NATO
OTAN

INTERNATIONAL STAFF
EMERGING SECURITY CHALLENGES

NATO CIS SERVICES AGENCY
NATO INFORMATION ASSURANCE TECHNICAL CENTRE

NCIRC
NATO
COMPUTER INCIDENT
RESPONSE CAPABILITY

NATO Perspective
on
Cyber Defence and Botnets

9-March-2011

Virginia Aguilar, ESCD
Ömer Hasret, NCSA / NCIRC

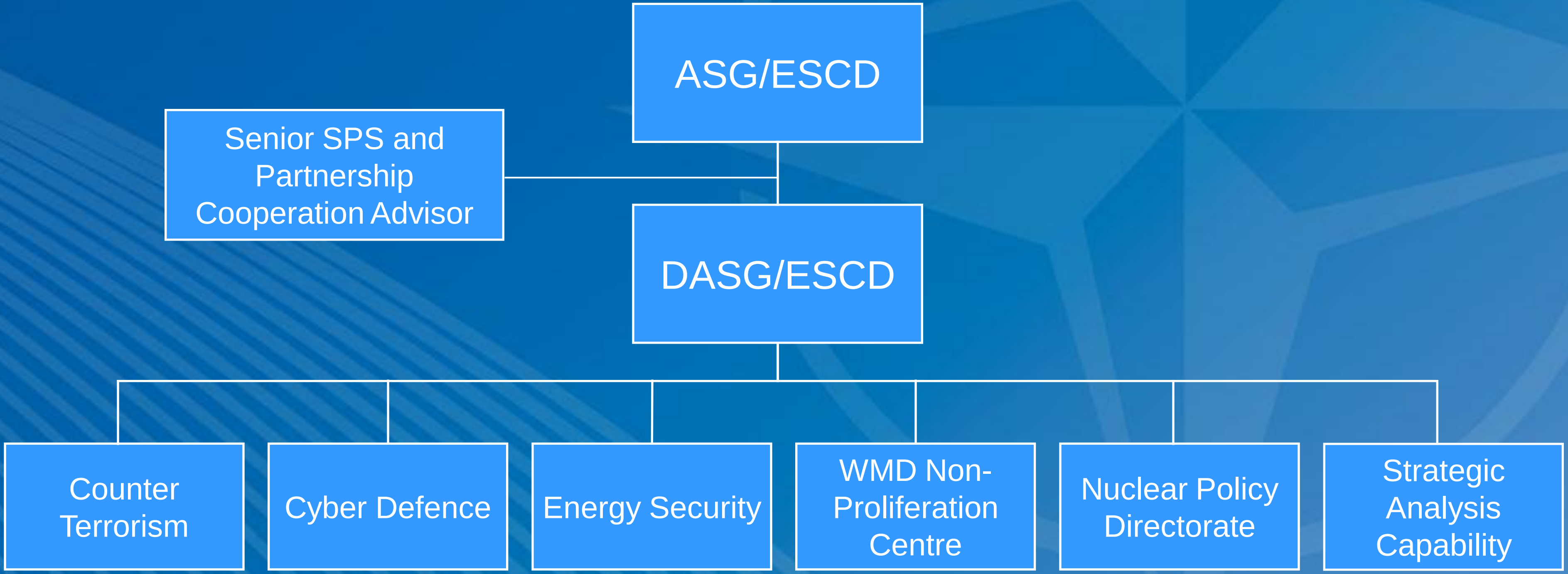
Background

- Threats in the Cyber Space.
- Some milestones in Security Awareness:
  - Estonia
  - Georgia
  - Mariposa botnet
  - Stuxnet

Background

- Strategy overview
  - Prague Summit
  - NCIRC Initial Operating Capability
  - 1st Cyber Defense Policy
  - CDMA
  - NATO 2020 Report
  - Creation of Emerging Security Challenges Division (ESCD)
  - Lisbon Summit, November 2010

ESCD Structure



ASG/ESCD

Senior SPS and Partnership Cooperation Advisor

DASG/ESCD

Counter Terrorism

Cyber Defence

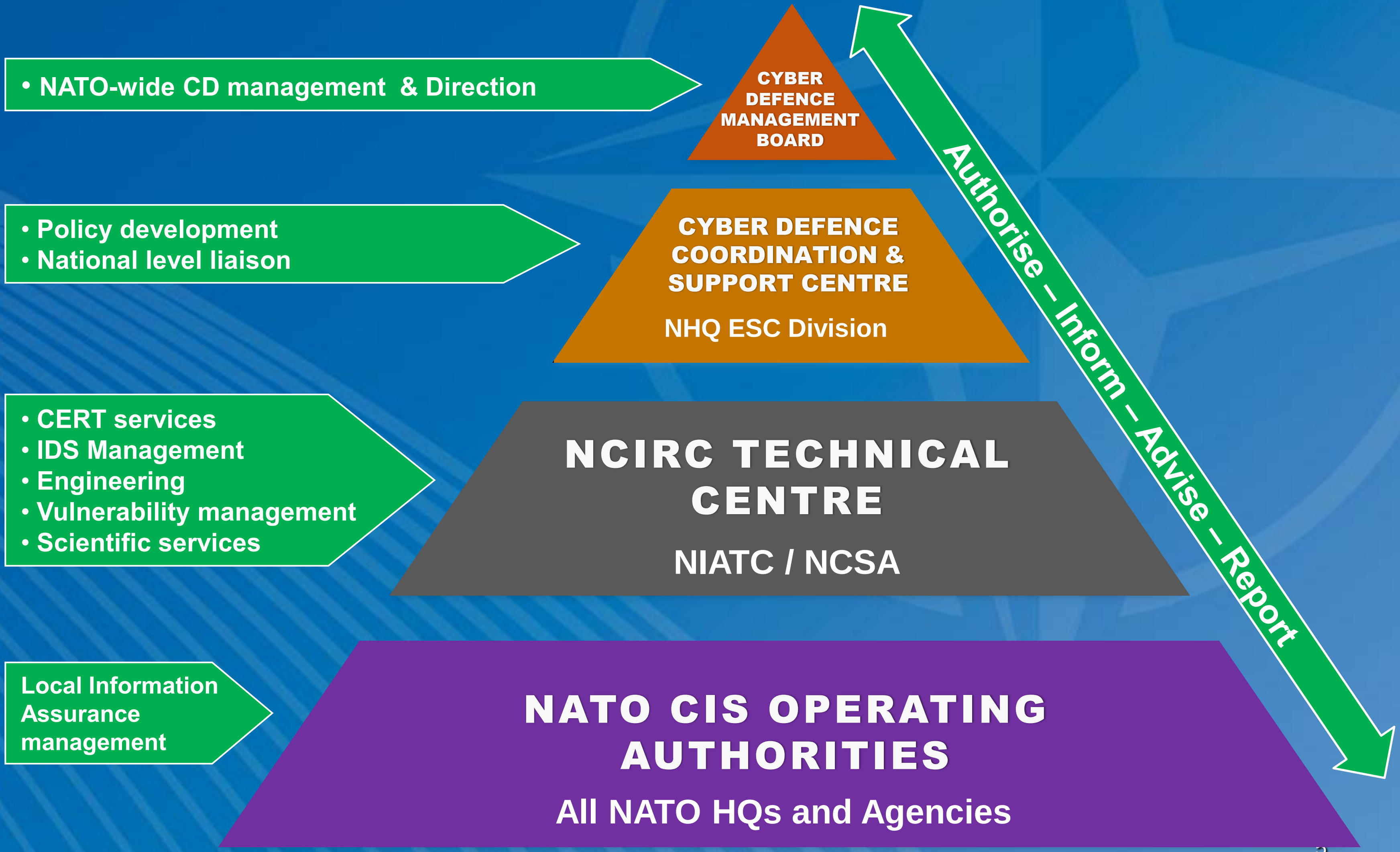
Energy Security

WMD Non-Proliferation Centre

Nuclear Policy Directorate

Strategic Analysis Capability

NATO Cyber Defence



- NATO-wide CD management & Direction

CYBER DEFENCE MANAGEMENT BOARD

- Policy development
- National level liaison

CYBER DEFENCE COORDINATION & SUPPORT CENTRE

NHQ ESC Division

- CERT services
- IDS Management
- Engineering
- Vulnerability management
- Scientific services

NCIRC TECHNICAL CENTRE

NIATC / NCSA

Local Information Assurance management

NATO CIS OPERATING AUTHORITIES

All NATO HQs and Agencies

Cyber Defence Roadmap

- Cyber Defence Concept under development.
- Policy Update, by April 2011
- Action Plan, by June 2011
- NCIRC FOC by December 2012

Cyber Defence Collaboration

- Collaboration between Nations, Partners and other Organisations
- Central Governance
- Cyber Defence Exercises
- NATO Information Assurance Symposium
- Science for Peace and Security Programme
- Collaboration with CCDCOE

NATO Lisbon Summit

- Develop further CD capabilities
- Update NATO CD policy & plans
- Centralized CD services for NATO
- Achieve NCIRC FOC by 2012
- Better integration of NATO cyber awareness, warning and response with member nations
- More engagement with EU and UN

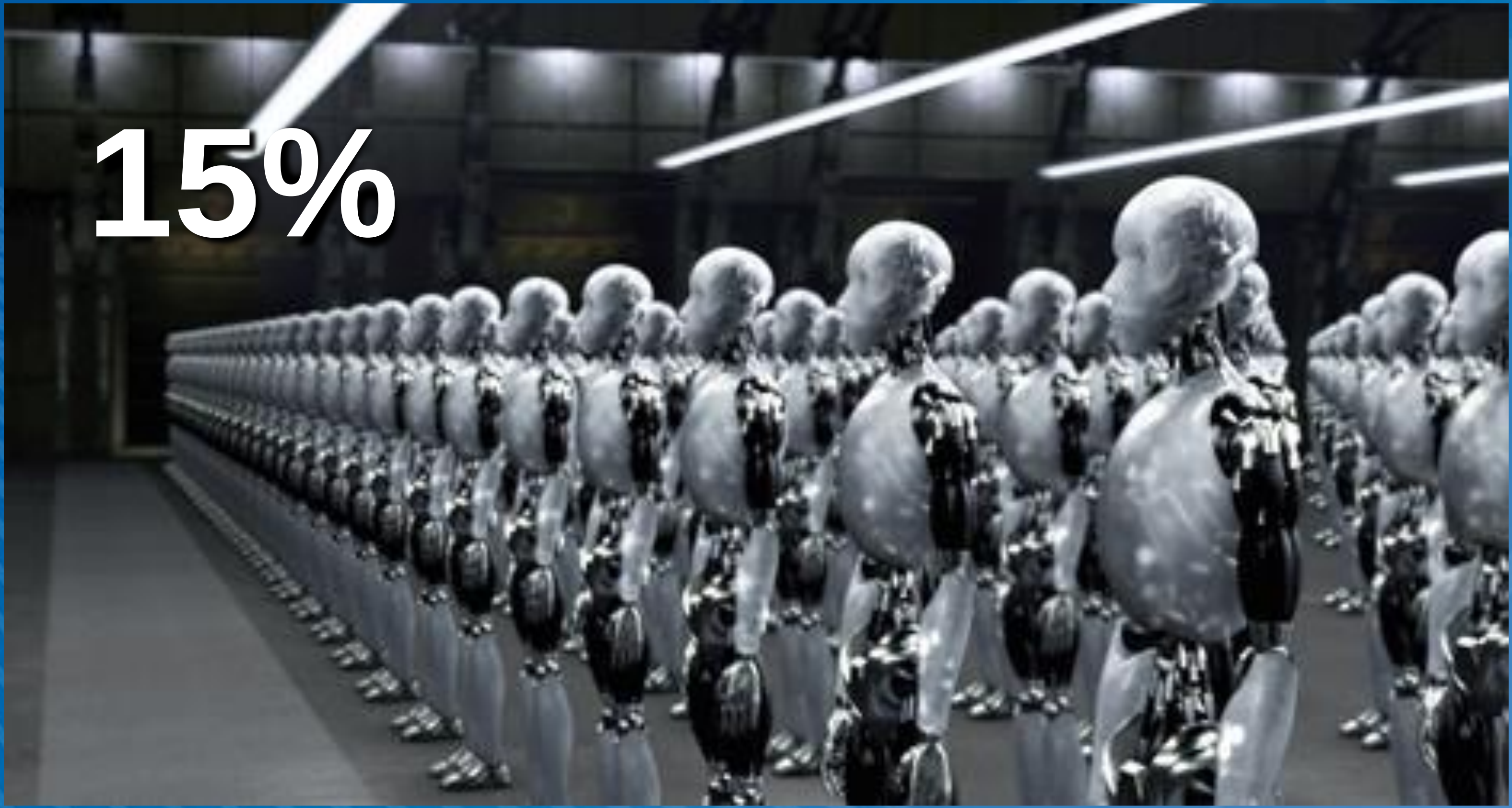
Active Engagement - Modern Defence

30,000,000

Security events per day

Viewed by security event analysts after customized filtering

Average number of incidents created



15%

Percentage of botnet related incidents

NATO is a target

- Politically motivated cyber activists
  - DDoS
  - Web site defacement

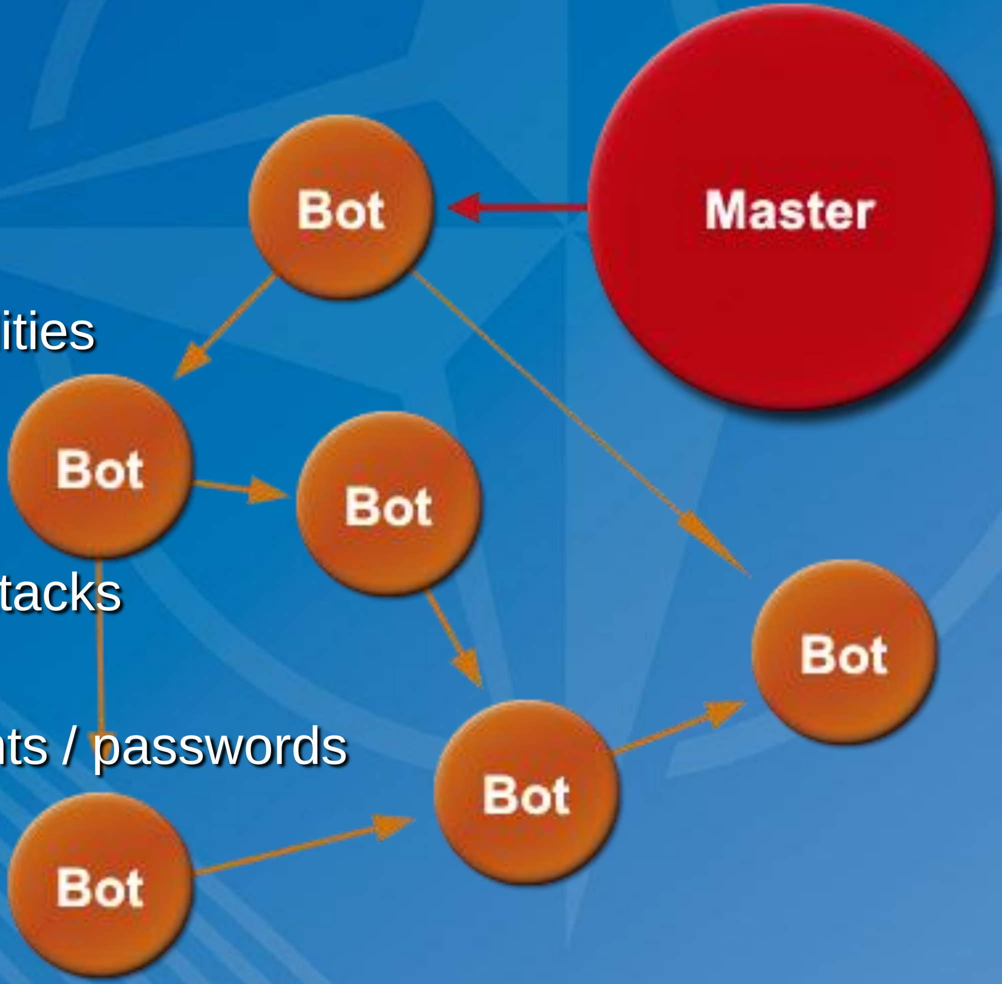
- Fame seeking attackers
  - Mostly intent on web site defacement

- Global threats to Internet users
  - Botnets, mass malware, etc.

- Cyber espionage
  - Targeted attacks
  - Bot characteristics

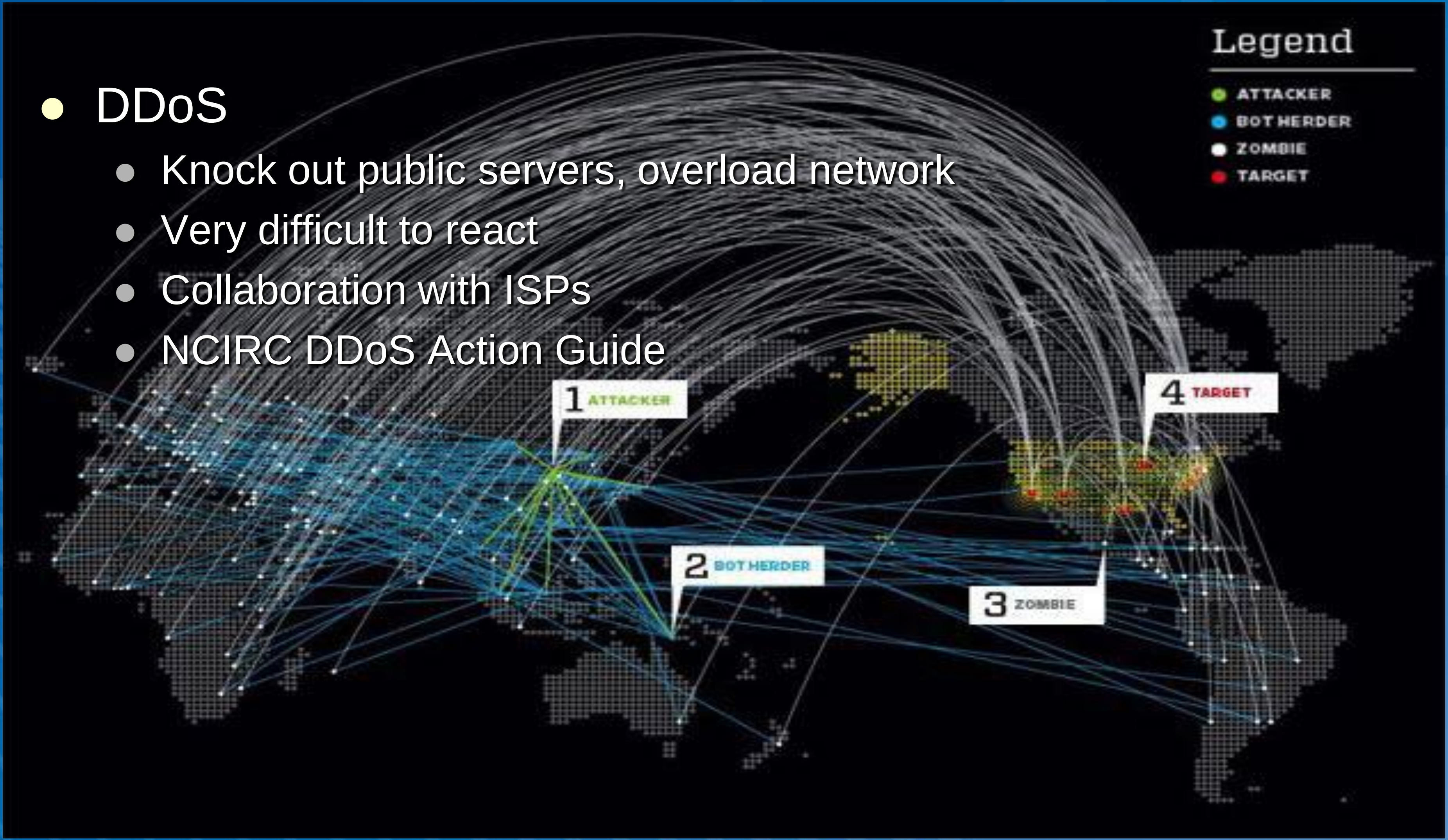
NATO and Botnets

- Cyber attacks by botnets
  - DDoS
  - Spam
  - Network scan for vulnerabilities
- Bot infection malware
  - Both targeted and global attacks
  - Information theft
  - Compromising user accounts / passwords

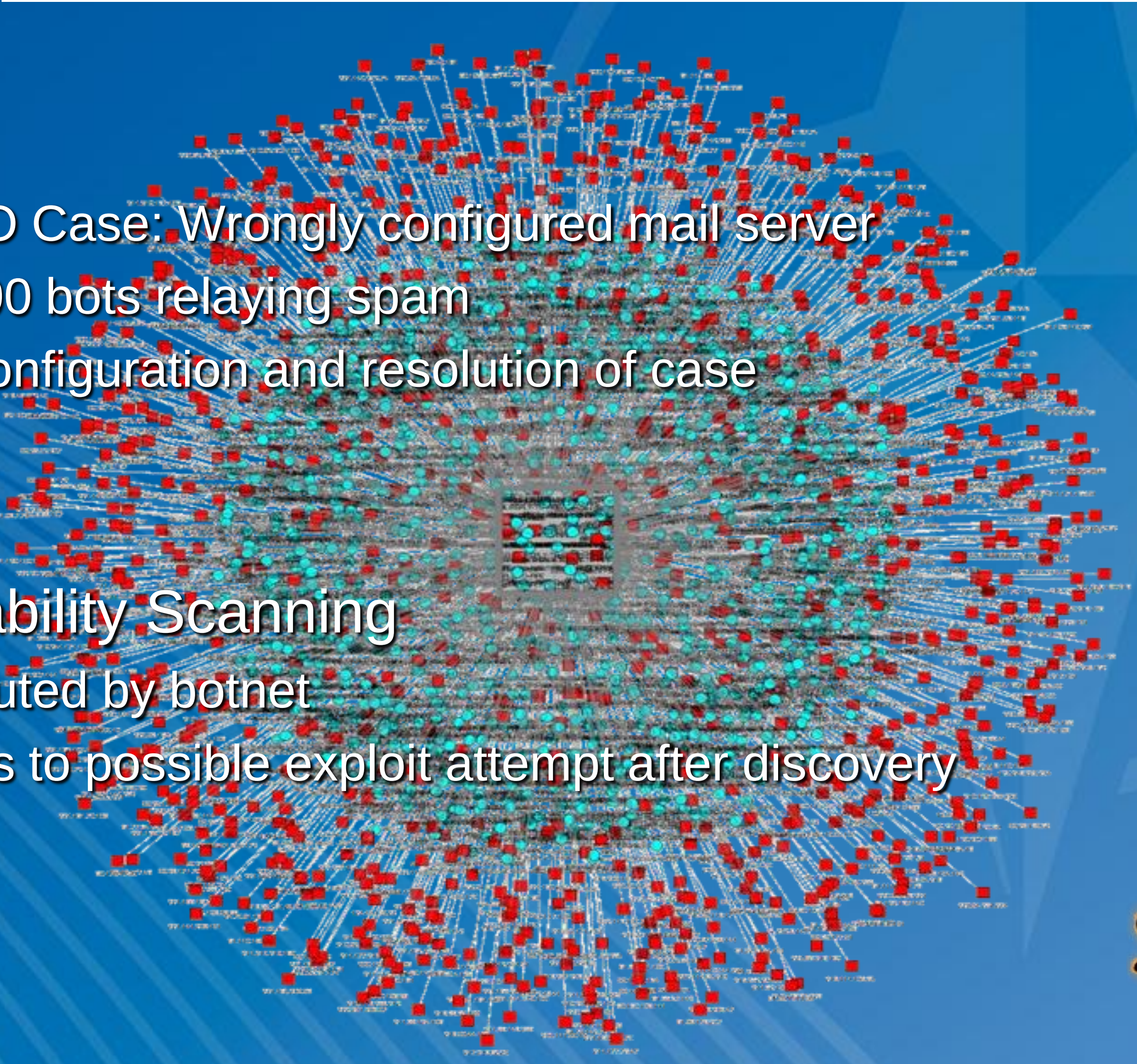


Cyber Attacks by Botnets

- DDoS
  - Knock out public servers, overload network
  - Very difficult to react
  - Collaboration with ISPs
  - NCIRC DDoS Action Guide



Cyber Attacks by Botnets



- Spam
  - NATO Case: Wrongly configured mail server
  - 25,000 bots relaying spam
  - Re-configuration and resolution of case
- Vulnerability Scanning
  - Executed by botnet
  - Leads to possible exploit attempt after discovery

Bot Infection Malware

- Global mass malware
  - Affecting all internet users, public
    - Rimecud, Pushbot, Virut, Zbot, Conficker, etc.
    - New variants regularly appear
  - Relatively easy to collect information
    - Global exposure means global reaction
    - Security vendors prepare reports
  - Close collaboration with vendors

Bot Infection Malware

- Targeted Attacks
  - Several unique attempts every month
  - Weaponized documents (mostly PDFs)
  - Using 0-day vulnerabilities
  - Several layers of obfuscation
  - Totally new sample, no prior detection
  - Reverse engineering INDISPENSABLE

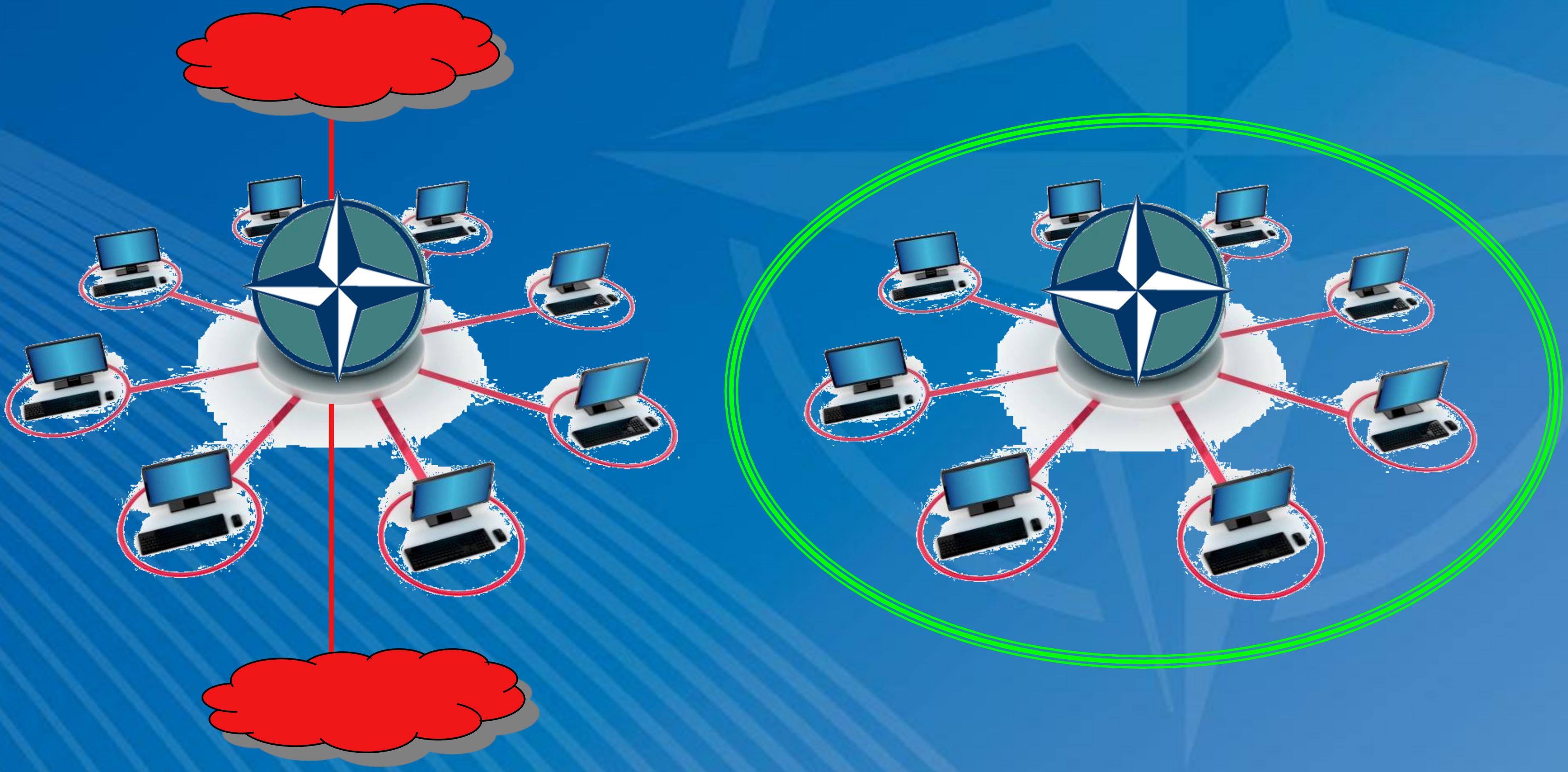
Bot Infection Malware

- Targeted Attacks (cont.)
  - Close collaboration with vendors
  - Customized detection signatures
  - Reverse engineering malware
  - Rapid reaction by collaboration of several layers
    - Blocking at perimeter firewall
    - IDS / IPS updated with custom signatures
    - Tracking of vulnerability and implementing workarounds and patches

Collaboration against Botnets

- National CERTs (Military & Civilian)
  - POC for incidents concerning their nation
- shadowserver Foundation
  - Information sharing
  - Monitoring NATO IP addresses
- ISPs
  - Access to powerful traffic monitoring and analysis tools
  - Help in reacting to incidents
- Security vendors

Protecting NATO Networks



NATO UNCLASSIFIED RELEASABLE TO THE PUBLIC

Protecting NATO Networks

- Challenges
  - Network access control
  - Removable media!!!
  - Patch management
  - Timely update of AV definitions

Directives & Guidance

- Technical directives, guidance documents
- Perimeter and network security
  - Firewalls
  - Intrusion Detection & Prevention Systems
- Host-based protection mechanisms
  - Centrally managed anti-malware, anti-spyware
  - Device / port control
- Web Proxy
- Patch management
- Regular vulnerability assessments

Directives & Guidance

- Strict configuration and change management process
  - Penetration testing
  - Compatibility testing
- Centrally managed security settings
  - OS, virtual environments, mobile devices
- Security accreditation
  - Projects
  - Networks
- SecOPs for all IT equipment, network access

Security Education

- Constant security training
  - Both technical and managerial aspects
- User Awareness
  - Mandatory security briefings
  - Posters, flyers, screensavers, wallpapers, Bulletins
  - Online situational awareness training material

User Awareness

even if you can't see it
there might be a threat
keep your AntiVirus Software up-to-date
for further information contact your InfoSec officer at:
Designed by
NCIRCTC@NCIRC.NATO.int
www.NCIRC.NATO.int +32 65 44 6666

Don't click…
… on suspicious E-Mails
ISAF
Designed by
NCIRCTC@NCIRC.NATO.int
www.NCIRC.NATO.int +32 65 44 6666

Conclusion

- Centrally collect and monitor all security events
- Make use of event correlation engines
- Intelligently filter events down to manageable numbers
- Recruit “good” security event analysts
- Acquire malware sandboxing and reverse engineering capability

Botnet cases at NATO

- Case 1
  - 00:03 – Shadowserver report 2 NATO IPs
    - Connection to a known Conficker C&C
  - 00:10 – Deputy Director NCIRC gets informed via phone call
  - 01:00 – Security Event Analyst starts working on the incident
    - Does full packet capture analysis and IDS checks
    - Confirms bot infections, not targeted
  - 02:00 – Both sites get notified
    - Advice on clean-up steps
  - Before next morning:
    - Both systems re-imaged, minimum user impact

Botnet cases at NATO

- Case 2
  - 10:07 – Custom IDS signature triggers
  - 10:08 – Incident Handlers notified by Analyst
    - Incident Handling Officers liaise with remote site
  - 10:23 – Security Event Analyst discovers vector
    - Download of FakeAV
    - Reconstructs sample and forwards to anti-malware
    - Watches out for data egress
  - 10:45 – Analyst observes data egress
    - in the form of machine name, OS, browser version, timezone, logged-on user, etc.

Botnet cases at NATO

- Case 2 (cont.)
  - 10:46 – Bot receives command from HTTP server
    - Sleep for two hours
  - 11:08 – Sample reverse-engineering complete
    - Results confirm C&C address
    - Further C&C addresses are discovered
  - 11:20 – Security Event Analyst updates custom signatures on IDS
  - 11:20 – Discovered C&C addresses are blocked at firewalls
  - 11:36 – Site confirms re-imaging of infected host

Questions

Virginia Aguilar Garcia

Cyber Defence Analyst

Emerging Security Challenges

email: aguilar.virginia@hq.nato.int

Ömer Hasret

Head, CIS Protection Services

NATO Computer Incident Response Capability

email: omer.hasret@ncirc.nato.int