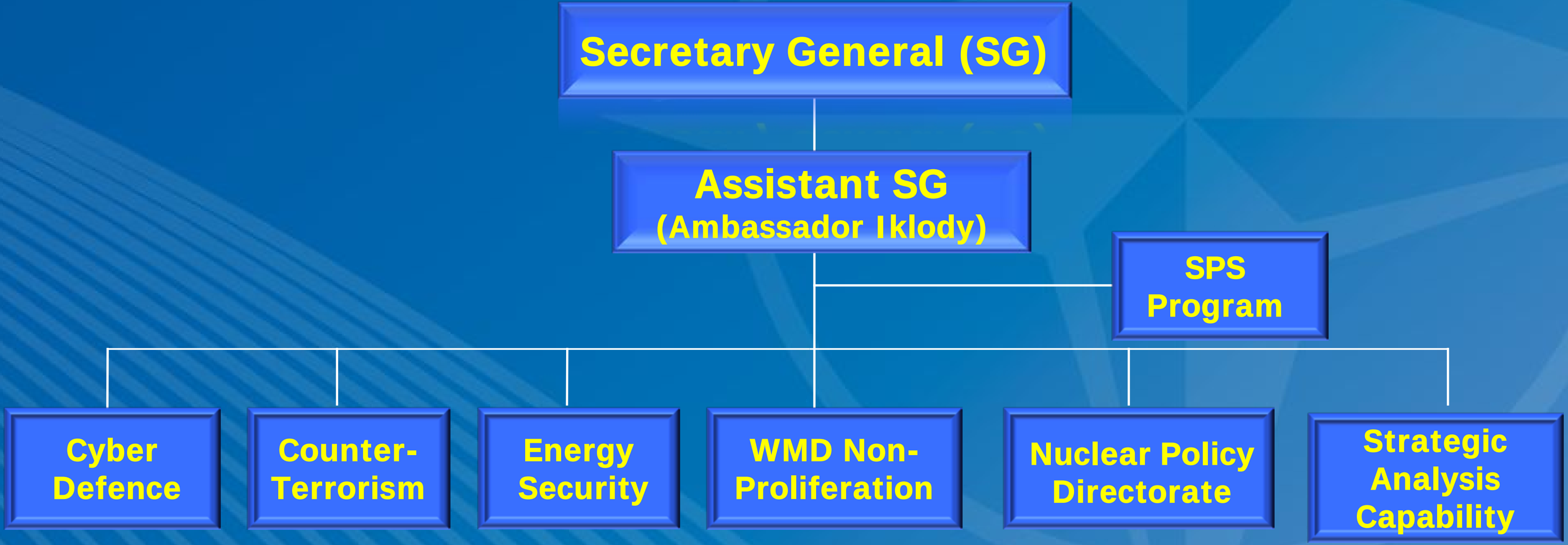
Defending Cyberspace; Global Challenges require Global Responses

Suleyman ANIL
Head, Cyber Defence
Emerging Security Challenges Division
NATO HQ, Brussels

24th Annual FIRST Conference
MALTA
17 - 22 June 2012

NATO Team in 2005 FIRST Singapore

NATO HQ
EMERGING SECURITY CHALLENGES DIVISION



Secretary General (SG)

Assistant SG
(Ambassador Iklody)

SPS Program

- Cyber Defence
- Counter-Terrorism
- Energy Security
- WMD Non-Proliferation
- Nuclear Policy Directorate
- Strategic Analysis Capability

NATO

A political and military Alliance

We want to be sure that we can walk around freely in a safe and secure environment. Security in all areas of everyday life is key to our well-being, but it cannot be taken for granted.

political ?

military ?

NATO

28 Member Nations

41 Partner Nations

NATO’s Prevention and Awareness Efforts

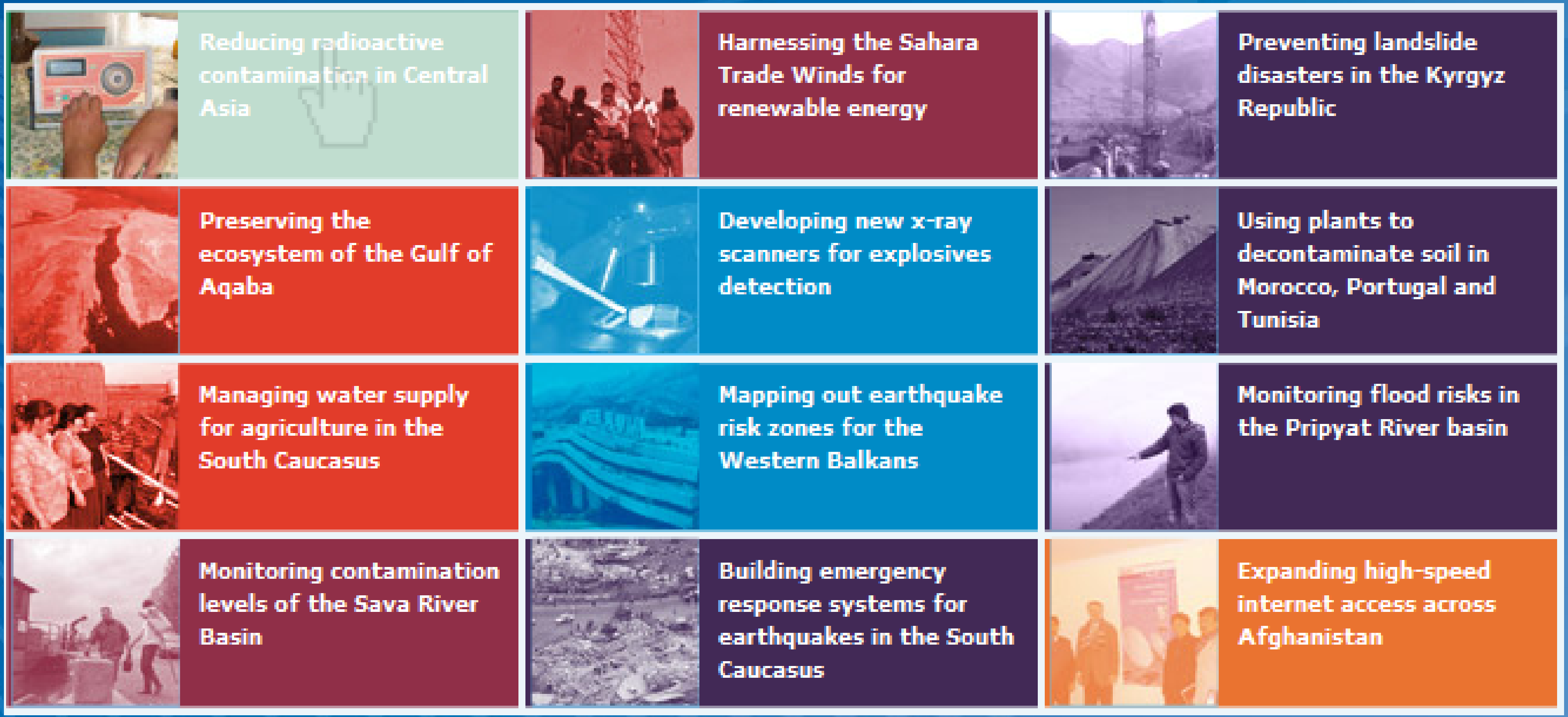
NATO Science for Peace and Security Programme Grants

(www.nato.int/science)

Who can apply; Anybody from NATO & Partner Nations

How to apply; Follow the instructions at www.nato.int/science

Which subject to apply; Any Cyber Defence/CERT related subject



Reducing radioactive contamination in Central Asia

Harnessing the Sahara Trade Winds for renewable energy

Preventing landslide disasters in the Kyrgyz Republic

Preserving the ecosystem of the Gulf of Aqaba

Developing new x-ray scanners for explosives detection

Using plants to decontaminate soil in Morocco, Portugal and Tunisia

Managing water supply for agriculture in the South Caucasus

Mapping out earthquake risk zones for the Western Balkans

Monitoring flood risks in the Pripyat River basin

Monitoring contamination levels of the Sava River Basin

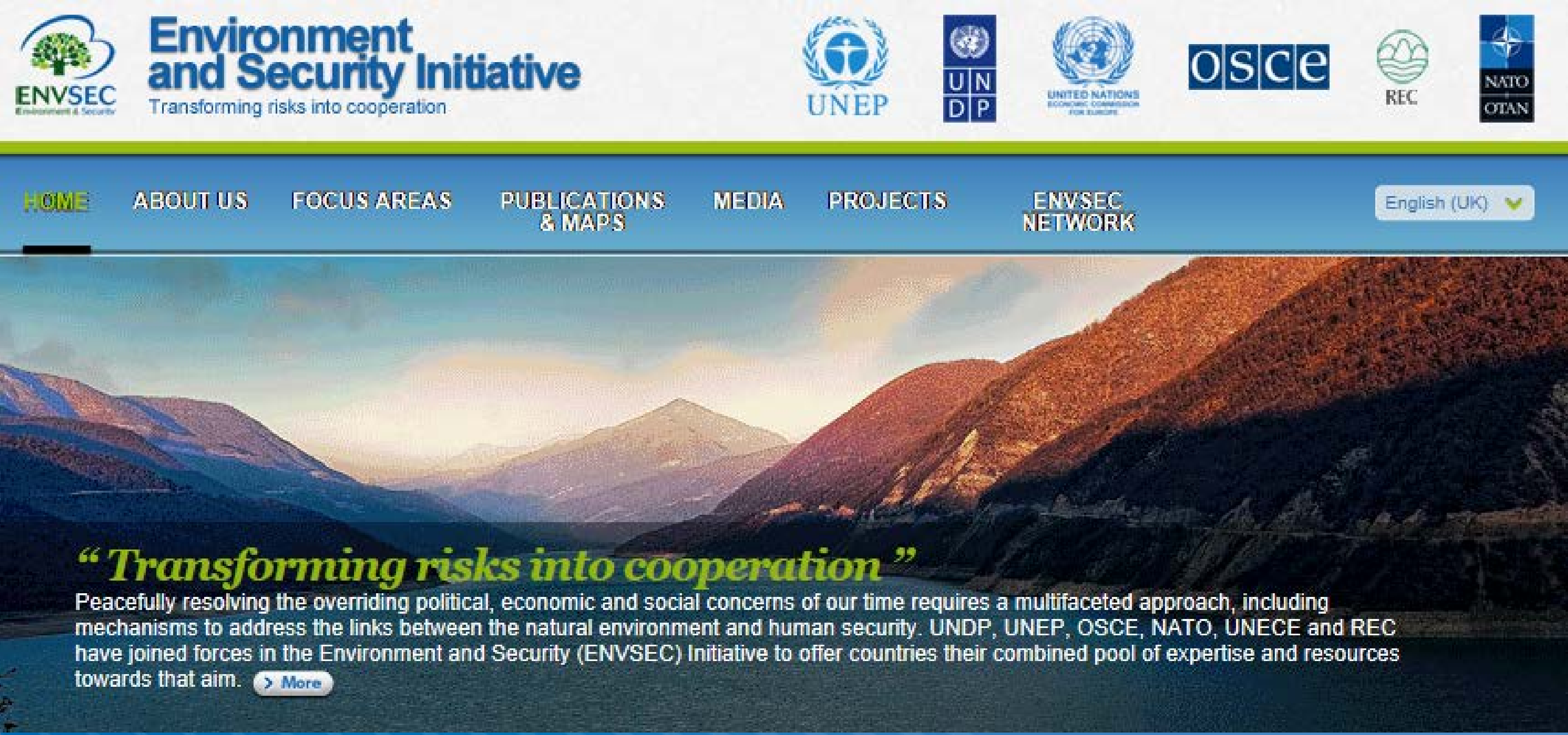
Building emergency response systems for earthquakes in the South Caucasus

Expanding high-speed internet access across Afghanistan

NATO and Counter Terrorism

STANDEX; Distance detection of Suicide Bombers.

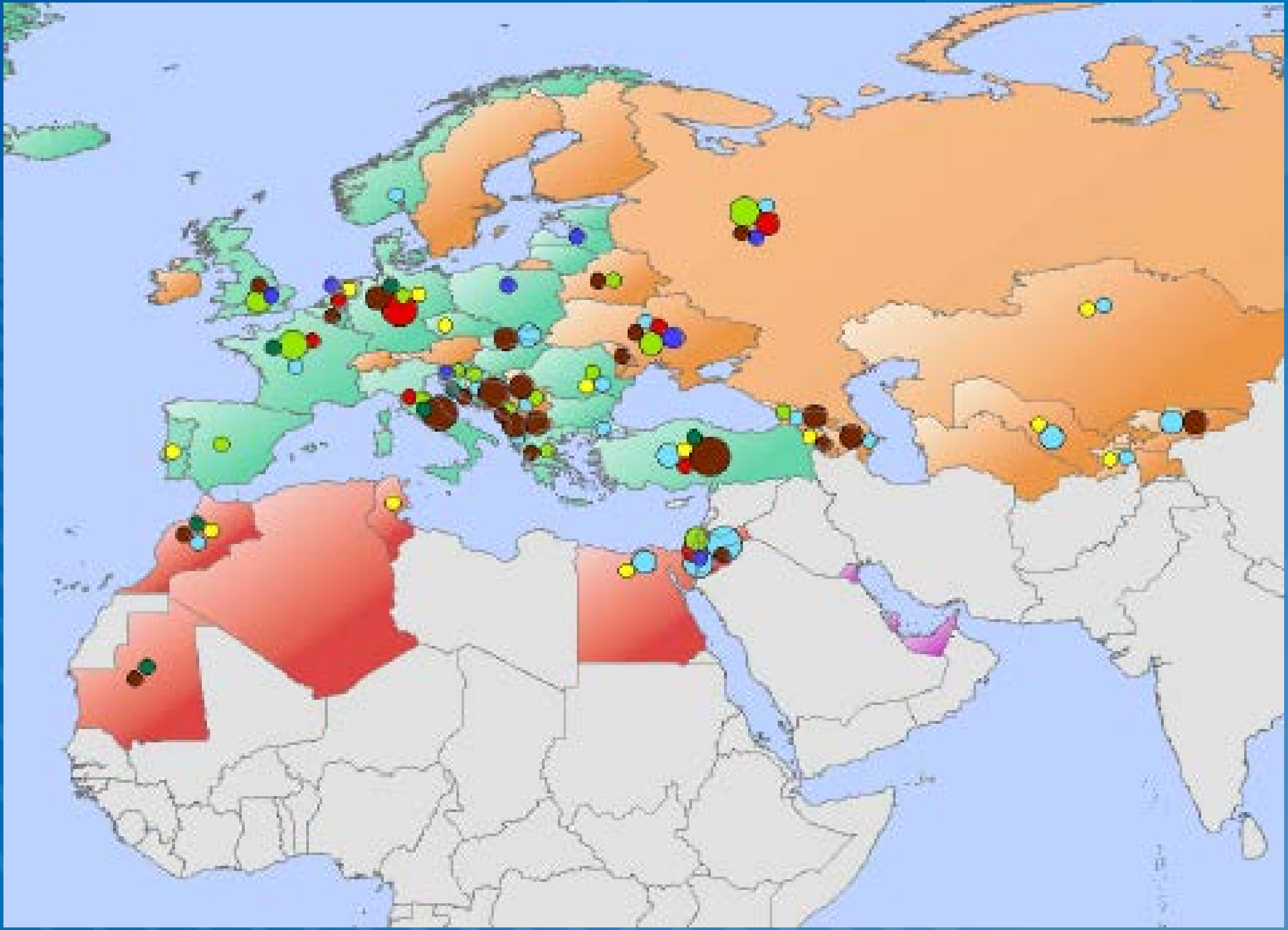
NATO and Environment Security



"Transforming risks into cooperation"

Peacefully resolving the overriding political, economic and social concerns of our time requires a multifaceted approach, including mechanisms to address the links between the natural environment and human security. UNDP, UNEP, OSCE, NATO, UNECE and REC have joined forces in the Environment and Security (ENVSEC) Initiative to offer countries their combined pool of expertise and resources towards that aim. > More

NATO Science for Peace and Security Programme Projects



NATO's Approach to Cyberspace – a new "Global Common"

http://www.act.nato.int/globalcommons

NATO
OTAN

ALLIED COMMAND TRANSFORMATION

ASSURED ACCESS TO THE GLOBAL COMMONS

Maritime | Air | Space | Cyber

FINDINGS AND RECOMMENDATIONS

NATO’s “Cyberspace”

- “nato.int” Domain,
- Closed Networks.

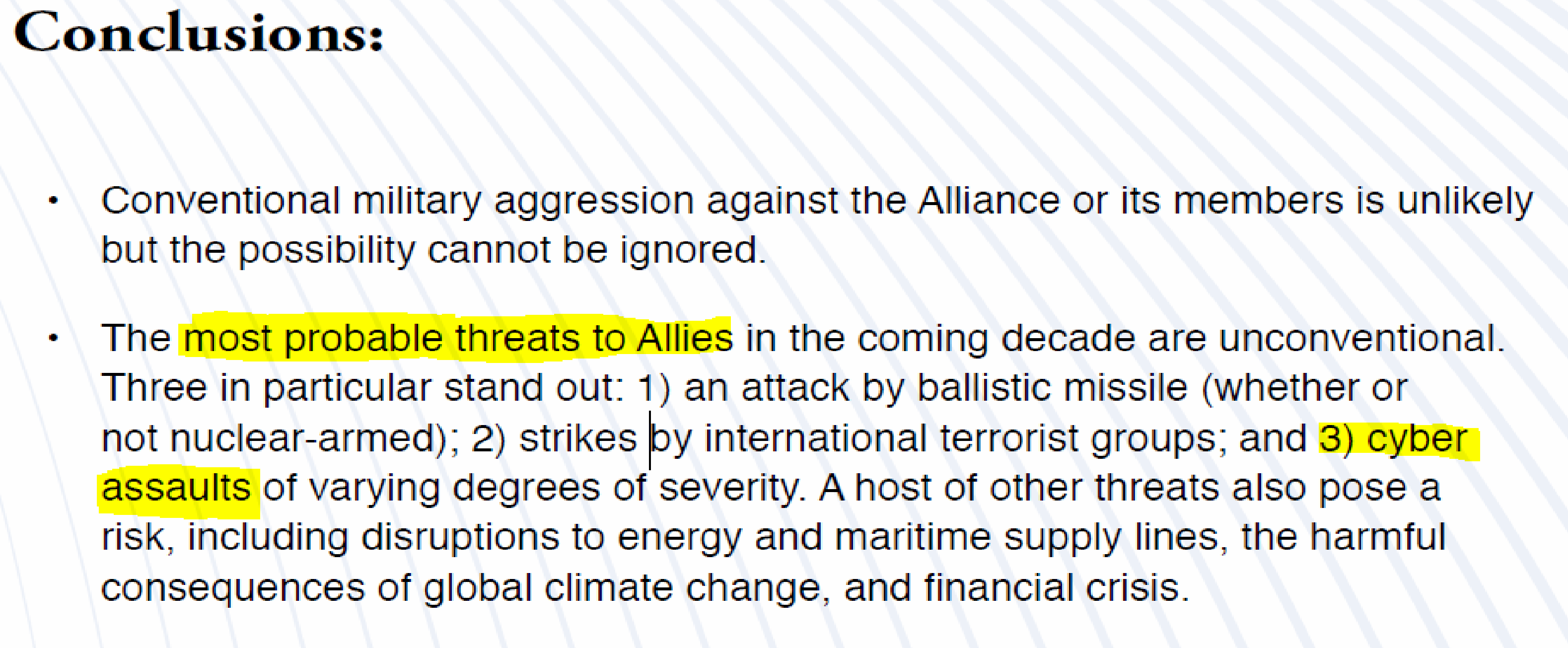
NATO Threat Landscape for 2010-2020

http://www.nato.int/strategic-concept/index.html

NATO 2020:

ASSURED SECURITY; DYNAMIC ENGAGEMENT

ANALYSIS AND RECOMMENDATIONS
OF THE GROUP OF EXPERTS
ON A NEW STRATEGIC CONCEPT
FOR NATO



Conclusions:

- Conventional military aggression against the Alliance or its members is unlikely but the possibility cannot be ignored.
- The most probable threats to Allies in the coming decade are unconventional. Three in particular stand out: 1) an attack by ballistic missile (whether or not nuclear-armed); 2) strikes by international terrorist groups; and 3) cyber assaults of varying degrees of severity. A host of other threats also pose a risk, including disruptions to energy and maritime supply lines, the harmful consequences of global climate change, and financial crisis.

NATO Strategic Concept for 2010-2020

http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

“(Para. 12) Cyber attacks …can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability.”

…

Collective defence. NATO members will always assist each other against attack, in accordance with Article 5 of the Washington Treaty. NATO will deter and defend against any threat of aggression, and against emerging security challenges .”

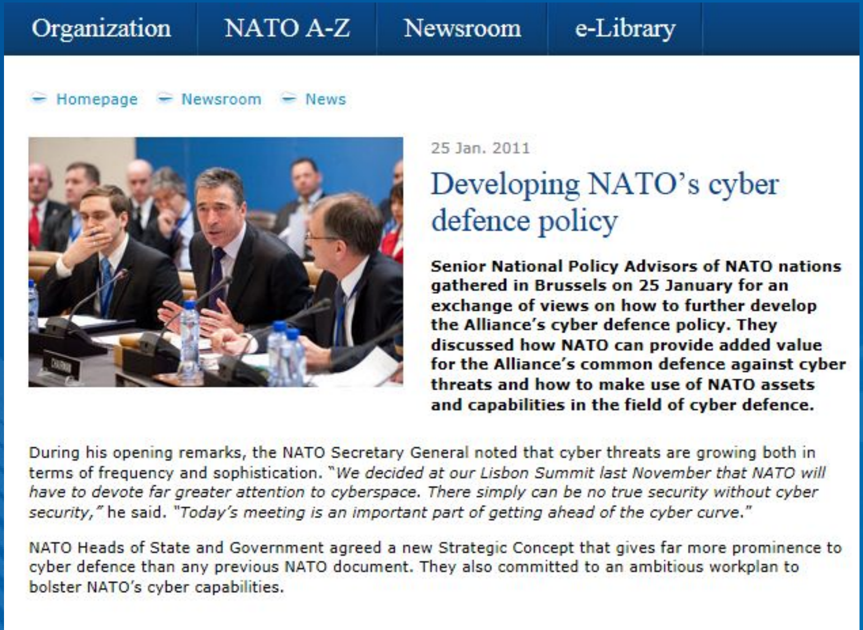
LISBONNE
SUMMIT 19-20 XI 2010 SOMMET

NATO Lisbon Summit

Declaration of Heads of States and Governments

http://www.nato.int/cps/en/natolive/official_texts_68828.htm?selectedLocale=en

"Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to assess, detect, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alliance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection. We will use NATO's defence planning processes in order to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimise information sharing, collaboration and interoperability. To address the security risks emanating from cyberspace, we will work closely with other actors, such as the UN and the EU, as agreed. We have tasked the Council to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth cyber defence policy by June 2011 and to prepare an action plan for its implementation."



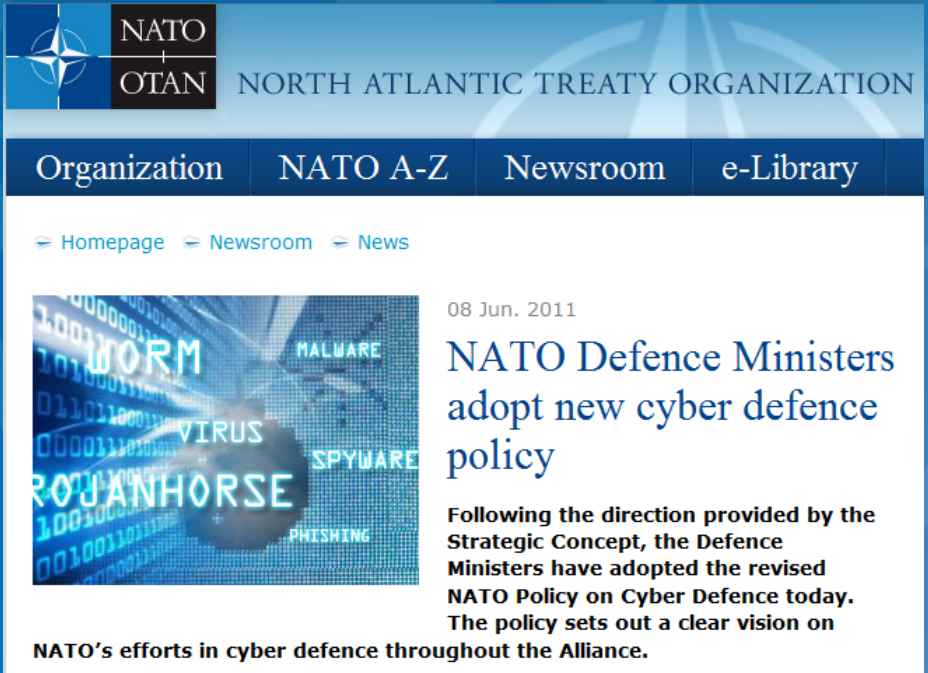
25 Jan. 2011

Developing NATO's cyber defence policy

Senior National Policy Advisors of NATO nations gathered in Brussels on 25 January for an exchange of views on how to further develop the Alliance's cyber defence policy. They discussed how NATO can provide added value for the Alliance's common defence against cyber threats and how to make use of NATO assets and capabilities in the field of cyber defence.

During his opening remarks, the NATO Secretary General noted that cyber threats are growing both in terms of frequency and sophistication. "*We decided at our Lisbon Summit last November that NATO will have to devote far greater attention to cyberspace. There simply can be no true security without cyber security,*" he said. "*Today's meeting is an important part of getting ahead of the cyber curve.*"

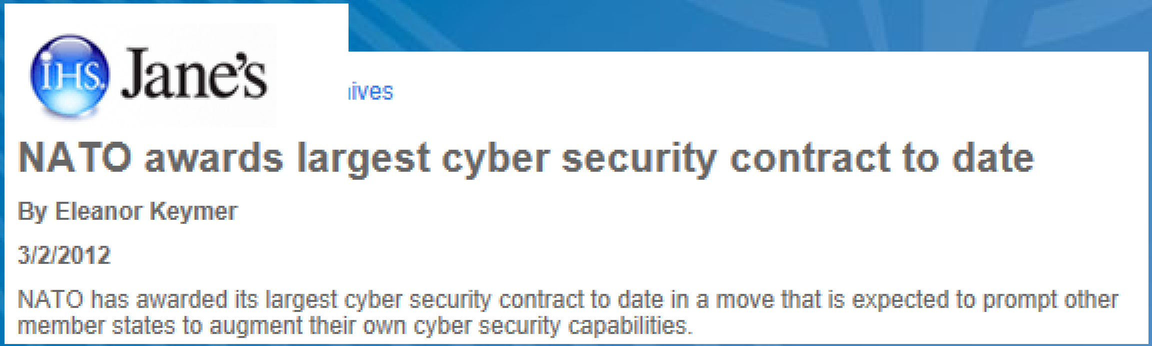
NATO Heads of State and Government agreed a new Strategic Concept that gives far more prominence to cyber defence than any previous NATO document. They also committed to an ambitious workplan to bolster NATO's cyber capabilities.



08 Jun. 2011

NATO Defence Ministers adopt new cyber defence policy

Following the direction provided by the Strategic Concept, the Defence Ministers have adopted the revised NATO Policy on Cyber Defence today. The policy sets out a clear vision on NATO's efforts in cyber defence throughout the Alliance.



NATO awards largest cyber security contract to date

By Eleanor Keymer

3/2/2012

NATO has awarded its largest cyber security contract to date in a move that is expected to prompt other member states to augment their own cyber security capabilities.

NATO OTAN

CHICAGO
SUMMIT • 20-21.V.2012 • SOMMET

Head of States Summit May 2012

Summit Declaration

(http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode=pressrelease)

…reaffirm the cyber defence commitments made at the Lisbon Summit…

…further integrate cyber defence measures into Alliance structures and procedures…

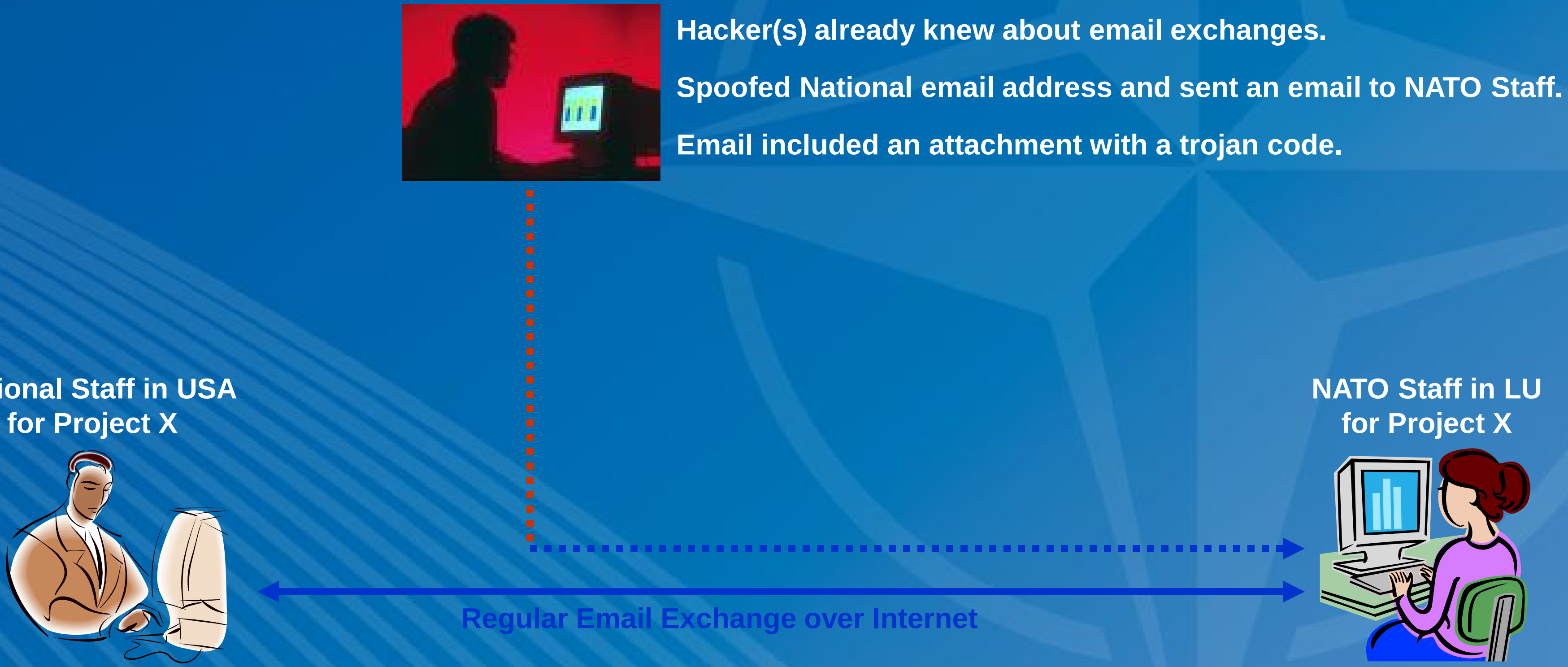
…As individual nations, we remain committed to delivering national cyber defence capabilities…

How is NATO contributing ?

- Awareness Raising at Government levels,
- Capacity Building (NDPP, Partnership Programs),
- Exercises (“Cyber Coalition”) and Training,
- Situation Awareness / Intel Sharing,
- Crisis Management / Collective Defence Procedures,
- Cyber Defence MoUs

NATO's Awareness Raising with Nations – APTs

March 2005 - NATO Reported first APT detection



Hacker(s) already knew about email exchanges.

Spoofed National email address and sent an email to NATO Staff.

Email included an attachment with a trojan code.

National Staff in USA
for Project X

NATO Staff in LU
for Project X

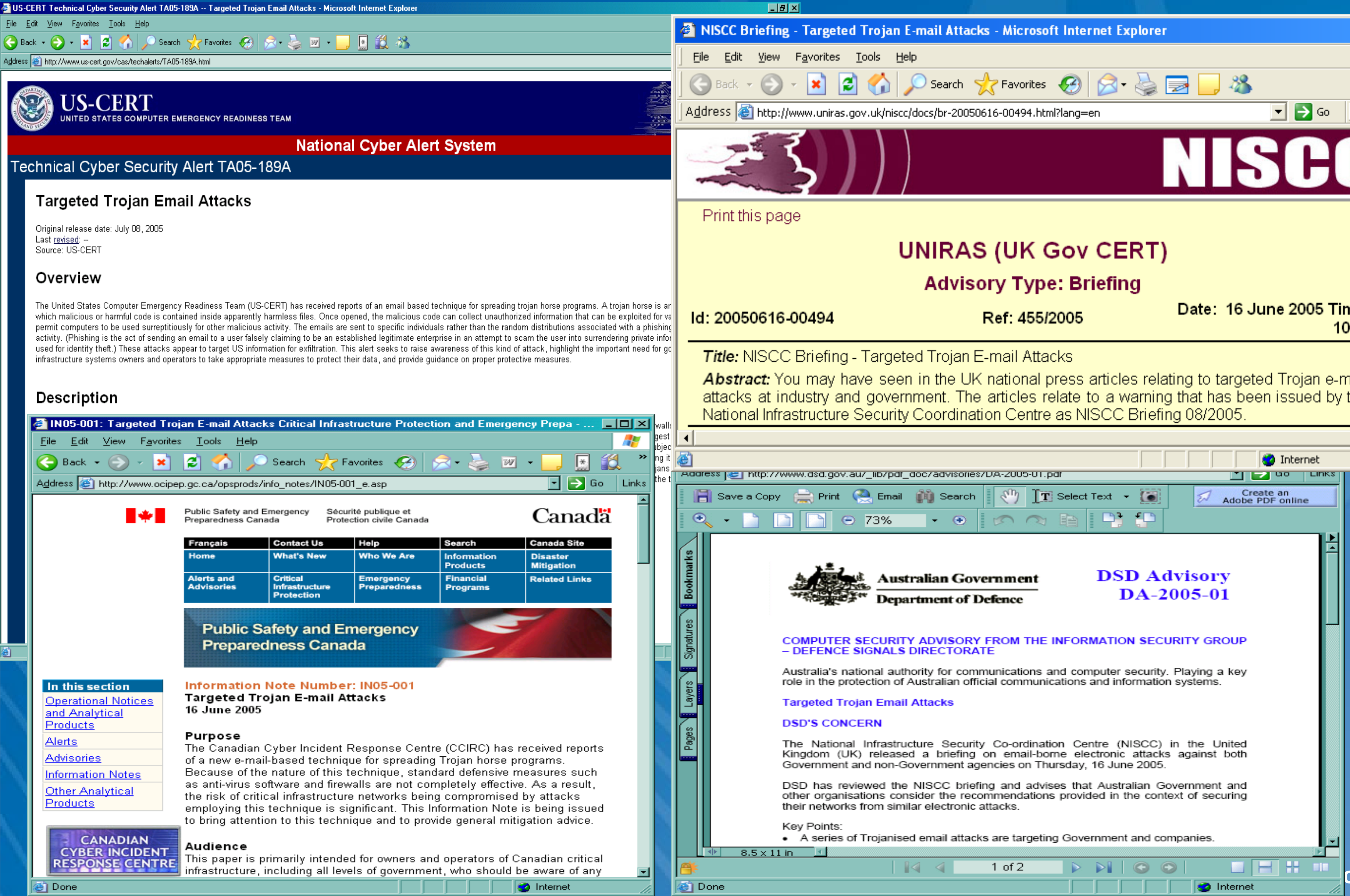
Regular Email Exchange over Internet

NATO Staff thinks that email is from
National Staff and opens the attachment.

Trojan infects the NATO computer.
Virus scanners would not detect the trojan code.

NATO's Awareness Raising with Nations – APTs

3 months later (June 2005) – Nations started reporting


US-CERT Technical Cyber Security Alert TA05-189A -- Targeted Trojan Email Attacks - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.us-cert.gov/cas/techalerts/TA05-189A.html
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
National Cyber Alert System

Technical Cyber Security Alert TA05-189A

Targeted Trojan Email Attacks

Original release date: July 08, 2005
Last revised: --
Source: US-CERT

Overview

The United States Computer Emergency Readiness Team (US-CERT) has received reports of an email based technique for spreading trojan horse programs. A trojan horse is an which malicious or harmful code is contained inside apparently harmless files. Once opened, the malicious code can collect unauthorized information that can be exploited for va permit computers to be used surreptitiously for other malicious activity. The emails are sent to specific individuals rather than the random distributions associated with a phishing activity. (Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private infor used for identity theft.) These attacks appear to target US information for exfiltration. This alert seeks to raise awareness of this kind of attack, highlight the important need for go infrastructure systems owners and operators to take appropriate measures to protect their data, and provide guidance on proper protective measures.

Description

NISCC Briefing - Targeted Trojan E-mail Attacks - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.uniras.gov.uk/niscc/docs/br-20050616-00494.html?lang=en
Go Links
NISCC
Print this page

UNIRAS (UK Gov CERT)

Advisory Type: Briefing

Id: 20050616-00494 Ref: 455/2005 Date: 16 June 2005 Time: 10:52

Title: NISCC Briefing - Targeted Trojan E-mail Attacks

Abstract: You may have seen in the UK national press articles relating to targeted Trojan e-mail attacks at industry and government. The articles relate to a warning that has been issued by the National Infrastructure Security Coordination Centre as NISCC Briefing 08/2005.

Internet
IN05-001: Targeted Trojan E-mail Attacks Critical Infrastructure Protection and Emergency Prepa - ...
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.ocipep.gc.ca/opsprod/info_notes/IN05-001_e.asp
Go Links
Public Safety and Emergency Preparedness Canada
Sécurité publique et Protection civile Canada
Canada
Français Contact Us Help Search Canada Site
Home What's New Information Products Disaster Mitigation
Alerts and Advisories Critical Infrastructure Protection Emergency Preparedness Financial Programs Related Links
Public Safety and Emergency Preparedness Canada
In this section
Operational Notices and Analytical Products
Alerts
Advisories
Information Notes
Other Analytical Products
CANADIAN CYBER INCIDENT RESPONSE CENTRE
Done
Internet

Information Note Number: IN05-001
Targeted Trojan E-mail Attacks
16 June 2005

Purpose
The Canadian Cyber Incident Response Centre (CCIRC) has received reports of a new e-mail-based technique for spreading Trojan horse programs. Because of the nature of this technique, standard defensive measures such as anti-virus software and firewalls are not completely effective. As a result, the risk of critical infrastructure networks being compromised by attacks employing this technique is significant. This Information Note is being issued to bring attention to this technique and to provide general mitigation advice.

Audience
This paper is primarily intended for owners and operators of Canadian critical infrastructure, including all levels of government, who should be aware of any

Address http://www.dsd.gov.au/_lib/pdf_doc/advisories/DA-2005-01.pdf
Go Links
Save a Copy Print Email Search Select Text
Create an Adobe PDF online
73%
Bookmarks Signatures Layers Pages
Australian Government
Department of Defence
8.5 x 11 in
1 of 2
Done
Internet

DSD Advisory DA-2005-01

COMPUTER SECURITY ADVISORY FROM THE INFORMATION SECURITY GROUP – DEFENCE SIGNALS DIRECTORATE

Australia's national authority for communications and computer security. Playing a key role in the protection of Australian official communications and information systems.

Targeted Trojan Email Attacks

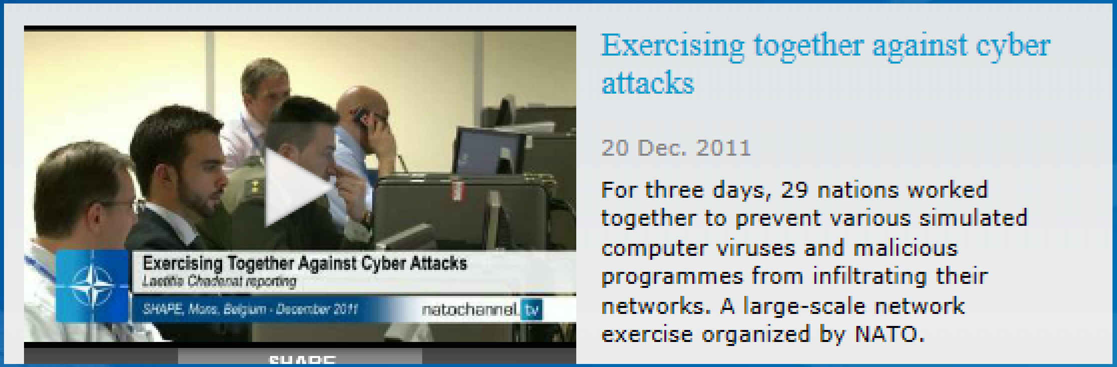
DSD'S CONCERN

The National Infrastructure Security Co-ordination Centre (NISCC) in the United Kingdom (UK) released a briefing on email-borne electronic attacks against both Government and non-Government agencies on Thursday, 16 June 2005.

DSD has reviewed the NISCC briefing and advises that Australian Government and other organisations consider the recommendations provided in the context of securing their networks from similar electronic attacks.

Key Points:
- A series of Trojanised email attacks are targeting Government and companies.

Engaging with Nations, Partners, EU, Youth, Industry...


Exercising Together Against Cyber Attacks
Laetitia Chadenat reporting
SHAPE, Mons, Belgium - December 2011
natochannel.tv
SHARE

Exercising together against cyber attacks

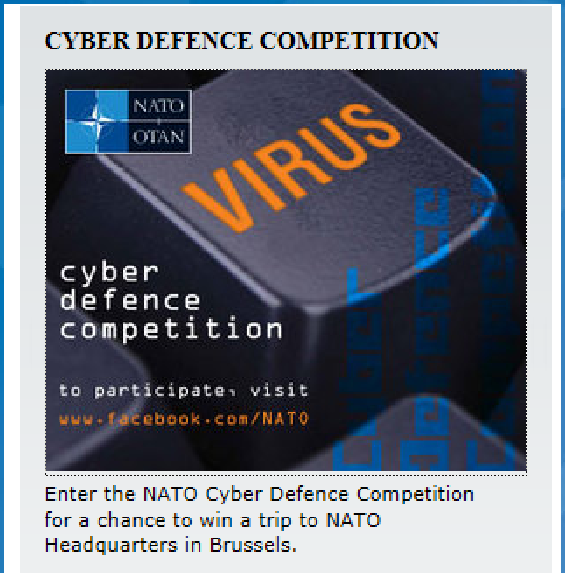
20 Dec. 2011

For three days, 29 nations worked together to prevent various simulated computer viruses and malicious programmes from infiltrating their networks. A large-scale network exercise organized by NATO.

10 Nov. 2011

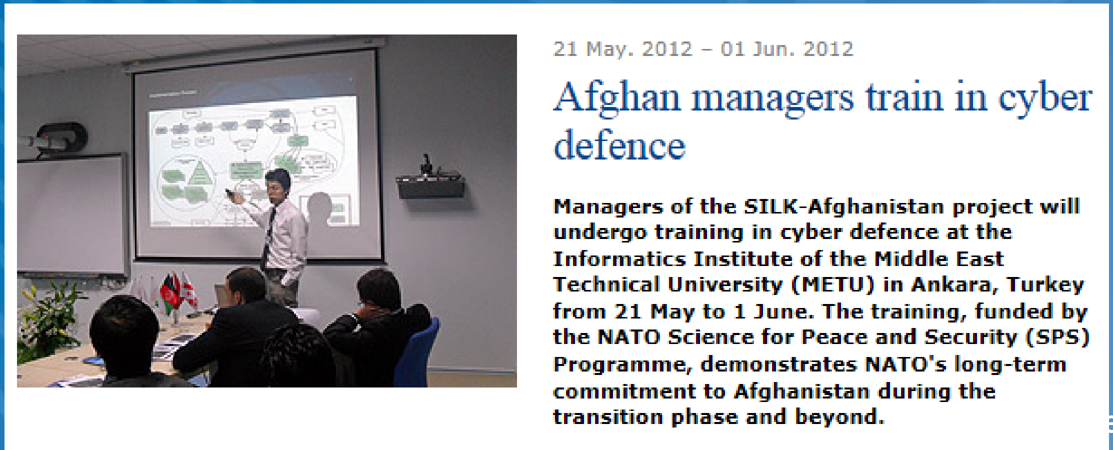
Working with the private sector to deter cyber attacks

In today's world, life without computers is unimaginable. From personal gadgets to state infrastructure, the prevalence of computers has changed almost everything about the world we live in. It has also generated new threats to international security through the multiplication of often sophisticated cyber attacks. To help resist and deter these threats, NATO has been working with some of the world's biggest private cyber security companies to share knowledge and experience.



CYBER DEFENCE COMPETITION

Enter the NATO Cyber Defence Competition for a chance to win a trip to NATO Headquarters in Brussels.

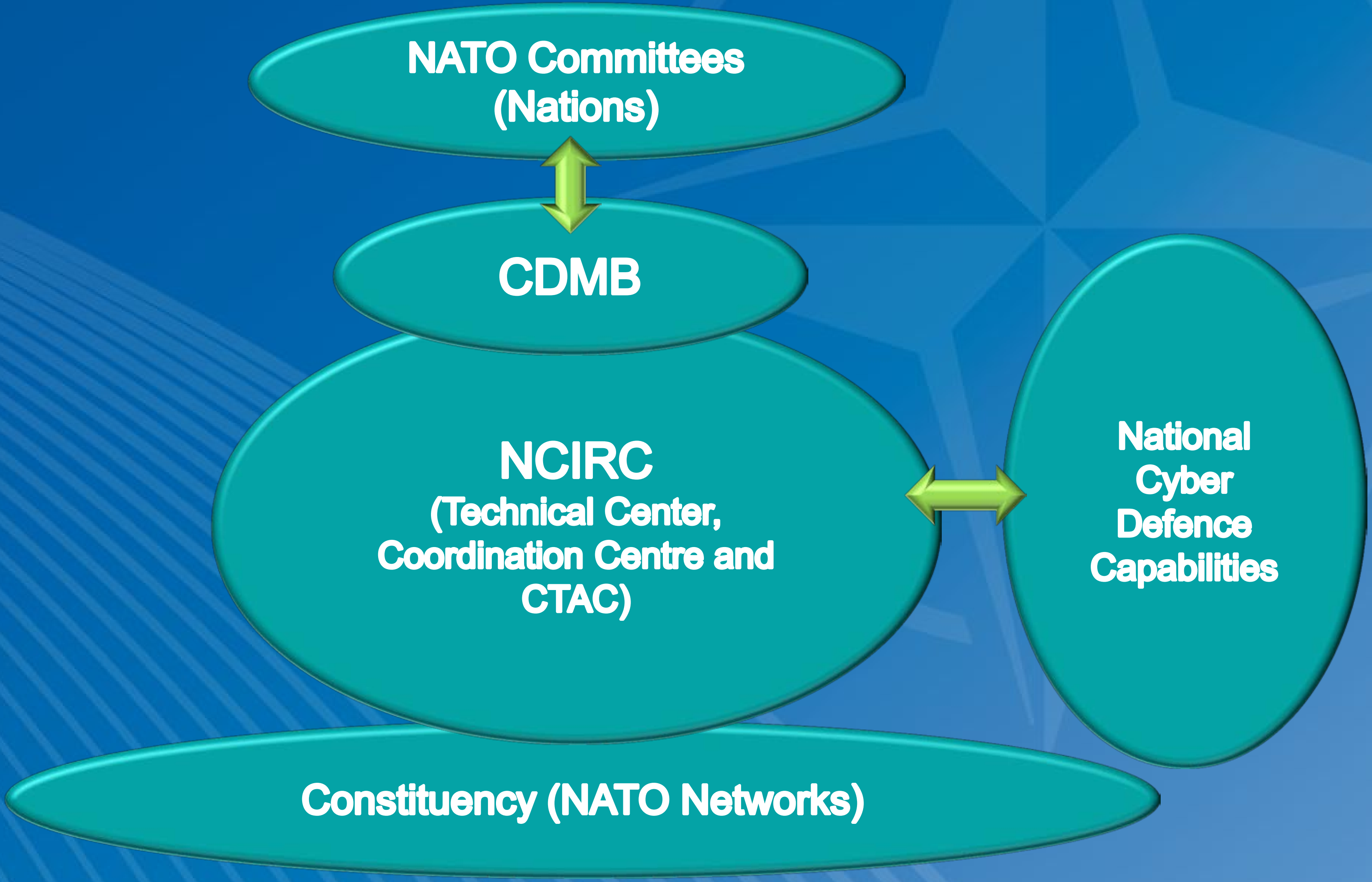


21 May. 2012 – 01 Jun. 2012

Afghan managers train in cyber defence

Managers of the SILK-Afghanistan project will undergo training in cyber defence at the Informatics Institute of the Middle East Technical University (METU) in Ankara, Turkey from 21 May to 1 June. The training, funded by the NATO Science for Peace and Security (SPS) Programme, demonstrates NATO's long-term commitment to Afghanistan during the transition phase and beyond.

Cyber Defence Governance in NATO



NATO Committees (Nations)

CDMB

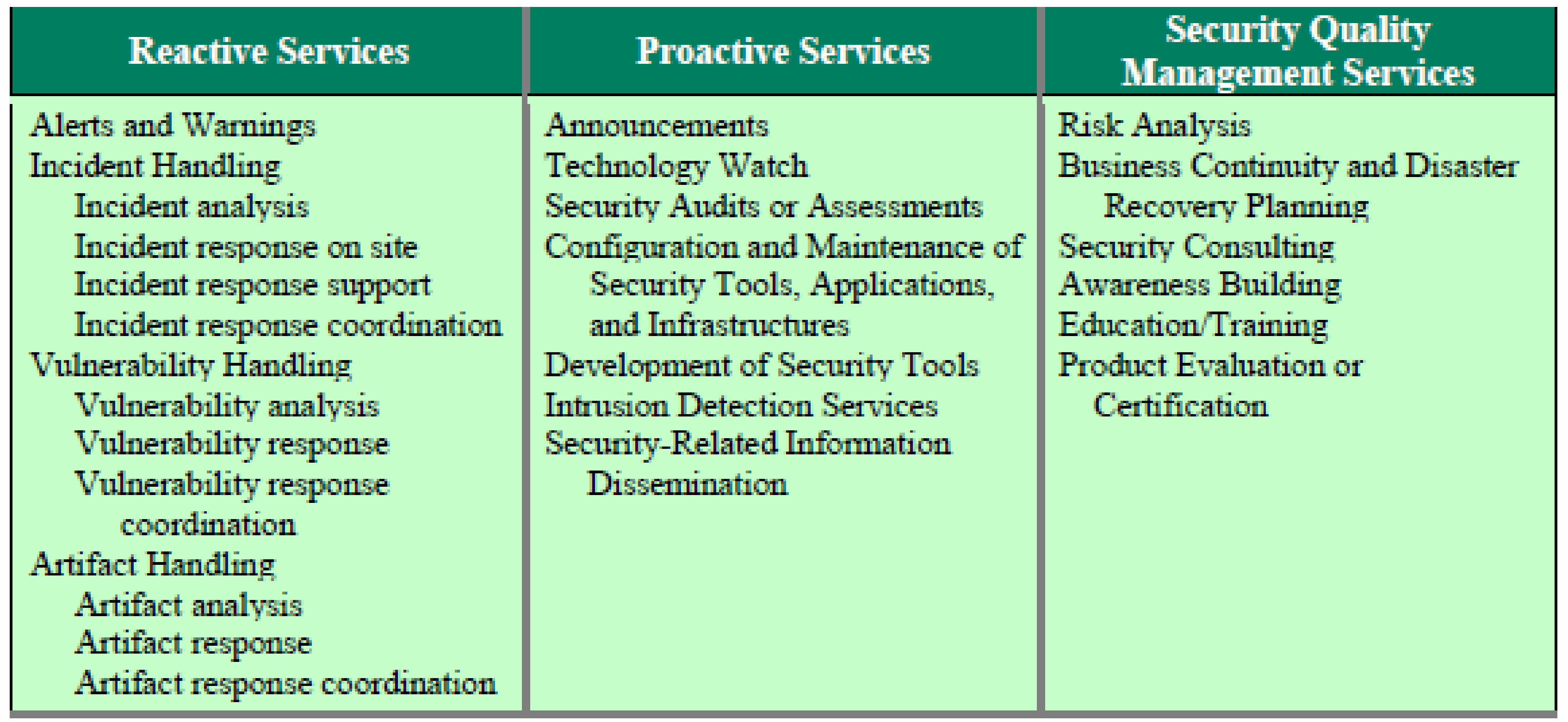
NCIRC (Technical Center, Coordination Centre and CTAC)

National Cyber Defence Capabilities

Constituency (NATO Networks)

Cyber Defence in NATO – Capability

NCIRC (all of below and more)



Reactive Services	Proactive Services	Security Quality Management Services
Alerts and Warnings Incident Handling Incident analysis Incident response on site Incident response support Incident response coordination Vulnerability Handling Vulnerability analysis Vulnerability response Vulnerability response coordination Artifact Handling Artifact analysis Artifact response Artifact response coordination	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

http://www.cert.org/csirts/services.html

What does NCIRC see ?

- On average; 300 incidents/month,
- A lot of probing,
- Many APTs,
- Hacktivists (pre-summits, events),
- Lots and lots of low-level events/ noise,
- Many “Insider” violations.

Cyberspace; Unprecedented Opportunities

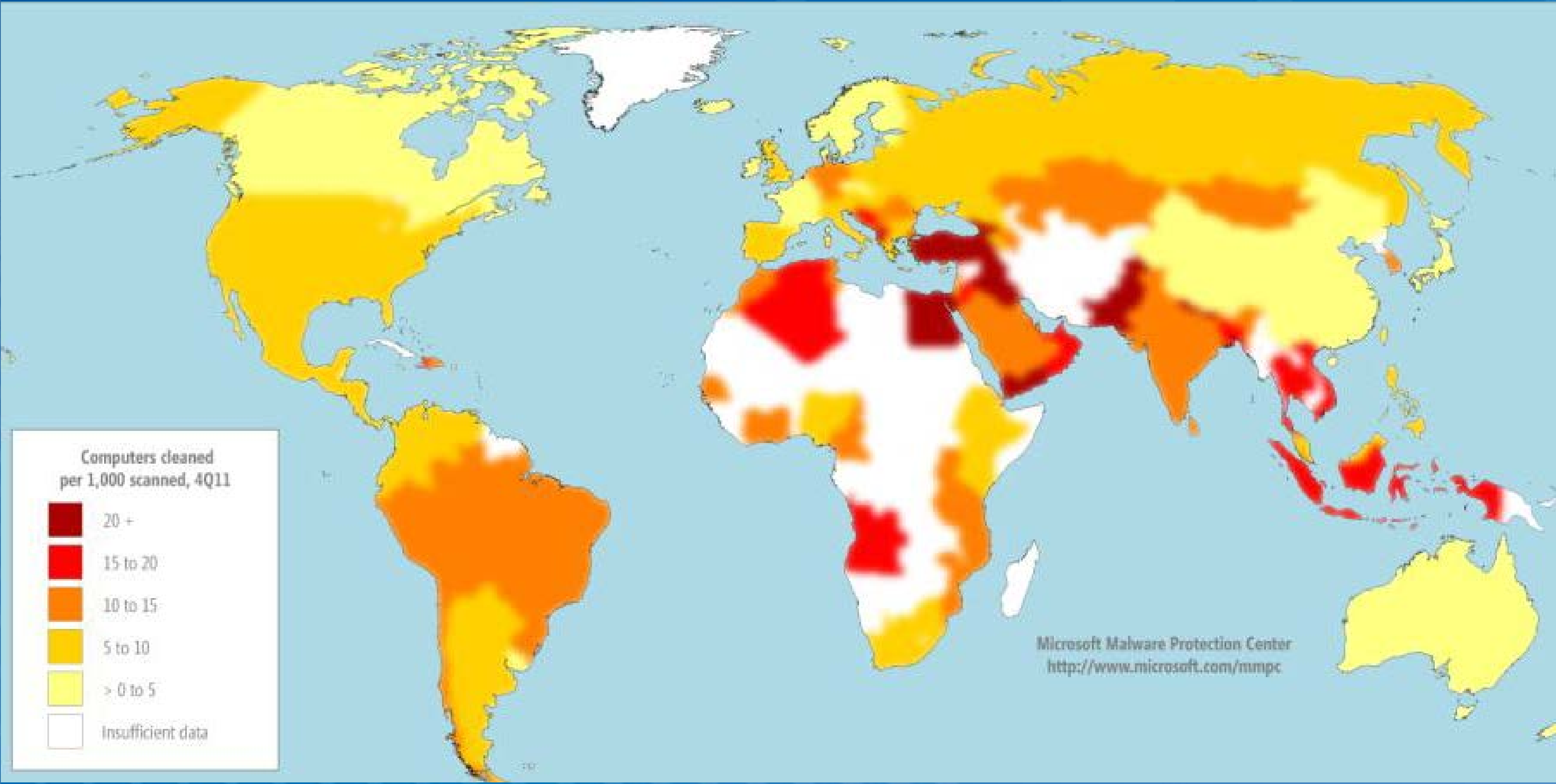
- %30 impact on increase in Global GDP.

- 400bn GDP increase and 14 million new jobs.

- 388bn annual decrease in cybercrime.

- New “Cyber Generation”. Children 5 years old:
  - who can use a mobile phone to call: 23%
  - who can tie own shoe laces: 11%

But, we have a global "Hygiene" problem.



Microsoft Malware Protection Center
http://www.microsoft.com/mmpc

How do we “clean up” ?

- Keep your “cyberspace” clean,
- Assist others who need help,
- Need a Global Initiative.

Thank you.

Suleyman ANIL

s.anil@hq.nato.int