UNIVERSITÀ DEGLI STUDI FIRENZE
DSPS DIPARTIMENTO DI SCIENZE POLITICHE E SOCIALI

JEAN MONNET CENTRO DI ECCELLENZA

FESTIVAL D'EUROPA 2015 Festival d'Europa

The EU and Member States in Global Affairs: Any sign of convergence?

5-6 May 2015

Cyber Defense and Cyber Security Policies in the UK and Germany

Marco Mayer, Sant'Anna School of Advanced Studies

Luigi Martino, University of Florence (CSSII)

We'll talk about:

Cyber Security

Cyber Defense

Cyber Intelligence

Why?

All of these issues are related to Cyber National Policies within the Cyber Domain

Introduction:

- The cyber domain is technologically driven and market power is highly concentrated in a small group of private digital entities;
- Thus, to fully understand the Germany and UK cases we should also consider the role of the private companies (i.e. British Telecom and Deutsche Telekom).

The UK Cyber Security Approach

Background and Aims:

- Cyberspace is also considered a "warfare domain"
- Cyberspace as a National Interest Priority
- Cyber-security Information Sharing Public-Private-Partnership (CiSP)
- "Special" Foreign Relations (i.e. USA-Israel-Qatar)

UK Cyber Security Approach

The government has allocated **£860 million until 2016** to establish a National Cyber Security Programme.

This vision is set out in the UK Cyber Security Strategy, published in November 2011.

This strategy considers the cyberspace: ***"As a National Interest Priority".***

The UK Cyber Security Strategy has 4 objectives:

- **making the UK one of the most secure places in the world to do business online and tackling cyber crime**
- making the UK more resilient to cyber attack and better able to protect our interests in cyberspace
- helping to shape an open, vibrant and stable cyberspace that supports open societies
- building cyber skills, knowledge and capability the UK needs

The UK Cyber Security Strategy

December 2014

OBJECTIVE 1

MAKING THE UK ONE OF THE MOST SECURE PLACES IN THE WORLD TO DO BUSINESS ONLINE

750 organisations in CISP: the Cyber-security Information Sharing Partnership for industry & Government

Cyber Essentials: 5 critical controls to protect businesses from common cyber threats

Cyber security exports £1.040bn in 2013, 22% increase on 2012 & on track for £2 billion target by 2016

Guidance: **'10 Steps** to Cyber Security' & small business version

AND TACKLING CYBER CRIME

National Cyber Crime Unit in the National Crime Agency: **30 live domestic & international** operations to disrupt serious cybercrime

9 cyber units in each of the Regional Organised Crime Units: over **85 live operations**

HMRC's cyber team: more than **£100m** fraud prevention this year

OBJECTIVE 2

A UK THAT IS MORE RESILIENT TO CYBER ATTACK AND BETTER ABLE TO PROTECT OUR INTERESTS IN CYBERSPACE

CERT-UK: new Computer Emergency Response Team for national incidents & international CERT liaison

GCHQ working to detect & defend against cyber threats

All local authorities & councils on the Public Service Network

£860 million
over 5 years, delivering the UK Cyber Security Strategy

OBJECTIVE 3

A UK HELPING TO SHAPE AN OPEN, VIBRANT AND STABLE CYBERSPACE THAT SUPPORTS OPEN SOCIETIES

Ongoing series of **'London Process' global conferences** shaping the debate on cyberspace

15 international visits to the UK hosted by FCO

30 International **Cyber Security Capacity Building** Fund projects

OBJECTIVE 4

A UK THAT HAS THE CYBER KNOWLEDGE, SKILLS AND CAPABILITY IT NEEDS

SCHOOLS
Cyber security in computer science **GCSE**

APPRENTICESHIPS
200 Tech Partnership entry-level jobs, first HMG & industry apprenticeship frameworks

CAREERS & PROFESSIONALISM
Initiatives for computer science students & graduates:

- Cyber Security Challenge & Cyber Growth Partnership: **mentoring** & **'cyber camps'**
- Campaign via **Graduate Prospects** website
- **Virtual hub** for those joining or in the field

HIGHER EDUCATION
4 Higher Education Academies
6 Master's degrees in General Cyber Security certified by GCHQ

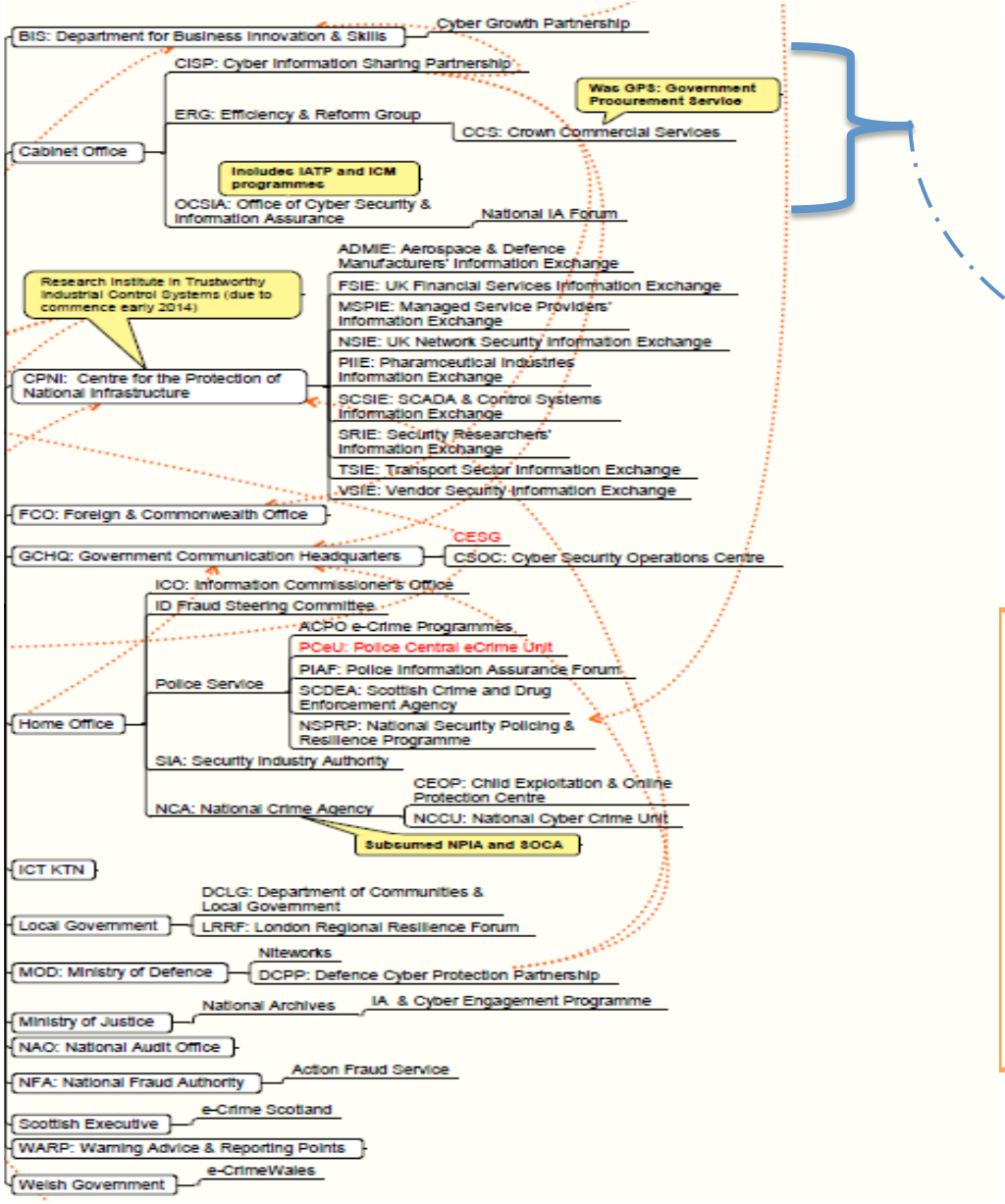
RESEARCH
3 Research Institutes
11 Academic Centres of Excellence in Cyber Security Research
2 Centres of **Doctoral Training, 66 PhDs** from 2017

WIDER EDUCATIONAL SUPPORT
24,127 sign ups for first round of Open University's Massive Open Online Course "Introduction to Cyber Security"

AWARENESS RAISING
Cyber Streetwise campaign: Over 2 million more adults use safer online behaviours after phase 1

Cabinet Office

The UK Cyber Security Organization Chart



Upgraded at Prime Minister Level
Office of Cyber Security and Information Assurance

The OCSIA ***supports the Minister for the Cabinet Office***, the Rt Hon Francis Maude MP and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates action relating to enhancing cyber security and information assurance in the UK. The OCSIA is headed by James Quinault

Office of Cyber Security and Information Assurance

Aims and objectives:

The OCSIA is responsible for implementing a number of cross cutting agendas including:

- Providing a strategic direction on cyber security and information assurance for the UK including e-crime;
- Supporting education, awareness, training and education (for example, Get Safe online and the Cyber Security Challenge);
- Working with private sector partners on exchanging information and promoting best practice;
- Ensuring that the UK's information and cyber security technical capability and operational architecture is improved and maintained;
- **Working with the Office of the Government Senior Information Risk Owner (OGSIRO) to ensure the resilience and security of government ICT infrastructures such as the Public Sector Network (PSN) and G-cloud engaging with international partners in improving the security of cyberspace and information security.**

CiSP
A CATALYST FOR COLLABORATION

Cyber-security Information Sharing Partnership (CiSP)

The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, **is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.**

CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information.

British Telecom Supporting Minister Of Defense to protect against the Cyber Threat

Challenge

- MOD wanted to integrate existing system security information sources to create a centralised security capacity and expand its situational awareness

Solution

- BT designed and deployed a fully accredited cyber-defence solution called eCND (enhanced computer network defence) to deliver round-the-clock support

Value

- eCND is helping the MOD identify potential vulnerabilities more effectively, reducing the window of exploitation open to threat sources

“Special” Foreign Relations

UK-USA

The United States and the United Kingdom work closely on a range of cybersecurity and cyber defense matters. For example, the U.S. Computer Emergency Readiness Team (US-CERT) and CERT-UK collaborate on computer network defense and sharing information to address cyber threats and manage cyber incidents.

To deepen this collaboration in other areas, the United Kingdom’s Government Communications Headquarters (GCHQ) and Security Service (MI5) are working with their U.S. partners – the National Security Agency and the Federal Bureau of Investigation – to further strengthen U.S.-UK collaboration on cybersecurity by establishing a joint cyber cell, with an operating presence in each country.

The cell, which will allow staff from each agency to be co-located, will focus on specific cyber defense topics and enable cyber threat information and data to be shared at pace and at greater scale.

Cambridge *vs* Cambridge

<u>January 2015:</u> President Obama and David Cameron announce 'Cambridge v. Cambridge' hackathon

As part of a series of cybersecurity initiatives made public today during British Prime Minister David Cameron's visit with President Barack Obama, the two nations announced that MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) will face off against the University of Cambridge this fall for a special student hackathon dubbed "Cambridge v. Cambridge."

The multiday competition is part of continued efforts by the two nations to collaborate on cybersecurity and harness their collective brainpower to help combat global cyberattacks

“Special” Foreign Relations

UK-Israel

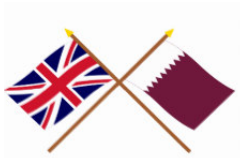
March 2015

The Memorandum of Understanding (MoU) was signed at the Israeli Prime Minister’s office by Liam Maxwell, Government Chief Technology Officer, on behalf of the UK Government Digital Service (GDS), and by Harel Locker, Director-General of the Israeli Prime Minister’s office.

The MoU states that the 2 countries will:

- exchange information and experiences around open markets, open standards and open source
- work together to make sure that each country has the capability and ability to develop digital public services
- develop other ways of working together internationally.

“Special” International Relations



UK-Qatar

<u>November 2014:</u> UK signs agreement with Qatar to fight Jihad and cyber threats

The United Kingdom and Qatar recently signed an agreement on Jihad and cyber warfare issues. Emir of Qatar, Sheikh Tamim bin Hamad al-Thani and the UK Prime Minister David Cameron met in London a few days ago to sign the security pact. Both countries agreed to share classified intelligence in order to track and counter jihadists and cyber warfare operations.

This agreement includes close cooperation with the UK GCHQ cyber intelligence agency on cyber threats and fighting terrorism. On the top, the UK will sell Qatar cyber security products and services in order to strengthen their security measures. This cooperation arrives at a crucial period for the Middle East as the Islamic State attempts to annihilate the entire Middle East region through terrorist acts.

In terms of security and cyber, Qatar could not find a better partner than Great Britain. A month ago in Kuwait, the United States also affirmed its desire to cooperate with Europe and Arabs countries in order to fight the Islamic State, which is currently the most significant terrorist threat to Middle East and West.

UK *vs* EU

The UK is facing opposition from other EU countries, which want EU cyber security rules to apply widely to operators of 'digital service platforms' such as Amazon and not only to operators of critical infrastructures (banking, energy, health and transports, cables, hubs, etc).

The disagreement concerns the precise scope of the Network and Information Security (NIS) Directive. EU countries are negotiating over the final wording of the rules, which are scheduled to be agreed by June and to come into force in 2018.

What is the NIS Directive?

The **Network and Information Security** (NIS) Directive was first published by the European Commission in February 2013 in a bid to bolster the **security of critical infrastructure in the EU** and ensure that cyber security incidents affecting that infrastructure that have a real-world impact are reported to regulators. **The Commission's original proposal also envisaged a new cross border cyber security information sharing regime.**

Since the plans were first published, MEPs and government officials from the 28 EU countries have been working to refine the proposed new framework. Once finalised, EU countries will have to implement the Directive into national law.

The Different Approaches on Cyber Defense in the UK and Germany

Two Different Approaches about Cyber Defense

The Proactive Cyber Defence or Active Cyber Defense (ACD) defining characteristic is based on aggressive action taken outside the defender's home network.

The defining characteristic of *Fortified Cyber Defence* (FCD) is that approach's preventive, introspective focus.

FCD measures seek to establish defensive perimeters through systems of firewalls and antivirus software in order to minimise the chances of access to target systems and networks.

UK Cyber Defense

Proactive Cyber Defence Approach

“For years, we have been building a defensive capability to protect ourselves against these cyber attacks. That is no longer enough. You deter people by having an offensive capability”.

Philip Hammond,
Secretary of State for Foreign and Commonwealth Affairs

UK Cyber Defense:
The Proactive Approach

The UK Cyber Security Strategy identifies the proactive measures taken to disrupt threats to and from networked communications systems.

The Ministry of Defence (MoD) is tasked with improving the UK's ability to detect threats in cyberspace and to "anticipate, prepare for and disrupt" such threats.

This strategic approach falls neatly into Proactive Cyber Defense but implies the extension of action beyond the confines of national or UK government networks .

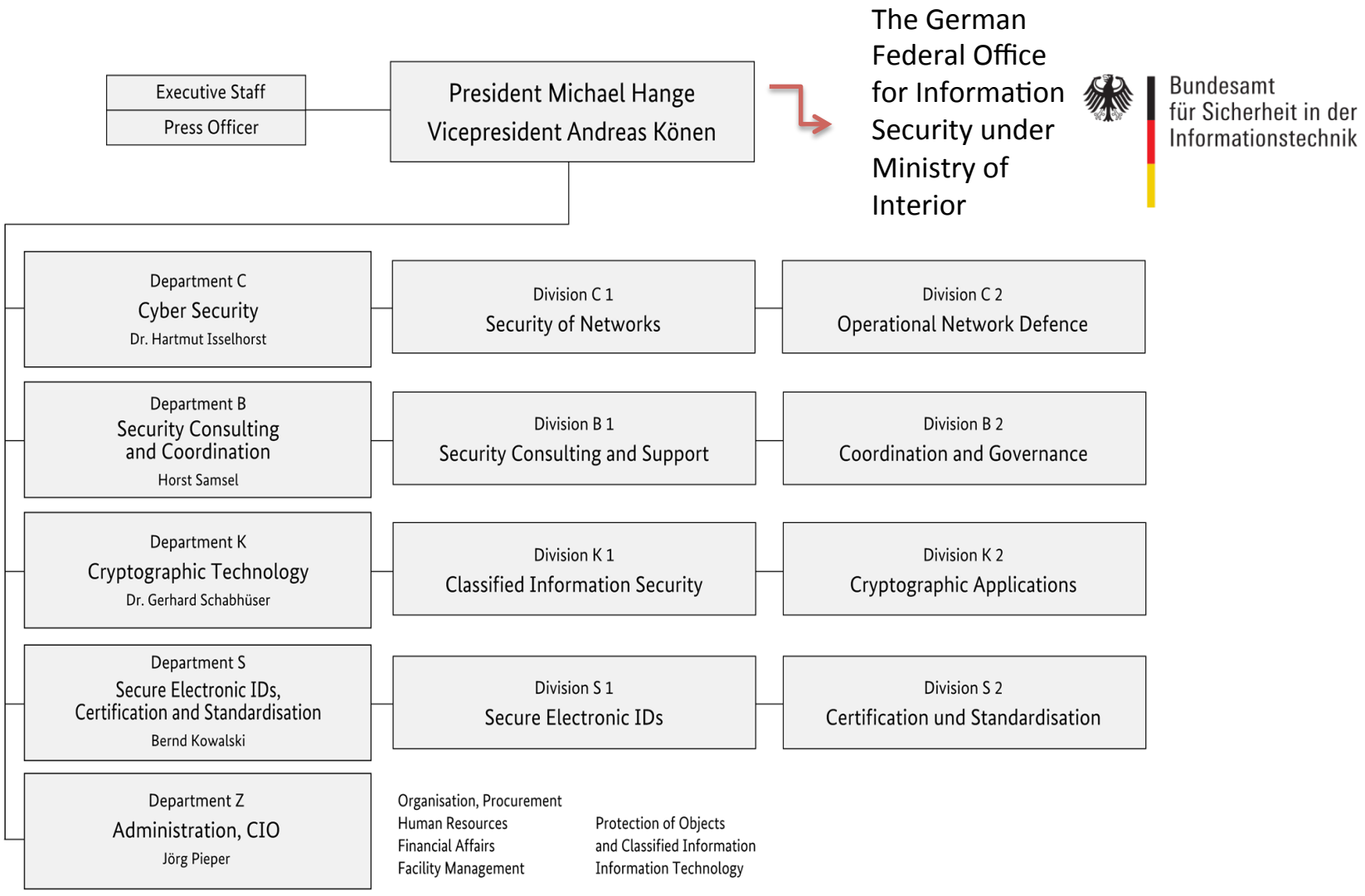
The fact that the MoD has been assigned these tasks, despite UK cyber security strategy being led by the Cabinet Office – a civilian organ of central government – demonstrates a willingness to deploy military resources to provide cyber defence and security.

Germany Cyber Defense and Cyber Strategy

Bundesamt für Sicherheit in der Informationstechnik

Fortified Cyber Defense

Germany Cyber Defense and Cyber Strategy



Germany Cyber Security Organizations

To what extent do you assist the German armed forces (Bundeswehr) in cyber defense?

"BSI is a civilian and preventive authority. More particularly, it has a protective function for key government networks. BSI detects targeted and non-targeted attacks on key government networks and defends against these attacks, in its role as an IT security provider. BSI's further responsibilities include approval of IT security products and services used within the German federal government. This leads to cooperation between the German Federal Ministry of Defense and BSI. The *Bundeswehr* is responsible for cyber defense in the military sense".

Michael Hange ist seit dem 16. Oktober 2009 Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Bonn

The German Federal Intelligence Service (*Bundesnachrichtendienst*, BND), the German Federal Criminal Police Office (*Bundeskriminalamt*, BKA), the German *Bundeswehr* and others are taking care of German security interests and attempting to contain the threat.

Germany and cyber intelligence capabilities

Germany is currently developing cyber intelligence capabilities in order to prevent future cyber-attacks. According to Germans, this new development is an "early warning" system which is capable of detecting imminent foreign cyber-attacks. The system will mainly monitor foreign social media.

The Germany Federal Intelligence Service will invest €28 million into its Strategic Technical Initiative of 2015. Germany began to realize the importance of cyber intelligence as open source intelligence is a powerful strategy, especially to monitor social media and websites, which can help gather valuable intelligence in order to prevent cyber-attacks.

Germany (Cyber) Foreign Relations

Germany has consistently stressed that governments should not use cybersecurity concerns as a pretext for interfering with individual rights. The revelations by Edward Snowden about the National Security Agency (NSA) and surveillance have motivated Berlin to take a leading role on these issues**.** **Together with Brazil, Germany sponsored a UN General Assembly Resolution on the right to privacy in the digital age, which was adopted by consensus in December 2013.**

Germany *and the* EU

Mr. Oettinger (***top German official in Brussels and the commissioner for the digital economy and society***)

- **Insisted that the current dominance of the digital sector by U.S. companies is "not forever."** "I'm sure we can come back with investments in infrastructure, with human capital, with science and education and research and universities, with clear strategies to leverage startups," he said. *(Wall Street Journal, April 2015)*

- **Declared that The European Union is the largest single market in the world, but it still consists of 28 fragmented digital markets, a structure Digital Commissioner Günther Oettinger hopes to transform into a "Digital Union of Europe."** (*EurActiv Germany March 2015*)

Deutsche Telekom launches European network

March 02, 2015

- First services in three countries (Croatia, Hungary and Slovakia
- **Group to invest more than EUR 6 billion in Europe-wide network expansion through 2018**
- Up to 100,000 connections migrated to IP technology each week
- Fixed-network transmission speed will rise to 500 Mbit per second

EU and Germany

Thomas de Maizière (Federal Minister of the Interior) declared:

"I support the EU in its efforts to make rules for the Member States to ensure IT security. Our common goal must be to increase the level of IT security throughout the EU, on the basis of decisive national action. With its draft IT Security Act, the Federal Government has presented a number of specific measures to increase IT security in Germany. We have made similar proposals in the ongoing discussion of an EU directive on measures to ensure a high common level of network and information security in the Union. My impression is that the German position is also understood at European level. **Germany has thus taken a leading role in an area that will become increasingly important at a time when digital vulnerability is growing.“** *(Source: Official web site of Federal Ministry of Interior)*

Germany Cyber Defense Approach:

Fortified Cyber Defence (FCD)

- **Germany, conversely of the UK's approach, provides an example of a national policy promoting of the fortified cyber defense (FCD).**

- **The focus for the German Cyber Security Strategy is ensuring that malicious intrusions are unsuccessful within a preventive security framework. This is achieved through certain key objectives, including training and international cooperation as well as tackling cyber-crime.**

In order to bridge the UK and Germany different approaches is NATO the answer ?

NORTH ATLANTIC TREATY ORGANIZATION

In June 2014, NATO Defence Ministers endorsed the new cyber defence policy, which is currently being implemented. The new policy and its implementation will be kept under close review at both the political and technical levels within the Alliance and will be refined and updated in line with the evolving cyber threat.

At the Wales Summit in September 2014, Allies approved a new action plan which along with the new policy contributes to the fulfilment of the Alliance's core tasks.

In June 2014, NATO Defence Ministers endorsed the new cyber defence policy, which is currently being implemented. The new policy and its implementation will be kept under close review at both the political and technical levels within the Alliance and will be refined and updated in line with the evolving cyber threat.

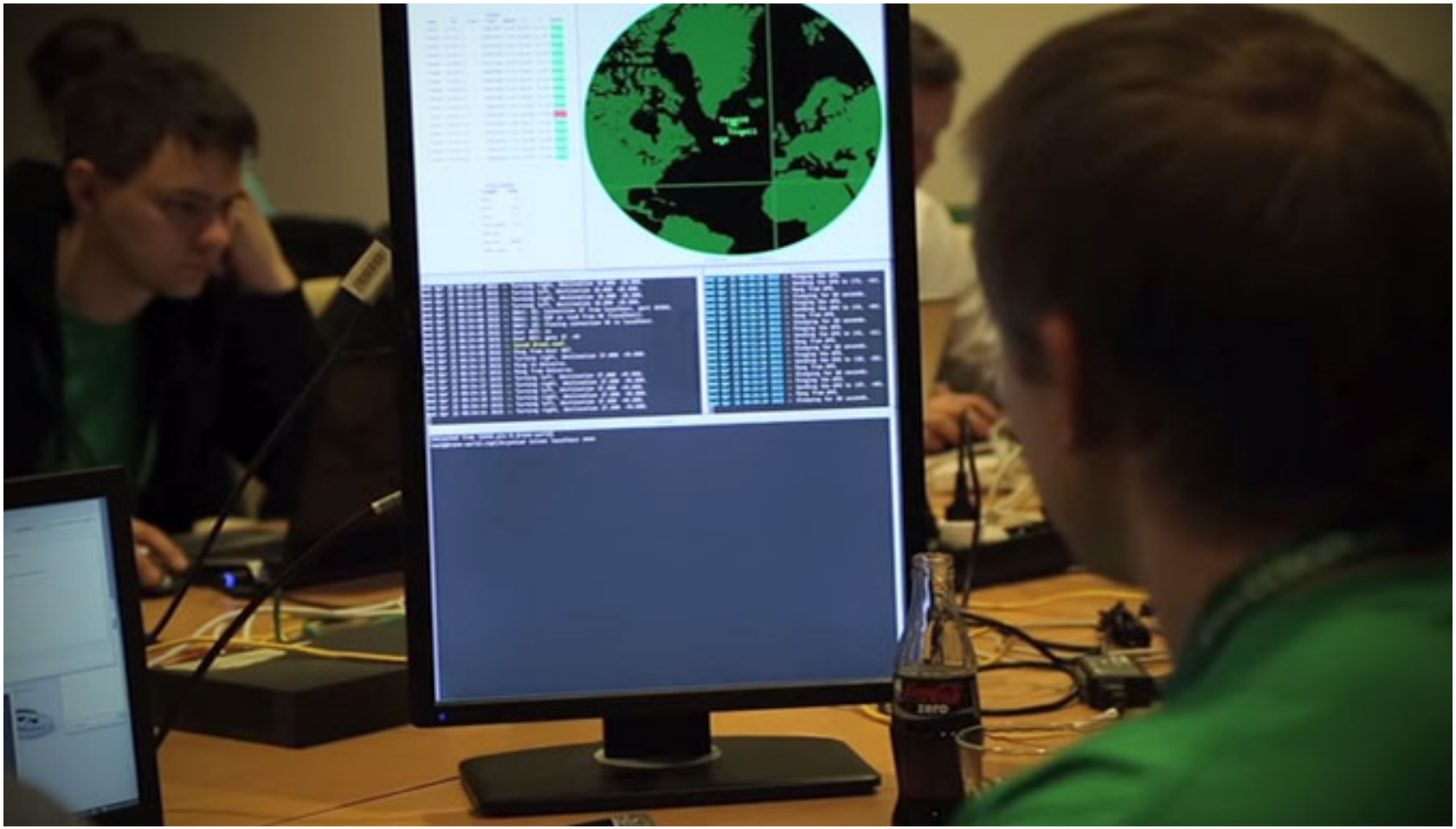
At the Wales Summit in September 2014, Allies approved a new action plan which along with the new policy contributes to the fulfilment of the Alliance's core tasks.

NATO Cyber Capabilities

Background

- NATO's main cyber responsibility is to defend its own networks, while Allies protect theirs. NATO also helps Allies to boost their defences. NATO does this by sharing information about threats, by helping to develop capabilities, and through education, training and exercises.
- The creation of the Rapid Reaction Team was a result of the Alliance's revised cyber defence policy of 2011, which was enhanced at the 2014 Wales Summit and is now part of the Alliance's collective defence framework.
- Cyber attacks could reach a level posing a threat to the prosperity, security and stability of the Euro-Atlantic states, and their impact could be just as disastrous as a conventional attack. **At the Wales Summit , NATO leaders decided that a cyber attack could trigger Article 5, the Alliance's collective defence clause.**
- The NATO Computer Incident Response Capability (NCIRC) is responsible for the defence of NATO's communication and information systems.

Locked Shields is an annual real-time network exercise April 2015



Thank you!

Contact us:

Marco Mayer
mayerkos@yahoo.it

Luigi Martino
luigimartino.unifi@gmail.com