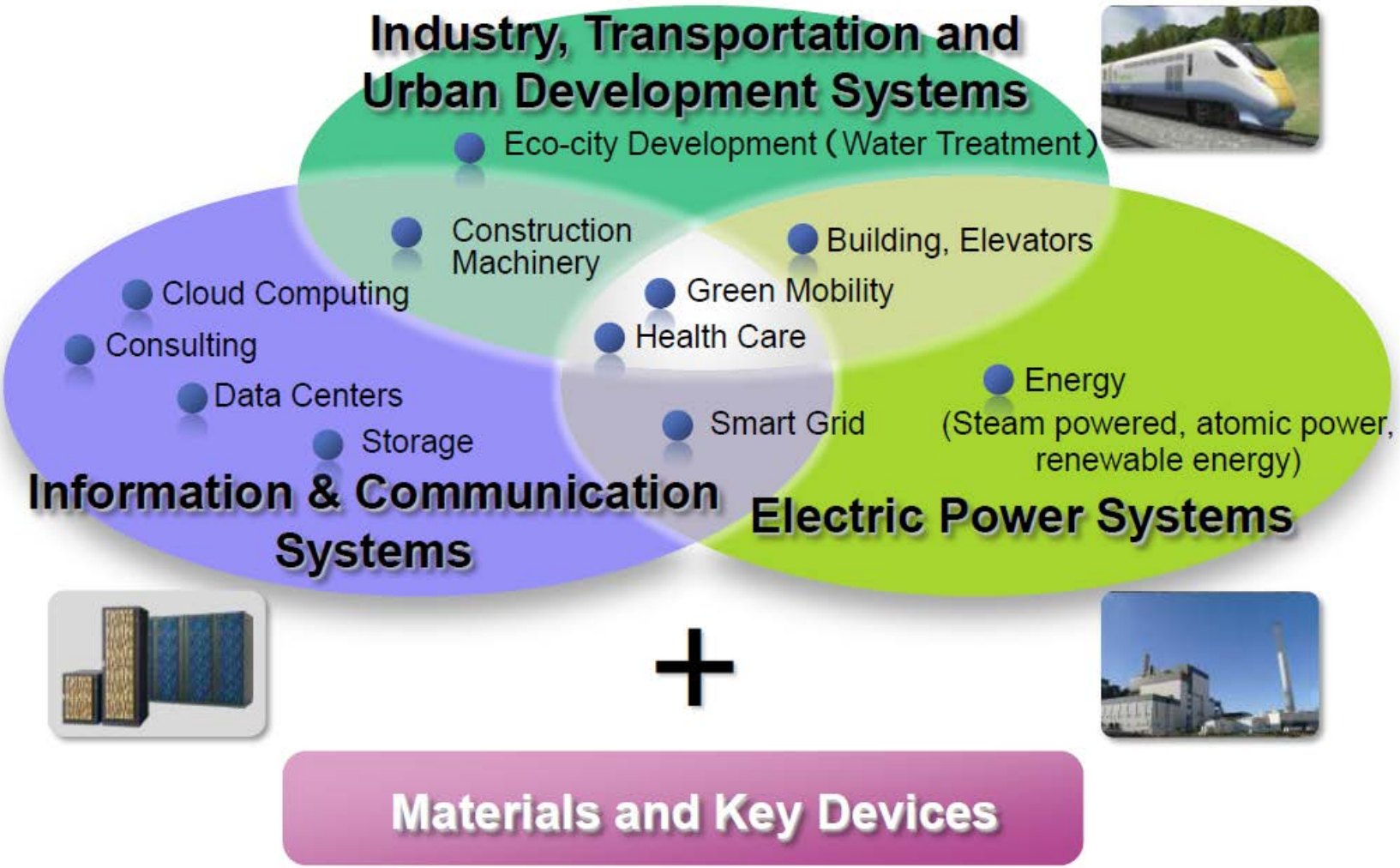
CI and Emerging Technology

- Emerging technology has the potential of improving critical infrastructure
  - Reducing costs
  - Improving reliability and resiliency
  - Expanding capabilities
- Systems/IoT, need to be standardised, interoperable and open
- The risks have to be understood and mitigated
  - Security and safety must be embedded from inception
  - Assume failures and employ fail-safe or fail-secure solutions

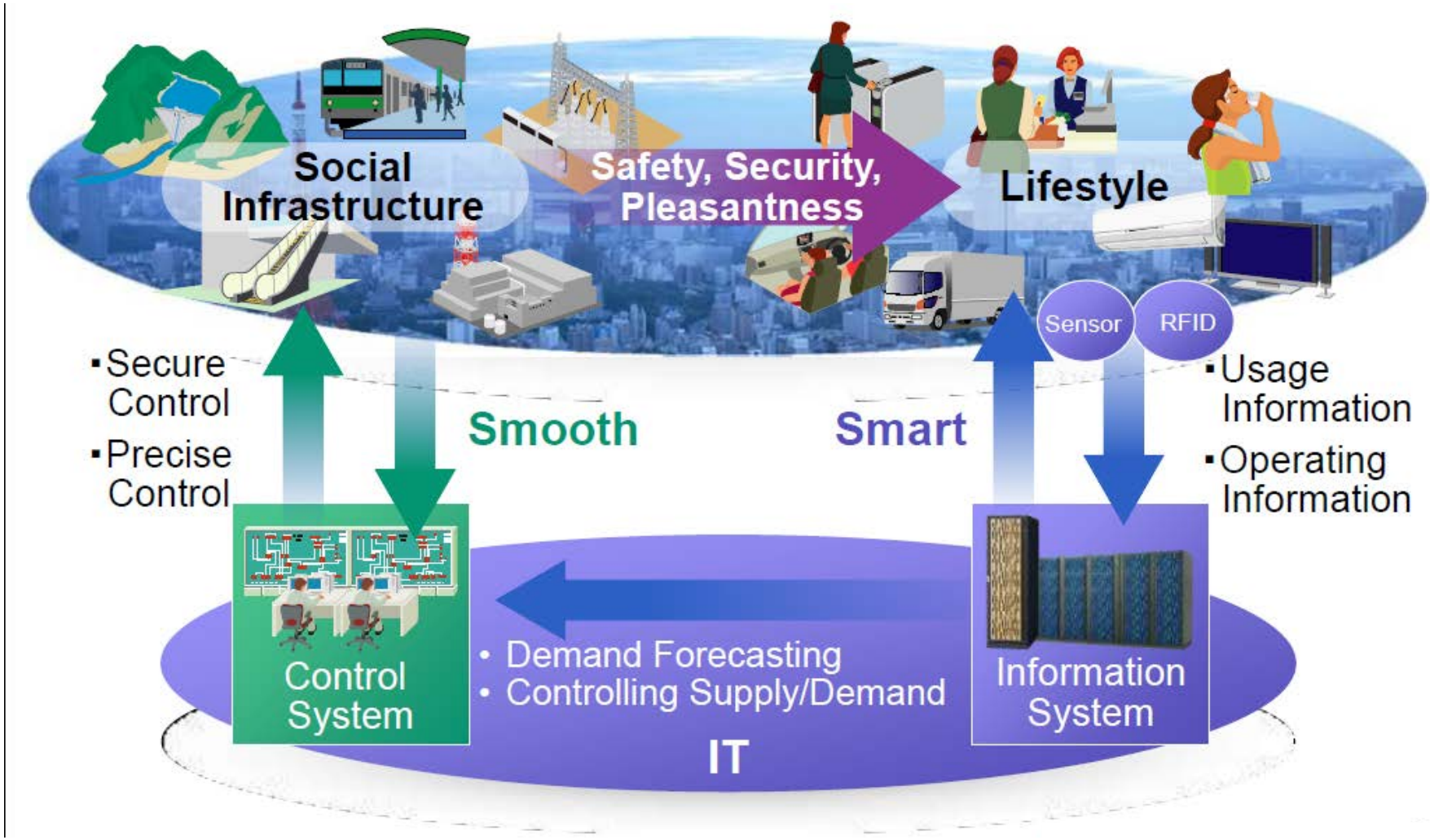
Looking to the Future

• • •

Social Infrastructure (Hitachi View)



Social Infrastructure Requires Collaborative Systems

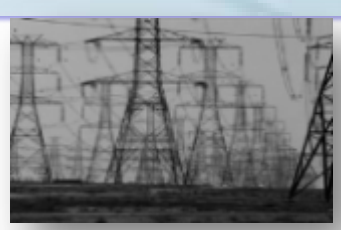


Securing smart sustainable city systems

- Highly complex ICT systems
- Highly interconnected components (IoT)
- High volume of data

Securing the Smart Sustainable City

Smart grids



Intelligent transportation

Connected healthcare

Public safety & security

Wireless & hotspots

Conclusions

- **Smart city deployments imply vulnerability**
  - Complex, heterogeneous ICT implementations
  - Diverse stakeholders
  - Hyper-connectivity, IoT, Big Data, Cloud Computing
  - Data is the digital currency - Data governance is the new focus
  - Intelligence + Processes + People + Tools
- **Cyber-attacks and data breaches are dangerous and costly**
  - Human lives - Data - Financial - Reputation - Credibility
- **Cyber-threats are here to stay**
  - Smart city must be conceived with *Cybersecurity* and *Resilience* in mind

Thank You

eric.hibbard@hds.com