Technical Evaluation Report

NATO Modelling and Simulation Group MSG-121

Modelling and Simulation Support for Cyber Defence

1.0 BACKGROUND AND JUSTIFICATION

The rapidly evolving environment of Cyber threats against the Alliance has necessitated a renewed focus on the development of Cyber Defence policy and capabilities. At the Lisbon Summit in November 2010, NATO Heads of State and Government decided to enhance NATO's cyber defence capabilities. The aim of a NATO Cyber Defence capability is to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems. Modelling and Simulation experience in research, analysis and training should be leveraged to assist in Cyber Defence capability.

The NATO Modelling and Simulation Group (NMSG) has initiated task group (TG) MSG-117 to investigate how M&S can be used in support of the Cyber Defence development effort. This multi-national TG chaired by GBR and NLD has started its activity in late 2012. Research topics may include, but are not limited to, research, analysis, and training. The TG will have closed meetings and discussion up to NATO classified level. In order to also engage the wider M&S community, a separate activity (MSG-121) was started was to organise a one-time open Workshop in support of MSG-117.

2.0 OBJECTIVES AND RESULTS

The objective of the MSG-121 Workshop is to exchange information on current national and NATO activities and initiatives on the use of modelling and simulation in support of cyber defence, and proposals on how M&S might support certain still unaddressed aspects of cyber defence needs. The results are also used to help provide working definitions and characterisation of Cyber Defence for use by the M&S community.

The WS topics to be covered include:

- National overviews of the use of M&S for Cyber Defence
- Common set of definitions and characterization of Cyber Defence
- M&S representation of various types cyber attacks
- M&S for assessing threats and risks on networks and information systems
- M&S for assessing the impact of cyber attack
- Cyber awareness education methods
- Cyber training and simulation capabilities or initiatives
- Integration of cyber attack representation in existing M&S environments
- Cyber training and education programmes
- After action review and assessment methods for Cyber Defence education and training.

Output from this Workshop will inform national Cyber Defence initiatives, and NATO development of the NATO Computer Incident Response Capability Next Generation (NCIRC NG) as well as NMSG-117 on Exploiting M&S to support Cyber Defence." The formal deliverables from the workshop consists of the presentation material and a summary report (this document).

3.0 ORGANISATION

The Workshop was organised by MSG-121 Chairs:

- Mr Bharat Patel, Dstl, GBR
- Mr Wim Huiskamp, TNO, NLD
- Mr Gary Allen, PEOSTRI, USA

The NMSG MSCO provided support (Mr Adrian Voiculet, Ms Illeana Ganz) w.r.t. registration, logistics, AV etc.

NATO Organisations and Nations were asked to provide presentations on national overviews and relevant topics and/or attend and contribute to the objectives of the workshop.

The Workshop has been coordinated with the Simulation Interoperability Standards Organisation (SISO) and co-located with the Spring 2013 SISO Simulation Interoperability Workshop (SIW), 8-12 April 2013, San Diego, USA. SISO Liaison was Mr Mark McCall, SISO Executive Director.

The overall planning schedule is shown below:

- MSG-121 Technical Activity Proposal Submitted to NMSG – Oct 2012
- Call for Participation to NATO S&T Panels – Jan 2013
- Announcement in SISO SIW agenda – Jan 2013
- Planning Mtg MSG-117/MSG-121 – Feb 2013, Portsmouth, GBR
- Workshop Session preparation – Feb-March
- Workshop – 11 April 2013, San Diego, USA

4.0 AGENDA

April 11th, Thursday (Open Session)

0830-0900 Welcome and Introductions (BP, WH, All)

0900-0915 Workshop Objectives and Output Bharat Patel (Dstl, GBR)

0915-0930 NMSG Overview - Wim Huiskamp (TNO Defence, Security and Safety, NLD)

0930-1000 NMSG-117 OverviewMarieke Klaver (TNO Defence, Security and Safety, NLD), Stella Croom-Johnson (Dstl, GBR)

1000-1030 Break

1030-1100 NATO Briefing

Presenter Corinne Lonchampt (ACT C4ISR, FRA), participation thru Skype.

1100-1130 Netherlands National Cyber Defence M&S Activities and InitiativesCyber Awareness Training in Netherlands
Presenter Mr Bert Boltjes (TNO Defence, Security and Safety, NLD), supported by Mr. Ad van Lier (NLD Mod).

1130-1200 Test infrastructure of the Military Test Center (WTD81) in Greding (DEU).

Presenter: Mr. Walter Hader (Military Test Center, Greding, DEU).

1200-1330 Lunch

1330-1745 Discussion session. Panel of four Chair persons introducing four main topics and leading discussion.

1330-1415 Topic 1: How might M&S support Cyber Awareness Training and Education?
Chair and Intro: Maj Mark Young and maj Scott Roach (Canadian National Defence).

Presentation Cyber Awareness Challenge – Michelle Brauer (Team Carney, USA)

1415-1500 Topic 2: How might M&S support Cyber training and exercises?
Chair and Intro: Frank Jonat (Cassidian, DEU) / Christian Wolf (DEU MoD)

1500-1530 Break

1530-1600 Topic 3: Cyber Situational Awareness, how might M&S support threat and risk assessment?
Chair and Intro: Bharat Patel (supported by Jeff Howe (Cassidian, GBR) who cannot participate)

1600-1645 Topic 4: What type of M&S environments are needed to support cyber defence?
Chair and Intro: Wim Huiskamp (TNO Defence, Security and Safety, NLD)

Definitions of LVC for Cyber
Presenter Katherine L. Morse, David L. Drake (JHU/APL, USA)

Developing a Complex Environment to Evaluate the Impact of Cyber Actions On Operations
Presenter maj Baretto (GMU, Bra AF), participation thru Skype

1645-1700 Wrap-Up (Chairs)

5.0 ATTENDANCE

The workshop had good attendance from representatives of the armed forces, cyber taskgroups, research organisations and industry. The appendix provides a detailed overview of participants and their affiliations. Total number of participants was around 35. Initial registrations were even higher, but economic circumstances (US sequestration) and scheduling conflicts had some impact. In addition, several people indicated their interest in the topic and requested information and access to the presentation slides.

Several workshop participants also indicated their interest in becoming a full member of the MSG117 task group and appropriate actions have been taken post workshop.

Figure T-1: Opening Address (Mr. Huiskamp).

Figure T-2: Discussion Session (Mr. Patel).

Two presenters could not participate in person and used Skype to address the audience. This worked well, but prevented them from attending the other presentations and engaging in the discussions.

6.0 SUMMARY

The full presentations are available on the NMSG sharepoint website (see appendix) and will be accessible to all registered participants.

6.1.1 NMSG Briefing, Wim Huiskamp, co-chair MSG-121 (TNO, NLD & NMSG)

Modelling and Simulation is increasingly important for supporting current and future operations of NATO. The Mission of the NATO Modelling and Simulation (M&S) Group (NMSG) is to promote co-operation among Alliance bodies, NATO Member Nations and Partner Nations to maximise the effective utilisation of M&S. Primary mission areas include M&S standardisation, education, and associated science and technology. The NMSG provides M&S expertise in support of the tasks and projects within the NATO Science and Technology Organisation and from other NATO organisations.

S&T cooperation and M&S Standardisation activities are fundamental to exploit NATOs M&S potential. The NMSG was designated as "Delegated Tasking Authority" for NATO M&S standardization in 2003 and therefore also works in close cooperation with SISO (Simulation Interoperability Standards Organization), which is underpinned by a formal technical cooperation agreement (signed in 2007).

6.1.2 MSG-117 Exploiting Modelling and Simulation to Support Cyber Defence Briefing, Stella Croom-Johnson, co-chair MSG-117 (Dstl, GBR) Marieke Klaver, co-chair MSG-117 (TNO, NLD)

The rapidly evolving environment of Cyber threats against the Alliance has necessitated a renewed focus on the development of Cyber Defence policy and capabilities (*NATO 2020: New strategic Concept for NATO*).

Modelling and Simulation experience in research, analysis and training should be leveraged to assist in Cyber Defence capability. The NATO Modelling and Simulation Group (NMSG) has initiated task group

(TG) MSG-117 to investigate how M&S can be used in support of the Cyber Defence development effort. This multi-national TG chaired by GBR and NLD has started its activity in late 2012. MSG-117 main objectives are:

- To investigate and recommend what aspects of Cyber Defence can be supported with Modelling and Simulation.
- Activity will focus on Education, Training, Exercise, Evaluation, Concept and CONOPS Development and their validation, Cyber Threat Assessment, enhancing cyber defence capabilities and technical solutions.

The MSG-117 approach has been to select ten topics of interest:

1. Concept of operations (CONOPS) conceptual models of Cyber Defence;
2. CIS threat assessment and effect, Vulnerability assessment, and Dynamic risk assessment ;
3. Modelling decision support system including Course Of Action analysis;
4. Cyber CAX and training programs, after action review and metrics for training effectiveness;
5. Cyber awareness education;
6. Cyber Defence validation;
7. Critical dependencies of national CIS;
8. Common set of definitions for Cyber Defence M&S exploitation;
9. Full chain of events of cyber attacks;
10. M&S environments, synthetic environments, standards, processes.

The task list was down-selected to 5 for immediate attention (3, 4, 5, 8 & 10). Each task is ‘owned’ by 2 nations (M&S, Cyber experts). The objective is to gain insight in National Training Needs Analysis and obtain relevant documents identified in TG meetings.

6.1.3 NATO Brief ACT C4ISR
Corinne Lonchampt (ACT C4ISR, FRA)

NATO relies on its CIS capability. Cyber attacks are therefore a serious concern. ACTs involvement in Cyber defence is significant and is part of supporting the implementation of Capability Package (CP) 0A0155 projects (including future increments of NCIRC FOC). ACT is also working on developing a roadmap for future NATO’s IA/Cyber Defence Capabilities beyond NCIRC FOC implementation.

The Cyber Defence Action Plan includes 22 items:

1. NCIRC FOC
2. Centralized Cyber Protection
3. Strong Authentication
4. **Education, Training and Exercise**
5. **Lessons Learned**
6. CD Counter Intelligence
7. Enhance Disciplinary Procedures
8. Streamline CD Acquisition

9. **Assessment of CD Measures**
10. Update NATO Documents
11. **Methodology for critical dependencies on National CIS**
12. Develop CD MMR
13. CD in NDPP Targets
14. **Burden Sharing Concept**
15. Cyber Threat Assessment
16. **Cyber Defence CoE PoW**
17. **Cyber Defence Definitions**
18. CD Cooperation with EU
19. CD Contact with other IOs
20. Roadmap for Partner Interaction
21. Identify Key CD Industries
22. Cooperation with Academia

ACT is Lead NATO Body for 7 (in bold) of the 22 Cyber Defence Action Items. The action plan is at revision 11 within 2.5 years. This shows how fast developments are.

NATO is currently focusing on defensive and technical cyber issues, the presenter discusses the Transformational Questions that ACT is concerned with:

- Should NATO consider cyberspace in a broader operational context?
- Should NATO recognize Cyber as the 5th operational domain?
- Should NATO have a policy, coordinating and/or planning role in cyberspace operations?

Examples are given of nations (e.g. NLD) that have declared in their cyber defence strategy “The digital domain or cyberspace is the fifth domain for military operations, along with air, sea, land and space”.

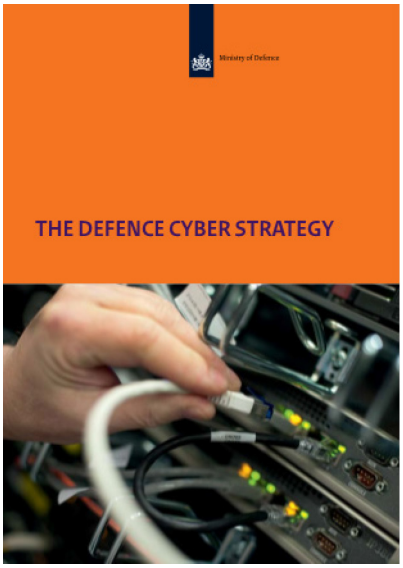


Figure T-3: The Dutch Defence Cyber Strategy Document.

The Legal perspective on existing international law applicable to cyber warfare also deserves more attention. The 'Tallinn Manual'' addresses cyberspace in the context of armed conflicts and the nation's right to self-defence. NATO article 5 is considered to apply to cyber attacks also. The Tallinn Manual is not an official document (although the press often sees it that way), but instead an expression of opinions of a group of independent experts acting solely in their personal capacity. It does not represent the views of the CCD CoE, the Sponsoring Nations, or NATO. It is also not meant to reflect NATO doctrine.

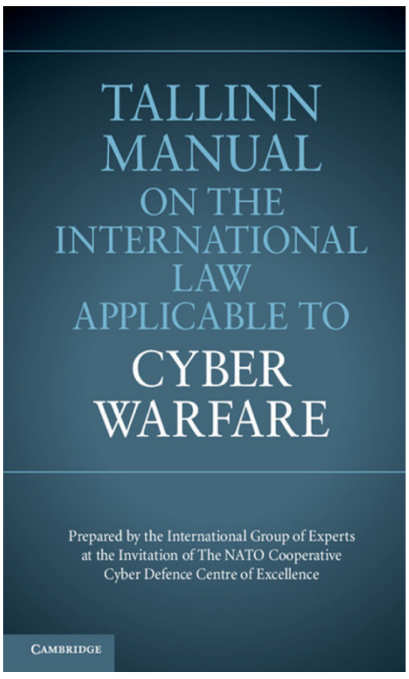


Figure T-4: Tallinn Manual.

Question: Should NATO also address offensive means of cyber warfare?

Reply: we should, but it is a political decision.

Question: Where may M&S be used?

Reply: Training and CD&E seems to be most promising area. ACT is very interested in results from this workshop and MSG117 to gain more knowledge on the potential of M&S for cyber defence.

6.1.4 NLD MoD Cyber Policy & Timeline
Bert Boltjes (TNO, NLD), Ad van Lier (NLD MoD)

The (Dutch) Cyber Defense Strategy (see above) defines the direction, coherence, and focus on the integrated approach and the development of military capability in the Cyber domain. The strategy is an essential element for the future effectiveness and relevance of our armed forces. (Quote J.S.J. Hillen, Minister of Defence NLD, June 2012).

The objective of the Dutch MoD is to ‘’Establish an Operational Cyber capability to predict, influence or obstruct the actions of opponents and to protect against similar operations conducted by opponents” This capability is provide by the Cyber Taskforce (CTF). The CTF Timeline:

- Start 1-1-2012, Total investment of 50M€ over 4 years;
- Establishment of the “Taskforce Cyber” beginning of 2012;
- Defence Cyber Command, operational in 2015;
- Defence Cyber Expertise Centre, operational in 2014.

Some examples of the current activities include a Cyber Awareness Training e-learning application….

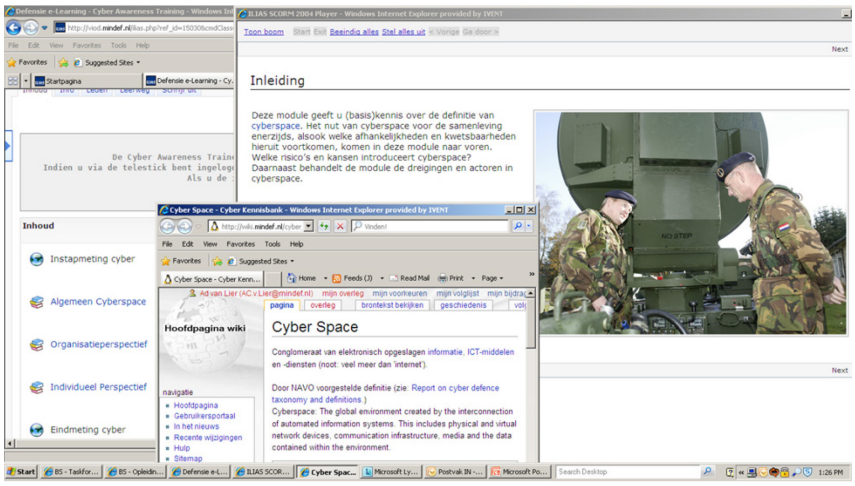


Figure T-5: Cyber Awareness WIKI Page.

….and development of scenarios that are used in cyber training to develop team skills.

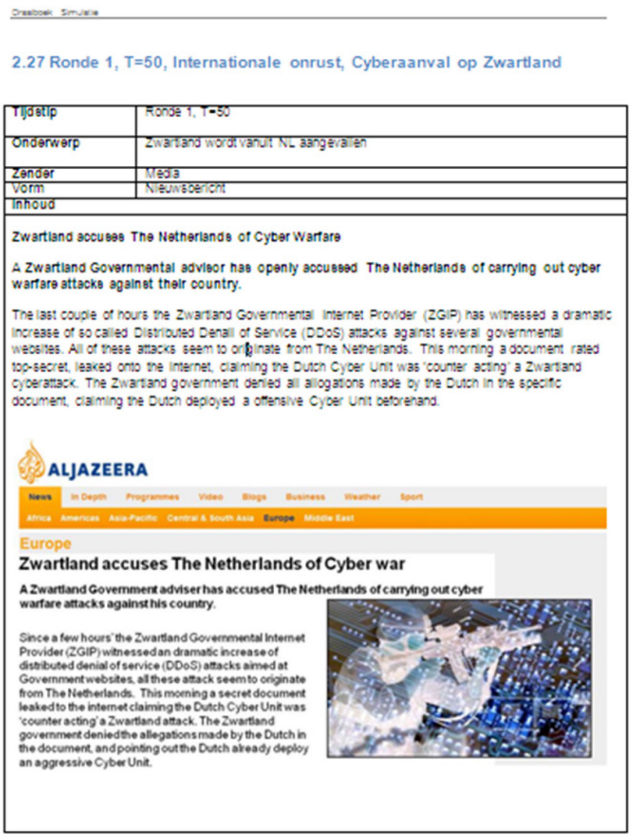


Figure T-6: Cyber Event scenario for Team Training.

The CTF is also interested in M&S environments to support training and experimentation. This is the background for the NLD involvement with MSG-117: Cyber ranges can act as simulators…(emulating, replicating virtualizing, stimulating, visualizing). M&S environments can act as tools for cyber scenarios, e.g. What if…?, consequences of actions (not) taken.

The Cyberlab will be developed incrementally, using a mix of commercial tools and proprietary developments.

6.1.5 M&S Support for Cyber Defence
Bert Boltjes (TNO, NLD)

TNO has a strong Modelling, Simulation and Gaming capability which is used to support the Ministry of Defence in many domains, including Concept Development and Experimentation (CD&E). The Cyber Security R&D is provided in support of: Ministry of Defence, Ministry of Security and Justice, NATO. M&S is seen as important tool to support Cyber security R&D.

Defence-related R&D on information security is mainly focused on

- Knowledge applied to 'high profile' and complex organisations
- Information assurance studies in support of MoD
- Critical Infrastructure Protection
- Vulnerability studies (e.g. ''The Hague Safe Haven'' project)

Figure T-7: Strategies.

Project Example: Awareness trainer for Cyber – MoD.

A demonstrator that will help raising the awareness level of the higher-ranked military personnel on Cyber. The trainer consists of a WIKI running on the MoD's network with hundreds of annotated relevant Cyber documents, e-learning package on the MoD's network and a scenario packed with multimedia injects to train decision makers in a table-top simulation game.

Figure T-8: Cyber Awareness Trainer.

Current R&D is performed into Integration of Cyber effects in training simulations. Focus is on integrating possible effects of cyber on operations:

- Reduced availability
- Loss of integrity
- Loss of information

Detailed network simulation tools (e.g. OPNET Modeller) are available. This does however involve a significant modeling effort and often the environment becomes quickly outdated by new types of attack. The

focus is more and more on effects of cyber and possible countermeasures rather than on detailed modeling of a specific threat. Work in progress:

- Vulnerability Situational Awareness Tools
- Critical Infrastructure Protection Gaming
- Merging Information from real and simulated systems
- Lessons learned integration
- Playing "What-if" Scenarios

Figure T-9: What-If Games.

TNO applies techniques and interactive tools (touch table) for conceptual modelling of complex systems for the cyber domain. This leads to better understanding between stakeholders and supports development of valid simulation systems.

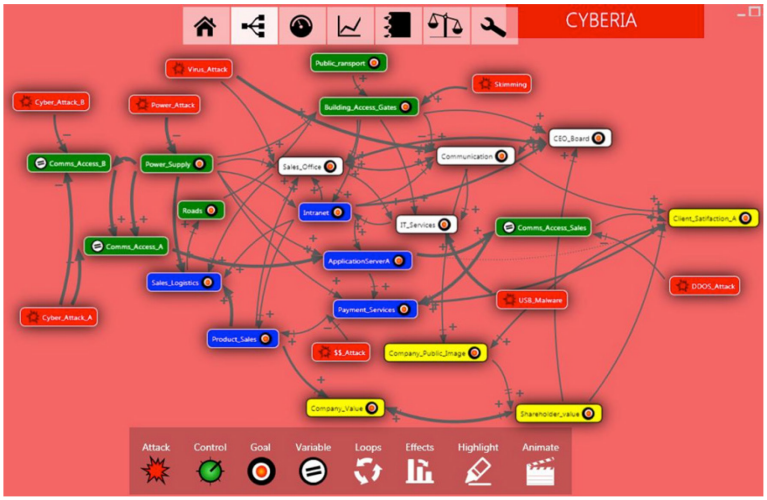
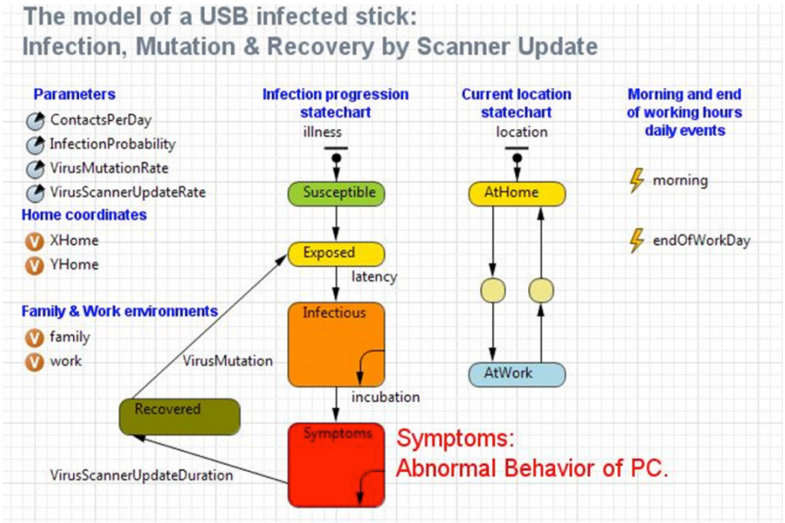


Figure T-10: Interactive System Dynamics Modelling of Cyber effects: identify stakeholders and their interactions.

An example is shown of a simulation that models how viruses spread through infected USB-sticks used at home and at work. The effectiveness of anti-virus software is demonstrated.



6.1.6 National Cyber Defence M&S Activities and Initiatives DEU Test infrastructure of the Military Test Center Walter Hader (Military Test Center, Greding, DEU)

The Bundeswehr Technical Center for Information Technology and Electronics (ca 280 FTE) was established in 1961. The IT security section is responsible for evaluations, analysis of attacks against IT infrastructure, crypto devices and cyber defence in general. The DEU CERT is also part of the IT center. The center maintains and uses a test lab for vulnerability assessments (eg Intrusion Detection Systems IDS). This lab has tools to generate network traffic, simulate networks and systems and analyze effects of attacks and countermeasures. The lab performs simulated tests and live tests. The test hardware can generate > 2 million types of attack. The center is only engaged in defence and not in offence.

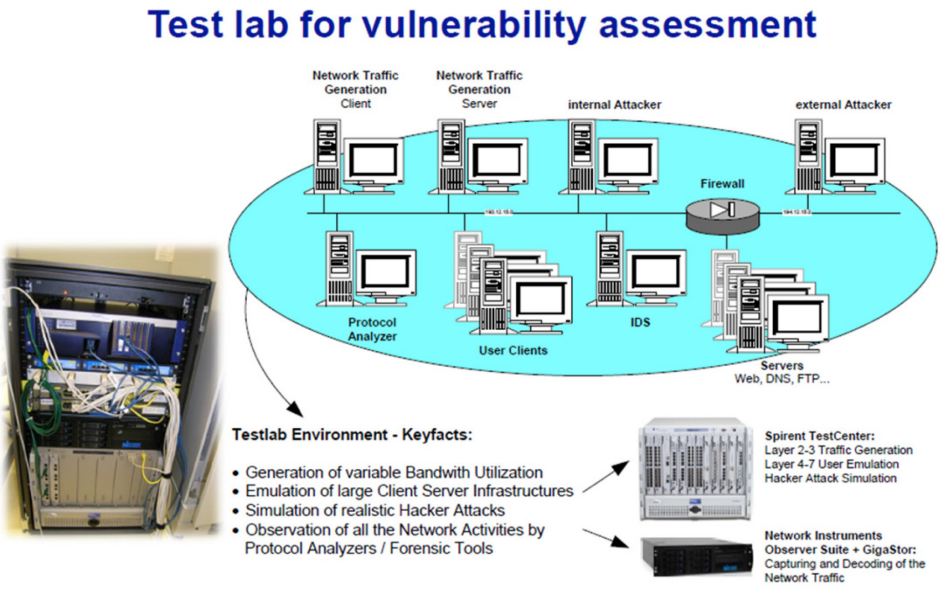


Figure T-11: German Bundeswehr Testlab in Greding.

A new lab provides ca 80 systems in cubicles that can be used for simulated experiments. This may include simulations (e.g. VBS2), some of which may be remotely linked (e.g. Tornado fighter simulator, Cassidian).

Hardware in the loop can be included using outdoor or indoor container systems. Outdoor training range is about 100 Ha and suitable for heavy military vehicles.

External network connections include internet, NATO CFBLnet and Bundeswehr WAN.

Question: What is your biggest challenge?

Reply: human factor, we can't model that

Reply: military network is not like enterprise networks and it is layered.

Reply: military networks rely more and more on civilian critical infra and chain effect of attacks will impact military ops also

Discussion Topic 1: How might M&S support Cyber Awareness Training and Education?
Chair and Intro: Maj. Mark Young (Canadian Nat. Def.), Maj. Scott Roach (Canadian Nat. Def.)

Cyber has never been an issue so far in military process, but this will change. In future there will be a cyber officer in the staff (J3 Cyber). Cyber awareness training is a significant challenge for the Canadian Armed Forces (CAF) since it is considered relevant for all staff (64K and 15K reserve). The CAF is in the process of investigating how M&S can be used for cyber awareness (interactive courseware, training at home, in barracks). The presenters discussed the CAF initiatives and experiences on cyber training:

- Defence Network wide education CBT on Security and Cyber related issues. Planned roll-out is summer 2013. Ultimately access should be Linked to user accounts.
- Also in preparation is a Cyber Officers Course (pilot Apr/May 13).

- CDS Cyber CCIR's (2011)
- Experiments and Exercises

Generation of Policy & Doctrine is a result of participation in current exercises/experiments for future employment. Examples:

- MNE Campaign (NATO / US J7)
- Cyber SA experiment run Oct 2012 (GBR)
- MCDC (2013 - 2015)
  - Cyber Focus areas
    - Norway - Operational (Operational Planning and the Cyber Domain)
    - Italy - Technical (Cyber Capabilities and Data Analysis)
- Cyber Coalition 13
- Cyber Flag14
- CAGE (Coalition Attack Guidance Experiment) support the employment of a J3 Cyber
- JOINTEX (support the development of simulation requirements for Cyber awareness both OCD/DCO). JOINTEX4 was constructive, JOINTEX5 will include Live elements.

CAF uses different M&S Tools to Support Cyber Awareness training and experimentation:

- Programming
- Engineering Models (Physics Engines)
- Classroom (E Learning)
- Interactive Courseware (CBT, WBT)
- Hardware / Software
- Cyber Range

The CAF Synthetic Environment Coordination Office (SECO) support to Cyber Task Force consists of:

- Training Needs Analysis (TNA) (Cyber TF)
- Assist in the development of the Cyber awareness training requirements
- Capability Gap Analysis
- Business Case to Satisfy the Capability Gap (if required)
- Develop a TAP (Technical Acquisition Program)
- Acquisition Strategy (assessment metrics, standards through life support, etc etc)

Presentation Cyber Awareness Challenge – Michelle Brauer (Team Carney USA)

Games developed for the Defense Information Systems Agency (DISA). Access a video preview at www.teamcarney.com/samples.

Cyber Awareness Challenge is a serious game that simulates the decisions Federal and DoD government information systems' users make every day as they perform their work. It presents instructional topics through first-person simulations and mini-games that allow the player to practice and review concepts in an interactive manner. Audience includes civilian and military employees and contractors both within the U.S. and deployed overseas, and members of the Intelligence Community.

The goals included

- Satisfy Government's annual information assurance awareness compliance training mandate in a new and different way
- Target audience is used to taking the same type of training every year
- Reach a large target audience
- All authorized users of DoD and Federal information systems (3 million+ users)
- Must be Section 508-compliant

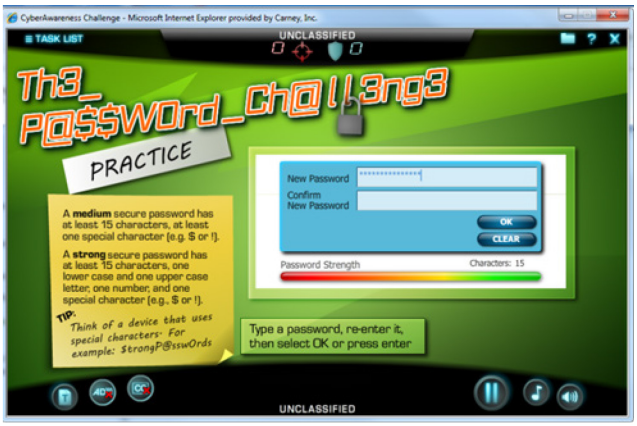


Figure T-12: Keep your password safe...

Figure T-13: Cyber Awareness Game.

The game was introduced recently and it is too early to evaluate results with target audience. However, the application was selected as a finalist in the 2012 I/ITSEC Serious Games Showcase and Challenge and is the winner of Federal Information Systems Security Educator's Association (FISSEA) 2012 award for Best Role-Based Training.

Question: What is 'awareness'?

Reply: ranges from 'no USB stick' to 'something looks wrong on my screen'. It means different things to different people and has many aspects/levels. Awareness helps you to understand what you should do next. Be aware on what you do/say on the phone/Facebook to avoid data mining/social engineering.

Comment: The game is not telling you why your answer is right/wrong. That would help you to recognize and respond correctly in other similar circumstances.

Comment: The game will have a maintenance issue to stay up to date.

Comment: The game answers should not be known/exchanged between students.

Comment: The game is 'canned', could be linked with interactive models.

M&S can show you consequences of your actions/decisions. Faster than real-time if needed (e.g. virus spread on infected USBs and virus detection software countermeasures.)

Discussion Topic 2: How might M&S support Cyber training and exercises?
Chair and Intro: Frank Jonat (Cassidian), Christian Wolf (DEU MoD)

Main issues are:

- The increasing complexity of cyber threats is facing the military community.
- At the same time resources are more and more limited, hence there is an urgent need to increase efficiency and effectiveness of staff.
- The military community needs both well trained specialists in cyber defence and an increase of cyber awareness of "non cyber" staff in general.

Challenges:

- Cyber Training should range from cyber defence activities at technical levels up to operational and tactical levels.
- A Test Bed or Cyber Range should be used to run exercises in an environment that does not connect to the real tactical networks. However:
  - the simulated Internet/Intranet/Extranet should be as life like as possible
  - the trainee should not be able to tell real from simulated environment (immersion).

M&S provides many advantages to support successful exercises:

- Defined scenarios create repeatable exercises.
- Repeatable exercises make results/teams comparable. Repeat to see improvements.
- Using Hardware-in-the-loop enables trainees to have a life-like experience
- Using man-in-the-loop will enhance this life-like experience.

Question: Should we simulate all levels at same time (IT people, network operators, sys admin, commanders)?

Reply: general consensus is that you need to select/decide on the level at which your training is aimed and simulate the levels above and level below your target training audience.

Discussion: we can simulate HW, but we cannot simulate man in the loop.

Discussion: we use operational C2 systems in training. Can we use the hardware that vendors use to test their C2 systems? The issue is that HWIL is not scalable. Some HW (e.g. radar) is not easy to emulate.

Discussion Topic 3: **Cyber Situational Awareness, how might M&S support threat and risk assessment?**
Chair and Intro: Bharat Patel (DSTL, UK MOD)

Failsafe systems are too expensive, locked-down systems are not acceptable. We need to understand the threats and asses impact. Regarding risk assessment we first need to identify the assets, the threats and the impact. M&S could help in many ways, for example run numerous 'user profiles' (and 'hacker profiles') against a network and find 'notional threats'.

What should be the scope for Defence and Security? We need to select/decide:

- The types of IS and networks
  - National critical Infrastructures
  - NATO operations infrastructure
  - Dynamic operational networks to deploy NEC, ISTAR systems, platforms and sub-systems
  - Reach-back to more permanent enterprise networks
    - Intranet
    - Internet
    - Specialist
- The types of threats
  - Directed
  - Disruptive
  - Opportune
- The sources of threats
  - Nation
  - Group
  - Individual

Why M&S?

- Can M&S assess the likely impact of threats on
  - Planned Campaign or Missions
  - Information systems
  - Networks

- Can M&S assess the risks in network design to lead to
  - Better revised designs
  - Failsafe measures
  - Detection measures
  - Protection measures
  - Decision aids in operations
- Can M&S assess unknown threats

How can M&S be used?

- Should Cyber be assessed as a separate entity?
- Is it mostly Constructive simulation or analysis?
- What would Virtual or Live simulations add?
- What level of abstraction would be acceptable?
- How do we represent human aspects?
- How do we model or represent the various threats?
- Do we model Hackers?
- Do we need to model threat networks?
- What are the metrics for threat or risk assessment?
- Completeness of representation
- V&V

Discussion: we need metrics for cyber training transfer

Discussion: we don't need to model the hacker, but we should model the hacker methods

Discussion: we should not use M&S as separate tool against cyber, but use it as integral aspect of defence. Canada considers cyber as integral part of planning process.

Comment: to improve awareness operators should switch between red and blue side

Question: Should the cyber domain be assessed as a separate entity?

Discussion: US Marines consider cyber offensive as EW

Discussion: we differentiate Air and Navy because they deal with different domains, different weapons etc. Same principle applies to cyber.

Discussion Topic 4: **What type of M&S environments are needed to support cyber defence?**
Chair and Intro: Wim Huiskamp

Presentation Cyber-Specific Definitions of Live-Virtual-Constructive – Katherine L. Morse, David L. Drake (JHU/APL).

Background:

- JHU/APL is performing a task for Army OTC to identify LVC enablers and gaps for representing cyber (attacks and effects) in Army operational test events.
- Accurately identifying what is an LVC enabler or gap requires defining what representations of cyber are L, V, and/or C.
- The proposed definitions are offered for discussion and feedback.

Proposed Definitions:

Live: actual real-world assets operating on/with real-world systems; vulnerable and reachable to attacks, exploits, and performance degradation from the physical and/or simulated domains.

Examples:

- Packet, protocol, or frequency level attack and response
- Real operators, real network devices, real machines, real non-emulated/simulated software

Virtual: High fidelity representations of real-world assets where ease of (re)configuration, replication, restoration and physical limitations make a virtual asset preferred over the live one. There is no physical representation of the real-world system and thus only provides a cyber "attack surface."

Examples:

- Actual live attack on a virtual machine, which is then propagated to systems under test
- Replay of a logged actual live attack onto the live or virtual systems

Constructive: Parameterized simulated or emulated assets operating on/with simulated systems, but not vulnerable to direct live or virtual exploits and manipulation; characterized by large-scale global/enterprise-level network and effects representations.

Examples:

- Internet-scale traffic generation, background noise and high-volume gray-space
- Virus infection & worm propagation simulations

Operational tests should include cyber effects since it happens in real-life. Question is how to represent cyber across LVC in a consistent way.

Presentation Developing a Complex Environment to Evaluate the Impact of Cyber Actions On Operations - Major Alexandre de Barros Barreto, Visiting Researcher Center of Excellence in C4I, George Mason University, Instituto Technologico de Aeronautica (ITA) Brasil.

The presenter works with the ITA/GMU C2 Collaborative Research Test bed, which is a set of Commercial Off-the-Shelf (COTS) tools that provides a realistic and complex simulation environment to conduct C2 research experiments. This environment also provides network simulation using the Exata toolsuite.

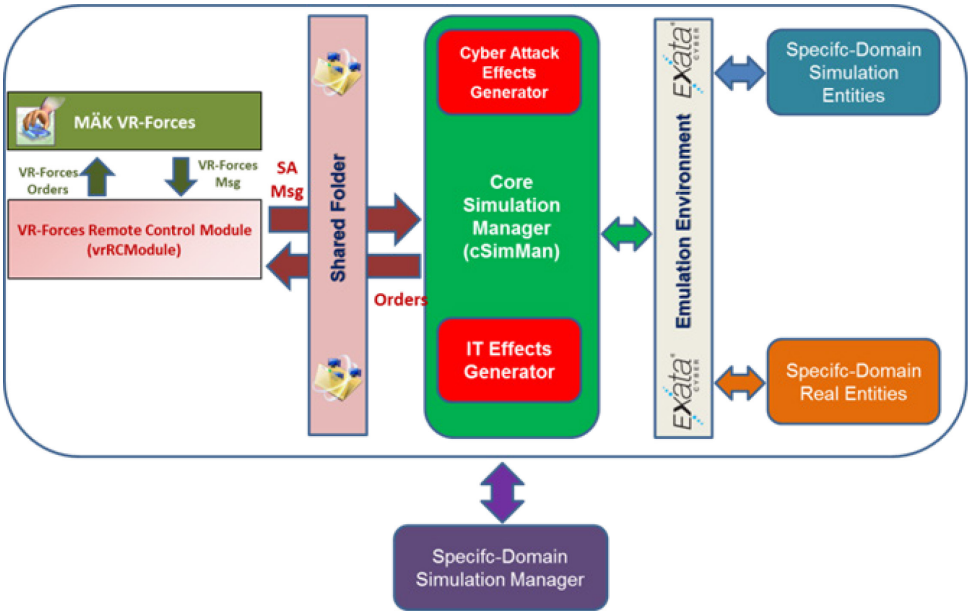
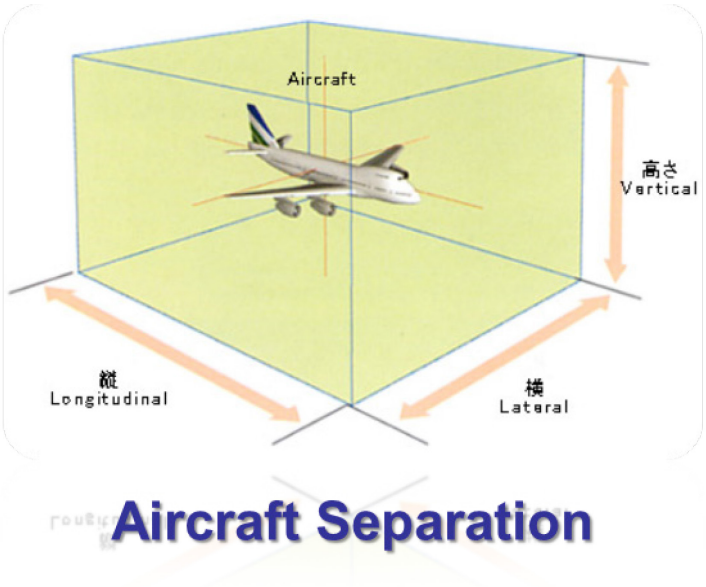


Figure T-14: C2 Collaborative Research Testbed,

The described research concerns the domain of air traffic control. This is a complex, technology dependent application area where cyber attacks can have potential high impact. Safety needs to be guaranteed under all circumstances.



The scenario models Air Traffic Control operations in the Campos Basin. The Campos Basin is a petroleum rich area located in the Rio de Janeiro state (80% of Brazil's petroleum production). Oil development operations include heavy helicopter traffic between the continent and oceanic fields during daytime, with an average of 50 minutes per flight.

The goal of the experiment is to simulate the effect of multiple cyber-attacks and failures on Campos Basin operation, and to understand the impact these attacks and fails might have on the security and safety of air transportation operation. The scenario investigates situations that may arise in attacks during upcoming events like the Brazil Soccer World Cup or Olympics.

Conclusions so far indicate:

- Cyber-Argus Framework presents an approach for connecting the cyber and physical domains, with the objective of assessing the impact that actions in the former have in the latter.
- The Cyber-Argus's Philosophy defines the impact through the understanding of mission requirements and tasks. It uses the knowledge of the enemy, but it doesn't need to be complete.
- The Cyber-Argus impact assessment provides local and global indexes that enable the Analyst to understand which node is more resilient in a specific slot-time.
- This is research in progress in an area where clear answers are usually not attainable, mostly due to the complexity as well as to the level of subjectivity involved in real time impact assessment.

Discussion: Cyber is a new domain next to sea, air, land.

7.0 CONCLUSIONS & RECOMMENDATIONS

The presentations and discussions were very useful, and good examples were presented of M&S in support of cyber defence.

The workshop achieved exchange of NATO and national strategic approaches to cyber Defence. It exchanged current approaches within nations to address cyber defence scenarios, with insight into current examples of M&S developments in support of cyber defence.

The workshop addressed key questions in strategic scope of cyber defence, the role of training and education, and the need for assessment methods to understand the cyber threats and risks.

It also increased the awareness amongst the simulation community of the NATO and national initiatives in cyber defence, and encouraged new members to join the MSG117 Task Group

It is recommended that the output of this workshop be used by the MSG-117 task group as input for their work, and be presented at the next NMSG annual conference.

It is also recommended that SISO should look at cyber related issues relating to simulation interoperability issues relating cyber (definitions, data models, security in distributed simulations etc.,)

8.0 ACKNOWLEDGEMENT

The MSG-121 co-Chairs (Mr Bharat PATEL and Mr Wim HUISKAMP) express their thanks to all presenters and participants for their valuable contribution to the success of the event.