Agenda

- WG Composition
- Last meeting
- AJP-3.15 Way Ahead
- NATO C-IED Action Plan Revision 2 (APR2)
- Next meetings
- Programme of Work
- Recommendations / Decisions
- Questions / Discussion
WG Composition

C-IED WG

Military Working Dog (MWD) Expert Panel
STANAG 2623 / AMWDP-1 team

CIED Mar. Environ. (CME) Panel
STANAG 2294 / ACIEDP-1 team

Doctrine and Terminology Panel
STANAG 2295 / AJP-3.15 team

Interoperability Panel
STANAG 2298 / ACIEDP-2 team

AtN Stanag
Exploitation Pub´s revision
Last Meeting

15th Meeting of the C-IED WG
Date: 5-8 April 2016
Place: London, UK

79 delegates
16 NATO Nations: including BEL, CAN, CZE, DEU, DNK, ESP, FRA, GBR, ITA, NLD, NOR, POL, ROU, SVK, TUR, USA
+ SWE
+ ACT, SHAPE, LANDCOM, MARCOM, C-IED CoE, CoE CSW, EOD CoE, MILENG CoE, IS/DI

Highlights
• 1st co-located MWD Panel session. Revision effort ongoing for AMWDP-1(B)
• AJP-3.15(C) writing session.
• NATO CIED APR2: approval by NAC is expected soon.
• Acknowledge the possible creation of a NATO Military CIED Committee
  • C-IED interoperability requirements discussed; interaction with JINT WG will be critical.
• Further development of Voluntary C-IED Capability Matrix
• Discussion on creation of CME Panel.
• Update on status of Threat Weapon Signature Standardization Proposal.
• Informative Briefings on: FRA Briefing on Exploitation Laboratory Operations in Mali; Underwater Search and use of Unmanned Systems; and Exercise Bison Counter
## AJP-3.15 way ahead

<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 May 2016</td>
<td>Custodian to finalize SD2 and post it to the CIED WG forum</td>
<td>Custodian</td>
</tr>
<tr>
<td>9 August 2016</td>
<td>Delegates are invited to provide feedback using the comments matrix</td>
<td>CIED WG delegates</td>
</tr>
<tr>
<td>19 September 2016</td>
<td>Custodian to provide an updated draft, with adjudicated collated comments matrix</td>
<td>Custodian</td>
</tr>
<tr>
<td>First week of October 2016</td>
<td>AJP-3.15 writing session to occur</td>
<td>AJP-3.15 writing team</td>
</tr>
<tr>
<td>Prior to the 16th CIED WG meeting</td>
<td>Custodian to post proposed FD onto CIED WG forum, in order for the CIED WG to endorse the publication at that meeting.</td>
<td>Custodian</td>
</tr>
<tr>
<td>16th CIED WG Meeting (NOV16)</td>
<td><strong>Writing team seeks CIED WG endorsement</strong></td>
<td>CIED WG</td>
</tr>
<tr>
<td>After CIED WG endorsement</td>
<td>Forward to AJOD WG to approve ratification process</td>
<td>Start ratification process</td>
</tr>
</tbody>
</table>
A. Develop the full spectrum of Technical Exploitation Interoperability Standards (Level 2 Lab) and Doctrine.

B. Initiate the development of NATO AGREED terminology for the complete Technical Exploitation process (Level 1 through Level 3).

C. Develop a multi-domain AtN STANAG in order to facilitate understanding and interoperability requirements necessary to conduct C-IED related AtN activities in the land, maritime, cyber, and air/space domains.

D. Review Level 1 & 2 NATO Doctrinal Publications and MC 133/4 and propose to the respective custodians appropriate C-IED input.

E. Include C-IED in the Maritime Environment (CME) aspects during the revision of STANAG 2298 / ACIEDP-2 in order to facilitate a Level 1 Exploitation capability in the maritime domain and support joint operations.
Concerns

The MCLSB is asked to note that:

• Concerns:
  – C-IED Terminology / Lexicon
  – Overlapping / duplications / gaps on Exploitation.
  – Attack the Network (AtN) Publication → collective effort.
IED Lexicon / Characterization
Exploitation Schema

- Device profile; physical description and categorization of the IED information.
- Device signature; unique similarities in device construction techniques and methodologies, materials used in device construction that in conjunction with tactical data create unambiguous signatures (assembler and emplacer).
Command Operated/Radio Control, Commercial, Mobile Phone/No Modified

Arming Switch/ No Time Power Unit, No Anti-Tampering Features, Low Power/VHF-SHF/GFSK/2G GSM/Fitted with Semiconductor
Device Technical Signature

- Physical dimensions, description of the components.
- What material is used to get secured the components?
- Type of wire used and method of attachment.
- Patterns.
- How are the contacts attached?
- Type of initiator, markings on and characteristics.
- Type and voltage of power source (configuration).
- Type of explosive and charge configuration.
- Alternative Switches.
- Time Power Unit.
C-IED Expolitation analysis
Related exploitation doctrine.

### JINT WG
- AJP-2.1. Intel. procedures
- AJP-2.5. (SD) Intel. Exploit.
- AJP-2.7. (FD) JISR
- AlntP-10 Technical exploit.
- AlntP-13 (SD) HNAT
- AlntP-14 (SD) JISR in support of Ops.
- AlntP-15 (FD) Countering threat anonymity.

### C-IED WG
- AJP-3.15 (SD) C-IED
- ACIEDP-1 C-IED TRG
- ACIEDP-2 C-IED WIT

### CBRN WG
- AJP-3.8 CBRN Defence
- ATP-3.8.1 Specialist CBRN Defence Capability
- ATP-3.8.1 CBRN Defence on Ops

### EOD WG
- ATP-3.18.1 EOD
- AEODP-03 V I. IEDD Ops
- AEODP-03 V II. IEDD Ops
- AEODP-06 EOD Reporting

### MILENG WG
- ATP-3.12.1 Military Engineering
- ATP-3.12.1.3 Route Clearance
- ATP-3.12.1.1 B-1 Military Search
DEFENCE INVESTMENT DIVISION

TECHNICAL EXPLOITATION ACTIVITIES AROUND NATO

AJP-2.5
(MCJSB JINT WG)

AIntP-10 Technical Exploitation Standard
Future AIntP-xx
Future AIntP-xx

AJP-3.8 CBRN DOCTRINE
(MCJSB/NAAG JCBRND CDG)

ATP-3.8.1 Vol 2 Specialist CBRN Defence Capabilities
CBRN Forensics Report
AEP-66 SIBCRA Handbook

AJP-2.1
INTELLIGENCE PROCEDURES
(JINT WG)

AIntP-15
Countering Threat Anonymity (Biometrics)

AJP-3.15 C-IED DOCTRINE
(MCLSB C-IED WG)

ACIEDP-01 C-IED Training Requirements
ACIEDP-02 Weapons Intelligence Team Capabilities
Considering Threat Weapon Signatures

CNAD - NAFAG - ACG/3 TEAM OF EXPERTS ON ECM FOR RCIED

RCIED Database
Electronic Exploitation for RCIED
Naming Conventions

JDEAL
(EDA-NLD)
## POTENTIAL FOCUS ON TECHNICAL CAPABILITIES AND PROCEDURES

<table>
<thead>
<tr>
<th>Annex</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>B</strong></td>
<td>Triage</td>
</tr>
<tr>
<td><strong>D</strong></td>
<td>Latent and Patent Print Examination Capability – <em>MASINT WG?</em></td>
</tr>
<tr>
<td><strong>E</strong></td>
<td>Deoxyribonucleic Acid (DNA) Analysis Capability – <em>MASINT WG?</em></td>
</tr>
<tr>
<td><strong>F</strong></td>
<td>Firearms and Tool Marks Examination Capability</td>
</tr>
<tr>
<td><strong>G</strong></td>
<td>Electronic Exploitation Capability – <em>ToE on ECM for RCIED</em></td>
</tr>
<tr>
<td><strong>H</strong></td>
<td>Mechanical Exploitation Capability</td>
</tr>
<tr>
<td><strong>I</strong></td>
<td>Explosive Materiel Exploitation Capability</td>
</tr>
<tr>
<td><strong>J</strong></td>
<td>Document and Media Exploitation Capability</td>
</tr>
<tr>
<td><strong>K</strong></td>
<td>CBRN Exploitation Capability – <em>JCBRND CDG</em></td>
</tr>
<tr>
<td><strong>L</strong></td>
<td>Other Material Exploitation Capability (fibres, fabric, and cordage)</td>
</tr>
</tbody>
</table>
Exploitation-related doctrine. Identified Gaps.

1. **AJP 2.5** (B) Intel Exploitation of persons and materiel.
   - Terminology.
   - Clarifying exploitation inclusion in the Intel cycle.
   - Alignment.

2. **Aint P10** Tech Exploitation.
   - Define “Limited Level 2”?
   - Including / Modifying Templates for Chain of custody

3. **AintP 13** Study Draft HNAT concept
   - Alignment.

4. **AintP 15** JISR
   - Alignment.

5. **AIntP 15** Countering threat anonymity/Biometrics
   - Concept for I2/ Unified NATO software for Exploitation, integration with I2, -NABIS and national ABIS- Integration of the 3 Levels in an unique system?

**OTHERS.**
- Training for Lab 2 commanders / Staff/
- Integration of Lab 2 Products on ALL FUSION CELLS / INTEL.
Exploitation-related doctrine. Identified Gaps.

1.- **EODP 06** Reporting.
   (Unified) Templates for Exploitation Products.

2.- **AJP – 3.8** Doctrine for CBRN Defense.
   Including Forensic sampling as part of exploitation.
   Related ATP 3.8.1CBRN I and II. capabilities / OPS

3.- **AJP 3.15** (C) Study draft. CIED.
   Terminology.
   Inclusion of aligned, clear concepts.

4.- **Stanag 2298** WIT Capabilities.
   Chain of custody.
   Reports.

**OTHERS**

   Procedures to include exploitation products from L3 in the Intel cycle.
   Catalogue of nation’s Capabilities.
Identified gaps / needs.

- Specialized containers for air transport. Requirements?
- Review AlntP10 updated tables.
- Reinforce collection procedures for WIT?
- ACIEDP-2 ?
- Reviewing AlntP10 annexes equipment requirements to build up capabilities.
- Level 3 requirements – what does Level 3 need to receive? Forms, ways and contents.
- Procedures for Level 2 capability. Could it be done at NATO level as a StandRec?
- Definition of chain of custody. Are procedures required?
- Reports formats from AEODP-06.
- Consider maritime environment. Especially for equipment and capabilities. Annex to extant publications?
- Standard CIED lexicon.
- Better formatting for exchanging information.
- Software requirements –reporting, DB.
- Integrating exploitation continuum concept into AJP 3.15
- Review NDPP capability codes and statements. (WIT and level 2 labs).
- CIED WG IP as basis for Tech exploitation Col.
- Develop schedule review for all technical exploitation related publications (CIED WG DTP).
- Develop security classification guidance for exploitation products.
Possible proposals

**Doctrinal standardisation:**
- Clarify revision schedule of exploitation-related publications.
- Submit text proposals to relevant NSO WGs to be included in the regular revision process of other publications.
- Develop a standard C-IED lexicon, including exploitation-related terms.
- Integrating the “exploitation continuum” concept into AJP-3.15 (C).
- Consider capability and materiel aspects of CME.
- Definition of chain of custody. (Check NATO MP STANAGS).
- Possible level 3 doctrine (including requirements for explosives samples transport).
- Propose to bring AlntP-10 under the responsibility of CIED WG.
Possible proposals

**Technical standardisation:**

- Review NDPP capability codes and statements, especially regarding WIT and Level 2 labs.
- Turn level 1 to level 3 equipment requirements into tech capability requirements.
- Requirements for explosives samples air transport. (containers and air assets for theatre movement standards).
- Data formatting and exchange requirements for information sharing (and the associated minimum software requirements).
- Review AlntP-10 annexes equipment requirements to build up capacities.
- Consider materiel aspects of CME.
Possible proposals

**Procedural standardisation:**

- Review collection procedures for level 1. Consider possibility either to revise Handbook or to draft a new publication (SIBCRA-like).
- Level 3 requirements: forms, content, submission ways.
- Consider possible Standardisation Recommendation on procedures for Level 2 operation. AIntP-10.
- Consider possible Standardisation Recommendation on Level 2 enabling capabilities.
- Study the need for chain of custody procedures. AIntP-10.
- Exploitation reports formats need to be updated, and separated from EOD reports. ACIEDP-2.
- Appointing CIED WG Interoperability Panel as the basis to set up a Technical Exploitation Community of Interest.
- Develop security classification guidance for exploitation products.
Questions