Defense Trade Advisory Group (DTAG)

Cyber Working Group

Plenary Session

October 29, 2015

Cyber Working Group Members

Rebecca Conover (Co-Chair)

Lawrence Fink (Co-Chair)

Marjorie Alquist

Michelle Avallone

Fred Czarske

Kelly Hochstetler

Julia Court Ryan

William Schneider

Susan Willard

Larry Ward

Agenda

- DTAG Task
- Defining “Cyber Technology”
- Themes and Findings
- Recommendations
- Questions

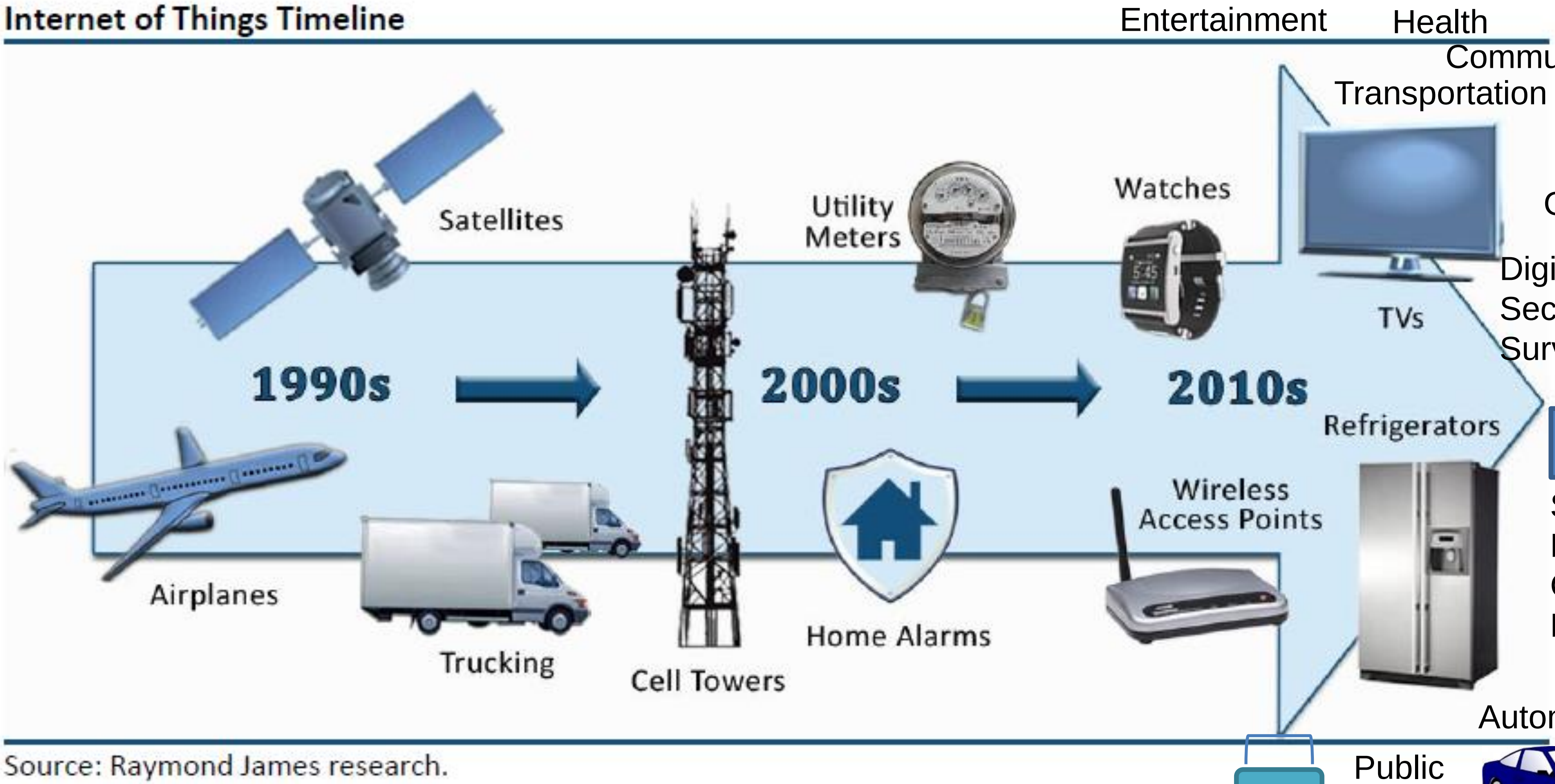
DTAG Task

- Define and categorize "cyber products" in an export control context and determine:
  - Which cyber products, if any, should be included on the U.S. Munitions List
  - The types of controls appropriate for each cyber category
  - The potential impact on cyber products, including but not limited to Big Data Analytics
  - How the recommendation differs from how cyber products are controlled today and why

Methodology

- Examined historical regulatory controls and trends in computing and cyber products
- Studied cyber product development and global availability of the related technology
- Defined the 3 cyber product categories with assistance from in-house cyber experts
- Researched proposed and existing cybersecurity rulings and industry comments
- Explored existing regulations and jurisdiction rulings affecting cyber and big data analytics
- Studied cyber product development and global availability of the related technology

Cyber Through the Years



Advertising

Entertainment

Health

Communications

Transportation

Energy

Gaming

Digital Security & Surveillance

Smart Buildings, Cities, Homes

Automobiles

Public Sector

Shopping/ Retail

Source: Raymond James research.

Adapted for DTAG use.

Defining "Cyber Technology"

- What is Cyber?
  - Items and activities involving a computer network
  - "Internet of Things" is characterized as items connected with electronics, software, sensors, etc. creating a network of connectivity
- Cyber Technology Categories
  - Cyber Security
  - Data Collection
  - Big Data Analytics
- Cyber Technology not considered
  - Encryption
  - Cloud Computing Controls (Harmonization Rule & Prior DTAG tasking)
  - Cryptography USML Category

Themes and Findings

- Cyber technology is becoming omnipresent in virtually all human endeavors and activities world wide and heading to a future of ubiquitous computing

- There is little or no technical distinction between offensive and defensive cyber capabilities

- Broad technical controls hinder scientific progress and R&D

- Cyber security capabilities are developed, enhanced and tested by utilization of hacking and malware items

Cyber Security

"…These tools are key to securing your enterprise because these are the same kinds of tools that attackers use. If you don't find your holes and seal them, they will exploit them."

Quote from the website of a software company selling pen test tools

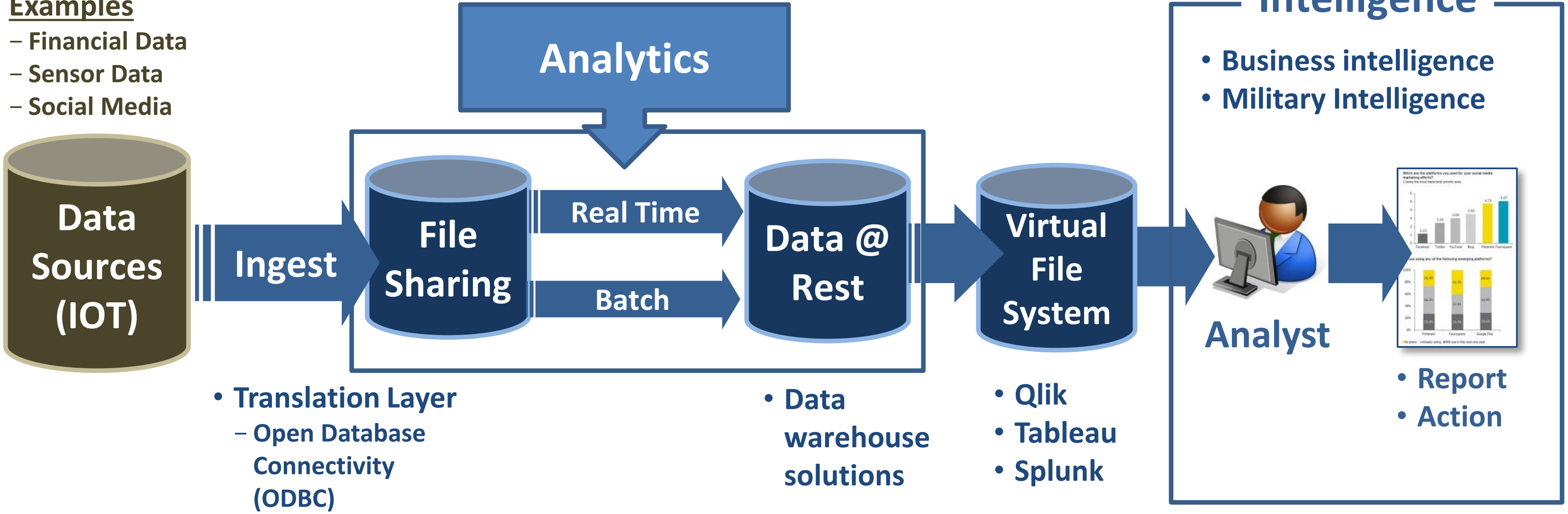
Themes and Findings (cont'd)

- Cyber products for commercial and military purposes are developed using fundamentally the same computing products and technologies that are globally developed and available
- The rapidly evolving nature of cyber technology does not lend itself to controls based on technical parameters associated with performance capabilities
- There is no difference between military and commercial big data hardware and technology building blocks
- Cyber products (including data analytics) are designed and available worldwide across borders

Big Data Analytics

- Structured
- Partially Structured
- Unstructured
- Examples
  - Financial Data
  - Sensor Data
  - Social Media

- Machine learning
- Natural Language Processing
- Open source
- Tailored Code



Intelligence

- Business intelligence
- Military Intelligence

Analytics

Data Sources (IOT)

Ingest

File Sharing

Real Time

Batch

Data @ Rest

Virtual File System

Analyst

- Report
- Action

- Translation Layer
  - Open Database Connectivity (ODBC)
  - Structured Query Language (SQL)

- Data warehouse solutions

- Qlik
- Tableau
- Splunk

Recommendations

1. Cyber products currently controlled under the EAR are dual-use and should not transfer to the ITAR
   - Would be contrary to ECR; DTAG did not identify cyber products or technology that warranted additional control

2. Remove or significantly revise USML Category XI(b)
   - Necessary control is captured under other categories such as USML XIII or XVII; unique military customization may be controlled as a defense service

3. Controls on cyber products (including data analytics) should be predominantly end-use or end-user based
   - Technology-based controls may be counterproductive to national security due to the collaborative development process imperative for cyber security products

Summary

- In order to stay at the forefront of technical advancement, only a very few cyber products should be controlled under the ITAR
- Dual-use and ITAR end-uses both benefit from the advancement of technology
- The Dept. of State should only control cyber products if they are classified or are positively enumerated on the USML.
- Heavy control on cyber products may have a negative impact on the development of cyber security measures to protect against cyber attacks

Defense Trade Advisory Group (DTAG) Cyber Working Group

Questions?