Il Ruolo delle Università nelle politiche di sicurezza cibernetica e di protezione delle infrastrutture critiche per il Paese

Roberto Baldoni (baldoni@dis.uniroma1.it)
www.cis.uniroma1.it

4th Conference on Information Warfare
"Protezione delle Infrastrutture Critiche Nazionali"
Roma 19 Giugno 2013

CIS SAPIENZA
RESEARCH CENTER FOR CYBER INTELLIGENCE AND INFORMATION SECURITY

RISK ASSESSMENT / SECURITY & HACKTIVISM

Internet Explorer zero-day exploit targets nuclear weapons researchers (Updated)

"Watering hole" attack targets workers browsing federal government website.

by Dan Goodin - May 4 2013, 3:25am E

TECHNOLOGY LAB / INFORMATION TECHNOLO

Power company targeted by 10,000 cyberattacks per month

Electric grid is under daily assault, Congressional report finds.

by Jon Brodkin - May 22 2013, 6:37pm E

HACKING

6 March 2013

«Security and development are an inseparable binomial»

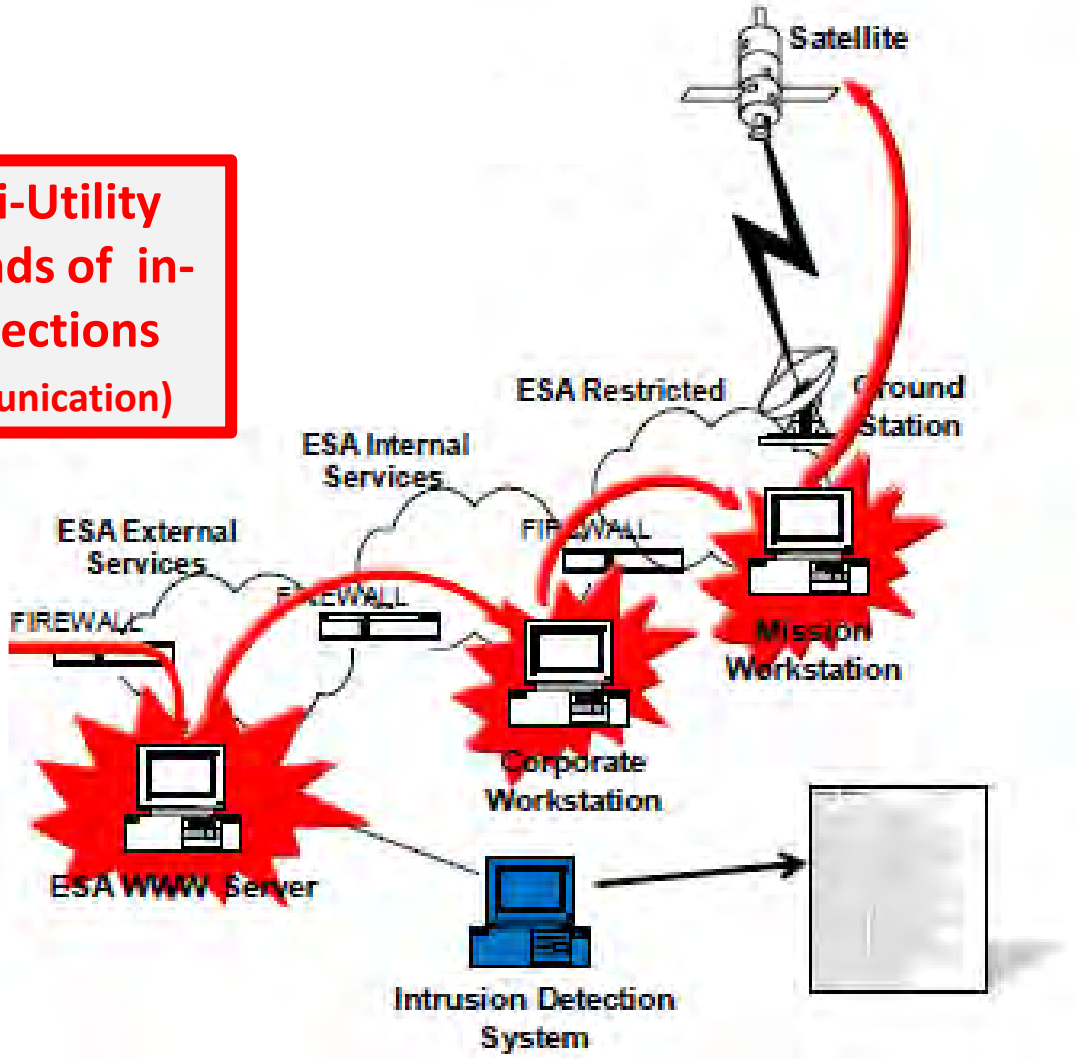
«New threats are emerging to the economy to the finance, to the energy market …»

"…We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems"

2 February 2013

"We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy"

Medium/Large Multi-Utility experiences thousands of in-out anomaluos connections per day (private communication)



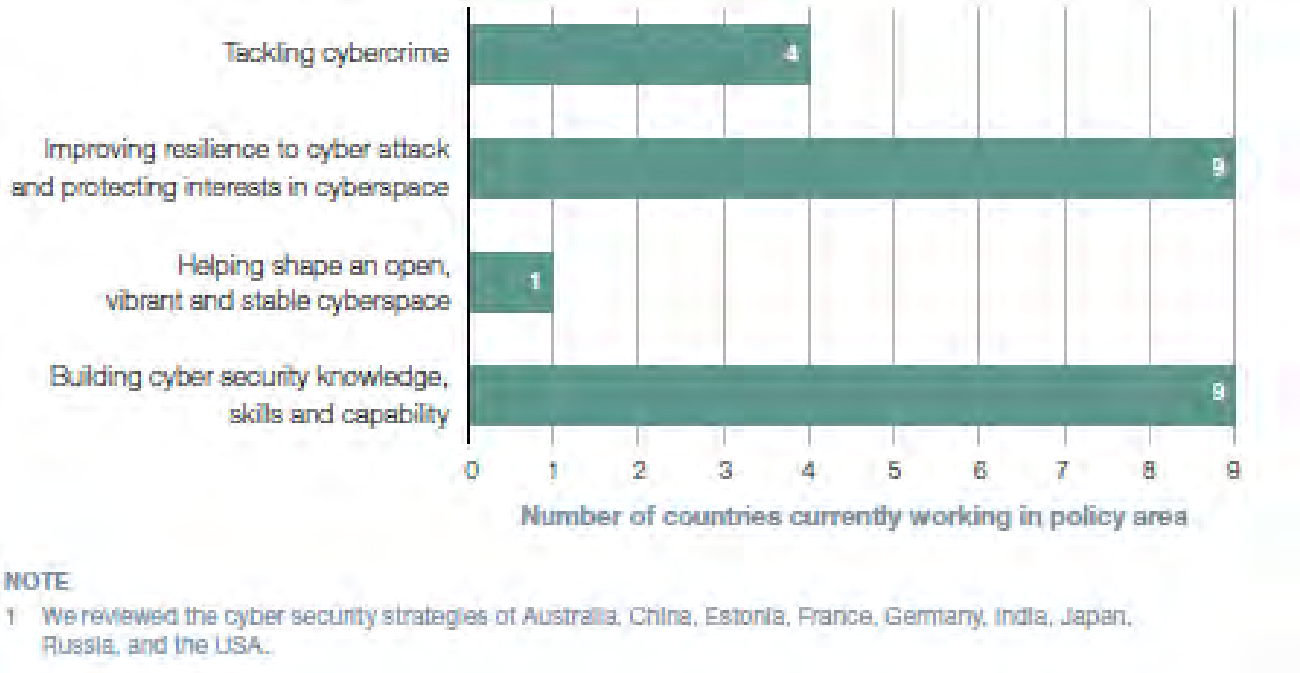
WHAT GOVERNMENTS ARE DOING

Implementing CyberSecurity Strategy

- To tackle cybercrime and make the Nation one of the most secure places in the world to do business
- To make the Nation more resilient to cyber attack protecting economic, scientific and industrial interests
- To help shape an open, stable and vibrant cyberspace which the citizens of the Nation can use safely and that supports open societies
- To build the Nation's cross-cutting knowledge, skills and capability to underpin all cyber security objectives

UK objectives

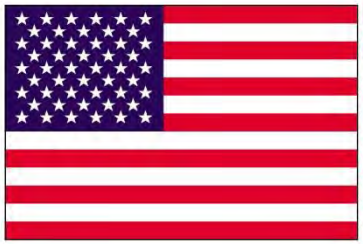
Shared objectives and Actors



- **Involvment of several Ministries and Government Organizations**

CyberSecurity Strategy standpoints

- US (Obama's Executive Order Feb 12th 2013)
  - information warfare is a **priority for the Nation,** it represents a current and future threat.
  - "Cybersecurity framework" from NIST in 6 mounths
- UK (cyber security strategy implementation 2011-1015)
- Canada (action plan 2010-2015)



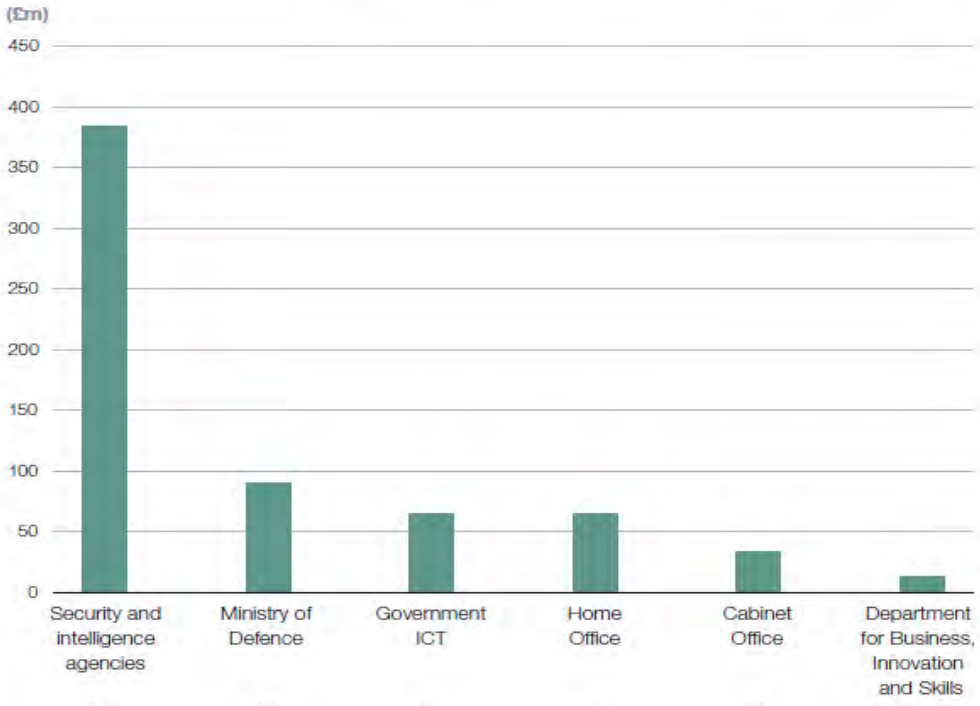
2013 Cybersecurity Funding Breakdown (source DHS)

- **$345 million:** The National Cybersecurity Protection System (NCPS) is an integrated intrusion detection, analytics, information-sharing and intrusion-prevention system that supports DHS responsibilities
- **$236 million:** The Federal Network Security Branch manages activities designed to enable federal agencies to secure their IT networks.
- **$93 million:** The US-Computer Emergency Readiness Team (US-CERT Operations)
- **$64.5 million:** to support cyber investigations conducted through the Secret Service and Immigration and Customs Enforcement.
- **$12.9 million:** to support high-quality, cost-effective virtual education and training

- Definition of Research challenges funded by NSF, DHS and DARPA

UK Cybersecurity Funding

£650 million			
2011-12 £105m	2012-13 £155m	2013-14 £180m	2014-15 £210m



	Security and intelligence agencies	Ministry of Defence	Government ICT	Home Office	Cabinet Office	Department for Business, Innovation and Skills
£ million	384	90	65	65	33	13
Percentage	59%	14%	10%	10%	5%	2%

NOTES

1 Nominal values.

2 The funding shown for each department is the total amount allocated over the four years 2011-12 to 2014-15.

Source: UK Cyber Security Strategy: Protecting and promoting the UK in a digital world, Cabinet Office, November 2011

Italy standpoint

- Jan 2013 – DPCM on cyber security
- Strategy Implementation
- Major involvment of telco companies
- Creation of a Scientific Committee

- no funding!

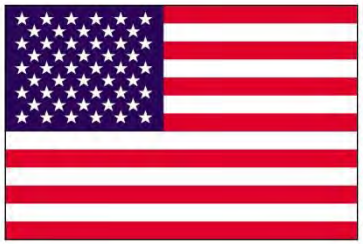
THE ROLE OF ACADEMICS

Threats are continuously evolving

Cyber security strategy needs

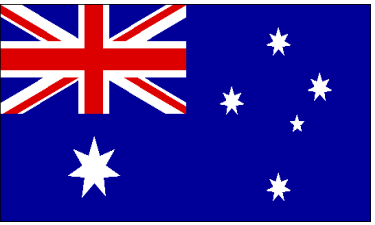
- Continuous Research
- Continuous Education

This is THE University mission!



Let's look at CERTs: Best Practices

- US-CERT has been created through an agreement between DHS and CMU in 2013.
- US-CERT partners
  - Private sector critical infrastructure owners and operators
  - Academia (CMU, PURDUE,…)
  - Federal agencies
  - Information Sharing and Analysis Centers (ISACs)
  - State and Local partners



Let's look at CERTs: Best Practices

- Edith Cowan University is partner of Cert-Australia on vulnerability and mitigation research programs looking at initiatives such as smartgrids and smart metering technologies and their security implications

Looking at UK

- GCHQ launched a programme to develop cyber security talent in schools and universities.
- GCHQ, in partnership with the Research Councils' global uncertainties programme and the Department for Business, Innovation and Skills awarded 'academic centre of excellence in cyber security research' status to eight UK universities
- GCHQ launched a research institute for the science of cyber security

www.gchq.gov.uk/press/pages/cyber-security-research-centres-of-excellence.aspx

Google Calendar | Google | La Repubblica.it - H... | Roberto Baldoni's h... | Altri Preferiti

Home | About Us | History | Challenges

Press

You are here: GCHQ > Press > **UK Universities awarded Academic Centre of Excellence status in Cyber Security Research**

UK Universities awarded Academic Centre of Excellence status in Cyber Security Research

The first eight UK universities conducting world class research in the field of cyber security have been awarded "Academic Centre of Excellence in Cyber Security Research" status by GCHQ in partnership with the Research Councils' Global Uncertainties Programme (RCUK) and the Department for Business Innovation and Skills (BIS). We hope other universities will also become Centres in the near future as part of an ongoing process.

The Centres of Excellence will benefit the UK by:

- Enhancing the UK's cyber knowledge base through original research
- Providing top quality graduates in the field of cyber security
- Supporting GCHQ's cyber defence mission
- Driving up the level of innovation

The Centres of Excellence will help make the UK government, business and consumers more resilient to cyber attack by extending knowledge and enhancing skills in cyber security.

The eight Universities chosen as Centres of Excellence in Cyber Security Research are:

University of Bristol	**Imperial College London**
Lancaster University	**University of Oxford**
Queen's University Belfast	**Royal Holloway, University of London**
University of Southampton	**University College London**

These Centres will be the first to attain Academic Centre of Excellence in Cyber Security Research status and will benefit from:

- Closer collaboration with GCHQ, the UK Cyber Community and industry
- Partnership endorsement in associated publications and prospectuses
- Better understanding of Government and industrial cyber issues
- Helping to formulate the future Cyber Security research agenda
- Extra funding opportunities and £50,000 capital investment

Other experiences: (public-private-academic partnerships)

- Japan
- India
- Estonia
- Germany
- ……

Italy standpoint

- Jan 2013 definition of the DPCM on «cyber security»
- Strategy Implementation
- Major involvment of telco companies
- Presence of a scientific committee

Concluding Remark #1

- A National Cyber Security Scenario cannot prescind of the Academia contribution

- Continuous research and education needed
- Public-private partnership

- Selecting centers of excellence in Italy where finding competences and critical mass

Concluding Remark #2

- **We have to ACT now!**

- A today story: “accountant” in Fiumicino
  - Using a windows 7’s vulnerability, someone got into its private network
  - All his own files have been encrypted
  - Nice email explaining how to do a “special” bank transfer in order to decrypt files

- The problem is vital for the economy at every level (everyone is under attack from individuals to large industries to organizations)

Concluding Remark #3

- Security is a nationwide shared objective (not only related to military sector)
- Information flow within a PA information system has to be fully mastered (no leak)
- Secure supply chain

Concluding Remark #3

- Security is a nationwide shared objective (not only related to military sector)
- Information flow within a PA information system has to be fully mastered (no leak)
- Secure supply chain

Concluding Remark #4

- Italian DPCM on Cyber security is an important step
- Still the command chain is overly complex wrt the velocity of the deployment of an attack
- First thing to do: IMPLEMENTING A CERT!

Concluding Remark #5

- Less events more implementation!