NORTH ATLANTIC TREATY ORGANISATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
HEADQUARTERS, SUPREME ALLIED COMMANDER TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

5000 TSX 0170/TT-7579/Ser: NU0462

TO: See Distribution

SUBJECT: Commanders' and Staff Handbook for Countering Improvised Explosive Devices

DATE: 10 August 2011

1. The Improvised Explosive Device (IED) has become a feature of the modern battlefield and is likely to remain a serious challenge in the future. In responding to this challenge, NATO must remain adaptable and flexible while developing robust and effective Counter-IED (C-IED) policies and procedures for current and future operations. C-IED activities should also be widely understood and integrated within and across all levels of command (particularly Intelligence and Operations) and not relegated to a single functional area.

2. The *Commanders' and Staff Handbook for Countering Improvised Explosive Devices (C-IED)* is provided at Enclosure 1 and has been developed to provide guidance on "what needs to be done" rather than "how to do it". The Handbook was developed during the Operational C-IED Command and Control Experiment (September 2008) and validated during the NATO C-IED SOP Handbook Validation Experiment (May 2011). It describes outputs, staff responsibilities and enablers for commanders and staff to consider when integrating C-IED into the preparation, planning and execution of operations, and how to incorporate C-IED activities into all staff functional areas. It is designed for use by commanders and staffs at the operational and tactical levels.

3. NATO organizations and Nations are encouraged to disseminate the handbook widely. They are also invited to submit feedback, in support of periodic revisions of the document, to the ACT C-IED Integrated Product Team Leader, Col John Greaves, john.greaves@act.nato.int; +1-757-747-4244.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION

R G Cooling CB
Vice Admiral, GBR N
Chief of Staff
Allied Command Transformation

ENCLOSURE:

1. Staff Handbook for C-IED Input to Preparation, Planning and Execution of Operations

DISTRIBUTION:

External –

Action:

SHAPE (Attn: COS; NMRs)
JFC BS
JFC NP
JCL
COS ISAF
COS IJC
Comdt NATO School
NATO JEWCS
Dir C-IED COE
Dir MILENG COE
Dir COE DAT
Dir HUMINT COE
Dir EOD COE
Dir JCBRN COE
Dir JAPCC
Dir CSW COE
Dir CCD COE
HQ ALCC
Non-NATO ISAF Troop Contributing Nations MoDs
USJS J7

Internal –

Action:

DCOS MCD
ACT Distribution list II
ACT Distribution list III – National Liaison Representatives
ACT Distribution list V - PFP Staff Element (PSEs)
ACT Distribution list VI - PFP National Liaison Representatives

Information:

DCOS CD
DCOS JFT

Commanders' and Staff Handbook

for

Countering Improvised Explosive Devices (C-IED)

15 July 2011

Intentionally Blank

Preface

Aim and Purpose

This handbook is designed to assist commanders and staffs in understanding, planning, and conducting Counter-IED (C-IED) staff processes in an operational environment. It recommends the organisation, process, and capabilities to facilitate the planning, integration, and execution of C-IED activities in operational staff functions.

Background

The adaptive IED challenge will remain a potential threat across the full range of Alliance operations. Consequently, integrating C-IED activities and enablers (people and equipment) for defensive (Defeat the Device) and offensive (Attack the Networks) operations requires clearly documented and practised staff processes. Stove-piped C-IED expertise and operations have proven unreliable to support overall operational objectives and theatre campaigns synergistically. As a result, NATO has conducted two C-IED specific experiments to define and validate the optimal staff organisation and processes to fully integrate and maximise C-IED activities in the overall operational campaign. This information is contained in the following handbook and is provided as a recommended guide to operational commanders and staffs.

As NATO's C-IED Capability Monitor, I encourage the Alliance and associated Nations to implement these validated techniques and guidance in order to improve the synergistic effects that an integrated C-IED effort will provide to Alliance operations.

Kjell-Ove O. Skare

Kjell-Ove Skare
Major General, NOR A
NATO C-IED Capability Monitor

COMMANDERS' AND STAFF HANDBOOK FOR COUNTERING IMPROVISED EXPLOSIVE DEVICES (C-IED)

REFERENCES

A. AJP 3.15A – Countering IEDs.
B. STANAG 2294 – C-IED Training Standard- Ed.1 dated 20 Jan 09.
C. AAP 6 – NATO Glossary of Terms and Definitions.
D. AAP 15 – NATO Glossary of Abbreviations used in NATO documents and Publications.

CONTEXT

1. There is likely to be an IED threat in all military deployments and this should be a key consideration when undertaking the preparation, planning and execution of current and future NATO deployed operations. Generic detail of the threat environments and the C-IED approach are described in Reference A but for each deployment further specific operational analysis must be undertaken to ensure a mission focussed approach. Key to this is the generation of C-IED awareness and capability within the staff at every level of command.

2. This handbook sits under References A and B and is intended to be complimentary to existing NATO doctrinal publications and formation HQ operational planning and capability development. It should be noted that although the handbook is aligned with the AJP 3.15A, it seeks only to provide an operational and tactical level staff perspective. It is designed for use within military HQs at all levels and is equally applicable for National C-IED capability development. It will be a living document and updated and amended in conjunction with NATO publications and the lessons identified/ lessons learned process.

3. This handbook does not seek to define staff HQ or national operational planning processes for C-IED but should be used as a reference manual during the planning and execution of operations. Every operational deployment will have different requirements, depending upon environmental and operational variables; therefore the Commander must identify appropriate C-IED activities and processes within his staff functions as a priority.

4. C-IED is a relatively new phenomenon and has yet to be fully institutionalised into existing military staff training and functions. All staff must be aware of this fact and take every opportunity to develop wider awareness and understanding to better integrate C-IED aspects into all training and processes.

AIM OF THE HANDBOOK

5. The aim of the handbook is to outline outputs, staff responsibilities and enablers for Commanders and staff to consider when integrating C-IED into the preparation, planning and execution of operations, and to foster an Attack the Network mindset.

CONCEPT AND APPLICABILITY

6. It is widely acknowledged that IEDs will be a major threat for all levels of current and future operations and it is therefore imperative that national and NATO Formation and Unit HQs are able to prepare for, plan and conduct C-IED activities. Clearly defined C-IED outputs will enable the force to undertake these activities throughout the JOA in order to achieve the mission.

7. **Definition**. Reference A defines C-IED as follows:

> ***The collective efforts at all levels to defeat the IED system by attacking the networks, defeating the device and preparing the force.***

8. C-IED approaches the IED as a systemic problem and C-IED actions aim to defeat the IED System. However, IEDs are only one of a number of forms of asymmetric attack used by insurgents, criminals, terrorists and other malign actors. The networks (e.g. Narcotics, Financial, Cyber, Piracy, Human Trafficking, IED, Terrorism, etc.) overlap and, therefore, will concurrently service the plethora of other requirements and activities of the adversary. A*ttack the Networks* activities should take place at all levels: strategic, operational and tactical and, as the networks are predominantly personality-based, activities will focus against adversarial personalities and processes/activities as well as against IEDs/facilities/materials and their production, and will require a broad approach to the problem.

9. As there is an overlap of activities within the networks, they concurrently support the different aspects of the insurgents' or adversaries aims and objectives. Understanding of, and intelligence on, these networks will be vital to not only the overall attack the network process but also the ability to identify the nodes and linkages within the financial, commercial, and communication sectors as well as an adversary's own structures and interactions within the population. Most importantly, understanding these networks will highlight the adversary's critical vulnerabilities; the target for all operational planning and activity. Thus planning for C-IED actions must include consideration of, and actions against, the adversarial networks in the widest context and recognition and understanding of friendly force Attack the Network operations taking place to achieve unity of effort and meet the Commander's intent.

10. As the breadth of Attack the Network activities can transcend boundaries at all levels, from national through political to military, it is vital to engage with those functions, activities and personalities that are involved in the fight. This will entail military planners and commanders stepping outside their ‘comfort zone’ and engaging with entities from organizations that they may have had little or no contact with. This requires flexibility and adoption of new mind sets and appreciation of differing priorities and perspectives and, as personally uncomfortable and challenging as this may be, it is vital to success in attacking the networks and the C-IED system they support.

11. C-IED operations should not be planned or executed in isolation and must be fully integrated into the national or NATO force strategic objectives. A C-IED capability is generated when a series of tasks, activities and techniques are undertaken and integrated within the wider context of operational and tactical activities. C-IED may be undertaken within the full spectrum of operations although it is likely to be a greater factor within hybrid threat environments such as an insurgency, terrorism campaigns and during Stabilisation, Security, Transition and Reconstruction Operations (SSTRO). C-IED should be viewed as an activity to achieve the overarching mission rather than a distinct and separate function.

12. C-IED activities can take place at the local, national, regional, and international level. Subsequently, designing an operation to defeat the IED threat requires a comprehensive strategy that integrates and synchronizes series of actions and tasks from the tactical to the strategic levels of command and requires interaction with non-military organizations and the populace. As with the wider hybrid operations C-IED actions may be categorized as direct (focused on the enemy) or indirect (focused on the population). Whether direct or indirect, C-IED operations can be proactive or reactive and applicable to one or more of the three C-IED pillars. The guidance within the handbook is designed to be scalable, flexible and applicable to a variety of structures and requirements.

C-IED APPROACH AND AREAS OF ACTIVITY

13. **C-IED APPROACH**. Reference A directs that the C-IED approach is to be made up of three mutually supporting pillars in order to defeat the IED system. These are:

a. Attack the Networks.
b. Defeat the Device.
c. Prepare the Force.

14. The C-IED *Areas of Activity* provide an integrated approach to focus the C-IED effort effectively and must be an integral element of the staff function and

coordination at, and across, all levels. At the operational and tactical level the *understand* activity underpins the process and is critical to orientating the staff in order to undertake the other four activities. The *pursue* and *predict* activities are more applicable to Attack the Network operations whilst *protect i*s undertaken to Defeat the Device and *prepare* is a key Prepare the Force activity. Operational level staff are likely to be focused on *understand, pursue* and *predict* but must understand and support *protect and prepare* activities. Fig 1 illustrates the relationship between the activities, C-IED approach pillars at the operational and tactical levels.

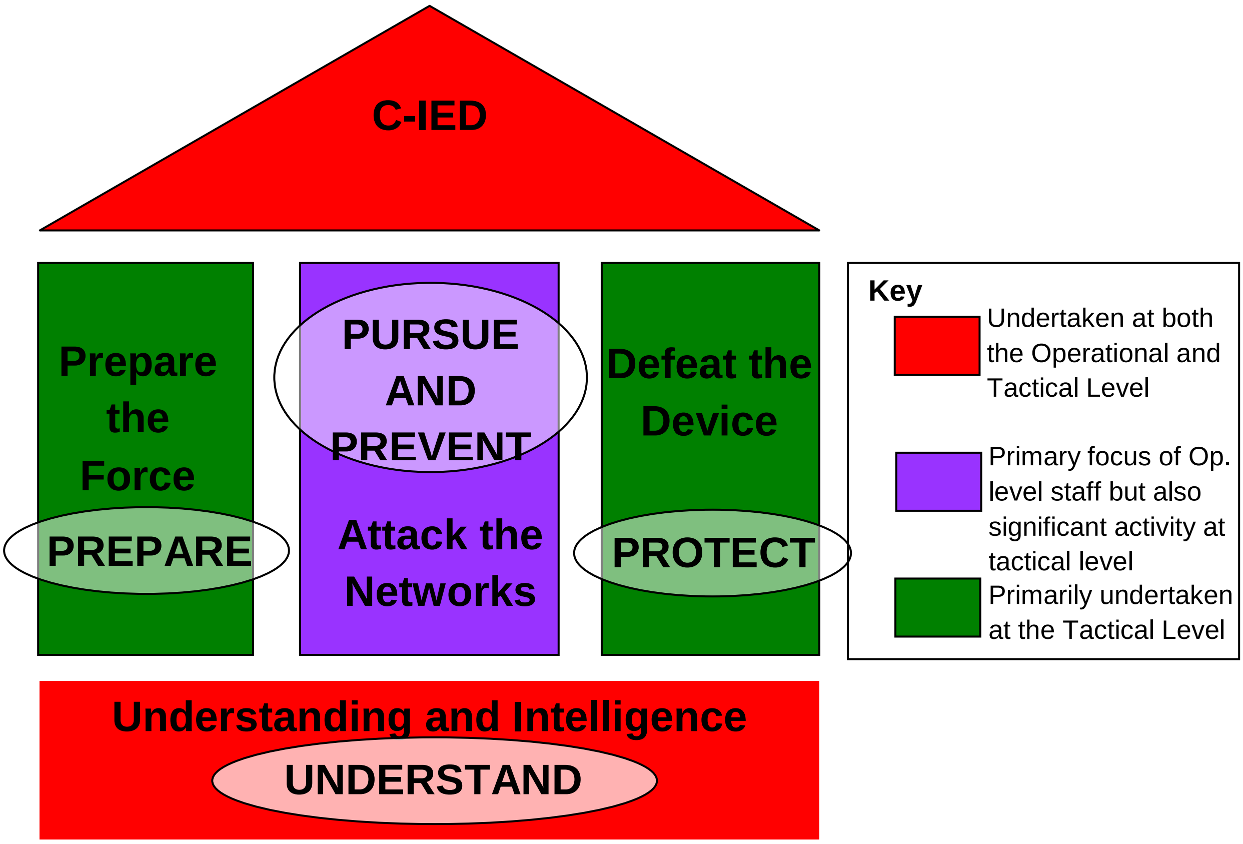

C-IED
Prepare the Force
PREPARE
PURSUE AND PREVENT
Attack the Networks
Defeat the Device
PROTECT
Understanding and Intelligence
UNDERSTAND
Key
Undertaken at both the Operational and Tactical Level
Primary focus of Op. level staff but also significant activity at tactical level
Primarily undertaken at the Tactical Level

Fig 1: Schematic to show C-IED Areas of Activities within the C-IED approach pillars at the operational and tactical levels.

15. These C-IED *Areas of Activity* are described in more detail below.

a. **Understand.** This activity underpins the *pursue, prevent, protect* and *prepare* activities and is fundamental to the development of a comprehensive picture of the IED system and its interaction with the human, physical and information environments in which it operates.

(1) What to Understand?

Operational Environment
The background culture and social dynamics of the population
The adversary
The IED network characteristics and criticalities
IEDs as a weapon
Friendly Forces capabilities (incl HN)

(2) How to understand?

Effective Intelligence Preparation of the Battlefield (IPB)
Cultural and social training and awareness
Engagement with people
Analysis of IED network criticalities and vulnerabilities
Post incident exploitation
Host Nation assistance to include security force aspects

(3) Using the following sources:

Cultural advisors, Historical data and adversary analysis
ISR (incl SIGINT, IMINT, MASINT, DOCINT, ELINT and HUMINT)
Exploitation - Material - (technical, biometric, forensic, media,)
Personnel - (biometric, tactical questioning, detainee questioning)
Open Source Intelligence (OSINT)
Specialist technical intelligence (EW, Weapons Intelligence and use of scientific expertise)

(4) Being supported by the following activities:

All sources analysis
Geospatial Intelligence
IS databases and analytical tools

Secure communications
Common lexicon and reporting
Intelligence sharing and liaison activities
Measurements of effectiveness

b. **Pursue**. Those full-spectrum cross-governmental actions inside and outside the JOA to degrade an adversary IED capability.

(1) What elements of the IED Network to pursue?

International Leadership and support
Regional and Local leadership and support
Infrastructure and Facilities
Resourcing and supply of IED components
IED makers
IED emplacers, initiation and adversary exploitation teams

(2) How do we pursue?

Identifying criticalities and vulnerabilities of the IED network
Network focused intelligence collection plan
Targeting of network-critical nodes (physical and influence)
Population centric operations to isolate the adversary

(3) By using the following:

Products of *understanding* activity
Targeted operations against network-critical personnel
Targeted operations against supply routes and facilities
Key Leader and population engagement to isolate the networks
Operational level input into and coordination with:
    Political and Diplomatic activities
    HN judicial system
    Economic measures
    NGOs and OGDs
Info Ops
Reconstruction activities

(4) Supported by the following:

Network-focused intelligence collection plan (operationally driven)
Pro-active mindset of combat arms
SOF
FIRES
ISR

Exploitation Intelligence (media, technical and biometric)
Info Ops integration into operations
CIMIC integration into operations

c. **Prevent**. Those activities influence activities inside and outside the JOA that deter involvement in IED system and reject IEDs as an adversary tactic. These activities may include:

(1) What activities of the IED system do we wish to prevent?

Direct involvement in the IED system
Support to the IED system
The use of IEDs as an adversary tactic

(2) How do we prevent the IED system from operating effectively?

Deterring involvement in and support to the IED system by shifting the balance of risk/motivation.
Encouraging the population to reject IEDs as an adversary tactical Operational level input into international, political and diplomatic influence activities to deter adversarial networks

(3) Using the following:

Products of *understanding* activity
Kinetic targeting (deterrent)
Tailored information operations at all levels (international to local)
Development of HN governance within police, judicial and prison systems
Coordinated Ops/info ops and CIMIC focused operations
Appropriate posture, presence and profile of Friendly Forces

(4) Supported by:

Robust kinetic targeting policy
Liaison with other military and non-military agencies
Well defined and understood concepts of operation
Measurements of effectiveness

d. **Protect**. Those measures that improve Host Nation and alliance freedom of movement and security. These will be undertaken at the tactical level but enabled by the operational staff.

(1) What are we protecting against?

Loss of support within home nations

The denial of FF freedom of movement
FF and HN casualties
Damage to FF and HN property and equipment

(2) How do we protect?

Limit the strategic effects of IEDs
Prediction of IED locations
Detection of emplaced IEDs
Neutralization of IEDs
Mitigation of IED target effect

(3) Using the following:

Products of *understanding* activity
Operational input to strategic communications
Mission planning timelines and resources
Search and Route Clearance capabilities
IEDD (or EOD if national terminology)
Use of EW Force Protection equipment and TTPs
Use of Force Protection TTPs
Physical protection (defensive constructions, armour and PPE)

(4) Supported by:

Established military/political STRATCOM links
Situational awareness
Exploitation Intelligence
Geospatial intelligence
Coordinated Research and Development between NATO and nations
Medic Capabilities

e. **Prepare.** Those activities that build capability within host nation security forces and alliance forces to conduct full-spectrum offensive C-IED operations within the IED threat environment. These activities may include the following:

(1) What are the preparation requirements to undertake across the DOTMLPFI[1]? The following lines of development should be considered in order to defeat the IED system for the given campaign:

[1] Doctrine, Organisation, Training, Materiel, Leadership and Education, Personnel, Facilities, Interoperability.

Physical (equipment and manning), Conceptual (procedures) and Behavioural (mindset and skills) abilities to undertake:

Understanding
Pursue
Prevent
Protect

(2) How do we prepare?

Relevant and flexible C-IED doctrine and policies

Flexibility and scalability of structure to meet the requirements

Realistic and comprehensive individual and collective training of:

Environmental and cultural awareness

Equipment training

Force Protection TTPs

Attack the Network TTPs

Staff training

Integrated equipment capability programmes and sustainable lines of logistic communication to/in theatre.

Flexibility of mindset and education of the force

Ensuring appropriate interoperability of forces, equipment, communication and IT systems

Building indigenous HN security force capability

(3) By using the following:

Products of *understanding* activity in a timely manner at training establishments/exercises

Institutionalising C-IED individual training

Realistic C-IED play during Mission Specific and Mission Rehearsal training and exercises

(4) Supported by:

IT systems to provide information/intelligence to home nations training

Use of simulators

Lessons learnt process

C-IED TASKS AND RESPONSIBILITIES

16. **C-IED Specified Tasks**. In order to undertake these Areas of Activity staff must identify and complete a number of C-IED-specific tasks, which should deliver towards one or more of the three pillars. Suggested tasks are listed at Annex A along with their contribution to the C-IED pillars to assist in ensuring C-IED staff work is effect-focussed. The process for integrating these into the HQ should be:

a. Commander must nominate an OPR to oversee and coordinate all C-IED activities. This role is pivotal to the success of the attack the network processes and the assimilation of C-IED into the spectrum of military operations. The OPR will act as the Commander's C-IED staff officer, when not deployed, with a watching brief to remain current with IED developments and attacks worldwide. On operations the OPR will facilitate, manage, and lead the C-IED effort, by drawing together and co-ordinating the expertise and efforts of the other staff branches, and become the Commanders' primary C-IED SME and C-IED operations advisor. Further details of his role appear later in Annex A and Annex B – Appendix 6.

b. Commanders and staff must first identify those tasks necessary to ensure mission success within the campaign plan.

c. For each task a responsible department/branch/individual must be identified. Annex A also lists the C-IED Core Functions each task is likely to match.

d. Each task must be subject to a 'Mission analysis' to identify detail, resource or information gaps, supporting information sources and timelines.

e. Resource requirements must be filled but, if not, the gaps must be managed.

f. Development of the task process to include coordination. Communication between of C-IED related stakeholders, both horizontally and vertically is vital to success and must become a routine process for all involved.

g. Continued revision to ensure relevancy.

17. **Staff Functions contributing to C-IED**. C-IED activities must be undertaken in conjunction with other staff activities and external organisations. Whilst in some situations a distinct C-IED cell may be appropriate, in most operational and tactical level HQs, C-IED operations will be considered by members of the existing staff as required under the direction of the C-IED OPR. The staff functions that most contribute to C-IED are:

a. Information and Knowledge Management.
b. Intelligence Fusion and Analysis.
c. ISR.
d. Exploitation.
e. Targeting.
f. Operations and Plans.
g. Force Protection.
h. IEDD/ (or EOD if national terminology)
i. Information Operations.
j. Search and Route Clearance.
k. Training and Lessons Identified/Learned.
l. Civil-Military Co-operation (CIMIC).

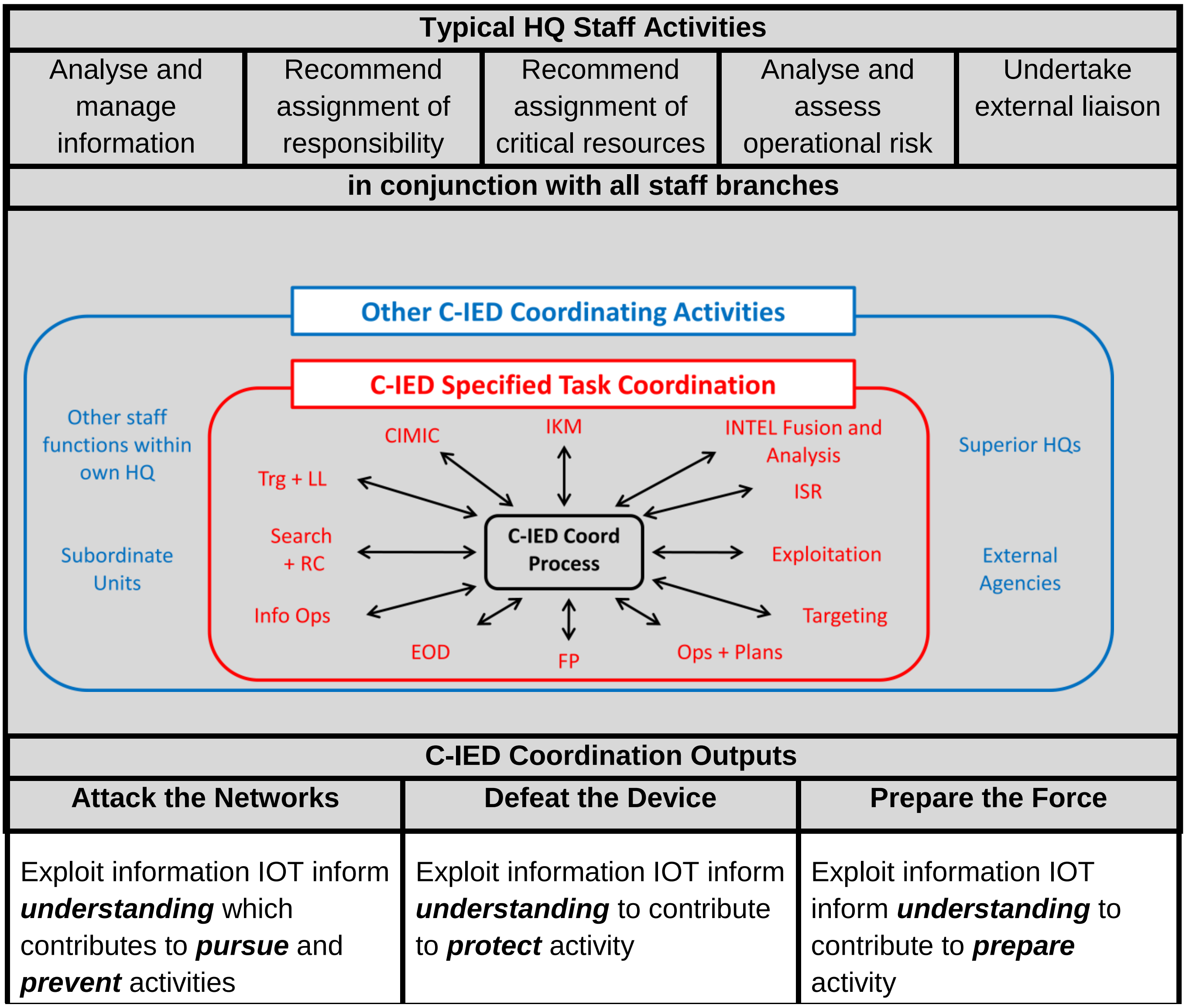
C-IED STAFF ACTIVITIES

18. The operational situation may demand a C-IED cell to be permanently established or possibly just on a temporary basis in order to address a particular issue. Regardless of the existence or structure of any C-IED cell it is suggested that C-IED activities must be incorporated into the existing battle rhythm of the HQ and should be coordinated by the C-IED OPR.

19. Having confirmed the C-IED tasks and required inputs, it is necessary to identify and design appropriate processes in order to achieve them. This must include coordination or information exchange within the core C-IED staff contributors, wider HQ staff and outside agencies. These processes will vary according to the mission, the threat, level of command, HQ structures, available resources and the commanders' intent.

20. There are a number of groupings, media, forums and activities which will contribute to staff processes, some of which will be applicable for C-IED. During the initial integration of C-IED within the staff there may be a requirement for formal C-IED related groupings/meetings to take place. Guidelines for these activities, for potential responsibilities and possible structures are at Annex C.

21. **C-IED Coord**. There is a clear requirement for robust coordination between these processes and across the wider staff and external organisations, both vertically and horizontally. The responsibility for such coordination need not necessarily be the sole task of individuals and may be one of a number of responsibilities for an existing staff appointment. The schematic at Fig 2 illustrates the possible C-IED coordination within the staff.



Typical HQ Staff Activities				
Analyse and manage information	Recommend assignment of responsibility	Recommend assignment of critical resources	Analyse and assess operational risk	Undertake external liaison
in conjunction with all staff branches				

C-IED Coordination Outputs		
Attack the Networks	**Defeat the Device**	**Prepare the Force**
Exploit information IOT inform ***understanding*** which contributes to ***pursue*** and ***prevent*** activities	Exploit information IOT inform ***understanding*** to contribute to ***protect*** activity	Exploit information IOT inform ***understanding*** to contribute to ***prepare*** activity

Fig 2 – Schematic of C-IED coordination within the staff

C-IED TERMINOLOGY AND REFERENCES

22. Consistent and clear C-IED terminology is vital to understanding specialist areas of C-IED and ensuring that operational analysis can be undertaken effectively. Many definitions of C-IED terminology are yet to be ratified which compound the difficulties of developing coherence within the staff HQ. Annex D contains a list of approved abbreviations and terms from References D, E and other approved publications but also includes informal explanations to assist staff working within a C-IED environment.

23. C-IED should be integrated into operational planning, which itself is undertaken within existing doctrine and associated publications. As a result, C-IED staff activity will require reference to a variety of publications. In order to assist in

developing capability and operational planning Annex E lists C-IED related publications in addition to those directly referenced in this handbook.

SUMMARY

24. This handbook serves as a foundation for staff to develop threat, mission and resource specific C-IED capabilities and input to operational preparation, planning and execution of operations. It is designed to be flexible and scalable and therefore should be used by commanders and HQ staff in conducting their own assessment of relevancy and requirements.

Annexes:

A. C-IED Specified Tasks within HQs.
B. C-IED Inputs and Specified Tasks within HQs
C. C-IED Structures and Responsibilities within HQs.
D. C-IED-Related Terminology.
E. C-IED Associated References.

ANNEX A TO
ENCLOSURE 1 TO
5000 TSX 0170/TT-7579/SER: NU0462
DATED 10 AUG 11

C-IED SUGGESTED SPECIFIED TASKS WITHIN HQs

This annex lists the suggested specified tasks that may be required for national or HQ staff personnel to undertake when developing a C-IED capability or operating or preparing to operate in an IED environment. The relevance of each output or task will depend on the mission, threat, HQ size and structure and level of C-IED capability required. Most of the outputs require coordination of C-IED activity between existing staff branches but every output contributes to at least one of the three C-IED approach pillars:

a. Attack the Networks (AtN).

b. Defeat the Device (DtD).

c. Prepare the Force (PtF).

Ser	Staff Functions Contributing to C-IED	Possible Specified Task	Purposes	Contribution to C-IED Approach Pillar			Comment
				AtN	DtD	PtF	
1	Coordination	Coordination of all C-IED activity and outputs within the staff and between the HQ and other units and agencies.	IOT defeat the IED system	X	X	X	Normally undertaken by the Operations branch so this function has been included in the Core C-IED functional area.
2	All Branches	Provide specialist input to briefing senior staff as required	IOT support the decision making of the commander and staff.	X	X	X	
3	Information and Knowledge Management	Create and manage a fit-for-purpose C-IED database.	IOT provide visibility on the operational picture IOT support IPB IOT support pattern analysis	X	X	X	To include personal profiles, mapping, engagements, NGOs, local leaders, enemy

	(IKM)		IOT identify the IED Network IOT inform operational analysis				personnel - not just IED locations and timings.
4	Information and Knowledge Management (IKM)	Create a common lexicon of C-IED terminology	IOT ensure consistency in reporting and information and knowledge management IOT enable accurate Operational and Intelligence Analysis to be undertaken	**X**	**X**	**X**	
5	Information and Knowledge Management (IKM)	Monitor and collate IED incidents by location, type, target and enemy TTP	IOT identify migration of IED threats (devices and networks) across AORs IOT retain situational awareness	**X**	**X**		PIRs, CIRs, DPs and COAs
6	INTEL Fusion and Analysis	Coordination of C-IED IPB	IOT contribute to generic IPB	**X**	**X**		Input information requirements and decision points connected to the IED network
7	INTEL Fusion and Analysis	Predict and identify IED network activities and patterns of behaviour: Financing Recruiting Training IED Construction	IOT understand the IED network IOT contribute to IPB IOT contribute to targeting process	**X**	**X**		Using pattern analysis, predictive modelling and war gaming
8	INTEL Fusion and Analysis	Predict and identify IED network personnel, structures and personal relationships	IOT understand the IED network IOT contribute to IPB IOT contribute to targeting process	**X**	**X**	**X**	Using pattern analysis, biometric intelligence, local level engagements and cultural understanding
9	INTEL Fusion and Analysis	Predict and identify IED network lines of communication: IED material supply sources Supply routes Communication networks Facilities	IOT understand the IED network IOT contribute to IPB IOT contribute to targeting process	**X**			Using geospatial analysis, exploitation results and SIGINT
10	INTEL Fusion	Analyse IED network TTPs to	IOT inform Friendly Forces Force	**X**	**X**	**X**	

	and Analysis	understand tactical emplacement and targeting methods	Protection TTPs. IOT understand enemy IED network capability IOT detect migration of threats and components. IOT identify where and when it is possible to detect the IED network				
11	INTEL Fusion and Analysis	Make assessments on the current and future threats and their effect on operations	IOT retain operational momentum in Force Protection and AtN operations	**X**	**X**		Including intentions, technology and TTPs of IED networks.
12	INTEL Fusion and Analysis	Link intelligence detection assets and other intelligence sources to IED related PIRs and decision points	IOT contribute to IPB	**X**	**X**		
13	INTEL Fusion and Analysis	Coordinate the fusion of exploitation inputs with other INTEL	IOT contribute to IPB and information and knowledge management.	**X**			
14	INTEL Fusion and Analysis	Coordinate the communication of C-IED intelligence to external agencies as appropriate	IOT improve the ability of all organisations to contribute to C-IED strategy.	**X**			Including HN and NGOs
15	ISR	Contribute to planning of ISR asset usage	IOT focus ISTAR assets on relevant elements of the IED system. IOT best meet C-IED PIRs and CCIRs IOT detect enemy locations, movement and utilising of known threat frequencies	**X**	**X**		
16	ISR	Assistance with interpreting C-IED related SIGINT data regarding IED network communications	IOT provide IED related expertise to SIGINT analysts	**X**			
17	ISR	Contribute to HUMINT intelligence focussing and interpretation	IOT ensure that specialist C-IED related information is gathered and results analysed.	**X**			Including tactical questioning and detainee questioning
18	ISR	Contribute to OSINT intelligence focusing and interpretation	IOT ensure that specialist C-IED related information is gathered and results analysed.	**X**			

19	Exploitation	Provide specialist C-IED support to Media Exploitation (MEDEX)	IOT ensure that C-IED related information is gathered and results analysed	X			
20	Exploitation	Issue and manage technical and tactical exploitation policy for Level 1-3.	IOT create a fit-for purpose and all encompassing technical exploitation capability	X	X		
21	Exploitation	Issue and manage biometric exploitation policy for Level 1-3.	IOT create a fit-for purpose, legal and all encompassing technical exploitation capability	X	X		HN security forces likely to require liaison and LEGAD involvement required
22	Exploitation	Create a Level 2 exploitation capability within theatre	IOT provide expert timely and operationally focussed physical and biometric intelligence and evidence across boundaries	X	X		
23	Exploitation	Define Level 2 Exploitation priorities	IOT make best use of resources to meet intelligence and post-incident management requirements.	X	X		
24	Exploitation	Develop links between Level 2 + 3 facilities including reach-back and information sharing facilities.	IOT increase intelligence on enemy/insurgent/ terrorist personnel between theatre and NATO nations	X	X	X	
25	Exploitation	Write and issue Weapons Intelligence (Level 1 exploitation) SOPs	IOT construct a common policy and standard for the collection and initial analysis of IED incident sites.			X	
26	Exploitation	Identify and define differing capabilities within national Weapons Intelligence Teams (WIT) or national equivalent.	IOT create a detailed understanding of WIT capability.			X	
27	Exploitation	Direct and monitor WIT asset lay-down within AOR	IOT make best use of WIT resources.	X	X		
28	Exploitation	Tasking and recovery policy for WIT or national equivalent.	IOT make best use of WIT resources.	X		X	Tactical level only
29	Exploitation	Develop WIT awareness training within C-IED training	IOT ensure that WIT assets are used to best effect. IOT ensure the value of exploitation is understood and Level 2 and 3 outputs are understood and accessible	X	X	X	
30	Exploitation	Liaise with HN authorities security	IOT improve HN exploitation	X	X	X	

		services to integrate HN exploitation capability	understanding and capability				
31	Exploitation	Undertake technical exploitation of IED related components and identify external sources of IED components	IOT identify technical and forensic evidence to improve technical intelligence IOT inform the commander of strategic and political involvement	**X**			Exploitation Staff. To include component identification and characteristics, electronic exploitation, IED construction, explosives analysis, tool markings, enemy TTPs etc
32	Exploitation	Monitor technical exploitation reports from other theatres	IOT identify threat migration in or out of theatre	**X**	**X**	**X**	
33	Exploitation	Recover biometrics and input into biometric database	IOT identify personnel within IED network	**X**			Exploitation Unit Staff
34	Exploitation	Input into Biometric Working Groups	IOT align biometric exploitation collection and database management	**X**			Exploitation Unit Staff
35	Exploitation	Provide feedback to tactical level units of biometrics and exploitation successes.	IOT ensure continued enabling of exploitation efforts by tactical units	**X**	**X**		
36	Exploitation	Writing or disseminating C-IED Flash Reports or Awareness reports	IOT rapidly disseminate new threats and enemy TTPs (by technology or region) to friendly forces.		**X**	**X**	
37	Exploitation	Coordinate and manage exploitation RFIs	IOT enable exploitation information to be available throughout the staff IOT provide appropriate exploitation information to outside agencies	**X**	**X**	**X**	
38	Exploitation	Fuse and analyse exploitation reports to identify sources of components	IOT ensure that intelligence information is integrated	**X**			
39	Exploitation	Develop and publish HN releasable exploitation reports	IOT improve HN situational awareness and contribute to AtN operations	**X**	**X**	**X**	
40	Exploitation	Monitor the process of IED material through exploitation chain	IOT ensure exploitation priorities match operational information requirements	**X**	**X**		
41	Exploitation	Coordinate external expertise on weapons and armour	IOT fully understand IED target effect and FF armour /PPE effectiveness.	**X**	**X**		

42	Exploitation	Ensure exploitation guidelines are in line with relevant judicial authorities	IOT ensure effective prosecution of IED network personnel is possible	**X**			
43	Targeting	Contribute to targeting process and prioritisation of IED network activities and patterns of behaviour: Financing Recruiting Training IED Construction	IOT disrupt IED network ability to undertake enabling activities.	**X**			
44	Targeting	Contribute to targeting process and prioritisation of IED network personnel	IOT deny IED network ability to conduct operations IOT mount capture/kill operations against IED network personnel IOT ensure wider intelligence gathering is not unduly affected by personnel targeting	**X**			
45	Targeting	Predict and identify IED network lines of communication: IED material supply sources Supply routes Communication networks Facilities	IOT disrupt IED network ability to undertake enabling activities. IOT assist in focussing ISR IOT raise issues that are outside the military sphere of influence	**X**			
46	Operations and Plans	Provide lead, direction and coordination for C-IED related activities within all staff branches	IOT ensure C-IED capability is effects focussed	**X**	**X**	**X**	
47	Operations and Plans	Coordinate C-IED related input into routine SITREPs	IOT ensure commanders and staff retain C-IED situational awareness.	**X**			
48	Operations and Plans	Assessment and evaluation of Friendly Forces and HN movement TTPs	IOT assist in validation TTPs for Force protection		**X**	**X**	
49	Operations and Plans	Plan operations to deny IED network freedom of movement	IOT reduce IED network effectiveness	**X**			
50	Operations and Plans	Provide general direction for the prioritisation of C-IED intelligence	IOT ensure exploitation and intelligence gathering opportunities are used without	**X**	**X**		

		gathering opportunities against tactical operations	inappropriate impact on J3 operations.				
51	Operations and Plans	Establish and manage guidelines on pre-detonation and BIP-ing of IEDs	IOT ensure Force Protection TTPs are consistent with security of civilian personnel		**X**		
52	Operations and Plans	Coordinate C-IED contributions to OPLANs and FRAGOs as required	IOT ensure coordinated C-IED capability and direction to the force	**X**	**X**	**X**	
53	Force Protection	Advise on EOF measures to counter Suicide IED according to specific threat criteria	IOT provide enable force protection by proportional use of force in accordance with ROE and threat		**X**	**X**	
54	Force Protection	Train and enable tactical units to undertake geospatial analysis	IOT assist tactical level units in improving Force Protection		**X**	**X**	To include terrain analysis of IED hotspots/VPs, supply routes, IDF firing points, and dead ground studies.
55	Force Protection	Prediction and dissemination of likely IED targets and locations	IOT provide support to attacking IED emplacers. IOT inform Force Protection measures	**X**	**X**		Utilising geospatial tools
56	Force Protection	Monitor and evaluate friendly forces force protection capabilities	IOT retain the ability to manoeuvre		**X**	**X**	To include equipment and TTPs.
57	Force Protection	Monitor the RCIED threat frequency list.	IOT to inform all owners of EW FP equipment on RCIED threats		**X**		Threat bands should be created by Level 2 technical intelligence assets.
58	Force Protection	Identify EW Force Protection characteristics for national, NATO and civilian EW systems.	IOT contribute to Electromagnetic Spectrum Management throughout the battle space	**X**	**X**		Some nations are reluctant to declare full operating specification of EW equipment but will liaise direct with spectrum management authorities.
59	Force Protection	Issue and manage policy for force protection EW equipment use within friendly forces	IOT conform to electronic spectrum management policy.		**X**		To include HN security forces and deconfliction between different nations and equipments.

60	Force Protection	Monitor and evaluate EW force protection equipment and TTPs effectiveness in relation to the threat	IOT confirm that equipment, procedures and threat fills are appropriate to threat		X	X	
61	Force Protection	Issue and maintain the policy on EW pre-detonation of IEDs	IOT ensure force protection TTPs are consistent with security of civilian personnel		X		
62	EOD	Establish and maintain situational awareness of Explosive Remnants of War (ERW) locations, demining and clearance operations within the JOA	IOT predict possible explosives sources for IED networks. IOT improve situational awareness of security forces IOT gain information of explosives hazards and ensure ERW operations priorities met operational demands IOT identify the legitimate uses/storage and transit of explosives within AOR IOT be able to identify legitimate explosives should they enter the IED network.	X			To include mines, UXO, CBRN, former military stockpiles,
63	EOD	Issue and manage ERW policy	IOT ensure standard practice and understanding of ERW operations.	X			To include detection, clearance, relocation and disposal. Production of SOPs
64	EOD	Plan and manage ERW clearance and set priorities	IOT prevent ERW being used within IEDs IOT to make best use of resources to reduce ERW IOT retain situation awareness of geographic areas with ERW, quantities and types of explosives/munitions discovered.	X			Production of FRAGOs
65	EOD	Generate HN capability to deal with ERW	IOT generate HN capability to reduce explosive risk.	X		X	To include plan for training, equipment, management, mentoring and tasking.
66	EOD	Ensure ERW data is incorporated into the C-IED database	IOT improve situational awareness for security forces.	X	X		

67	EOD	Develop and manage mine and UXO awareness training programmes and educate within FF and the populace	IOT fulfil force protection requirements IOT mitigate explosive hazards to civilian personnel IOT prevent civilians supplying ERW to IED networks			**X**	
68	EOD	Issue and manage EOD policy	IOT ensure standard practice and understanding of EOD operations		**X**		
69	EOD	Identify EOD capabilities by nation (incl host nation)	IOT ensure situational awareness of friendly forces capabilities		**X**		
70	EOD	Direct force lay-down of EOD/IEDD assets within AOR	IOT make best use of EOD resources.		**X**		
71	EOD	Issue tasking and recovery policy for EOD/IEDD assets within AOR	IOT make best use of EOD resources.	**X**	**X**		Tactical level only
72	EOD	Generate and monitor EOD capability within HN	IOT generate HN capability to neutralize the threat.		**X**	**X**	To include plan for training, equipment, management, mentoring and tasking.
73	EOD	Monitor EOD reports and maintain EOD map and register.	IOT assist/ support HN on EOD tasks.	**X**	**X**		
74	IEDD	Issue and manage IEDD policy	IOT ensure standard practice and understanding of IEDD operations		**X**		
75	IEDD	Identify IEDD capabilities by nation (incl host nation)	IOT ensure situational awareness of friendly forces capabilities		**X**		Nations have different standards, capabilities and understanding of IEDD operations
76	IEDD	Direct force lay-down of IEDD assets within AOR	IOT make best use of IEDD resources.	**X**	**X**		Tactical level only
77	IEDD	Monitor IEDD reports and storyboards IOT evaluate IEDD TTPs in relation to threats	IOT identify equipment or TTP gaps within IEDD capability	**X**	**X**		IEDD TTPs are likely to be a national responsibility, but analysis can assist in LL process.
78	IEDD	Generate and monitor IEDD capability within HN	IOT generate HN capability to neutralize the threat.	**X**	**X**		To include plan for training, equipment, management, mentoring and tasking.
79	Info Ops	Coord C-IED contribution to Info	IOT create awareness of and education	**X**		**X**	

		Operations and act as C-IED SME	for explosive hazards and actions on within the civilian community IOT prevent IED network from receiving local support IOT disrupt relationships between different IED networks and local power-brokers				
80	Info Ops	Coordinate C-IED Information operations with NGOs and UN ERW operations	IOT provide consistency of advice to retain credibility	**X**			
81	Info Ops	Provide C-IED specialist advice to Strategic Communications	IOT increase IED awareness and provide balanced reporting in media	**X**		**X**	
82	Info Ops	Support the quick reaction to IED incidents with meaningful Info Ops outputs.	IOT mitigate effect of publicity by IED networks.	**X**	**X**		
83	Info Ops	Monitoring and assessment of IED network Info Ops campaign	IOT mitigate effects of adversary Info Ops having a strategic effect	**X**			
84	Search/ Route Clearance	Issue and manage search and route clearance policy and SOPs	IOT ensure standard practice and understanding of search and route clearance operations	**X**	**X**		To include offensive and defensive search.
85	Search/ Route Clearance	Identify specialist search and route clearance capabilities by nation (incl host nation)	IOT ensure situational awareness of friendly forces capabilities	**X**	**X**		
86	Search/ Route Clearance	Direct and manage intelligence led search and route clearance activities within JOA	IOT make best use of search and route clearance resources.	**X**	**X**		
87	Search/ Route Clearance	Issue and manage direction for minimum standards of search training for deployed personnel	IOT improve friendly forces force protection capability		**X**	**X**	
88	Search/ Route Clearance	Generate search and route clearance capability within HN security forces.	IOT generate host nation capability to detect IEDs and caches.	**X**	**X**	**X**	To include plan for training, equipment, management, mentoring and tasking.
89	Search/ Route Clearance	Ensure search and route clearance reports are incorporated into the C-IED database	IOT inform future operations and maintain situational awareness in AOR	**X**	**X**		

90	Training + LI/LL	Plan, direct and support alliance staff C-IED training and input to lessons learned	IOT develop C-IED capability within the staff	**X**	**X**	**X**	
91	Training + LI/LL	Plan, direct and support alliance C-IED force protection training and input to lessons learned	IOT develop C-IED force protection capability		**X**	**X**	
92	Training + LI/LL	Plan, direct and support alliance C-IED Attack the network training and input to lessons learned	IOT develop C-IED Attack the network capability	**X**		**X**	
93	Training + LI/LL	Coordinate C-IED input into RSOI training	IOT ensure situational awareness of all forces entering JOA	**X**	**X**	**X**	
94	Training + LI/LL	Plan, support and mentor HN Staff C-IED training	IOT develop C-IED capability within the HN staff	**X**	**X**	**X**	
95	Training + LI/LL	Plan, support and mentor HN C-IED force protection training	IOT develop HN C-IED force protection capability		**X**	**X**	
96	Training + LI/LL	Plan, support and mentor HN C-IED Attack the Network training	IOT develop HN C-IED Attack the Network capability	**X**		**X**	
97J	Training + LI/LL	Coordination of training for C-IED database and application users	IOT fully exploit capabilities of databases and software	**X**		**X**	
98	Training + LI/LL	Establish and maintain a C-IED lessons identified / lessons learned database	IOT comply with NATO LL policy to improve operational understanding and execution.	**X**	**X**	**X**	
99	CIMIC	Coordinate planning of C-IED activities in support of reconstruction operations C-IED Info Ops IEDD capability ERW Clearance Explosive hazard education	IOT support indirect C-IED operations IOT provide security to CIMIC operations	**X**	**X**	**X**	

C-IED INPUTS AND SPECIFIED TASKS WITHIN HQs

1. In order to achieve the specified tasks in Annex A, staff will need to identify inputs and design processes within the HQ. The relevant functions that have a contribution to C-IED are:

a. Information and Knowledge Management (IKM)

b. Intelligence Fusion and Analysis.

c. ISR.

d. Exploitation

e. Targeting.

f. Operations and Plans.

g. Force Protection.

h. EOD – including ERW and IEDD.

i. Info Ops.

j. Search and Route Clearance.

k. Training and Lessons Identified/Learned.

l. Civil-Military Co-operation (CIMIC).

2. Appendices 1-12 of this Annex show the links between inputs required for each of these functional areas in order to carry out the specified tasks (as per Annex A). As with the tasks the inputs will differ within nations or staff HQs according to structure, staff functionality and missions and the input lists are intended as guidance for HQs to develop their own procedures. Each function may be liable to provide specialist input to briefing senior staff but as this information will be from across the relevant function it has not been included as a unique flow diagram.

3. **C-IED Coordination Function**. The C-IED Coordination function is the primary enabler to effective production of C-IED SPECIFIED TASKS. This responsibility usually sits within the Operations and planning staffs and so has been included in Appendix 6.

Appendices:

1. Information and Knowledge Management
2. Intelligence Fusion and Analysis.
3. ISR
4. Exploitation

5. Targeting.
6. Operations and Plans.
7. Force Protection.
8. EOD – including ERW and IEDD.
9. Information Operations.
10. Search and Route Clearance
11. Training and Lessons Identified/Learned.
12. CIMIC.

INFORMATION AND KNOWLEDGE MANAGEMENT FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • Intelligence Reports • Advice on classifications/releasability	EOD • EOD/ERW reports • IEDD reports and storyboards • IED analysis assistance	Training • Lessons Learned databases • Input into and from training activities
Exploitation • Level 1 and 2 Exploitation reporting requirements	Search • Search reports	CIMIC • KLE Reporting
Operations • OP SITREPS and reports • Operational context and picture	Plans • Information and Knowledge Management requirements for operational planning • Development of reporting policy	Liaison Activities • All engagement reports and returns (civil and military) • Reports from and to HN LOs • Access to other unit/national databases • Agreement on terminology Senior national representative advice on national caveats / releasability
Info Ops • Information Management requirements for Info Ops	CIS • Database technical and management support • Database Connectivity support	

EXAMPLE SPECIFIED TASKS

Create and manage fit for purpose C-IED database	Create a common lexicon of C-IED terminology	Monitor and collate IED incidents by location, type, target and enemy TTP

INTELLIGENCE FUSION AND ANALYSIS FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • Threat assessments and reports • Pattern Analysis and predictive modeling • Advice on classifications/releasability • Fused Intelligence – SIGINT, HUMINT, IMINTetc.	Operations • OP SITREPS and reports • Operational context and picture EOD • EOD and IEDD reporting	CIMIC • Reports on KLE and reconstruction and development projects.
Exploitation • Level 1 and 2 Exploitation reports and expert technical advice • Identification of exploitation opportunities • Links and reports to external exploitation agencies ISR • Results from C-IED interpretation of ISR products • ISR Priorities	Geo • Terrain analysis and assessments Plans • C-IED PIR and CCIRs requirements for operational planning and IPB • Operational planning detail to inform threat assessment to future ops	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Political and diplomatic advice • External to JOA situation awareness Training and Education • Share information in LL data base

EXAMPLE SPECIFIED TASKS

Coord of C-IED IPB	Predict and identify IED network activities and patterns of behavior: (financing, recruiting, training and IED construction)	Predict and identify IED network personnel and personal relationships	Predict and identify IED network Lines of communication (IED material ,supply sources, supply routes, communication networks, facilities)	Analyse IED network TTPs to understand tactical emplacement and targeting methods
Make assessments on the current and future threats and their effect on ops	Link intelligence detection assets and other intelligence sources to IED related PIRs and decision points	Coordinate the fusion of exploitation inputs with other INTEL	Coordinate the communication of C-IED intelligence to external agencies as appropriate	

ISR FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • Threat assessments and reports	Operations • OP SITREPS and reports • Operational context and picture	Plans • ISR Intelligence requirements for operational planning and IPB
Exploitation • Level 1,2 and 3 exploitation reports and expert technical advice • Identification of exploitation opportunities	EOD • EOD Reporting Technical Assistance to Intel staff IEDD • IEDD reporting	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Legal advice • External to JOA situation awareness
ISR • Results from C-IED interpretation of ISR products • ISR Priorities	Geo • Terrain Analysis and assessment	Coord RFI and tasks of other Joint ISR assets

EXAMPLE SPECIFIED TASKS

Contribute to planning of ISR asset usage	Assistance with interpreting C-IED related SIGINT data regarding IED network communications	Contribute to HUMINT intelligence focusing and interpretation	Contribute to OSINT intelligence focusing and interpretation

EXPLOITATION FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • Threat assessments and reports • C-IED exploitation requirements to support wider J2 area	EOD • EOD Reporting • Technical and trials assistance • IEDD reporting • Technical and trials assistance	Information + Knowledge Management • Coordination and integration of databases • Forum for the dissemination of threat data
Exploitation • Existing level 1, 2 and 3 exploitation reports within and outside JOA.	Logistics • Support for movement of exploitable material • Input from J4 MED reports on injury types	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Legal advice • External to JOA situation awareness
Operations • OP SITREPS and reports • Operational context and picture	Plans • Exploitation requirements for operational planning and IPB	
Geo • Terrain Analysis and assessment	Training • WIT awareness training requirement within wider C-IED training	

EXAMPLE SPECIFIED TASKS

Define Level 2 Exploitation priorities	Direct and monitor WIT asset lay-down within AOR			Input into Biometric Working Groups	Coordinate and manage exploitation RFIs
Issue and manage technical and tactical exploitation policy for Level 1-3.	Fuse and analyse exploitation reports to identify sources of components	Provide specialist C-IED support to Media Exploitation	Develop and publish HN releasable exploitation reports	Writing or disseminating C-IED Flash Reports or Awareness reports	Monitor the process of IED material through exploitation chain
Issue and manage biometric exploitation policy for Level 1-3.	Write and issue Weapons Intelligence (Level 1 exploitation) SOPs	Tasking and recovery policy for WIT or national equivalent.	Monitor technical exploitation reports from other theatres	Create a Level 2 exploitation capability within theatre	Coordinate external expertise on weapons and armour

Develop links between Level 2 + 3 facilities including reach-back and information sharing facilities.	Identify and define differing capabilities within national Weapons Intelligence Teams (WIT) or national equivalent.	Liaise with HN authorities security services to integrate HN exploitation capability	Undertake technical exploitation of IED related components and identify external sources of IED components
Provide feedback to tactical units of biometrics and exploitation successes.	Ensure exploitation guidelines are in line with relevant judicial authorities	Develop WIT awareness training within C-IED training	Recover biometrics and input into biometric database

TARGETING FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • IED network intelligence assessments and reports • IED network pattern and link analysis COIs and corroborating intelligence	Operations • OP SITREPS and reports • Operational context and picture	Training + LL • Lessons Learned databases • Input into and from training activities
Exploitation • Technical and Biometric exploitation assessments • Identification of exploitation opportunities	Geo • Terrain analysis, change detection and geospatial support	Liaison Activities • Coordination to and from other units, formations, organisations and agencies • Reports to and from HN LOs • Advice from LEGAD • Political and diplomatic advice • Liaison with SOF •
ISR • C-IED requirements and assistance to enemy network detection, identification and monitoring	Plans • Targeting requirements for operational planning	

EXAMPLE SPECIFIED TASKS

Contribute to targeting process and prioritisation of IED network activities and patterns of behaviour (financing, recruiting, training and IED construction)	Contribute to targeting process and prioritisation of IED network personnel	Predict and identify IED network lines of communication (IED material supply sources, supply routes. communication networks, facilities)

OPERATIONS AND PLANS FUNCTIONAL INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • Threat assessments and reports	EOD • EOD and IEDD Reporting and support • Advice on pre-detonation + BIP-ing of IEDs	Training + LL • SPECIFIED TASKS form Lessons learned process
Exploitation • Level 1 and 2 Exploitation reports and expert technical advice • Exploitation Policy within J3 priorities	Geo • Terrain analysis, assessments and geospatial reports	CIMIC • Reports on KLE and reconstruction and development projects.
ISR • Support from ISR asset on operations	Search and Route Clearance • Advice and support from search and route clearance specialists	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Political and diplomatic advice • Advice from LEGAD • Cultural advisors • Liaison with SOF • Liaison with CIMIC
Operations • OP SITREPS and reports • Operational context and picture • Prioritisation of resources	AIR • Support from AIR component for planning operations • Advice on air platform pre-detonation of IEDs	
Force Protection • Integration of ROE/EOF policy with ops	Plans • C-IED requirements for operational planning	

EXAMPLE SPECIFIED TASKS

Provide lead, direction and coordination for C-IED related activities within all staff branches	Assessment and evaluation of Friendly Forces and HN movement TTPs	Establish and manage guidelines on pre-detonation and BIP-ing of IEDs	Provide general direction for the prioritisation of C-IED intelligence gathering opportunities with tactical operations
Coordinate C-IED related input into routine SITREPs	Plan operations to deny IED network freedom of movement	Coordinate C-IED contributions to OPLANs and FRAGOs as required	

FORCE PROTECTION FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • Threat assessments and reports	AIR • Advice on air platform assets and capabilities	CIS and COMMS • ECM Spectrum management policy
Exploitation • Level 1 and 2 Exploitation reports and expert technical advice • Exploitation trials reports • RCIED threat frequency list	Search and Route Clearance • Advice and support to search training and route clearance capabilities	Training + LL • Specific Force protection SPECIFIED TASKS form Lessons learned process
Operations • OP SITREPS and reports • Operational context and picture	ECM maintenance • Technical input, advice and support from FP ECM equipment maintainers	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Specialist scientific advice • Advice from LEGAD
Geo Terrain analysis, assessments and geospatial support	Plans • C-IED force protection (incl EW) requirements for operational planning	

EXAMPLE SPECIFIED TASKS

Advise on EOF measures to counter Suicide IED according to specific threat criteria	Prediction and dissemination of likely IED targets and locations	Monitor the RCIED threat frequency list.	Issue and manage policy for force protection EW equipment use within friendly forces	Monitor and evaluate EW force protection equipment and TTPs effectiveness in relation to the threat
Train and enable tactical units to undertake geospatial analysis	Monitor and evaluate friendly forces force protection capabilities	Identify EW force protection characteristics for national, NATO + civilian EW systems.	Issue and maintain the policy on EW pre-detonation of IEDs	

EOD - IEDD/ERW FUNCTIONAL INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • Threat assessments and reports • Engineer Intelligence on ERW	Info Ops • Mine awareness requirements to Info ops campaign	Training + LL • HN training strategy
Exploitation • Level 1 and 2 Exploitation reports and expert technical advice	Search and Route Clearance • Search support to EOD planning and operations	CIMIC • ERW requirements for CIMIC projects and activities
Operations • OP SITREPS and reports • BIP Policy • ERW requirements for operations	EOD • ERW • Technical support to management of civilian ERW operations • IEDD reporting • Support to HN for IEDD operations.	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Specialist technical and scientific advice • Advice from LEGAD • NGO/ERW Agency Liaison
Engr Geo • to mine and UXO awareness and training • Manoeuvre support and clearance coordination support	Plans • IEDD and ERW requirements for operational planning	

EXAMPLE SPECIFIED TASKS

Establish and maintain situational awareness of ERW locations, demining and clearance operations within the JOA	Develop and manage mine and UXO awareness training programmes and educate within FF and the populace	Plan and manage ERW clearance and set priorities	Issue and manage EOD and IEDD policy	Issue tasking and recovery policy for EOD/IEDD assets within AOR	Monitor EOD reports and evaluate IEDD TTPs in relation to threats
Issue and manage ERW policy	Generate HN capability to deal with ERW	Ensure ERW data is incorporated into the C-IED database	Identify EOD/IEDD capabilities by nation (incl host nation)	Direct force lay-down of EOD/IEDD assets within AOR	Generate and monitor EOD capability within HN

INFORMATION OPERATIONS FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • IED network threat assessments and reports • Guidance on classifications and releasability	EOD • EOD technical support and assistance IEDD • IEDD Technical support and assistance to HN for IEDD operations. •	Finance • Financial support and guidance
Operations • OP SITREPS and reports • Operational context and picture	Plans • C-IED Info Ops requirements for operational planning	CIMIC • Coordination of Info ops input to CIMIC activities and projects
Info Ops • Info operations requirements to meet Strategic Communications policy and direction • Measurement of effectiveness of Info ops campaigns	Training + LL • SPECIFIED TASKS from Info Ops Lessons Learned process	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Political and diplomatic advice • Cultural advisors • Liaison with SOF

EXAMPLE SPECIFIED TASKS

Coord C-IED contribution to Info Operations and act as C-IED SME	Coordinate C-IED Information operations with NGOs and UN ERW operations	Provide C-IED specialist advice to Strategic Communications	Support the quick reaction to IED incidents with meaningful Info Ops SPECIFIED TASKS.	Monitoring and assessment of IED network Info Ops campaign

SEARCH AND ROUTE CLEARANCE FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • IED network threat assessments and reports	EOD • EOD technical support and assistance • EOD support to search and route clearance planning • IEDD reporting • Support to HN for IEDD operations.	Training + LL • SPECIFIED TASKS from search and route clearance Lessons Learned process
Exploitation • Level 1 and 2 exploitation reports • Information on NAIs	Geo • Terrain analysis,	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs
ISR • Support from ISR products and analysis	Movement • MSR use planning requirements • Convoy logistic patrol FP capabilities	
Operations • OP SITREPS and reports • Operational context and picture • Search requirements for offensive and defensive operations	Plans • C-IED Info Ops requirements for operational planning	

EXAMPLE SPECIFIED TASKS

Issue and manage search and route clearance policy and SOPs	Identify specialist search and route clearance capabilities by nation (incl host nation)	Direct and manage intelligence led search and route clearance activities within JOA	Issue and manage direction for minimum standards of search training for deployed personnel	Generate search and route clearance capability within HN security forces	Ensure search and route clearance reports are incorporated into the C-IED database

TRAINING AND LESSONS LEARNED FUNCTIONAL INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • IED network threat assessments and reports	EOD • EOD technical support and assistance to training IEDD • IEDD Technical support and assistance to HN for IEDD operations and training.	CIS • Support to C-IED database training
Exploitation • Level 1 and 2 exploitation reports • Technical support to training	Force Protection • Support to basic search and ECM training	Training + LL • SPECIFIED TASKS from Info Ops Lessons Learned process • HN training policy and direction
Operations • OP SITREPS and reports • Operational context and picture • Prioritisation of resources to support training	Plans • HN C-IED training requirements for operational planning	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Cultural advisors

EXAMPLE SPECIFIED TASKS

Plan, direct and support alliance staff C-IED training and input to lessons learned	Plan, direct and support alliance C-IED Attack the network training and input to lessons learned	Plan, support and mentor HN Staff C-IED training	Plan, support and mentor HN C-IED Attack the Network training
Plan, direct and support alliance C-IED force protection training and input to lessons learned	Coordinate C-IED input into RSOI training	Plan, support and mentor HN C-IED force protection training	Coordination of training for C-IED database and application users

CIVIL MILITARY OPERATIONS FUNCTION INPUTS AND SPECIFIED TASKS

EXAMPLE INPUTS

Intelligence • IED network threat assessments and reports	Info Ops • Coordination of Info Ops strategy and regional campaigns	Finance • Financial support and guidance
Operations • OP SITREPS and reports • Operational context and picture • Prioritisation of resources to support training	EOD • ERW and IED awareness and education support • Information on ERW and IED concentrations	Liaison Activities • Coord with other units, formations, organisations and agencies • Reports from and to HN LOs • Cultural advisors • Political and Diplomatic Advisors
Geo • Geospatial and geological support	Plans • C-IED CIMIC requirements for operational planning	
Force Protection • Support to basic search and ECM training	Training + LL • SPECIFIED TASKS from CIMIC Lessons Learned process • Advice on C-IED training requirements for workforce	

EXAMPLE OUTPUT

Coordinate planning of C-IED activities in support of CIMIC operations

C-IED Info Ops
IEDD capability
ERW Clearance
Explosive hazard education

C-IED STRUCTURES AND RESPONSIBILITIES WITHIN HQs

1. C-IED activity supports the mission and may not require a dedicated C-IED staff branch as it is an activity that should be undertaken throughout the HQ staff branches. There may be occasions, such as when initially developing capability, that a dedicated Task Force within the HQ staff is the most effective method of delivering the require effect, but these should generally be of short duration and must not work in isolation. This should be part of the responsibilities of the nominated C-IED OPR.

2. A fully resourced and functioning staff may require no independent C-IED personnel (less the C-IED OPR) as all the functions and specified tasks are allocated to existing personnel within the traditional staff branches and incorporated in existing staff processes.

C-IED PROCESSES WITHIN THE STAFF

3. The processes required to turn inputs into specified tasks will also differ within every nation or staff HQ although there are some forum or media that are likely to be utilised within these processes. The main tools or media that should be incorporated into HQ C-IED processes are:

a. Routine Staff Procedures.

b. Written reports.

c. Planning, Working, Focus or Coordination groups.

d. Liaison Activities.

e. Information System databases and applications.

f. Routine or bespoke briefings and updates.

C-IED GROUPS WITHIN THE HQ STAFF

4. In order to direct, focus and manage C-IED effort within HQs there is often a requirement to establish and hold groups, meetings or forums to deliver specific outputs. Individual HQ will have different requirements according to structure, mission and existing C-IED capability within the staff. There are a number of different C-IED related groups that may be formed depending upon the operational situation and circumstances. These will serve to develop and deliver C-IED capability both within the staff and for the wider force as follows:

a. C-IED Steering Group.

b. C-IED Working Group.

c. C-IED Focus Group.

d. C-IED Coordination Group.

5. Generic aims, tasks and outline terms of reference are suggested although commanders should develop their own C-IED architecture within the HQs to meet the requirements taking account of existing working groups and board structures. Lead personnel and members are suggested where applicable but may also require analysis and adjustment to ensure C-IED forums are effective.

6. The level of support within staff branches, e.g. the number of intelligence analysts tasked to monitor IED-related information alongside their normal duties, will vary depending upon the appropriate threat response.

7. **C-IED Steering Group**:

a. **Aims**: To provide C-IED strategy, policy and direction across the staff.

b. **Outputs and Terms of Reference**: Develop policy on C-IED capability within the staff based on the commander's intent. It will normally be required when developing a capability or in preparation for a specific mission. Direction will be given to C-IED Working Groups. The C-IED Steering Group function may not be a standalone grouping but an agenda item on a wider senior command forum.

c. **Lead**: COMD/COS.

d. **Members**: Chiefs of the staff branches within the HQ.

8. **C-IED Working Group**:

a. **Aims**: To direct methodology, delegate responsibilities and allocate resources according in order to meet the aims of the C-IED Steering Group.

b. **Outputs and Terms of Reference**: Typically used to develop C-IED capability across the force with a wide remit (DOTMLPFI). It will probably have executive powers to allocate resources and direct responsibility across the staff branches and may be permanent or temporary in nature.

c. **Lead**: Chief Operations

d. **Members**: Core representatives from:

(1) Operations
(2) Force Protection
(3) Info Ops
(4) JOC (situational information management)
(5) Operational Analysis
(6) Targeting
(7) Intelligence
(8) Technical Exploitation
(9) Biometric Exploitation
(10) Training
(11) IEDD (incl ECM matters)
(12) EOD (incl ERW)

(13) Search/Route Clearance

On-call representatives according to requirement:

(1) ISR
(2) LEGAD
(3) Provost
(4) CIMIC
(5) Geo
(6) Plans
(7) External agencies

9. **C-IED Focus Group**:

a. **Aim**: To focus on a specific area of C-IED in order to assist decision making or management of capability.

b. **Outputs and Terms of Reference**: It is likely that C-IED Focus Groups will be temporary in duration and have precise terms of reference in order to deliver specific outputs related to the specified tasks. Executive powers should be limited to these areas. Likely remits are to identify issues, provide recommendations to decision making or manage projects.

c. **Lead**: As directed according to the focus group aim. It is likely to be the lead/SME in a specialist function.

d. **Members**. As required to meet the output. It may include external personnel in order to leverage specialist expertise.

10. **C-IED Co-ordination Group**:

a. **Aim**: To coordinate C-IED information and actions within the staff in order to enable effective C-IED outputs.

b. **Outputs and Terms of Reference**: Usually a routine grouping which may form part of the battle rhythm. It is likely to have no executive power but should be able to make recommendations to amend communication or emphasis within the staff if required. This will be the main forum for ensuring that personnel undertaking C-IED work from across the staff branches are integrated and informed.

c. **Lead**: Chief Operations.

d. **Members**. Core representatives from:

(1) Operations
(2) Force Protection
(3) Info Ops
(4) JOC (situational information management)
(5) Operational Analysis
(6) Targeting
(7) Intelligence
(8) Technical Exploitation

(9) Biometric Exploitation
(10) Training
(11) IEDD (incl ECM matters)
(12) EOD (incl ERW)
(13) Search/Route Clearance

On-call representatives according to requirement:

(1) ISR
(2) LEGAD
(3) Provost
(4) CIMIC
(5) Geo
(6) Plans
(7) External agencies

CONTRIBUTIONS TO OTHER HQ STAFF GROUPINGS

11. As shown in the C-IED staff ‘specified tasks’ listing in Annex A to this handbook, input is required into numerous other staff groups or forums that may not be C-IED centric. HQ structures will vary and the names and functions of these forums will exist to meet specific requirements but some of the areas that require C-IED contribution are as follows:

a. Routine or specialist briefings to commanders.

b. ISR prioritisation.

c. Targeting.

d. Info Ops.

e. Force Protection.

f. Equipment Capability.

g. Exploitation.

h. Plans.

i. Biometrics INTEL /Biometric Enabling

j. NATO Force Training

k. Host Nation Training

l. CIMIC

m. ERW Programs

n. Lessons learned.

STAFF RESPONSIBILITIES

12. There should be no requirement for specific C-IED job descriptions within the staff and all responsibilities relating to C-IED specified tasks should be incorporated within the job descriptions of existing personnel. These specified tasks can be drawn from Annex A to his handbook. HQs should not attempt to incorporate all these tasks within the staff unless there is a clear requirement and where possible mission analysis should be undertaken to ensure the focus is relevant.

13. In order to enable individuals to deliver the required tasks within their C-IED responsibilities they must be able to access the required resources, either in the form of a product (inputs) or from access to relevant knowledge and expertise (enablers). Annex B to this handbook illustrates the inputs and possible enablers to each core and underpinning function in order to deliver to the specified tasks.

ANNEX D TO
ENCLOSURE 1 TO
5000 TSX 0170/TT-7579/SER: NU0462
DATED 10 AUG 11

C-IED RELATED TERMINOLOGY

This annex is designed to be an initial reference for staff undertaking C-IED staff activities. It comprises two sections:

Section 1 - Definitions

C-IED related definitions from reference publications as well as other definitions that are emerging or informal but in common use. Text *in italics* gives additional contextual information for the benefit of personnel who may be less familiar with C-IED and IED-related terminology, some of which is necessarily technical in nature.

Section 2 - Acronyms & Abbreviations

General military and technical acronyms and abbreviations that are likely to be encountered by staff performing C-IED activities.

SECTION 1 - C-IED RELATED DEFINITIONS

Asymmetric threat
A threat emanating from the potential use of dissimilar means or methods to circumvent or negate an opponent's strengths while exploiting his weaknesses to obtain a disproportionate result. [AAP-6 (2008)]

ARTEC (Armaments and Technology)
French terminology for level 1 weapons intelligence exploitation team although also undertakes non-C-IED tasks. (Informal)

Complex attack
A complex attack is an attack that involves the employment of more than one IED, or an attack using an IED in conjunction with small arms fire, direct, or indirect fire weapons. Complex attack scenarios often involve significant insurgent forces planning, and are often conducted in order to fix security forces within the kill zone(s).Complex attacks may also involve the use of multiple IEDs in order to target personnel responding to an initial attack. (Informal)

Conventional Munitions Disposal (CMD)
The detection, identification, render safe and final disposal of conventional military munitions that have not been incorporated in IEDs (Informal)

Counter-IED (C-IED)
The collective efforts at all levels to defeat the IED System in order to reduce or eliminate the effects of all forms of IEDs used against friendly forces and non-combatants according to the mission. (AJP 3.15).

Counter-RCIED Electronic Warfare (CREW)
US terminology for Force Protection ECM/EW. (Informal)

Daisy Chain
An IED with multiple linked main charges designed to function simultaneously when the IED is initiated. (Informal)

Electronic Counter Measures (ECM)
That division of electronic warfare involving actions taken to prevent or reduce an adversary's effective use of the electromagnetic spectrum (EMS) through the use of electromagnetic energy. There are three sub-divisions of ECM: electronic jamming, electronic deception and electronic neutralisation. [AAP-6 (2008)]
In the context of C-IED, ECM generally refers to RF inhibition (jamming) equipment used for force protection purposes. (Informal)

E**lectronic jamming**
The deliberate radiation, re-radiation or reflection of electromagnetic energy with the object of impairing the effectiveness of hostile electronic devices, equipment or systems. [AAP-6 (2008)]

E**lectronic neutralization**
In electronic countermeasures, the deliberate use of electromagnetic energy to either temporarily or permanently damage enemy devices which rely exclusively on the electromagnetic spectrum. [AAP-6 (2008)]

Electromagnetic spectrum
The entire and orderly distribution of electromagnetic waves according to their frequency or

wavelength. The electromagnetic spectrum includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays. (AcomP-01)

Electronic Warfare (EW)
Military action to exploit the electromagnetic spectrum encompassing: the search for, interception and identification of electromagnetic emissions, the employment of electromagnetic energy, including directed energy, to reduce or prevent hostile use of the electromagnetic spectrum, and actions to ensure its effective use by friendly forces. [AAP-6 (2008)]

Event geometry
A description of how an IED system was emplaced, its orientation, the distance to the target, line of sight etc. (Informal)

Explosive Ordnance (EO)
All munitions containing explosives, nuclear fission or fusion materials and biological and chemical agents. This includes bombs and warheads; guided and ballistic missiles; artillery, mortar, rocket and small arms ammunition; all mines, torpedoes and depth charges; pyrotechnics; clusters and dispensers; cartridge and propellant actuated devices; electro-explosive devices; clandestine and improvised explosive devices; and all similar or related items or components explosive in nature. [AAP-6 (2008)]

Explosive Ordnance Disposal (EOD)
The detection, identification, on-site evaluation, rendering safe, recovery and final disposal of unexploded explosive ordnance. It may also include explosive ordnance, which has become hazardous by damage or deterioration. [AAP-6(2008)]

Explosive Remnants of War (ERW)

In the context of C-IED, ERW refers to Explosive Remnants of War - those explosive items and munitions that remain in a theatre, often under little or no control, from previous conflicts. (Informal)
Note: The alternative abbreviation of ERW refers to its AAP-15 (2008) definition of Enhanced-Radiation Weapon (effectively a neutron weapon and not C-IED related).

False IED
An item that is reported in good faith as being an IED but is actually an innocuous item (Informal)

Firing switch
The switch used to initiates the IEDs. IEDs are often (but not always) referred to by type of firing switch (Pressure Plate IEDs, Time IEDs etc) (Informal)

Hoax
A simulated IED or IED event that is designed to disrupt operations, force coalition troops to deploy countermeasures, used to observe friendly TTPs or to otherwise develop a come-on situation from which an attack can be mounted. (Informal)

Hotspot
A point or area that has repeatedly been used as a location for IEDs. Some formations and operations give specific criteria for the definition of hotspots but these are local definitions. Note the difference between a hotspot and a Vulnerable Point (VP) is that IED will always have occurred in a hotspot whereas a VP may be a hotspot or a potential hotspot. (Informal)

Hybrid threat
The threat posed by any adversary with the ability to simultaneously employ conventional and non conventional means adaptively, in pursuit of their objectives. (Working definition in use with SACT Counter Hybrid Threats IPT)

Improvised Explosive Device (IED)
A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from non-military components. [AAP-6 (2008)]

Improvised Explosive Device Disposal (IEDD)
IEDD is the location, identification, rendering safe and final disposal of IEDs. (ATP-72)

IED system
An IED system is a combination of humans, processes and, materiel consisting of one or more opponent's entities with all related equipment, technology, skills, knowledge, personnel, and means of delivery and employment. (AJP 3.15)

Information Operations (Info Ops)
Actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, command and control networks and communications and information networks while exploiting and protecting one's own information and/or information networks. There are two main categories of Info Ops: defensive information operations and offensive information operations, depending on the nature of action involved. (MC 422)

Information
Unprocessed data of every description, which may be used in the production of intelligence. [AAP-6 (2008)]

Initiator
The initiator is the term given to the initial explosive item within an IED or conventional munitions. This is usually a detonator (or blasting cap) for high explosive charges but can also be a squib type item to initiate low explosive chains.

Initiation
The action of a device used as the first element of an explosive train which, upon receipt of the proper impulse, causes the detonation or burning of an explosive item. [AAP-6(2008)]

Operational level
The level at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objectives within theatres or areas of operations. [AAP-6(2008)]

Person-Borne IED (PBIED)
An IED worn or carried by a person who acts or serves as the delivery or concealment method for the device. A PBIED is often initiated by the person wearing or carrying the device, but remote / command or time initiation switches can also be included. These will normally be suicide IEDs but not always as sometimes the person is unwilling or incapable of undertaking the attack.

Render Safe Procedures (RSP)
The portion of the explosive ordnance disposal procedures involving the application of special explosive ordnance disposal methods and tools to provide for the interruption of functions or

separation of essential components of unexploded explosive ordnance to prevent an unacceptable detonation. (ATP-72)

Route Check[1]
The conduct of detailed reconnaissance and search procedures at specific points along a route by units utilising tactical formations and specifically issued search equipments. If IED indicators or suspected IEDs are observed, the unit will initiate 4Cs and IED reporting procedures. (Informal)

Route Clearance[1]
In land operations, the detection and if found, the identification, marking and neutralization, destruction or removal of mines or other explosive ordnance, improvised explosive devices and booby traps threatening a defined route to allow a military operation to continue with reduced risk. Note: Route clearance is normally conducted by military units. [AAP-6(2008)]

Route Search[1]
Route Search differs from Route Check or Route Clearance in that it is normally conducted by Advanced or Intermediate Search trained personnel using additional specialist equipment. A cordon may be required to provide security so that the Search Teams' primary focus is on searching. The entire route is normally searched rather than specific points; the result is that there is a higher level of assurance that the route can be safely trafficked. [ATP-73-1 (2006)]

Rules of Engagement (ROE)
Directives issued by competent military authority which specify the circumstances and limitations under which forces will initiate and/or continue combat engagement with other forces encountered. [AAP-6(2008)]

Search (Military)[1]
The management and application of systematic procedures and appropriate equipment to locate specified targets in support of military operations. Specified targets may include people, information and material resources employed by an adversary. Military search is subcategorised as Advanced and Intermediate, which require formal training, and Basic. [ATP 73-1 (2006)]

Tactical Level
The level at which activities, battles and engagements are planned and executed to accomplish military objectives assigned to tactical formations and units. [AAP-6(2008)]

Unexploded Explosive Ordnance (UXO)
Explosive ordnance which has been primed, used, armed or otherwise prepared for action, and which has been fired, dropped, launched, projected or placed in such a manner as to constitute a hazard to operations, installations, personnel or material and remains unexploded either by malfunction or design or for any other cause. [AAP-6(2008)]

Vulnerable Point (VP)
Vulnerable points are those locations where it is particularly advantageous for an adversary to place an explosive device or booby trap than elsewhere. [ATP 73-1 (2006)] *In the context of C-IED, a vulnerable point is a specific location that is assessed to be a likely site for IEDs to be emplaced because of terrain, channelling, pattern-setting or the enemy's previous employment.*

Weapons Intelligence Team (WIT)
WIT is a pool of specialists that investigate IED incidents when tasked. Their main task is to gather, analyse, collate and distribute technical/tactical intelligence and forensic evidence, in support of the exploitation KOA. (AJP 3.15)

[1] Search definitions and procedures vary between nations, units and equipment used. Where possible search operations should be planned in the terms of levels of risk, threat and assurance in order to provide the desired effect.

SECTION 2 - C-IED RELATED ACRONYMS & ABBREVIATIONS

ANFO	Ammonium Nitrate Fuel Oil (a type of Home-made explosives)
AP	Anti-personnel
AT	Anti-tank (usually landmine)
AJP	Allied Joint Publication
BCIED	Biological and Chemical Improvised Explosive Device
BCMD	Biological and Chemical Munitions Disposal
BDA	Battle Damage Assessment
BIP	Blow in Place
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CEXC	Combined Explosive eXploitation Cell (in-theatre Level 2 exploitation organisation)
C-IED	Counter Improvised Explosive Device
CIMIC	Civil-Military Cooperation
CMO	Civil-Military Operations
CIS	Communications and Information Systems
CJTF	Combined Joint Task Force
CMD	Conventional Munitions Disposal
CONOPS	Concept of operations
CPOE	Comprehensive Preparation of the Operating Environment (aka IPB)
CREW	Counter-RCIED Electronic Warfare
CWIED	Command Wire IED
DFFC	Directional Focussed Fragmentation Charge
DJSE	Deployed Joint Staff Element
DTMF	Dual-Tone Multi-Frequency (a technique used in RCIEDs)
ECM	Electronic Counter-Measures
EDD	Explosive Detection Dog (see also MDD and MWD)
EFP	Explosively Formed Projectile/Penetrator
EOC	Explosive Ordnance Clearance
EOD	Explosive Ordnance Disposal
EOF	Escalation of Force
ERW	Explosive Remnants of War
EW	Electronic Warfare
FP	Force Protection
HAZMAT	Hazardous Material
HE	High Explosive

HME	Home-Made Explosive
HMTD	Hexamethylene triperoxidediamine (explosive)
HMX	High-Melt Explosive (also known as High Melting eXplosive, High-velocity Military eXplosive, or High-Molecular-weight rdX) - Octahydro-1,3,5,7-tetranitro-1,3,5,7-tetrazocine
HN	Host Nation
HNSF	Host Nation Security Force
HQ	Headquarters
HRF	High Readiness Forces
HRS	High Risk Search
HUMINT	Human Intelligence
IED	Improvised Explosive Device
IEDD	Improvised Explosive Device Disposal
INFOOPS	Information operations
INFOSEC	Information security
IPB	Intelligence Preparation of the Battlespace (now known as CPOE)
ISR	Intelligence, Surveillance, Reconnaissance
JMETL	Joint Mission Essential Task List.
JCB	Joint Co-ordination Board.
JFC	Joint Force Commander
JOA	Joint Operational Area
JOPG	Joint Operational Planning Group
JTFC	Joint Task Force Commander
JTFHQ	Joint Task Force Headquarters
KLE	Key Leadership Engagement
LI	Lessons Identified
LL	Lessons Learned
LOC	Line of Communication
MDD	Mine Detection Dog (see also EDD and MWD)
MWD	Military Working Dog (may or may not be explosive detection trained). See also EDD and MDD)
NAI	Named Area of Interest
NEC	Net Explosive Content
NEQ	Net Explosive Quantity
NG	Nitro-glycerine (explosive)
NGO	Non-Governmental Organisation

NRF	NATO Response Force
OGA	Other Government Agencies
OGD	Other Government Departments
OPR	Officer of Primary Responsibility
PBIED	Person-Borne IED
PETN	Pentaerythritol tetranitrate (explosive)
PIR	Passive Infra-Red
PPIED	Pressure Plate IED
PSYOPS	Psychological operations
RCIED	Radio Controlled IED
RCP	Route Clearance Package
RDX	Research Department eXplosive (cyclotromethylenetrinitramine)
REST	Royal Engineer Search Team (UK advanced search capability)
RF	Radio Frequency
RFI	Request For Information
ROE	Rules Of Engagement
RSOI	Reception, Staging, Onward movement and Integration
RSP	Render Safe Procedure(s)
SIED	Suicide IED
SOF	Special Operations Forces
SOP	Standard Operating Procedure
SSE	Sensitive Site Exploitation
STANAG	NATO Standardisation Agreement
SVBIED	Suicide Vehicle Borne IED
TATP	Triacetone triperoxide (Explosive)
TCN	Troop Contributing Nation
TIM	Toxic Industrial Materials
TNT	Trinitrotoluene (explosive)
TTP	Tactics, Techniques and Procedures
VBIED	Vehicle Borne IED
VOIED	Victim-Operated IED
WBIED	Water-Borne IED
WIS	Weapons Intelligence Section (UK terminology for WIT)
WIT	Weapons Intelligence Team

ANNEX E TO
ENCLOSURE 1 TO
5000 TSX 0170/TT-7579/SER: NU0462
DATED 10 AUG 11

C-IED RELATED REFERENCES

This annex provides some of the reference publications which may be useful to staff in creating their own C-IED capability or input into operational planning:

AAP-6, NATO Glossary of Terms and Definitions (English and French)

AAP-15, NATO Glossary of Abbreviations Used in NATO Documents and Publications

AEODP-3(A), Principles of Improvised Explosive Device Disposal

AEODP-3(B) Vol1+2 Interservice Improvised Explosive Device Disposal Operations on Multinational Deployments

AJP-01(C), Allied Joint Doctrine

AJP-2, Allied Joint Intelligence, Counter Intelligence and Security Doctrine

AJP-2.1, Intelligence Procedures

AJP-2.2, Counter Intelligence and Security Procedures

AJP-2.3, Allied Joint Doctrine for Human Intelligence

AJP-2.5 Allied Joint Doctrine for Captured Persons, Materiel and Documents

AJP-3(A), Allied Doctrine for Joint Operations

AJP 3.2 Allied Joint Doctrine for Land Operations

AJP 3.4.1 Allied Joint Doctrine for Peace Support Operations

AJP 3.4.4 Allied Joint Doctrine for Counter-Insurgency

AJP 3.5 Allied Joint Doctrine for Special Operations

AJP-3.6(A), Allied Joint Electronic Warfare Doctrine

AJP 3.9 Allied Joint Doctrine for Joint Targeting

AJP 3.10 Pre-Ratification draft Allied Joint Doctrine for Information Operations

AJP 3.10.1 Psychological Operations

AJP 3.12, Allied Doctrine for Military Engineer Support to Joint Operations

AJP 3.14 Allied Joint Doctrine for Force Protection

AJP 3.15A Allied Joint Doctrine for Countering IEDs

AJP-5 Allied Joint Doctrine for Operational Planning

AJP-9 NATO Civil-Military Co-operation Doctrine

ATP-72 Inter-service Explosive Ordnance Disposal Operations on Multinational Deployments

ATP-73-1 Military Search

STANAG 2294 – C-IED Training Standards