

Panel on Government Sponsored Research

A Major Enabler for Cybersecurity - Vision for the Future

Angelos D Keromytis
Program Manager
Information Innovation Office

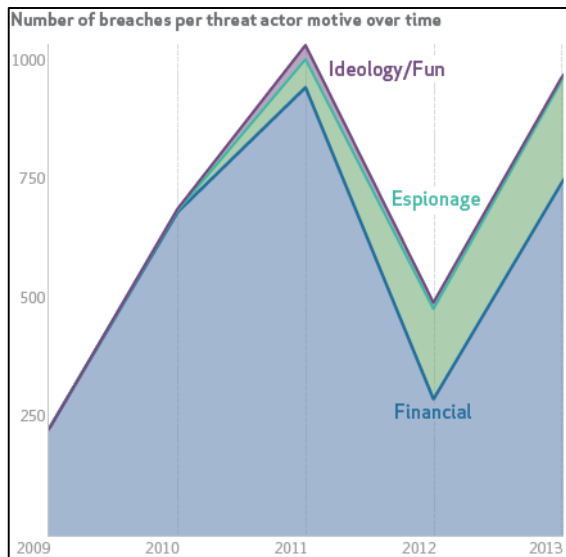
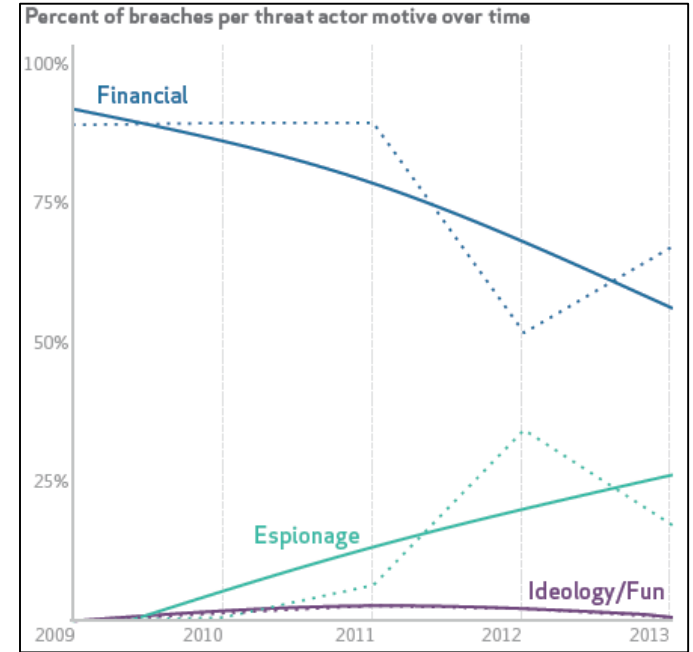
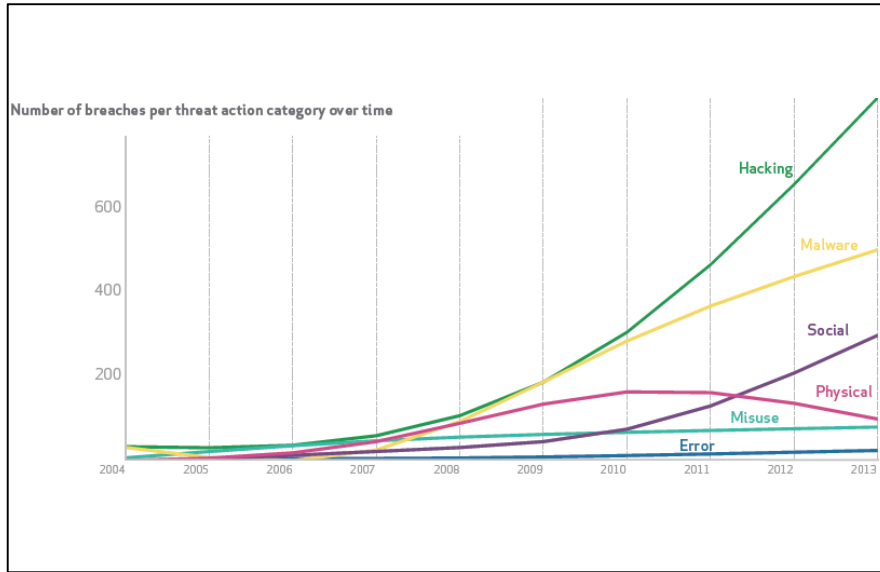
The views, opinions, and/or findings contained in this presentation are those of the presenter and should not be interpreted as representing the official views or policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the Department of Defense.

September 12, 2014





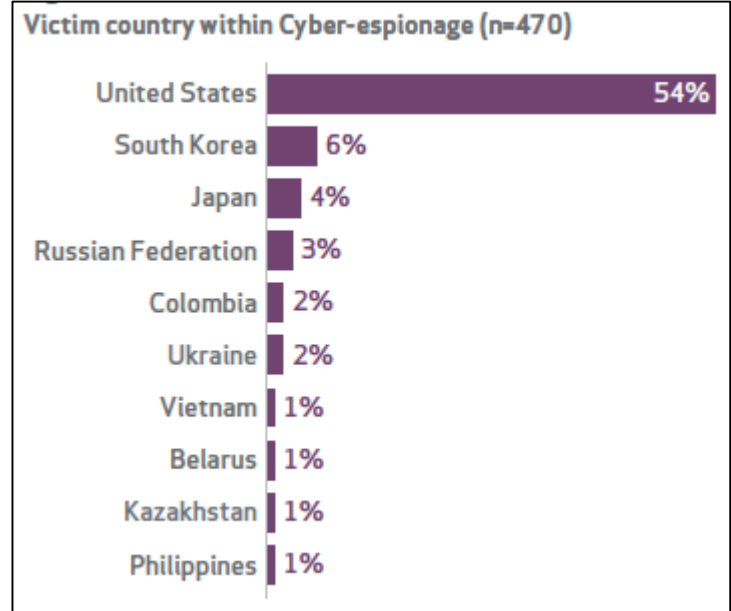
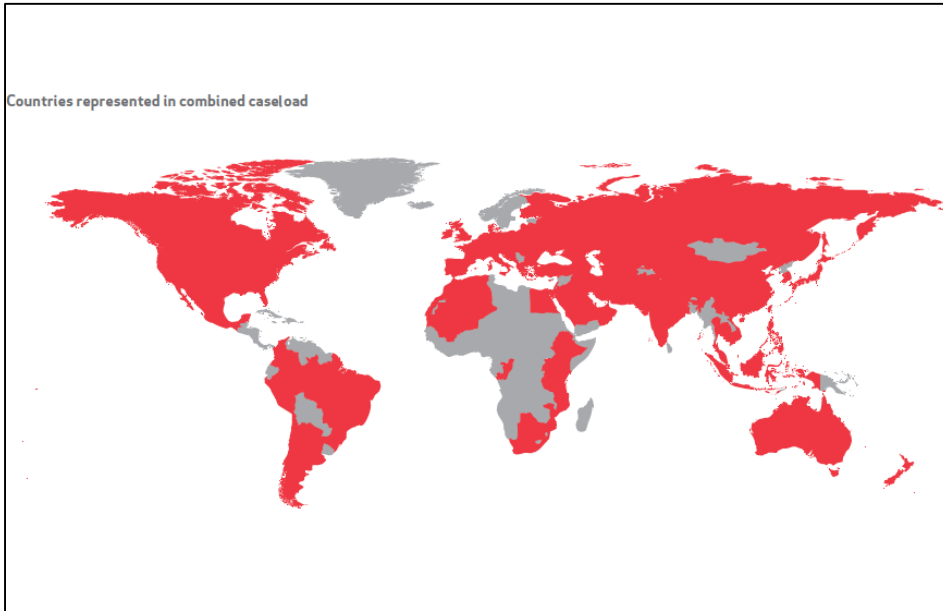
Significant and Increasing Activity...



Source: 2014 Verizon Data Breach Investigations Report
<http://www.verizonenterprise.com/DBIR/2014/>



...Targeted at Us



Caveat: self-selectivity, unknown ground truth...

Source: 2014 Verizon Data Breach Investigations Report
<http://www.verizonenterprise.com/DBIR/2014/>



Questions Posed to the Panelists

1. What are the top 5 cyber threats to national security in the coming decade?
2. What are the top 5 technology areas where funding and research is critical to national security in the coming decade?
3. How are the current funding opportunities aligned with (1) and (2), and what are the future plans within the government to better interact and provide incentives for the research community?
4. How can government help streamline cyber security technology transfer in both the commercial and the government space?
5. What are the cyber security strengths and opportunities in the greater New York area?



Panelists

- Kathleen Bogner – Office of the Director of National Intelligence (ODNI)
- Jeremy Epstein – National Science Foundation (NSF)
- Angelos Keromytis – Defense Advanced Research Projects Agency (DARPA)
- Sukarno “Karno” Mertoguno – Office of Naval Research (ONR)
- Konrad Vesey – Intelligence Advanced Research Projects Activity (IARPA)
- Cliff Wang – Army Research Office (ARO)
- Different personal and organizational perspectives, agency priorities



“Creating breakthrough technologies for national security is the mission of the Defense Advanced Research Projects Agency (DARPA). By making pivotal investments in new technology-driven ideas for the United States, DARPA imagines and makes possible new capabilities for overcoming the multifaceted threats and challenges that lie ahead.”



<http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2147487842>

- Examples: Stealth, Computing and Communications, Microelectronics, ISR, SatNav/GPS, UAVs, IR “night vision”
- How does it work?
 - 100 Program Managers (term-limited)
 - Recognize risk, threat and opportunity
 - Make reasoned argument for program need
 - Find performers who can answer the questions posed!
 - Little-to-no research done “in house”
 - Partnership with military Services for transition



National Security Threats: 16 Years

- 1998 FBI National Security Threat List (NSTL)

- Terrorism
- Proliferation
- Economic Espionage
- Espionage
- Foreign Intelligence Activities
- Targeting the National Information Infrastructure
- Targeting the US Government
- Perception Management

<http://www.wright.edu/rsp/Security/T1threat/Nstl.htm>

- 2014 DNI IC Threat Assessment

- Terrorism
- WMD and Proliferation
- Counterintelligence
- Cyber
- Transnational Organized Crime
- Counterspace
- Economic Trends
- Natural Resources
- Health Risks
- Mass Atrocities

http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf



Observations

- System compromise is inevitable
 - If only because they are operated by humans...
 - ...and they are too complex to fully understand
- Data collection is increasingly detailed and pervasive
- Remote action in physical domain is starting to become possible



Top 5 Cyber Threats in the Coming Decade

- Targeting “hidden” computing



- Blended (physical + cyber) attacks



- Privacy

- Information Integrity and Perception Management

- Yes, this is still a (“the” ?) top vector: legacy systems



Top 5 Tech Areas for NatSec in the Coming Decade

- Cyber, Bio, Space, Robotics, Micro-manufacturing (e.g., 3D printing)
- Within Cyber
 - Systems, Data, and Humans
 - Attribution and accountability
 - Data integrity
 - Secure Cyber Physical systems and architectures
 - Privacy



Current Priorities and I2O Programs

- Hardening legacy systems
 - VET, APAC, CSFV
- Clean slate systems design
 - CRASH, MRC, HACMS, MUSE
- Cyber and Human interaction
 - Active Authentication, ADAMS, SMISC
- Dealing with system complexity
 - ICAS
- Protecting information and communication
 - PROCEED, SAFER
- Understanding cyberwarfare
 - PLAN-X, Cyber Genome, Cyber Grand Challenge



Streamlining Technology Transition

- Direct transition to government (Services)
- SBIR/STTR
- DARPA Open Catalog: <http://www.darpa.mil/opencatalog/>



Cybersecurity Strengths & Opportunities in NY

- Big (and increasing) community in cybersecurity
- Financial Industry
- Advertisement and Media
- Entrepreneurial culture
- Cross-institutional effort modeled after New York Nanoscience Initiative?