Program práce CCD COE na rok 2016

Seminár „Spolupráca s CCD COE“

8. marca 2016

pplk. Ing. Zdeněk HORÁK

PREZENTÁCIA JE NEUTAJOVANÁ

Obsah

- Cieľ
- *Oblasť záujmu 1 Právo a politika*
- *Oblasť záujmu 2 Stratégia*
- *Oblasť záujmu 3 Technológie*
- *Oblasť záujmu 4 Vzdelávanie a cvičenia*
- *Oblasť záujmu 5 CyCon*
- Zhrnutie
- Kontaktné údaje

Cieľ

- Poskytnúť ucelenú informáciu o oblastiach záujmu a o projektoch, ktorými sa zaoberá CCD COE v roku 2016
- Podnietiť predstavivosť pri tvorbe požiadaviek na projekty v roku 2017

1. Právo a politika

- Oblasť práce – Podpora pre NATO a členské krajiny NATO v oblasti práva a politík
- Oblasť práce – Výskum práva a politík
- Oblasť práce – Tvorba Tallinn Manual

1. Právo a politika

- *Oblasť práce – Podpora pre NATO a členské krajiny NATO v oblasti práva a politík*
- Oblasť práce – Výskum práva a politík
- Oblasť práce – Tvorba Tallinn Manual

No / Name	16-01-01-A: **Support to Defence Policy Planning**
Short Description	The ongoing DPP process is using indicators on whether and how NATO Allies have implemented national level policy mechanisms (consistent with NATO Policy) for cyber defence. Such mechanisms might include the presence of a National Cyber Security Strategy, the establishment of a national and military CERT and participation in exercises.
Aim	The project will consider whether a 'one size fits all' approach is beneficial, or whether a more finely grained model (based on characteristics of a country) would be more relevant. The project will also look into the implementation possibilities of the Responsive Cyber Defence mechanisms into the NATO CD Policy.
Customer	NATO HQ ESCD
Products / Deliverables	Policy analysis
Schedule	The project has started in 2015 with the first phase deadline in Sept 2015; the second phase in April 2016 and the third phase in Sept 2016 (Summit)
Challenges / Problems / Risks	N/A
Mitigation	N/A

No / Name	16-01-01-B: **Cyber Domain Preparatory Workshop (SMPC 16)**
Short Description	There is a need for greater collaboration between the Alliance and Partners for mutual benefit specifically within the cyber domain and for awareness rising activities, e.g. to undertake a workshop with stakeholders from ACT (SPP, JFT, JETE and MPD), the COEs and the Partner community.
Aim	Develop options for practical co-operation between the Alliance and its partners (within extant partnership frameworks) to enhance cyber domain inter-operability.
Customer	NATO ACT SPP SIE
Products / Deliverables	Practical support and subject matter expertise in cyber domain (experts from L&P and Strat) to facilitate the planning and execution of a domain based workshop in March 2016 in the Hague.
Schedule	March 2016
Challenges / Problems / Risks	N/A
Mitigation	N/A

No / Name	16-01-01-C: **International Cyber Norms Development**
Short Description	In the past five years, international dialogue on cyber norms has intensified, culminating with the understanding by the UN GGE 2012/2013 and UN GGE 2014/2015 that international law, in particular the United Nations Charter, is applicable to activities in cyberspace. However, the international community is still far from universal consensus on the rights and duties of states in cyberspace.
Aim	The project will improve the general knowledge of NATO and its Allies' decision-makers on norm development in cyber space and give guidance for possible cooperation in order to address the lack of normative expertise in the field of cyber security and promote the discussions for resolving international cyber security issues.
Customer	EST
Products / Deliverables	- Workshop on the development of international cyber norms; - Support to national delegations dealing with the UN GGE process
Schedule	- Workshop during the CyCon - Support and consultations throughout the 2016
Challenges / Problems / Risks	N/A
Mitigation	N/A

No / Name	16-01-01-D: **Global Compendium of Cyber Incidents**
Short Description	The number of reported cyber incidents continues to climb, and its use as a tool of political coercion and as a potential compliment to kinetic war fighting operations is evident. The Global Compendium of Cyber Incidents would detail as much as is known about the use of cyber tools and techniques employed as well as background to the incidents and potential legal considerations.
Aim	Build a compendium that can be used for research and as a basis for discussion on the employment, effect and consequences of Cyber incidents. The target audience is nations and officials who have the need for a baseline of evidence to allow discussions to focus on the key events as presented by cyber experts.
Customer	GBR
Products / Deliverables	A collection of case-studies
Schedule	end of 2016
Challenges / Problems / Risks	N/A
Mitigation	N/A

No / Name	16-01-01-E: **International Cyber Developments Review (INCYDER)**
Short Description	A web-based interface which serves as a research tool and focuses on the legal and policy documents adopted by international organisations active in cyber security. The collection of documents is periodically updated and supported by a comprehensive system of tags that enable filtering the content by specific sub-domains. INCYDER also features descriptions and news about these selected organisations.
Aim	Improve knowledge and understanding of 16 international organisations' activities in the area of cyber security and cyber defence in order to support policy development and research.
Customer	NATO, SNs, CPs
Products / Deliverables	Updated reports on webpage https://ccdcoe.org/incyder.html - Updated organisation descriptions, document collection, news items
Schedule	Continuous
Challenges / Problems / Risks	N/A
Mitigation	N/A

No / Name	16-01-01-F: **Enforcing Governmental Guidelines in Crises Situations**
Short Description	A study on the legal possibilities for governmental agencies in charge of cyber security in different countries to issue and enforce mandatory guidelines both inside the governmental sector (to other agencies) and to organisations and persons in private and third sector (e.g. data communications companies, providers of vital services etc.) in order to maintain the secure operation of the cyber domain as a whole.
Aim	A full understanding of possible enforcement measures of governmental guidelines and existence of co-operation agreements across NATO nations to mitigate serious threats concerning cyber security in crisis situations.
Customer	EST
Products / Deliverables	Research paper focusing on the availability of enforcement measures in mitigating serious threats arising during crises situations concerning national cyber security.
Schedule	March 2016
Challenges / Problems / Risks	The project is a continuation of the 2015 work item. Experienced low interest in completing the survey questionnaire in SNs. In 2015 ITA, EST, ESP, CZE, FRA were covered.
Mitigation	

1. Právo a politika

- *Oblasť práce – Podpora pre NATO a členské krajiny NATO v oblasti práva a politík*
- *Oblasť práce – Výskum práva a politík*
- Oblasť práce – Tvorba Tallinn Manual

No / Name	16-01-02-A: **Tallinn Papers series**
Short Description	A "small paper" series consisting of periodic publications on the topical legal, policy and strategic issues of cyber security and cyber defence. The publications will promote high-level thinking on cutting-edge issues in cyber security and defence in Allies and beyond; will be an opportunity for in-house experts to share their thoughts and publish them in a respected forum; publications will also be sought from internationally recognized thinkers.
Aim	The series was established in 2014 and current work item is a continuation of this proven concept. The success of the Tallinn Papers is based on the short and non-academic format which makes the articles easy to read and follow.
Customer	NATO, SNs, CPs
Products / Deliverables	Series of up to 6 small articles
Schedule	Continuous
Challenges / Problems / Risks	Willingness of external authors to contribute
Mitigation	N/A

No / Name	16-01-02-B: **Removing security-threatening online content**
Short Description	Different international and regional agreements were written to ensure that people can speak and write freely about their views through the use of the media by his/her choice. In times when certain groups use the internet to organise riots, promote terrorism or recruit new group members by posting essays/videos/comments calling for violence motivated for example by religious beliefs or radical political views, questions arise whether limits have to be set for the freedom of expression in cyberspace.
Aim	The project aims to shed light on the diverse national ways of dealing with security-threatening online content and at what point does the removal weigh more than the exercise of free speech.
Customer	NATO, SNs, CPs
Products / Deliverables	Study on combatting security-threatening online content
Schedule	June 2016
Challenges / Problems / Risks	N/A
Mitigation	N/A

No / Name	16-01-02-C: **National Cyber Security Resources update**
Short Description	Combining the activities within the Cyber Security Strategies update and National Cyber Security Management Structures in NATO Nations, the project will monitor and inform about: 1) Developments regarding national CS strategies, with a focus on NATO Nations and Partners; 2) National cyber security organisational models in NATO countries, maintaining and updating the web-accessible 'knowledge base'.
Aim	Supporting national cyber security strategy research at the Centre and by the Centre's customers by offering easy, one-stop access to national cyber security policy and legal documents; contributing to awareness among NATO Allies about cyber security management in the varied national settings.
Customer	NATO, SNs, CPs
Products / Deliverables	NCSS inventory; NCS organisations review; update notices
Schedule	Quarterly updates
Challenges / Problems / Risks	N/A
Mitigation	N/A

No / Name	16-01-02-D: **Cyber Defence Cooperation of NATO Nations with the Industry/Private Sector**
Short Description	The study would map the current benchmark of NATO Nations' (SNs) defence organisations cooperating with the industry. It should identify the areas where cooperation is offering most value for national cyber defence capabilities, the perceived gaps in this domain, and best national practices. Analysis should be based on collecting information from military CERTs.
Aim	Understanding the current state of play and the dynamics in this area will provide food for thought for nations and NATO about how NATO can provide added value in facilitating international cyber cooperation and assistance among nations. The project can potentially support the development of NATO Industry Cyber Partnership programme by offering insight of the national expectations and gaps.
Customer	NATO, SNs, CPs
Products / Deliverables	Analysis paper (unclassified) based on data collected by means of a survey
Schedule	Nov 2016
Challenges / Problems / Risks	N/A
Mitigation	N/A

No / Name	16-01-02-E: **Small states and international cooperation in cyber defence**
Short Description	Work item 15-01-02-G from POW 2015 as approved by the SC: - Research on the obstacles of States with limited resources in achieving full-scale cyber defence capabilities. What are the policy options for small states to facilitate and promote cooperation?
Aim	Present an overview of the problem surrounding small states and cooperation in cyber defence, provide an analysis of possible policy options which could be used by policymakers of (both big and small) NATO member states.
Customer	NATO, SNs, CPs
Products / Deliverables	Research paper
Schedule	Nov 2016
Challenges / Problems / Risks	The research was suspended in 2015 because of rotations in the branch. Finalisation of the research is suggested for POW 2016.
Mitigation	N/A

1. Právo a politika

- *Oblasť práce – Podpora pre NATO a členské krajiny NATO v oblasti práva a politík*
- *Oblasť práce – Výskum práva a politík*
- *Oblasť práce – Tvorba Tallinn Manual*

No / Name	16-01-03-A: **Tallinn Manual 2.0**
Short Description	Identifying options according to the International Law for States to respond and take action in cyber operations directed against them or against installations on their territory or under their jurisdiction, during the peacetime regime.
Aim	Continuous project (requested by ACT in 2013). While in 2015 the research nearly completes the elaboration of a first draft of the Tallinn Manual 2.0 with a comprehensive presentation of the lawful responses to cyber-operations, further planning and resources are needed for the integration of the commentary from the States Meeting and the Group of International Experts (IGE) recommendations.
Customer	NATO ACT
Products / Deliverables	- Manual of an academic nature mapping states' lawful responses to cyber-operations outside of the context of Armed Attacks - Updated of the original TM
Schedule	Feb 2016 - States meeting in the Hague March 2016 – final IGE meeting April, May 2016 - language editing Nov 2016 – publication, launch and introduction of the complete product
Challenges / Problems / Risks	N/A
Mitigation	N/A

2. Stratégia

- Oblasť práce– Strategické riadenie kybernetického priestoru
- Oblasť práce – Vývoj strategických spôsobilostí

2. Stratégia

- *Oblasť práce– Strategické riadenie kybernetického priestoru*
- Oblasť práce – Vývoj strategických spôsobilostí

No / Name	16-02-01-A: **Cyberspace Operations Doctrine**
Short Description	Part 1: Identify areas or concepts that are applicable to the needs of NATO and in support NATO cyber policy. Project will require a review of national cyberspace doctrine. Part 2: Become custodian for AJP 3.xx series Cyber Operations publication. -Will work with EDX, L&P, TECH
Aim	Part 1: Identify areas or concepts that are applicable to the needs of NATO and in support NATO cyber policy. Part 2: Assist/lead Alliance nations with drafting doctrine
Customer	ACT
Products / Deliverables	1) Part 1: This review would lead to products that would highlight the best practices or main points that seem to be agreed to by Allies for injection into a future NATO Cyber doctrinal publication 2) Part 2: Draft NATO Doctrine for review by NATO bodies 3) Glossary update
Schedule	1) Part 1: May: Draft Report 2) Part 2: A. January-March: Assist in RFF process B. March-October: Doctrine workshops(3) C. December : Initial Draft complete 3) October: Glossary Update
Challenges / Problems / Risks	Part 1: Maybe difficult to find enough published policies. Part 2: will require a re-occurring commitment as custodian Due to staff rotation in STRAT branch this needs support from nations
Mitigation	

No / Name	16-02-01-B: **Impact of Cyber Capabilities on the Application of Power**
Short Description	Concept: To provide insight into the nature of future (military) cyber capabilities and the way in which nations and state sponsored parties will use these capabilities to achieve political objectives on the basis of current debate within academia, military and political circles -The course and workshop match up well with the USA request and the anticipated "Executive Level Cyber Seminar". -Includes support from L&P -Will include NATO request on studying: "Cyber Dimension of Hybrid Warfare"
Aim	Research which gives practical evidence of and advice towards how will nations use cyber capabilities to achieve their strategic objectives
Customer	NLD, USA and NATO ACT
Products / Deliverables	Academic Research paper Workshop and course material
Schedule	1) June: Draft academic research paper 2) November: Workshop 3) November: Final academic research paper
Challenges / Problems / Risks	
Mitigation	

2. Stratégia

- *Oblasť práce– Strategické riadenie kybernetického priestoru*
- *Oblasť práce – Vývoj strategických spôsobilostí*

No / Name	16-02-02-A: **Multinational Capability Development**
Short Description	This is a multinational effort to develop cyberspace operations concepts for NATO. CCD COE would be a part of research and document development.
Aim	NATO CCD COE helps ensure the final MDCO/MCDC deliverables are sound and challenge nations to move forward in the field of cyber defence. This effort will also directly contribute to Cyberspace operations doctrine project 16-02-01-A.
Customer	NATO ACT
Products / Deliverables	Advice, Participation in Working Group.
Schedule	1) January: Writing Workshop 2) April: Wargame FPC 3) May: Wargame 4) August: Concept test and draft non-academic analysis report inputs 5) September: Writing assignments 6) October: Final writing workshop
Challenges / Problems / Risks	
Mitigation	

No / Name	16-02-02-B: **Support to the NDPP (SFA and FFAO)**
Short Description	Review and comment on SFA and FFAO with regards to cyber issues. Support the writing of SFA and FFAO.
Aim	**A) Strategic Foresight Analysis** Ensure the required content in regards to cyber is including the upcoming draft of the SFA **B) Future Framework for Alliance Operations** The Framework for Future Alliance Operations, builds on SFA by identifying military implications that can aid defence planners in identifying long-term military requirements during step two of the NATO Defence Planning Process.
Customer	NATO ACT Strategic Plans and Policy, Strategic Analysis Branch
Products / Deliverables	**A)** 1) Provide comments and proposals on draft SFA documents 2) Participate in workshops to provide expertise for SFA development **B)** 1) Review and commenting on draft document. 2) Participate in 2-3 FFAO workshops, provide analysts report, as needed
Schedule	Since calling letters have not be transmitted, exact workshop dates are unknown
Challenges / Problems / Risks	
Mitigation	

SFA – Strategic Foresight Analysis
FFAO – Framework for Future Alliance Operations

No / Name	16-02-02-C: **New Models for Military Command and Control in Cyber Era**
Short Description	To investigate the key issues that distinguishes commanding cyber forces from traditional military structures. To the extent possible based upon available information, compare different national approaches by Allies to this issue, including strategy, doctrine and technical solutions. Produce a conceptual analysis to cyber command and control. -Material maybe used for doctrinal development -Will work with L&P and TECH
Aim	Describes how Allies should alter their current organizational structures and strategies, policies and doctrine to enable fast and, where possible, automated decision making, including automated responses or hack-backs
Customer	EST
Products / Deliverables	Research paper
Schedule	September: Research paper
Challenges / Problems / Risks	
Mitigation	

3. Technológie

- Oblasť práce – Výskum technológií

No / Name	16-03-01-A: **Firmware Forensics**
Short Description	Software (firmware) running on variety of devices integrated into computer systems (BIOS/UEFI, NIC, SSD/HDD etc) may be vulnerable to local and/or remote attacks, making these devices a great footholds for persistent rootkits and avenues to attack the software running on other parts of that computer. There are methods to diagnose an infection (with timing, EMF measurements etc) and ways to extract the running code from these devices.
Aim	To develop capability to find malicious software running in firmware of systems used by NATO and Allies.
Customer	EST
Products / Deliverables	Study Report
Schedule	Workshop Q4 2016 (Focus on Computer Devices Firmware) Extended Workshop Q2 2017 (Focus Mobile Devices Firmware)
Challenges / Problems / Risks	Completely new field of expertise
Mitigation	

No / Name	16-03-01-B: **Digital Battlefield Forensics**
Short Description	In the form of a study collecting best practices, with the hints of our forensics in-house knowledge and operational insights potentially coming from ACCI and operational units, including NATO Special Operations HQ. The idea is to provide a document addressing the procedures to collect and preserve digital data from the military operations.
Aim	Defining/Consolidating a toolset of best practices related to digital forensics collection in hostile operational environment tailored for different Armed Services.
Customer	ITA
Products / Deliverables	Study Report
Schedule	Q2 2016
Challenges / Problems / Risks	Cooperation with ACCI, NATO Special Operations HQ
Mitigation	

No / Name	16-03-01-C: **Forensics Body of Knowledge**
Short Description	Few years ago NATO CCD COE started with education of NATO personnel in the field of Digital Forensics. Since then a lot of work has been done, many theoretical and practical experiences have been acquired. To share ideas and knowledge from those activities is an opportunity to improve credibility of the Centre and provides networking capabilities with other organizations. Building a Body of Knowledge (BoK) is one of the way how to accomplish it.
Aim	Provide credible references for forensic investigations, and a place to rapidly obtain those references.
Customer	NATO, SNs, CPs
Products / Deliverables	Collection of tools and techniques for Forensics investigations.
Schedule	continuous activity
Challenges / Problems / Risks	Willingness of NATO agencies and organizations, universities to actively cooperate and contribute.
Mitigation	

No / Name	16-03-01-D: **Gap Analysis of Modern Detection Methods**
Short Description	Maintaining real-time situation awareness is difficult due to large data volume and high complexity within modern systems. Footprints for attacks can be found within system event messages, but are often detected after the damage has been inflicted. It is necessary to collect data from multiple sources, which can then be correlated into actionable information. This process is scientifically referred to as "information fusion".
Aim	First phase aims to analyse the detection capabilities of existing event monitoring solutions (Suricata, Snort, Bro, Moloch, SEC etc.). Second stage, in focuses on creating an original proof-of-concept solution by applying scientific methods and data mining techniques to fill the identified gaps from the first stage of the study.
Customer	NATO, SNs, CPs
Products / Deliverables	Technical conference paper in 2016 on detection capabilities of existing industrial monitoring solutions. Prototype solution to fill the identified gaps and an academic conference paper in 2017;
Schedule	Conference paper 2016 Prototype solution to cover detected gaps 2017
Challenges / Problems / Risks	
Mitigation	

No / Name	16-03-01-E: **IPv6 protocol stack implementation study**
Short Description	Mostly focusing on protocol stack implementations on most widely used operating systems within NATO networks – Microsoft Windows and GNU/Linux, this research will evaluate IPv6 kernel implementations, and their potential vulnerabilities that might lead to denial of service or remote code execution conditions. Implementation vulnerabilities could have a severe impact on the computer network performance, reliability and security.
Aim	The study will evaluate IPv6 stack implementation in modern operating systems with the goal to identify potential vulnerabilities allowing denial of service, information leakage or remote access attacks
Customer	NATO, SNs, CPs
Products / Deliverables	Technical research paper Proof-of-concept IPv6 protocol stack implementation vulnerability assessment tool
Schedule	Technicial research paper Q4 2016
Challenges / Problems / Risks	
Mitigation	

No / Name	16-03-01-F: **Support the development of a NATO Cyber Range Capability**
Short Description	Support ACT in the development of the technical requirements for a NATO Cyber Range Capability to support NATO's cyber education, training and exercise requirements. Provide SME support to ACT in implementing the requirements and specifications for a NATO Cyber Range Capability.
Aim	Develop the NATO Cyber Range capability
Customer	ACT
Products / Deliverables	Consultancy
Schedule	Continuous, per request
Challenges / Problems / Risks	
Mitigation	

No / Name	16-03-01-G: **Develop ICS/SCADA Lab**
Short Description	Develop modular ICS/SCADA Lab consisting of visual output (water dam, traffic lighting, (nuclear) powerplant, railway), PLC logic to control the visual output and HMI/SCADA control to visualize the modules for control. Also tap points and programming interfaces to modify the controllers to affect the visual outcome.
Aim	Train specialists to see and improve the security of critical infrastructure components, test and play out scenarios where one or more components (network, power, logic) are directly affected Ability to understand and enhance the CI devices, also building of inhouse knowledge base to be able to take part in critical infrastructure discussions and research.
Customer	NATO, SNs, CPs
Products / Deliverables	Modular ICS/SCADA lab
Schedule	Q4 2016
Challenges / Problems / Risks	
Mitigation	

No / Name	16-03-01-H: **NATO STO Support**
Short Description	Supporting the NATO STO organisation by participating in following Workgroups: IST-129 IST-108 MSG-117
Aim	Provide technical expertise to NATO Build a NATO network of cyber defence experts
Customer	NATO STO
Products / Deliverables	Input into the joint reports delivered by working groups.
Schedule	Most of the Workgroups have 2 meetings in a calendar year, exact schedule TBD.
Challenges / Problems / Risks	Some workgroups may be already in advanced state, so joining the WG in the middle of the work might be difficult. The approach will be to attend the first WS in 2016 in order to find out if we are able to add value to the Workgroup.
Mitigation	

4. Vzdelávanie a cvičenia

- Oblasť práce – Vzdelávanie a povedomie
- Oblasť práce - Cvičenia

4. Vzdelávanie a cvičenia

- *Oblasť práce – Vzdelávanie a povedomie*
- Oblasť práce - Cvičenia

No / Name	16-04-01-A: **Support CD E&T Department Head/ ETEE**
Short Description	**NATO CD E&T Plan (Military Committee)** ACT, with strong support from the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) and NCI Agency (including the NCISS), is designated as the Department Head for Cyber Defence"
Aim	Provide support to NATO CD E&T DH for ETEE development.
Customer	ACT JFT JETE
Products / Deliverables	Support TNA (*Host 1 TNA workshop*) Support TRA other disciplines (Join Targeting, Operations Planning and Assessment) Support (*Host*) Annual Discipline Conference (ADC) Advice in E&T Quality Assurance Participate in MNCD as stakeholder Deliver Education and Training Solutions
Schedule	TSC, IPB, TNA, TRA, ADC, MNCD (TBD)
Challenges/ Problems / Risks	Level of support unclear until specific request is received
Mitigation	Case by case decision, according with Centre's resources

No / Name	16-04-01-B: **Support NATO CD Awareness Campaign**
Short Description	In accordance with the CD Action Plan, ACT produced a concept regarding Cyber Defence Awareness in NATO. In 2014-2015 a reduced CD Awareness Campaign pilot was conducted. In 2015-2016 it will be conducted a NATO-wide CD Awareness Campaign
Aim	Support ACT CD awareness campaign.
Customer	ACT CAPDEV C2DS
Products / Deliverables	Support ACT in the management of a NATO-wide CD Awareness Campaign. NATO CCD COE e-Awareness Course Contribute to TIDE SPRINT
Schedule	Awareness stakeholder coordination meetings (TBD) Awareness events on invitation (TBD)
Challenges / Problems / Risks	Level of support unclear until specific request is received
Mitigation	Case by case decision, according with Centre's resources

No / Name	16-04-01-C: **Courses**
Short Description	Management, planning, preparation, administration and execution of NATO CCD COE courses.
Aim	Increase skills and knowledge for NATO and SNs specialist audience.
Customer	NATO, SNs, CPs
Products / Deliverables	- Technical Courses (7) - Technical Workshops (2) - Legal Courses (2) - Mobile Courses (4) - Operational Level Courses (2) - Executive Level Cyber Seminar (1) - NATO Accreditation of courses - Improvement of E&T Quality Assurance within NATO CCD COE
Schedule	See next slide
Challenges / Problems / Risks	- Currently demands exceed Centre's capabilities.
Mitigation	Train the trainers (IDFC pilot course)

No / Name	16-04-01-D: **Cyber Defence e-Learning**
Short Description	Update, improve and further development of CD Awareness e-Course. (Content and Platform)
Aim	Provide Cyber Defence awareness training on-line and under individual demand.
Customer	NATO, SNs, CPs
Products / Deliverables	Cyber Defence Awareness e-Course (CDAeC).
Schedule	**For training audience**: on demand. Platform is open permanently. **For NATO CCD COE**: - Course review (May-June) - Contract with developer (Aug) - Implementation of improvements (Sep-Oct)
Challenges / Problems / Risks	
Remarks	e-Course available on NATO CCD COE website > Events > Awareness e-Course

No / Name	16-04-01-E:**Cyber Defence Lessons Learned**
Short Description	Provide support to JALLC in analysis reports in the area of Cyber Defence, and manage CD COI LL Portal
Aim	– Support JALLC in conducting Analysis Reports – Conduct Analysis Reports in specific areas of expertise – Manage Cyber Defence Community of Interest LL portal – Manage LL related activities in the Centre
Customer	NATO JALLC
Products / Deliverables	- Analysis Reports on CD aspects (case by case) - NATO CCD COE LL. - LL CoI Portal
Schedule	- Annual NATO LL Conference (TBD) - COE LL Workshop (TBD)
Challenges / Problems / Risks	Level of support unclear until specific request is received
Mitigation	Case by case decision, according with Centre's resources

4. Vzdelávanie a cvičenia

- *Oblasť práce – Vzdelávanie a povedomie*
- *Oblasť práce - Cvičenia*

No / Name	16-04-02-A: **NATO CCD COE Technical Exercises**
Short Description	**Locked Shields (LS16)** Technical Red – Blue team exercise based on fictional scenarios. It allows the blue teams to exercise the protection of their ICT infrastructure in real world scenarios. **Crossed Swords (XS16)** The primary objective is to test the skills of teams of IT specialists in preventing, detecting, responding to and reporting about full-scale cyber-attacks.
Aim	To enable and prepare blue teams to protect their infrastructure in real cyber-attack situations and red team members to conduct successful attacks against blue team infrastructure.
Customer	NATO, SNs, CPs
Products / Deliverables	Planning Conferences, Test Run, Execution
Schedule	**LS16:** **10 Oct 2015**: Deadline for applications to participate and contribute **15 Oct 2015**: IPC **14 Jan 2016**: MPC **27-28 Jan 2016**: LS16 New Red Team Members Workshop **09-10 Mar 2016**: Red Team On-Site Workshop I **10 Mar 2016**: Test Run **31 Mar 2016**: FPC **18-19 Apr 2016**: Red Team On-Site Workshop II **19-22 Apr 2016**: Execution and Hot-wash **27-28 Apr 2016**: LS16 Strategy Workshop **09-13 May 2016**: LS16 Large- Scale Packet Capture Analyses Workshop **TBD May 2016**: After Action Review **CS16:**Test Run 09-11DEC 2015, Execution: 09-11 FEB 2016

- Technical Blue/Red Team Exercise
- 1 Red Team (65) VS 20 (320) Blue Teams
- CPT (220): Red (65), Green (60), Yellow (12), White (75).
- Total: 550 participants.
- Over 1200 attacks against the Blue Team systems
- 3.5 days, day=8 hours for training audience
- Game: teams in fictional roles, lab networks
- Almost unknown environment for BTs
- Friendly competition
- Defense is the focus of training

CROSSED SWORDS

- Responsive Cyber Defense scenario
- Hands-on
- Main training objectives
  - United team
  - Hit-and-run
  - Leave no traces
- Highly technical

No / Name	16-04-02-B: **Support Cyber Coalition**
Short Description	Validate cooperation, coordination, management and decision making NATO CD processes.
Aim	- Improve NATO CD decision making process. - Improve CD capabilities of NATO bodies and participating nations.
Customer	ACT
Products / Deliverables	Provide support to ACT for NATO Exercise Cyber Coalition 2016: - Elaboration of Storylines - Participation in the event
Schedule	- Exercise Definition Conference (January, NATO HQ) - Storyline Development Conference (February, NATO HQ) - IPC (March, NATO HQ) - Storyline Leaders' Scripting Workshop (May, The Hague) - MPC (June, place TBD) - NATO-only TTEx (September, NCIA Brussels) - National Scripting Conference (September, NCIA The Hague) - FPC (October, place TBD) - Execution (November, TBD) - CC16 AAR & CC17 Planning (December, NATO HQ)
Challenges / Problems / Risks	
Mitigation	

No / Name	15-04-02 C / **Support to TRIDENT exercises**
Short Description	Support the planning and execution phases of exercises TRIDENT JAGUAR, JUNCTURE and JOUST
Aim	- Provide CD SME to augment SHAPE evaluation team - Enable effective CD incorporation into TRIDENT exercises. - Improve achievement of Training Objectives by the Training Audiences.
Customer	- Lead: SHAPE J6, SHAPE J7, JWC - TA: JFC Naples, JFC Brunssum, NRDC-TURKEY
Products / Deliverables	- CD MEL/MIL - Evaluation reports
Schedule	**TRIDENT JAGUAR 2016 and 2017** - TRJR16 Phase II CRP evaluation (January) - TRJR16 MEL/MIL Development workshop (February) - TRJR16 MEL/MIL Scripting workshop (March) - TRJR16 Phase III Execution evaluation (May) - TRJR17 Phase II CRP evaluation (May) - TRJR17 MEL/MIL Development workshop (September) - TRJR17 MEL/MIL Scripting workshop (November) **TRIDENT JUNCTURE** - Phase II CRP evaluation (June) - MEL/MIL development workshop (July) - MEL/MIL Scripting workshop (September) - Phase III Execution evaluation (October) **TRIDENT JOUST** execution (April)
Challenges	CD SME is a critical resource (1 SME, 3 EXE, 2 or more sites)
Mitigation	

No / Name	15-04-02 D / **Support to STEADFAST PYRAMID/PINNACLE**
Short Description	Support planning and execution of exercise Pyramid/Pinnacle.
Aim	- provide SME to review cyber aspects of exercise documentation, validate cyber play in high level war game and support execution.
Customer	- JFT-JETE. - TA: NATO Senior Military Leadership
Products / Deliverables	- realistic cyber aspects for exercise, presentations.
Schedule	- War game validation Workshop (TBD) - Pyramid execution in Latvia (12-16 SEP) - Pinnacle execution in Latvia (19-23 SEP)
Challenges / Problems / Risks	N/A
Mitigation	

No / Name	16-04-02-E: **Support to CWIX/STEADFAST Cobalt**
Short Description	Support planning and execution of exercises Steadfast Cobalt , and CWIX
Aim	**COBALT**: NCIRC penetration testing. **CWIX**: Provide support in particular CD aspects (pen-test, monitoring, malware, etc.) CD SME to the ACT CWIX Analysis Team.
Customer	**CWIX**: ACT CAPDEV C2DS / JFTC - TRG SPT DIV **COBALT**: SHAPE J6, NCIRC
Products / Deliverables	**COBALT**: penetration tests. **CWIX:** CD Observations and penetration tests
Schedule	CWIX: IPC – 3-6 Nov 2015 FIN; MPC – 26-29 Jan 2016, DEU; FCC – 08-11 MAR 2016 POL, Execution 13-30 JUN 2016 IPC 2017 Oct 2016 COBALT: May/June TBD
Challenges / Problems / Risks	**COBALT**: dates might conflict with CyCon; **CWIX:** too long exercises (3 weeks / 3 people).
Mitigation	**CWIX**: Limit penetration testers online support for execution to 10 days.

No / Name	16-04-02-F: **Support to Baltic Ghost**
Short Description	Provide support for Exercise Baltic Ghost planning and execution (incident development / scripting / execution)
Aim	- Assisting in developing scenarios to test the procedures in a table top exercise. Test information sharing procedures among Countries in a crisis situation. - Provide a legal framework for the exercise which allows collective response to cyber events (possibly).
Customer	EST, LVA , LTU, USA
Products / Deliverables	- Support Nations in the development of scenarios. - Support Baltic Ghost lead. - Develop/provide a legal framework.
Schedule	Planning conference(s) and execution. Dates and locations TBD.
Challenges / Problems / Risks	
Mitigation	

5. CyCon

- Oblasť práce – CyCon 2016

No / Name	**16-05-01-A CyCon 2016**
Short Description	Organise and conduct the Centre's annual "International Conference on Cyber Conflict (CyCon)" covering "Cyberpower" in parallel sessions
Aim	– Provide a conference tailored to NATO's and SNs' needs, – increase Centre's visibility, – provide networking opportunity for the international CD community.
Customer	NATO ACT, Allies, SNs, government, military, academic, private sector, worldwide, covering all levels from senior management to Subject Matter Expert – approx. 450-500 participants
Products / Deliverables	– Workshop day (31. May 2016) – 2,5 days conference (01.- 03. June 2016) – Proceedings in electronic and printed format – Audio and video recordings of presentations online after the conference
Schedule	– August 2015 – May 2016 preparation phase – 31.05. - 03.06.2016 Conference
Challenges / Problems / Risks	– Dependency on external support for the conference content – Sponsor support to be confirmed
Mitigation	

No / Name	**16-05-01-B CyCon U.S.**
Short Description	Support to the Army Cyber Institute (ACI) of the United States Military Academy at West Point in organizing an international (joint) conference on Cyber Conflict in the United States. -Will work with L&P and TECH
Aim	The goal is to broaden the reach of CyCon and involve a wider audience, promote research and development in the area of cyber defence.
Customer	USA, NATO, SNs, CPs
Products / Deliverables	Participation in the conference Program Committee, elaboration of the conference topics and an agenda development
Schedule	Conference CyCon U.S. in the fall 2016
Challenges / Problems / Risks	Final decision is still to be made by USA
Mitigation	

Zhrnutie

- Pôsobnosť CCD COE je sústredená do 5 oblastí záujmu:
  - *Právo a politika,*
  - *Stratégia*
  - *Technológie*
  - *Vzdelávanie a cvičenia*
  - *CyCon*
- *Celkovo v roku 2016 CCD COE pracuje na 38 projektoch*

Kontaktné údaje

- **podplukovník Ing. Zdeněk HORÁK**
- Predstaviteľ SR v Riadiacom výbore NATO CCD COE,
- Generálny štáb ozbrojených síl SR
- 0960311440, 0903824243
- zdenek.horak @ mil.sk