L-3 Communications
National Security Solutions Group

Public-Private Collaboration in Cyber Research

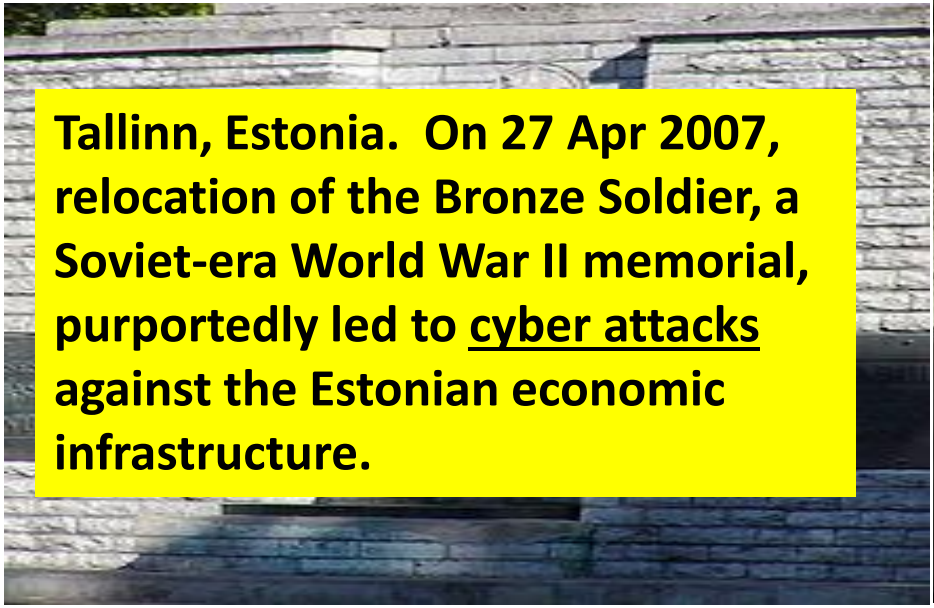
This presentation consists of L-3 Communications Corporation general capabilities and administrative information that does not contain controlled technical data as defined within the International Traffic of Arms (ITAR) Part 120.10 or Export Administration Regulations (EAR) part 734.7-11 (04-13).

About L-3 Communications

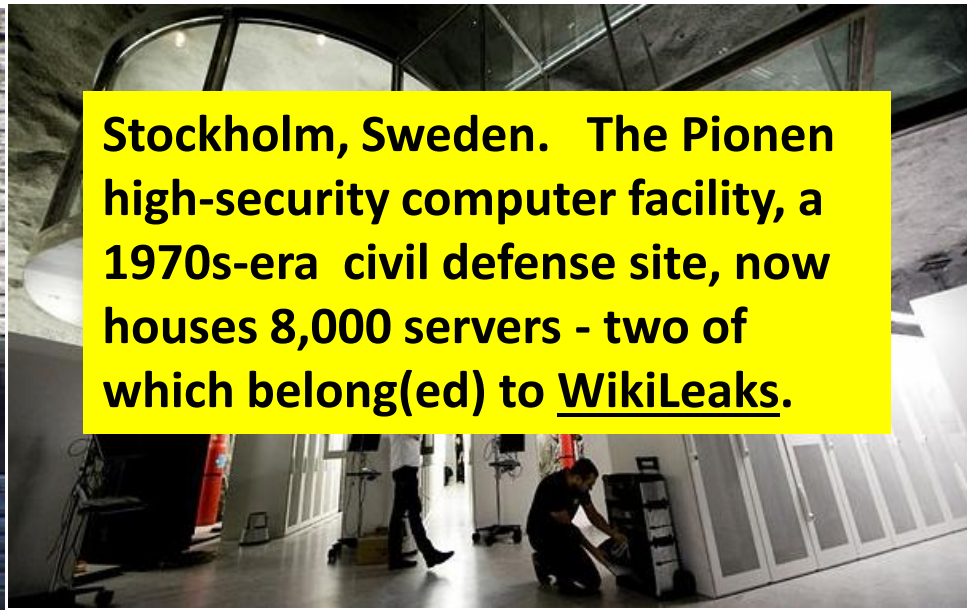
- **Headquarters in NYC**
- **Fortune 150, S&P 500**
- **Global Defense Company**
- **52,000 Employees Worldwide**

But First, A Short Cyber Quiz…

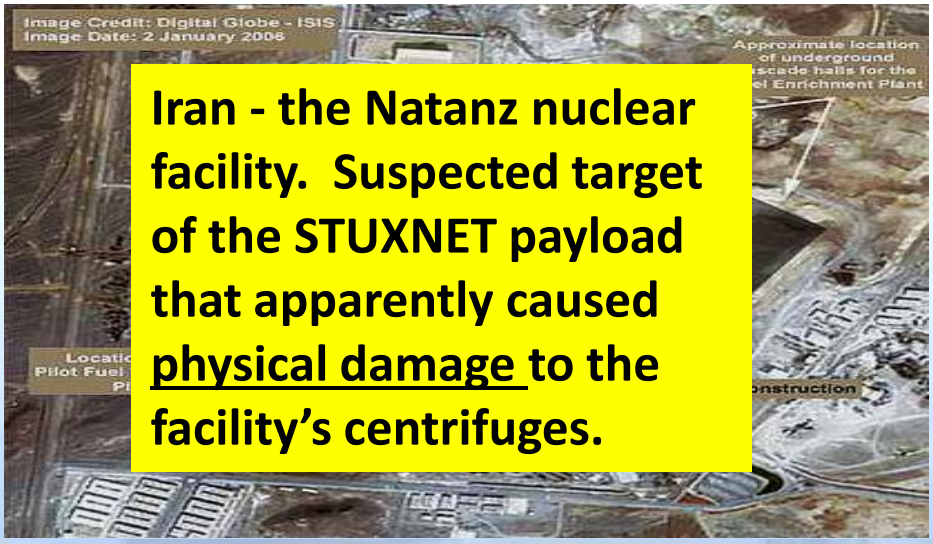
Answers...



Tallinn, Estonia. On 27 Apr 2007, relocation of the Bronze Soldier, a Soviet-era World War II memorial, purportedly led to <u>cyber attacks</u> against the Estonian economic infrastructure.



Stockholm, Sweden. The Pionen high-security computer facility, a 1970s-era civil defense site, now houses 8,000 servers - two of which belong(ed) to <u>WikiLeaks</u>.

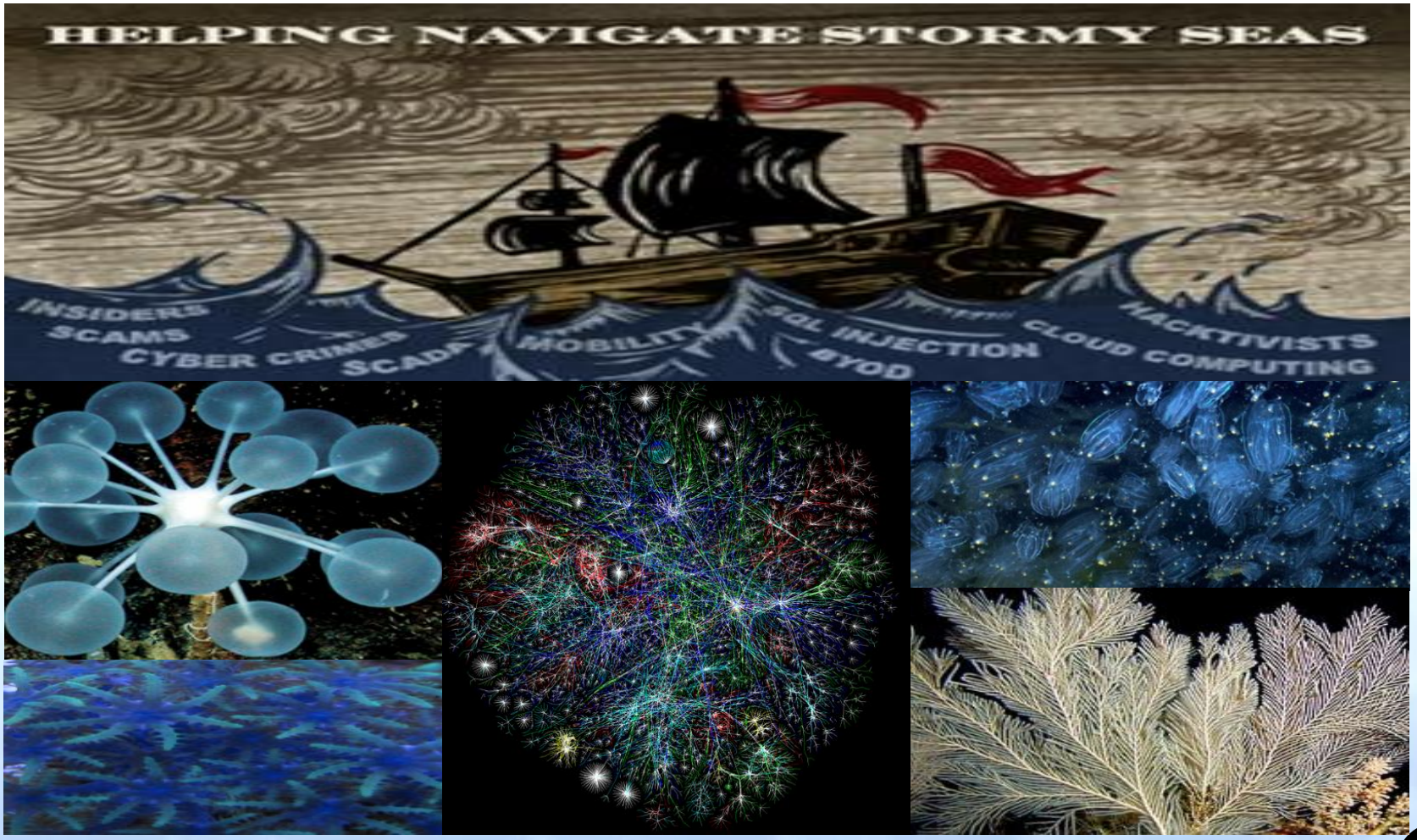


Iran - the Natanz nuclear facility. Suspected target of the STUXNET payload that apparently caused <u>physical damage</u> to the facility's centrifuges.

Tahrir Square, Cairo. There is on-going debate over the role of <u>social media</u> in the Arab Spring uprising.

Researching The Stormy Seas of Cyber

The fundamental nature of the cyber domain drives the need for advanced research to find new solutions.



Factors Driving Public-Private Collaboration in Cyber Research

- **Complexity of the Internet**
- **Sophisticated threat environment**
- **The need to share information**
- **Shared risk, expertise, and resources**

L-3 / NYU-Poly Cyber Research

- L-3 is proud to partner with The Polytechnic Institute of New York University in cyber security research
  - Steve Korns: stephen.korns@l-3com.com; 703-434-4558

- Dr. Kurt Becker - Associate Provost for Research & Technology Initiatives, Professor of Applied Physics, and Professor of Mechanical and Aerospace Engineering
  - Kurt Becker: kbecker@poly.edu kurt.becker@nyu.edu
    718-260-3608

NYU·poly

NYU·poly
POLYTECHNIC INSTITUTE of NYU

Research @ NYU-Poly

Research and
Technology Initiatives

- Our faculty's sense of continual discovery in the context of our i^2e (invention, innovation, and entrepreneurship) continuum shapes our research

- Faculty focus their research to meet society's challenges and devise solutions to real world problems, research with a purpose

- NYU-Poly represents a vibrant academic environment for discovery and original scholarship characterized by a rich exchange among disciplines

- Faculty collaborate across the university to expand the scope and reach of their research.

Research @ NYU-Poly

Cybersecurity Leaders at NYU-Poly

Nasir Memon
Professor of Computer Science
Cybersecurity Expert

Ramesh Karri
Professor of Computer Engineering
Cybersecurity Expert

Justin Cappos
Professor of Computer Science
Cybersecurity Expert

Models of University – Industry (- Government) Research Partnerships

1. The Project-specific, individual PI Research Agreement

- Individual research agreements engaging university researchers to address specific industry needs, with or without involvement of industry researchers

2. The Umbrella Model (L-3, Interdigital, Con Edison, …)

- Broad Umbrella Agreement addresses IP issues, publication issues, governing laws, possible indemnification, etc.
- Specific research projects are set up with faculty as SOWs under the umbrella agreement addressing tasks, milestones, personnel, payment plan, etc.

3. The NSF I/UCRC and NYS CAT Model

- Government funding is used set up a university-based Center
- Mandated matching from industry to support the Center; industry can shape research agenda, access to university talent, first look at emerging technologies

4. The Industrial Affiliates/Members Sustained Center Model

- Center defines a value proposition to a certain industry sector, e.g. WIRELESS
- Industry joins and supports Center via an Affiliates/Membership program
- Industry can shape research agenda, access to university talent, first look at emerging technologies

→ Similar to I/UCRC and CAT Model, but without the government support and the accompanying restrictions

Research @ NYU-Poly: Focus Areas

Urban Science, Engineering & Technology

- **More than 50% of the world's population lives in cities, with an urban infrastructure (transportation, water, energy, communications, waste) that is aging and often failing**

- **Our faculty from science, engineering, public policy, finance, management, medicine and law work to deliver the next wave of technological and operational solutions**
  - designing smarter power grids
  - engineering sustainable building materials that withstand natural and disaster/hazards
  - IT- and data-driven aspects of urban systems and smart cities are central

- **Urban Science, Engineering & Technology drives NYU's initiative "The Future of Cities"**
  - urban engineering (sensors, sensor systems, and actuators; cyber-communication and control systems; smart grid and integration of renewable energy, etc. …)
  - city planning, design, and development
  - social and behavioral sciences of cities and their inhabitants
  - legal and health issues in cities
  - ecology of cities
  - urbanization and the coastal zone (particularly after Superstorm Sandy !)

- **Urban Science, Engineering & Technology supports CUSP, the Center for Urban Science and Progress, a NYU-led consortium of university & industrial partners, and NYC agencies.**

Research @ NYU-Poly: Focus Areas

Information & Communication Technology

- Global cyber-information becomes denser, thicker, and "dirtier"
- Information from different sources in inconsistent/incompatible formats
- Need to understand the "geography" of the information to enable intelligent searches
- Need intelligent interfaces for instant retrieval of reliable info from all sources/formats
- Requires agile computers and secure systems to protect sensitive info and control access
- Research activities across NYU include:
  - Big data science
  - Statistics & biostatistics
  - Broadband communication, with emphasis on wireless, digital media, gaming, cybersecurity

Bioengineering

- Transition scientific discovery into new therapies
- Study biomolecular interactions:
  - Metabolic engineering to create biochemical pathways in plants & microbes
  - Surface protein interactions to optimize therapeutic and catalytic activity
  - Bioactive matrices for tissue regeneration
- Interaction between living systems and biomaterial drug delivery systems
- Engineered biocatalysts with tailored properties for therapeutic/biocatalytic functions using safe green fabrication to reduce hazardous chemical methods
- Smart biomaterials for controlled drug delivery and release
- Partner in NYU-wide Bioengineering Institute

Research @ NYU-Poly: Centers

Center for Advanced Technology in Telecommunications (CATT)

Created in 1983 as a NYS Center for Advanced Technology, CATT continues to fulfill its mission to stimulate economic development in information technology through research and education. Companies that partner with CATT in joint research gain access to state-of-the-art facilities , new technologies, and a team of experts who understand how to turn technological breakthroughs into commercially-viable products and services. CATT's research program focuses on 3 key areas that are crucial to the needs of businesses today: wireless networks, network security, network applications.

Center for Biocatalysis and Bioprocessing of Macromolecules

NYU-Poly is steeped in a tradition of excellence in polymer research. Today, NYU-Poly is embracing a new frontier at the interface of engineering, macromolecules, and the biological sciences. The Center for Biocatalysis and Bioprocessing of Macromolecules is involved in the exploration and development of enzymes for a wide range of polymer forming and modifying reactions. The Center provides industrial members with cutting-edge research on enzyme transformations related to polymer technology.

Research @ NYU-Poly: Centers

CRISSP

CRISSP combines security technology strengths with experts in psychology, law, public policy, and business from NYU. The goal of this center is to build new approaches to security and privacy that recognize that technology alone cannot provide the information security and privacy needed in today's interconnected world. CRISSP combines security technology strengths with experts in psychology, law, public policy, and business from NYU. The goal of this center is to build new approaches to security and education.

NYU WIRELESS

NYU WIRELESS is an interdisciplinary research center equipped to develop revolutionary circuits and systems for several business sectors, including the wireless industry, the distributed computing and data center industry, and the medical profession. NYU WIRELESS brings together faculty and students with expertise in mm wave wireless communications and circuits, distributed networking and computing, and many branches of medicine. NYU WIRELESS conducts about $10 million/year in funded research, and allows its industrial affiliates to maximize the value of their investment by leveraging industrial affiliates funds with large NSF, NIH, and other competitive research programs.

NYU·poly
POLYTECHNIC INSTITUTE of NYU

Research and
Technology Initiatives

Research @ NYU-Poly:
From Scientific Breakthroughs to the Marketplace

- **Many research breakthroughs lead to protectable intellectual property (IP) with the potential to be transformed into new technologies, products or devices, and new processes.** ***We encourage and support faculty who seek protection of their IP.***

- **The commercialization of university-owned IP may involve licensing, joint development agreements, and the creation of start-up companies. We work closely with NYU's Office of Industrial Liaison in our technology transfer and IP commercialization activities.**

- **In order to support start-ups, we have established business incubators/ accelerators at 137 Varick Street in Manhattan and at 20 Jay Street in Brooklyn. In less than 3 years, 24 companies have "graduated", meaning they grew so big or raised so much money they had to find space on their own. We helped them raise over $45M of venture capital, and these companies created nearly 500 new jobs, many for our students.**

- **One "graduate", ThinkEco, was chosen by Con Edison to bring its energy-saving "smart plug" to homes across NYC. ThinkEco's smart plugs reduced the energy usage of 10,000 New York City air conditioners during peak demand last summer – and helped prevent black- or brown-outs in NYC during one of the hottest summers on record.**

Hardware Performance Counters to Detect Kernel Rootkits in Mobile Platforms (e.g. Android)- Prof. Ramesh Karri; with L-3

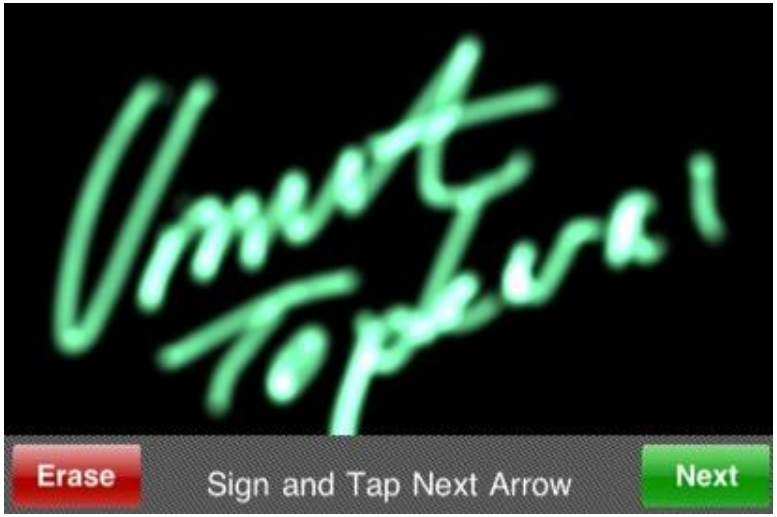
Kernel Rootkits

- **Kernel Rootkits:** ***subvert the operating system kernel***
  - have unrestricted access to system resources
  - attackers hide their presence, open backdoors into the system, gain root privilege, …

- **How can the rootkits be detected?**
  - *Prior art:* Host-based rootkit detection
    Check kernel static and dynamic objects, but they run inside the target they are protecting
  - *Prior art:* Virtual Machine Monitor VMM-based rootkit detection techniques
    Check kernel static and dynamic object, but run outside the target (in VMM)

- **NYU-Poly approach: VMM-based kernel execution path checking using Hardware Performance Counters (HPC) – Seeded by AFRL→ Supported by L-3**
  Validates execution path of guest system calls by checking the numbers of certain hardware events

A touching farewell to passwords? - Prof. Nasir Memon



Multi-touch interactions are commonly used by users. Can they be used to authenticate the users ?

<u>In other words:</u> Is there a combination of multi-touch interactions that contain sufficient unique biometric information of the user.

Is this easier for the user than remembering and typing a password?