# Evaluating the Security Implications of Innovation: Risk and Risk Reduction in the *Internet of Everything*

UMUC Faculty Presentation to FISSEA 2015
Valorie King, Richard White, Sam Chun

University of Maryland University College

# Is this the Internet of Everything?

# Or, is this how you see the IoE?

# INNOVATIONS

University of Maryland University College

# Quantized Self

- Body Sensors (Tattoos, Electro Myographics)
  - Gestures
  - Authentication
  - Threat Detection (CBRNE)
- Wearable Computers
  - Communications & Productivity
  - Health & Fitness
  - Augmented Reality (input / feedback)
- Implants & Medical Devices
  - Body Area Networks
  - Medication Delivery
  - Monitor / Augment internal systems
  - Prosthetics

# Infrastructures & Technologies

- Smart Homes
- Smart Communities
- Autonomous Vehicles
- Intelligent Transportation Infrastructures
- Utilities Infrastructures & Advanced Metering
- Banking Sector & Digital Currencies

# Enabling Technologies

- Graphene
- Neuromorphic Chips
- Brain-Computer Interfaces
- Physical Unclonable Functions (PUFs)
- Dielectric thin films
- Magneto-electric magnetic sensors
- Nano imprinting
- Nano machines

# TECHNOLOGY REVIEWS

# Technology Transfer

- Technology Identification & Maturation
  - Identifying promising technologies in R&D phases
  - helping technologies emerge from the R&D environment
- Technology Transfer Processes (Universities)
- Technology Transfer Initiatives  (DHS, DOE)
- Influence of funding availability & sources, i.e. venture capital, government grants, etc.

# Technology Development Life Cycle

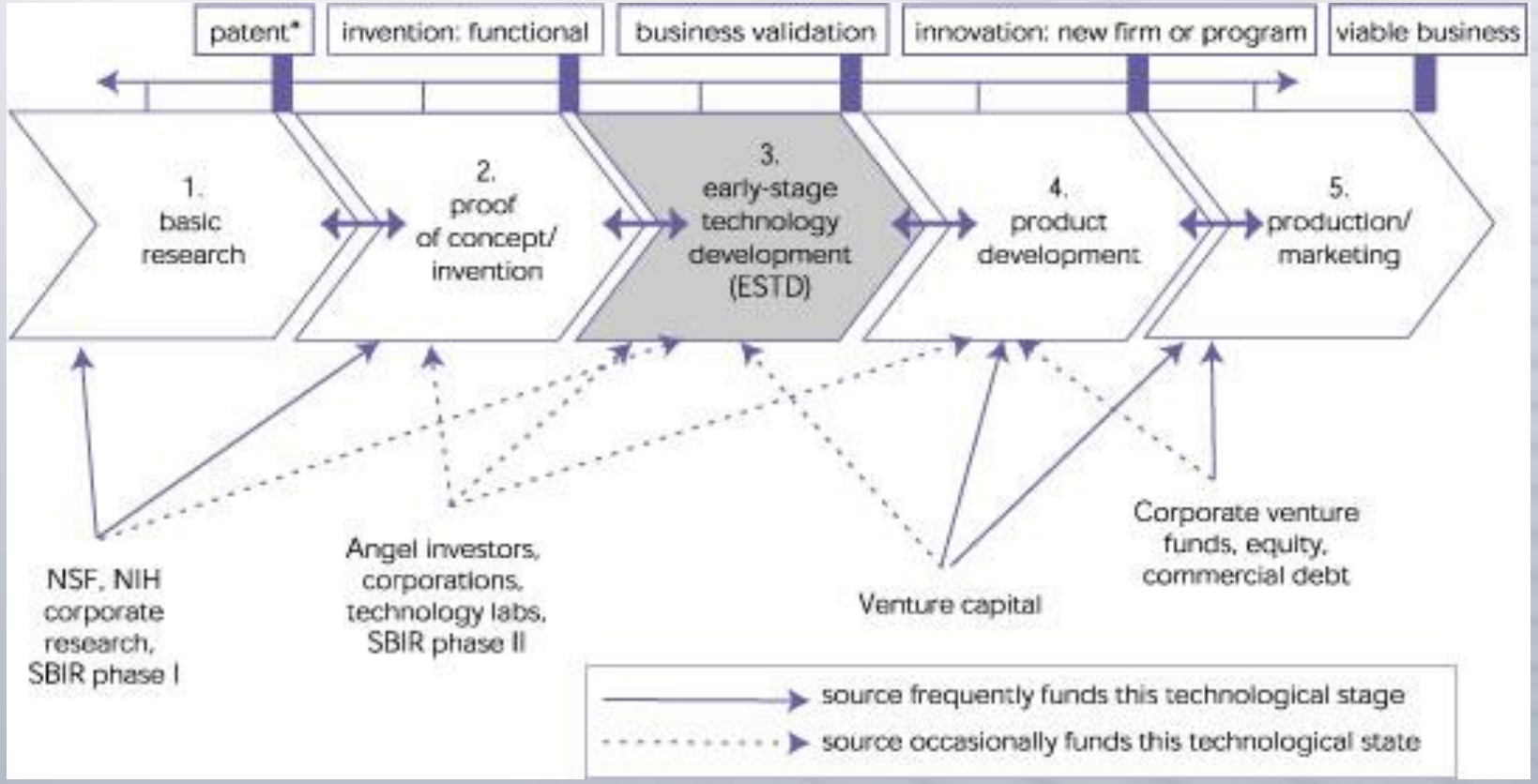




**Image Source: http://www.atp.nist.gov/eao/gcr02-841**

# Technology Identification & Evaluation Process

# RISK IDENTIFICATION

University of Maryland University College

# Cybersecurity & Emerging Tech

- Incorporating emerging technologies into products and services
  - What security features are needed?
  - Can we predict how these features will fail?
  - Can we identify *potential or expected* cybersecurity:
    - Gaps
    - Risks
    - Vulnerabilities

# Evaluation Methodologies

- Analysis of Alternatives
- Case Studies
- Delphi Technique (Expert Panels)
- Experiments
- Gap Analyses
- Meta-Analyses (Published Research)
- Pilot Studies & Implementations
- Product Assurance
- Risk Assessments

# Analysis of Alternatives

# Experiment-Based Evaluations

# RISK REDUCTION

University of Maryland University College

# Two Key Questions

- How can this technology or emerging application of technology be used to improve or support the security of devices and services which comprise the Internet of Everything?

- How can this technology be used by attackers, criminals, terrorists, etc. to achieve their goals and objectives within the context of the Internet of Everything?

# SUMMARY & CONCLUSIONS

# Cybersecurity for the IoE: Built-in or Bolted-on?

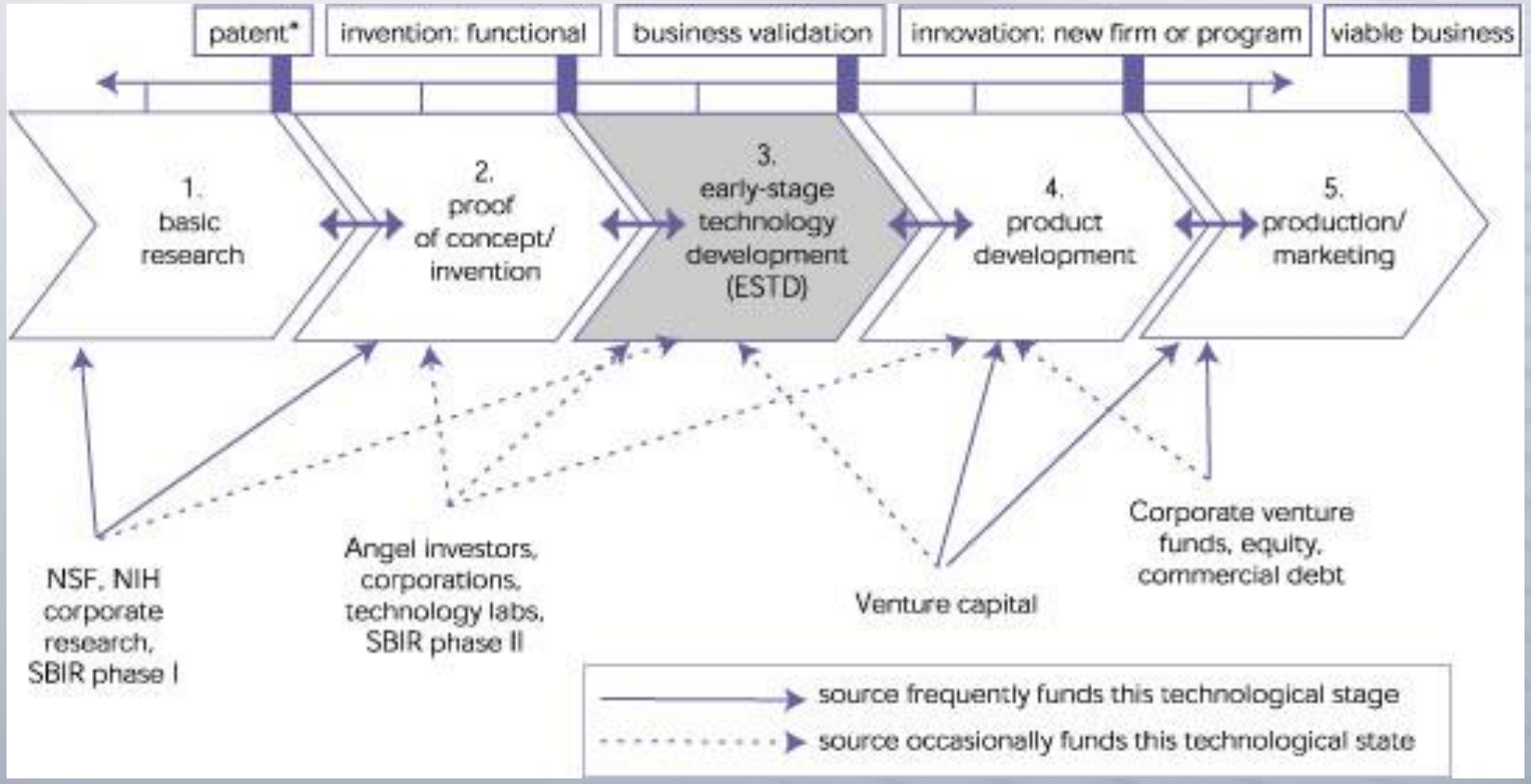


Image Source: http://www.atp.nist.gov/eao/gcr02-841

# Questions?

# Contact Information

- Valorie King (Course Chair):
  - Valorie.King@faculty.umuc.edu
- Richard White (Course Chair):
  - Richard.White@faculty.umuc.edu
- Samuel Chun (Faculty Member):
  - Samuel.Chun@faculty.umuc.edu