Defending Cyberspace; Global Challenges require Global Responses

Suleyman ANIL
Head, Cyber Defence
Emerging Security Challenges Division
NATO HQ, Brussels
NATO Team in 2005 FIRST Singapore
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.
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](http://www.nato.int/science)

Which subject to apply; Any Cyber Defence/ CERT related subject
NATO and Counter Terrorism

STANDEX; Distance detection of Suicide Bombers.
“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’s Approach to Cyberspace – a new “Global Common”

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

ASSURED ACCESS TO THE GLOBAL COMMONS
Maritime | Air | Space | Cyber
FINDINGS AND RECOMMENDATIONS
NATO’s “Cyberspace”

• “nato.int” Domain,

• Closed Networks.
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.
“(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.”
“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.”
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 Istanbul Summit last November that NATO will have to devote far greater attention to cyberspace. There 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.

IHS Jane’s
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.
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
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.

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

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.

Working with the private sector to deter cyber attacks
10 Nov. 2011
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.

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)
- Constituency (NATO Networks)
- National Cyber Defence Capabilities
# Cyber Defence in NATO – Capability

**NCIRC** (all of below and more)

<table>
<thead>
<tr>
<th>Reactive Services</th>
<th>Proactive Services</th>
<th>Security Quality Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts and Warnings</td>
<td>Announcements</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>Incident Handling</td>
<td>Technology Watch</td>
<td>Business Continuity and Disaster Recovery Planning</td>
</tr>
<tr>
<td>Incident analysis</td>
<td>Security Audits or Assessments</td>
<td>Security Consulting</td>
</tr>
<tr>
<td>Incident response on site</td>
<td>Configuration and Maintenance of Security Tools, Applications, and Infrastructures</td>
<td>Awareness Building</td>
</tr>
<tr>
<td>Incident response support</td>
<td></td>
<td>Education/Training</td>
</tr>
<tr>
<td>Incident response coordination</td>
<td></td>
<td>Product Evaluation or Certification</td>
</tr>
<tr>
<td>Vulnerability Handling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vulnerability response coordination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact Handling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artifact response coordination</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.cert.org/csirts/services.html">http://www.cert.org/csirts/services.html</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 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.
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