
NORTHROP GRUMMAN

# Northrop Grumman Cybersecurity Research Consortium

## GUIRR Spring Meeting
## Washington DC

## 9 February 2011

**Robert F. Brammer, Ph.D.**
**VP Advanced Technology and Chief Technology Officer**
**Northrop Grumman Information Systems**

# Key Points for This Presentation

NORTHROP GRUMMAN

- **Cybersecurity threats continue to grow in numbers, sophistication, and significance**
  - **Advanced Persistent Threat, intellectual property and other monetary theft, critical infrastructure, cyber warfare, …**
- **Northrop Grumman is the leading provider of security systems and services to the USA public sector (growing internationally, as well)**
  - **Defense, intelligence, civil government agencies (federal, state, local)**
  - **Information operations, cyber security, identity management, physical security (e.g., access management, surveillance, etc)**
- **Very dynamic arena -- Addressing the cybersecurity challenges requires continuing advanced research from many organizations**
- **We are reaching out to the leading research universities to complement our cybersecurity R&D program and have created this consortium for collaborative projects**

# Northrop Grumman Today

- ~$34 billion in revenues
- 120,000 people, 50 states, 25 countries
- Leading capabilities in:
  - Climate and environment
  - C4ISR and battle management
  - **Cybersecurity**
  - Defense electronics
  - Homeland security
  - Information technology and networks
  - Naval shipbuilding
  - Public health
  - Systems integration
  - Space and missile defense

# Major Factors Affecting our Cybersecurity Technology Strategy

NORTHROP GRUMMAN

- **Growth in range, size, and value of IT and CI applications**
  - **Implies needs for many types of security architectures and ability to handle massive amounts of data and make real-time cybersecurity decisions**
- **Cybersecurity has now become a national priority**
  - **Increased investment and many more players – rapidly changing arena requires continuing dialogs with many organizations**
- **Cybersecurity is a complex and multi-disciplinary subject**
  - **Many dimensions and domain-specific aspects**
  - **Technology developments but also strategic, economic, psychological, sociological, and legal developments**
- **Technology strategy must align with Northrop Grumman business strategy**
  - **Technology investments largely governed by business strategy**
  - **Need for some exploratory R&D**

# Planning the Northrop Grumman Cybersecurity Research Consortium

NORTHROP GRUMMAN

## Concept

- Create a research consortium for challenging cyber security problems
- Focus on leading schools and research relevant to NGIS strategies
- Scope includes joint Northrop Grumman-university research (IRAD and CRAD)

## Selecting Universities

- Graduate school ratings
- History and depth in cybersecurity
  - Research center, commercialization
- Recognition in cybersecurity – thought leadership, professional awards, research sponsors
- Northrop Grumman UR&R activities

## Objectives

- Develop leading edge technology concepts and discriminators – market shaping and increased PWin
- Increase Northrop Grumman thought leadership, technology intelligence, branding
- Increase graduate recruiting at top university cybersecurity programs

## Research Areas

- 14 research areas defined in RFP
  - See next chart
- Matched to Northrop Grumman cyber strategy
- 40+ proposals received, 10 selected

# Northrop Grumman Cybersecurity Research Consortium Research Areas

- Application Security
- Attribution
- Critical Infrastructure Networks
- Cybersecurity Modeling and Simulation
- Decomposable Systems
- Fast Forensics
- Identity Management
- Information Tagging Architectures
- Insider Threats
- IPv6 Transition
- Privacy
- Security Metrics and Related Performance Measures
- Situational Awareness
- Supply Chain Risk

# Northrop Grumman Cybersecurity Research Consortium

NORTHROP GRUMMAN

## Northrop Grumman

- Largest provider of security systems and services to the US public sector
- Customers -- DOD, Intelligence, Civil agencies, state/local governments

NORTHROP GRUMMAN

## Carnegie Mellon -- CyLab

- One of the largest research and education centers for cybersecurity
- Affiliated with the CERT-CC, the first security emergency response team

Carnegie Mellon

Carnegie Mellon CyLab
CONFIDENCE FOR A NETWORKED WORLD

## MIT – Comp Sci and AI Lab

- Internet pioneer with a long history of successful commercial spinoffs
- 4 Turing Award winners

Massachusetts Institute of Technology

CSAIL

## Purdue – CERIAS

- World's largest academic center addressing information assurance, security, and privacy
- ~25% of cybersecurity Ph.D's during the past 10 years

PURDUE UNIVERSITY

CERIAS

# Northrop Grumman Cybersecurity Research Consortium

NORTHROP GRUMMAN

NORTHROP GRUMMAN | Carnegie Mellon | Massachusetts Institute of Technology | PURDUE UNIVERSITY

- Develop leading technology capabilities
- Stimulate thought leadership, innovations, educational initiatives
- Recruiting at leading university cybersecurity programs

## Aligning Projects to Business Strategy

| | CMU1 | CMU2 | CMU3 | MIT1 | MIT2 | MIT3 | Purdue1 | Purdue2 | Purdue3 | Purdue4 |
|---|---|---|---|---|---|---|---|---|---|---|
| Awareness in all Domains | | X | | | | | | | X | |
| C2/Mission Management | | X | | | | | X | | | |
| CNO (Exploit, Defend, Attack) | | | X | | | | | | X | |
| Cybersecurity Services | | | X | X | X | | | | | X |
| Information Security Core Offerings | | | | | X | | | | | |
| Integrated Architectures | | | | X | X | X | | | | |
| Market Shaping Activities | | | | | X | X | | | | |
| Security Operations Centers | X | | | | | | X | X | X | |
| Sensors | X | X | | | | | | X | | |

## NGCRC Projects (2009-2010, 2010-2011)

- CMU – Real-time malware detection, automatic exploit generation, control network cybersecurity, mobile network and device security
- MIT – Secure software by design, secure audit trails, trusted cloud architectures with FPGAs, recovering system integrity with selective re-execution
- Purdue – Watermarking and provenance, scalable cyber-ranges, fast forensics, defending SOA's against collaborative attacks

## Accelerating the Technology Transition

- Approach includes strategic framework and shorter communication lines
  - Projects derived from market priorities, integration perspective, and strategic plan
  - Collaborative projects, networking, cooperative use of facilities
  - Education and professional development
- Northrop Grumman Cybersecurity Research Consortium expansion will include industry partners

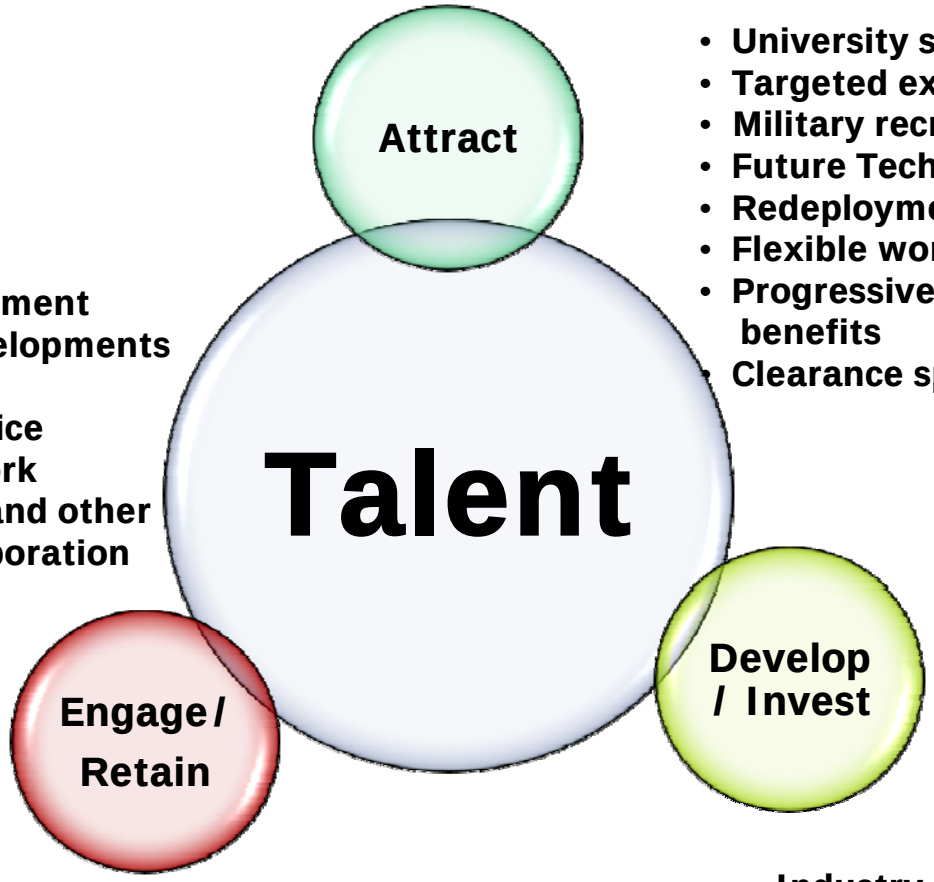
# An Assessment of the First 18 Months

NORTHROP GRUMMAN

- **Funded projects at top research universities in cybersecurity – CMU, MIT, Purdue**
- **Growing level of collaboration – learning to work together, joint work on IRAD projects, some joint CRAD proposals in development, university PI's starting to call us about CRAD opportunities**
- **Example results**
  - **CMU – Automatic generation of exploits demonstrated on several applications, database of malware developed for Northrop Grumman massive information project**
  - **MIT – "Secure by Design" technology tested on Northrop Grumman biometrics software, innovative approach to cloud security incorporated into Northrop Grumman strategy**
  - **Purdue – Approach for scaling cyber test range results being applied to UK test range planning, digital watermarking applications**
- **Encouraging beginning, but much room for growth**
  - **Evolving priorities**
  - **New or expanded projects**
  - **Additional universities, …**

# Cybersecurity Talent Development Strategy

NORTHROP GRUMMAN




- University strategies
- Targeted experienced recruiting
- Military recruiting
- Future Technical Leaders Program
- Redeployment – career pathways
- Flexible work offering
- Progressive compensation & benefits
- Clearance sponsorship strategy

- Enhance the work environment
- Advanced technology developments
- "Savvy" leader
- Cyber community of practice
- Advanced cyber lab network
- Utilize social networking and other types of distributed collaboration

- Industry and university research
- Expand Northrop Grumman Cyber Academy
- Progressive career path
- Certifications
- Internal rotational program
- Apprenticeships / mentoring

***Focus on continuing development and effective deployment of professional staff***


NORTHROP GRUMMAN