Releaseable to Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland

STANDARDS RELATED DOCUMENT

AEP-4803.1

NATO RADIO-CONTROLLED IED DATABASE CONCEPT OF EMPLOYMENT

EDITION A VERSION 2
APRIL 2020

NORTH ATLANTIC TREATY ORGANIZATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

20 April 2020

1. The enclosed Standards Related Document, AEP-4803.1, Edition A, Version 2, NATO RADIO-CONTROLLED IED DATABASE CONCEPT OF EMPLOYMENT, which has been approved in conjunction with AEP-4803 by the nations in the NAFAG, is promulgated herewith.

2. AEP-4803.1, Edition A, Version 2 is effective upon receipt and supersedes aep-4803.1, Edition A, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

NATO Team of Experts (ToE) on Electronic Countermeasures (ECM) against Radio Controlled Improvised Explosive Devices (RCIED)

NATO RCIED DATABASE

CONCEPT OF EMPLOYMENT
FINAL v2.2

Dec 2019

Keywords: RCIED DB, BICES, NATO ToE on ECM against RCIED

Abstract

The Concept of Employment (CONEMP) for the RCIED DB capability is intended as a user-oriented document that describes the anticipated operational employment and characteristics of the system to be developed by the NATO ToE on ECM for RCIED and NCI Agency in support of NATO capability requirements and interoperability objectives. The deployment of the RCIED DB onto the BICES network will provide the initial operating capability to NATO nations and 7NNN partner nations to share standardised exploitation reports of switches used in RCIEDs. This CONEMP describes the purpose, organisation and operation of RCIED DB system as deployed in BICES, including its capabilities and interoperability with other systems as well as requirements for data, training, administration and maintenance.

The work described in this report was carried out under the Team of Experts on Electromagnetic Countermeasures for Radio Controlled Improvised Explosive Devices (ToE on ECM for RCIED) Programme of Work and was concluded in 2019. The ToE on ECM for RCIED is a working group under the NATO Conference of National Armaments Directors, NATO Air Force Armaments Group, Aerospace Capability Group 3 on Survivability.

Approved: ______________________________

NATO ToE on ECM against RCIED
Brussels, BEL

This document consists
of vi + 35 pages
(excluding covers)

DOCUMENT CONTROL PAGE

VERSION HISTORY

Version	Author	Date	Reason for Change	Superseded Document
1	NCI Agency	25 Aug. 16	Initial draft	n.a.
1.1	Capt Thome	26 Sep 16	Addition to section No 4 and 5	
1.2	Capt Thome	06 Feb 17	Post ToE 07.12.2016 Add section 2 referenced Documents	
1.3	Sam Henze	10 April 17	Provide NATO political perspective to document	
1.4	Sam Henze	18 May 2017	Final edits under ToE guidance	
2.0	NCI Agency	09 Nov 2017	Final inputs under ToE guidance	
2.1 (NSO: Edition A Version 1)	NCI Agency	07 Dec 2017	Final refinement	
2.2 (NSO: Edition A Version 2)	Capt Thome and Sam Henze	2019	Add after ToE 2019	

SUMMARY

This Concept of Employment (CONEMP) documents gives a high level vision for the NATO Radio Controlled Improvised Explosive Devices Database (NATO RCIED DB) project. The NATO RCIED DB provides a NATO-based platform for sharing technical intelligence about RCIEDs amongst NATO and 7NNN countries. Such information, collected by allies and partners on missions all over the world, contributes to a mutual understanding of global threats and the development and spread of threat technologies. This will in turn support the development of effective electronic countermeasures against RCIEDs in the future as well as support operational planning. Individual nations may implement nationally-based "instances" of the RCIED DB for their national only use, with or without synchronization and interface with the NATO RCIED DB. As this CONEMP establishes, nations decide which of their data sets are releasable into the NATO RCIED DB – and which data they will maintain in their nation-only instance.

Table of Contents

1. INTRODUCTION

1.1 BACKGROUND

Improvised Explosive Devices (IEDs) have been a leading cause of casualties to NATO forces in operations and have had a strategic effect far beyond their limited tactical reach. Radio Controlled IEDs (RCIEDs) provide attackers with precision targeting, high standoff and rapid technological innovation supported inadvertently by the global commercial telecommunications industry. These qualities, along with their ease of use and low cost, make RCIEDs one of the most dangerous weapons likely to be faced by Allied forces in any land or littoral operation involving asymmetrical or hybrid adversaries.

1.2 SCOPE

This document describes the Concept Of Employment (CONEMP) for the RCIED Database (RCIED DB) as deployed on the BICES Network under NATO's Voluntary National Contribution Fund project[1]. The purpose is to provide the initial high-level concept for use of the database, particularly regarding the process for adding, publishing and sharing data. This CONEMP describes the intended approach to these processes together with providing a description of the technical features of both BICES and the intended implementation of the RCIED DB in order to meet these requirements. The key issues addressed in this initial CONEMP are security, access control, data ownership, data publishing, user & content management and control of data sharing (release).

In order to act as a stand-alone document, brief introductions to the RCIED Database and BICES are provided.

1.3 DOCUMENT OVERVIEW

Major sections of this document include:

- Section 1 describes the approach for developing the RCIED DB CONEMP.
- Section 2 provides a list of reference documentation
- Section 3 describes technical exploitation
- Section 4 gives information about system architecture and BICES SECURITY
- Section 5 describes the operational concept of NATO RCIED DB
- Section 6 gives information about RCIED DB procedures and software change management
- Section 7 provides a list with Acronyms and Definitions

1.3.1 Document Security

This Document is NATO UNCLASSIFIED and is releasable to the 7NNN countries, namely Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland.

1.3.2 Database Security

The NATO RCIED DB is classified up to SECRE* and must therefore be transported, stored and accounted for in accordance with the security principles and practices laid down in the NATO Security Manual C-M (2002) 49.

[1] AC259-D(2016)0046 VNCF RCIED Database Implementation Project approved 17 January 2017.

1.4 SYSTEM OVERVIEW

The RCIED DB system shall provide a repository for results of electronic exploitation of RCIED switches. The system is intended to facilitate the sharing and further use of such data.

The system will function on the BICES network, providing access across participating nations.

In the following figure this is depicted using high level constructs:

- The database resides on the BICES network
- Exploitation personnel can enter their results and other relevant data
- Operational users can access and use the data
- The system offers various management functions

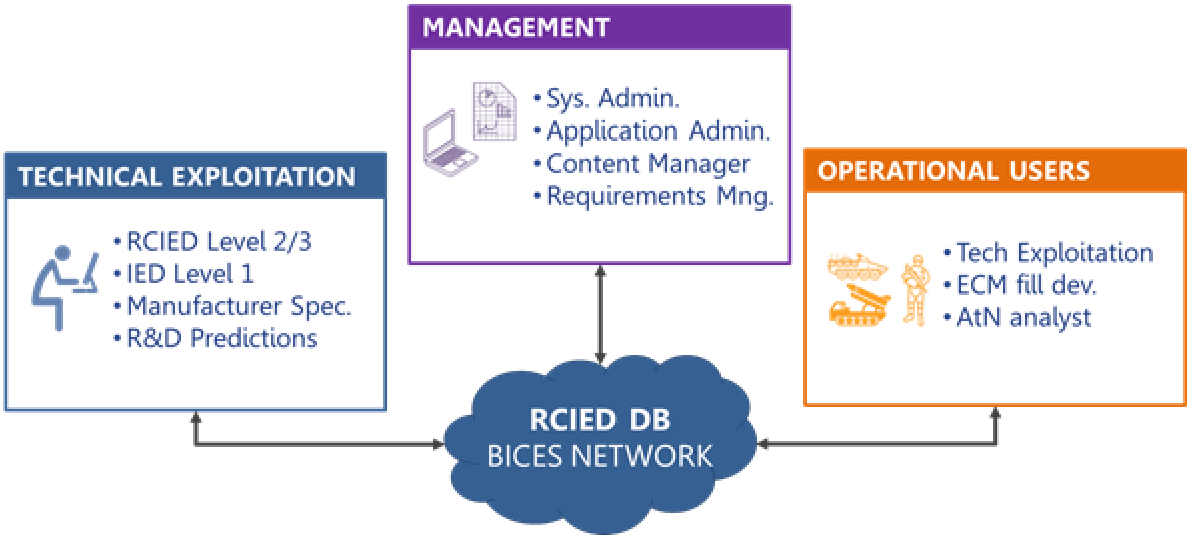


Figure 1 RCIED DB System Overview.

2. REFERENCED DOCUMENTS

2.1 NATO DOCUMENTS

- MC 64-10
- AAP-6, 2014, NATO Glossary of Terms and Definitions (English and French)
- AAP-15, 2014, NATO Glossary of Abbreviations used in NATO Documents and Publications
- AJP 3.6 B Allied Joint Doctrine for Electronic Warfare
- AJP 3.15 C Allied Joint Doctrine for Counter-Improvised Explosive Devices (C-IED)
- AC259-D(2016)0046 VNCF RCIED Database Implementation Project 17 January 2017
- STANREC 4803/AEP-4803 Procedures for Standardized Exploitation of RCIED Switches, Radio Technologies, and Other Electronic Components

2.2 PROJECT DOCUMENTATION

- Data Model Documentation, rcied-xsd-package-1.0.0
- NU RC-IED v1.1.0 User Guide
- NU RC-IED v1.1.0 System Administration Guide
- NU RC-IED v1.1.0 Security Test and Evaluation Report
- NU RC-IED v1.1.0 Installation and Configuration Guide

3. TECHNICAL EXPLOITATION

Technical exploitation will be driving the production of the information which will be stored in the RCIED DB. The quality of the RCIED DB content depends directly on the standardization of the terminology, the exploitation procedures, and the equipment used to conduct exploitation. A number of standardization efforts are ongoing within the NATO technical exploitation communities. Among these, the most relevant standards are:

- STANAG 6502/AIntP-10,
- STANREC 4803/AEP-4803

While STANAG6502/AIntP-10 addressed the general intel perspectives in the field of technical exploitation, STANREC 4803/AEP-4803 covers standard operating procedures (SOPs) for exploitation of RCIEDs - in particular from a radio technology, and electronic components perspective. The result of the exploitation process as described in STANREC 4803/AEP-4803 is the information which will be stored in the RCIED DB.

The terminology used in the RCIED DB data model (see 4.3.3) and in the application user interface will need to be maintained in order to reflect these ongoing standardization efforts. The NCI Agency will address this maintenance task as part of the periodic maintenance effort in accordance with the decisions of the Software Configuration Control Board.

The correspondence between the SOP in STANREC 4803/AEP-4803 and the use of RCIED DB will be illustrated in the RCIED DB SOPs and will explain at which stages the RCIED DB will be used, by which role and what information is stored in the RCIED DB**.**

4. RCIED DB DEPLOYMENT ARCHITECTURE

4.1 CURRENT SITUATION

4.1.1 Analysis of current procedures

RCIED exploitation reports are currently disseminated through NATO channels mainly as text files (pdf format) by e-mail, in close expert communities. A C-IED portal is available on BICES and some of these exploitation reports are also stored in a folder on this portal. Access to information, management of reports and searching for information are all difficult tasks and personal networks are essential for getting access to the right information at the right time.

In areas of operations, some national tools are offered to disseminate IED exploitation information. For example, in the ISAF and RSM missions the Weapon Exploitation and Analysis Tool (WEAT) is used to disseminate IED exploitation reports, which include electronic exploitation of RCIEDs. Such solutions are useful, however they are confined to the areas of operation, do not always cover all the details of RCIED exploitation and in some cases are not available to all NATO Nations.

The RCIED Database addresses some of these gaps and offers an improved solution to manage RCIED exploitation.

4.1.2 Motivation for a New System

During the past years the NATO ToE on ECM for RCIED has actively sought cooperation with other NATO information systems development programs in order to address the requirements for management of RCIED exploitation information. One such program was the NATO Emitter Database. However the lack of mature requirements prevented RCIED functionalities to be included in other information systems. Establishing the RCIED DB as its own project offered the possibility to mature the requirements through prototyping activity, which was achieved in 2014-2015. The deployment of this system on the BICES network as an operational capability will further support the refinement of operational and systems requirements, with the eventual ambition that the RCIED DB be integrated into the NATO Automated Information Systems via the C2 of EW Capability Package sometime around 2021.

4.2 CONSTRAINTS

4.2.1 Technical Constraints

Some of the technical constraints on the proposed system are:

- *System is web-based* – The systems will be installed on a central server and can be accessed by users over a wide area network. This offers the advantage of connecting users over a broad geographic area but at the same time is conditioned by users having access to the network.
- *System is deployed on a classified network*: The system will be deployed on the BICES classified network and will be accessible from the NATO Secre* Network as well. The system will not be accessible over Internet and special workstations connected to BICES network will be required to connect to the RCIED DB.

- *System interacts with other similar systems through file export/import* – In the first deployment phase the system will exchange data with other similar systems by using a file export/import mechanism.

4.2.2 Organisational and Policy Constraints

- *The RCIED DB System is an Interim Operational Capability* – The RCIED DB will be deployed in the BICES network as an interim solution until a long term capability will be made available through one of the NATO's Capability Packages. The Bi Strategic Commands (Bi-SC) Automated Information Systems (AIS) Reference Architecture [AC/322-D(2005)0037], describes NATO's Command and Control Information System used throughout the NATO Command Structure, in NATO Command Deployments and in NATO Exercises. The Bi-SC AIS is in turn one element of NATO's overall Communication and Information Systems (CIS) Capability, which includes a number of strategic sub systems such as the NATO Core Communications Network, Air C2, Theatre Missile Defence, and Deployable CIS and so on. RCIED information requirements have been included under the capability to be acquired under the Electronic Warfare Functional Services Capability Package, which will be a fully integrated element of the Bi-SC AIS.
- *RCIED DB will be one of the main sources for developing electronic counter measures against RCIEDs in NATO operations* – Information stored in the RCIED DB will support Counter RCIED Electronic Warfare (CREW) teams to develop fills suitable for specific areas of operations.
- *NCI Agency and BICES Executive Group (BGX) must take an active role in the development, operation and maintenance of the system* – NCI Agency is a Customer Funded organisation and Voluntary National Contribution Funding will be used to fund the NCI Agency support to the project. BGX is a Memorandum of Understanding Organisation and the project has been included in the BGX annual programme of work.
- *NATO TOE on ECM for RCIED will provide active Governance of the project and will act as the Senior User for the RCIED DB Application* – The TOE will monitor the implementation of the RCIED DB, will support the operationalization of the system and will act as Content Manager of RCIED DB.

4.3 DESCRIPTION OF THE PROPOSED SYSTEM

4.3.1 RCIED DB Application

RCIED DB is a standard server-client web application, which has been developed using a prototyping framework available at NCI Agency. This framework has been used to support rapid development of prototypes and to validate user requirements. The framework includes a number of components which provide a stable and rich baseline with common functionality like search, geospatial visualization, authentication and presentation.

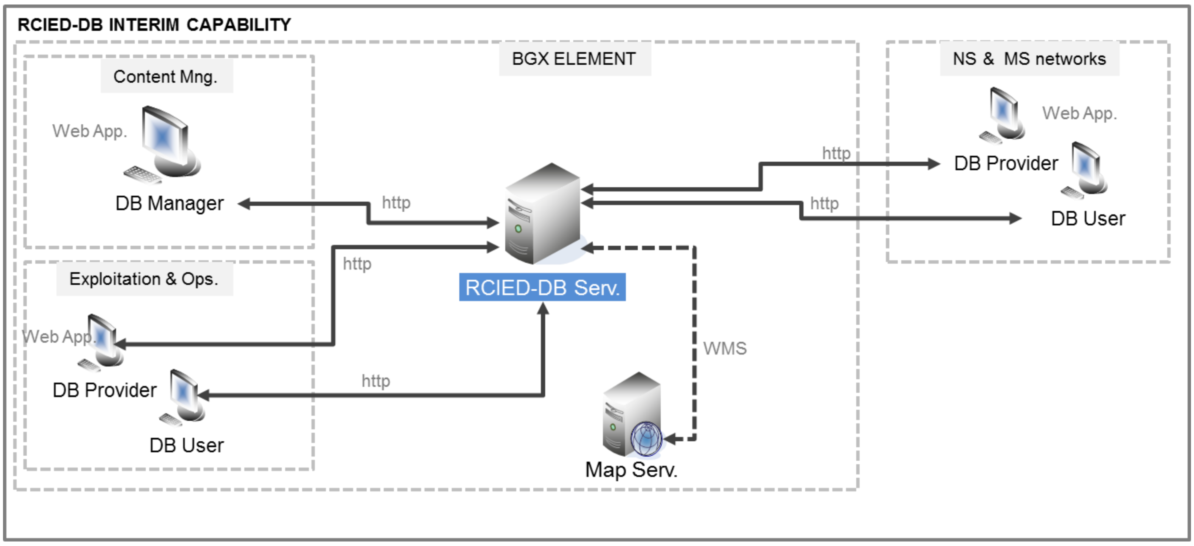


Figure 2 RCIED DB deployment onto the BICES network.

The client is running within a web browser that supports HTML 5 (Chrome or Internet Explorer 9 or later). The server being a web application hosted within MS IIS.

The RCIED DB application is interoperable with any WMS compliant service for its mapping capabilities. Normally, existing map services in the deployment network are used to retrieve map data. If such services are not available, an optional, open-source component (which comes with RCIED DB) can be installed and used to manage map data. This optional component (MS4W – Map Server for Windows) requires installation of the PostgreSQL database and the PostGIS spatial database extender for PostgreSQL object-relational database (see Figure).

4.3.2 Description of the Data Cycle

Six major steps of data lifecycle supported by the RCIED DB application are depicted in Figure . It is worth nothing that the application is adapted to the diversity in the RCIED domain, where reports on the same device can be slightly different and it is not advantageous to restrict the storage of information in class templates, which are periodically updated. However the user can group information available on a type of device by using search folders where all reports sharing common characteristics (e.g. RFT2) are stored.

Walking through the cycle, the first step is to create a record in the RCIED DB and store all the relevant information of the case. Information about the device category, status, test procedures, and radiofrequency parameters are among the parameters that will be included in the record. Once the analyst is confident that he has included all relevant data, he or she will submit the record for approval. The manager will be notified about the new submission and will review the data, approve the data and disseminate as required (e.g. file export or synchronised with other RCIED DB servers). As users become more familiar with the data they can begin to collaborate with other members. This collaboration could include sharing information they found in the data or asking questions about the data. Users can utilise search functionalities to monitor all data distributed through the RCIED DB on a specific topic. The RCIED DB contains 3 types of information: exploitation reports, manufacturer specification data and IED event information. The users have the possibility to link all these information types and create a more elaborated story.

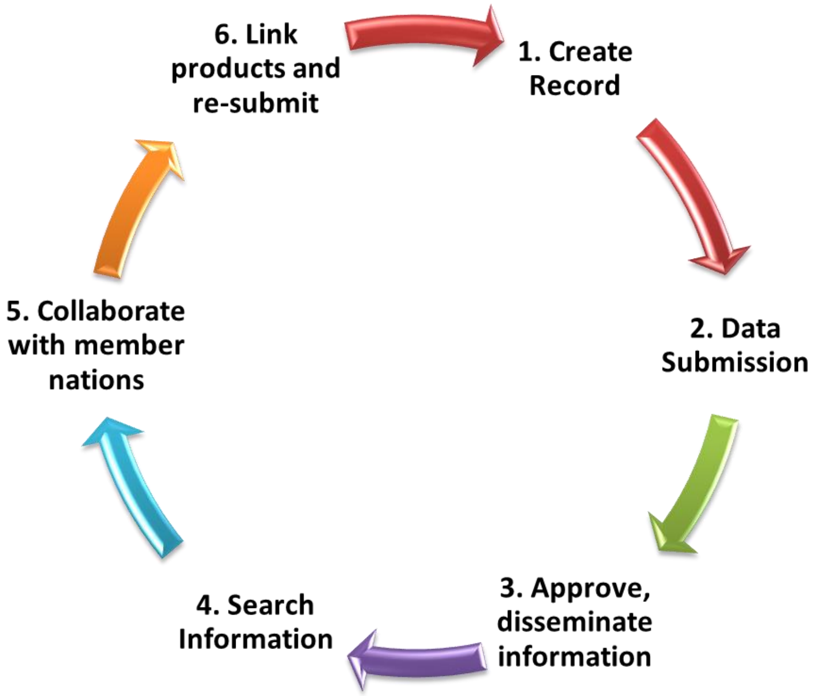

1. Create Record
2. Data Submission
3. Approve, disseminate information
4. Search Information
5. Collaborate with member nations
6. Link products and re-submit

Figure 3 Data Cycle supported by RCIED DB.

4.3.3 Data Model

As part of the RCIED DB development effort a data model was also developed to support standardization of exploitation reports. The data model covers all three information categories (exploitation reports, manufacturer specification data and events) and defines metadata and domain values used to store the data in the database. The data model was derived from existing text base reporting formats, from NATO standards (e.g. APP-11) and through analysis activities inside of the NATO ToE on ECM for RCIED. The current data model used within the RCIED DB application is depicted in Figure 4.

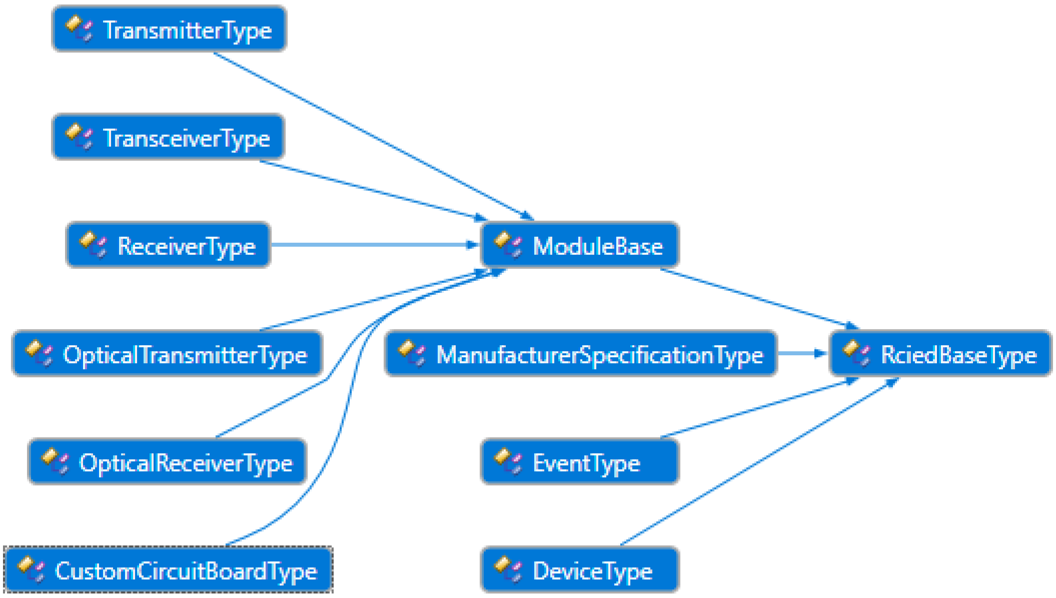


Figure 4 RCIED DB Data Model.

4.3.4 Technical Interoperability

The RCIED DB application will be deployed with an info server capability which can be configured to integrate automated data exchange with various end points. However in the initial deployment phase a file export/import mechanism will be used to exchange data with other similar systems available at national levels. For example the data model format developed as part of RCIED DB project can be used to standardize the file export/import format.

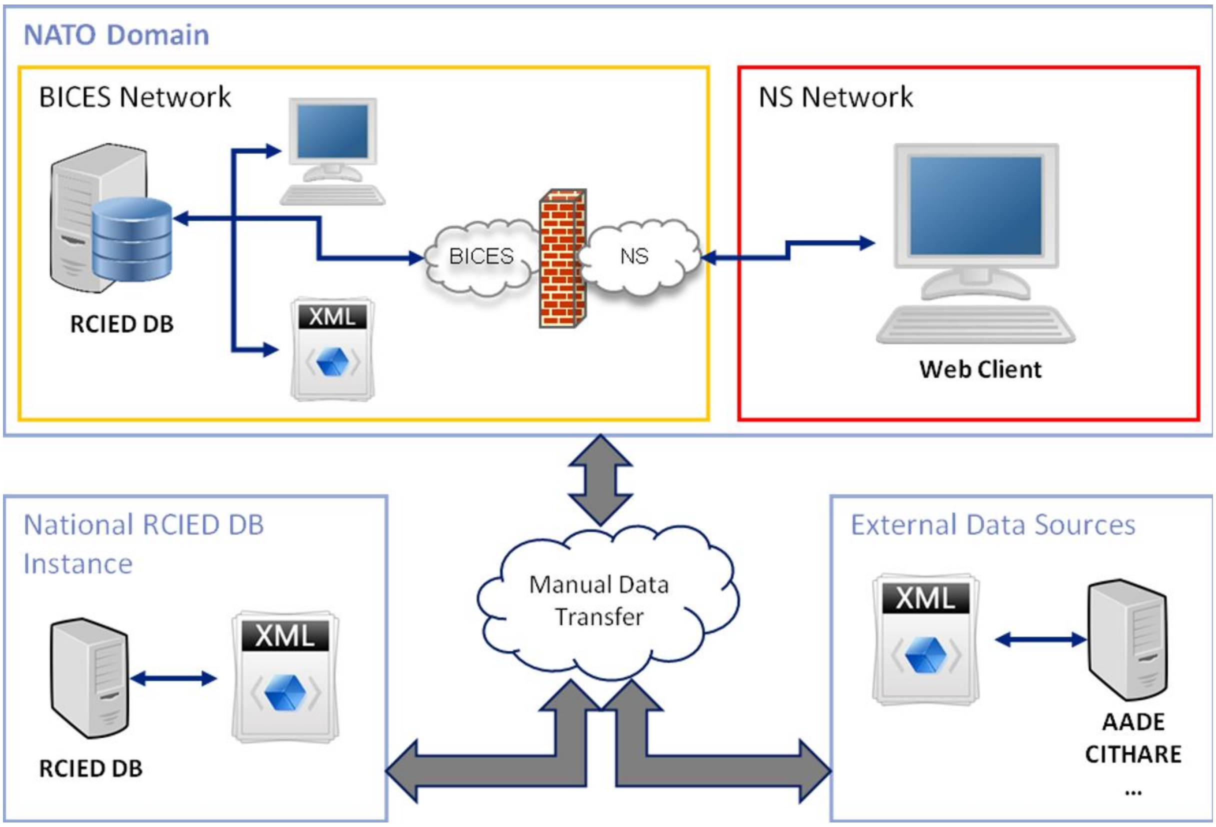


Figure 2 Initial deployment of the RCIED DB will exchange information with other similar systems through file export/import mechanisms.

Users can develop exploitation reports in national systems available outside of the NATO domain (national "instances"), and they can save these reports to an interoperable XML file. These files can then be manually transfered into the BICES domain and uploaded in the RCIED DB application by using an import function (see 5.2.3.6). The RCIED DB is designed to have the potential to synchronize with external databases, including national databases and national "instances" of the RCIED DB. However this technical feature is not yet implemented and is not covered in this CONEMP.

4.3.5 Modes of Operation

The software framework used by the RCIED DB application includes three modes of operation:

1. *Operational Mode* - This is the mode the system will be in for the majority of its operation. This mode allows all users to access the contents that they have permission to access
2. *Training Mode* – This is the mode used to train new users on the application. A data diode exists between the operational and training databases. Real information from the operational domain is pulled in into the training database where the users can modify this data. However, all the training activities are not replicated back into the operational domain and operations will not be impacted by training activities.
3. *Exercise Mode* – A third database exist inside of the RCIED DB application to support exercises. Again this is an isolated domain where exercises can be conducted on the same application.

4.3.6 BICES Features

The Battlefield Information Collection and Exploitation Systems (BICES) is a multi-national domain shared between the 28 NATO member nations (29 with the accession of Montenegro) as well as 7 non-NATO partner nations (7NNN) plus the European Union Military Staff (EUMS). The BICES system is for the purpose of exchanging National and NATO intelligence/information products up to NATO SECRE*. BICES provides a gateway to other classified NATO and coalition networks and National SECRE* RELEASABLE intelligence/information products. The capabilities are intended for national, NATO or coalition use in peace, crisis and war as determined by the BICES Board of Directors (BOD).

4.3.7 Network Access

The communication between server and clients is using the HTTP protocol over port 80. Native BICES workstations and NSWAN-enabled workstation (also from interconnected locations) should have access to the RCIED DB server.

4.4 DEPLOYMENT IMPACT

The implementation of the proposed RCIED DB system will impact on both NATO and national customers. The sub-sections below identify potential operational impacts, organisational impacts, and other impacts of RCIED DB deployment.

4.4.1 Operational Impact

The following operational impacts from the new system must be considered:

- *Change in business processes and operational procedures*: It is anticipated that RCIED DB will have to implement changes to the way it conducts business in order to achieve NATO’s mission, goals, and objectives in sharing and archiving data records. The RCIED DB system will offer the ability to handle more electronic data records, as well as records with a wider variety of formats, than the current architecture has been capable of addressing.
- *Single virtual location for detailed data that is multi-source and multi-modal:* The system will create a single location where users will be able to gain access to consolidate near real-time and archived data from multiple sources.
- *Designed to reinforce long-term stewardship of data.* The system will provide a means where nations will be able to store and share new data and updates to classes of devices.
- *Metadata for data:* The system will store metadata for all of its stored data. The metadata will add quality and usefulness to all of the information stored within the system.
- *Collaboration space for users:* The system will provide methods for members to collaborate with each other about updating and how they are using the data. This effort will give members the ability to collate data and subscribe to notifications.
- *System usage audit:* The system will be able to track the use of the system so members and managers of the system will be able to know what data and functions in the system are most useful to support ECM requirement.

- *Governing rules for the community:* The system will provide a means for users to agree to terms of use of the system. A governing system will protect contributors to the system and also set guidelines on how data sharing will be conducted. These governing rules will include intellectual property rights and security issues.
- *Lessons learned for use in deployment:* The experience gained from developing, operating, and managing the system will provide valuable insights, requirements, and lessons learned that will be utilised by implementers of connected NATO capability packages, including data providers, systems integrators, and applications developers.

4.4.2 Organisational Impacts

No organisational changes need to be made to meet the system needs. However a number of organisations with the appropriate expertise and experience will be required to develop, operate, and maintain the RCIED DB. With this in mind, some possible organisational impacts are provided hereafter:

- The commitment of resources (e.g. funding, time, staff) to support RCIED DB operation and maintenance,
- The development of education and increased training for both RCIED DB nation’s staff and NATO users.

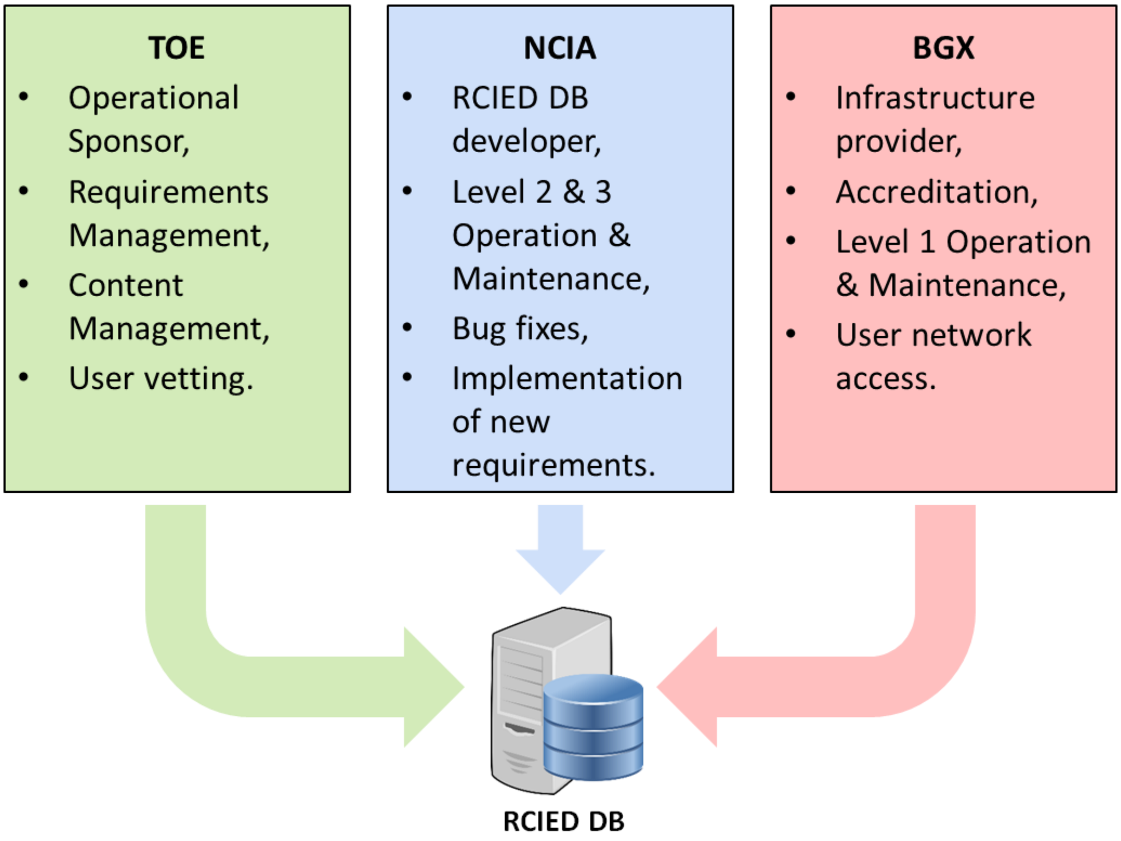
4.4.3 Impacts during operational transition phase

The full extent of impacts during deployment will not be known until the system has been used in operations. However, predicted impacts considered this far include:

- Articulation of business rules, templates, and other controls needed for operational implementation,
- Development of training requirements to be implemented in an increment,
- Training necessary for rollout of the increment.
- Involvement in meetings, and discussions,
- User and support involvement in reviews and demonstrations, evaluation of initial operating capabilities and evolving versions of the system, development or modification of databases, and required training
- Operational impacts during proposed system testing and final system data migration

4.4.4 Governance

One of the keys to successful delivery of the RCIED DB system will be the establishment of the appropriate governance structures and mechanisms to provide management and oversight of the program and its operation.



TOE

- Operational Sponsor,
- Requirements Management,
- Content Management,
- User vetting.

NCIA

- RCIED DB developer,
- Level 2 & 3 Operation & Maintenance,
- Bug fixes,
- Implementation of new requirements.

BGX

- Infrastructure provider,
- Accreditation,
- Level 1 Operation & Maintenance,
- User network access.

Figure 3 RCIED DB governance.

This will require a governance model focused on delivering capabilities that meet the needs of the NATO Headquarters, National Commands Authorities and Agencies, the NATO ToE on ECM for RCIED while at the same time ensuring responsible expenditure of NATO's investment.

Three organisations have primary responsibilities in the development, operation and maintenance of the RCIED DB. The key roles of these governing bodies are listed in Figure 6.

The governance principles to be followed are presented in **Table 1**.

Table 1: Governance Principles

GOVERNANCE PRINCIPLE	DESCRIPTIONS
Accountability	Clear roles, responsibilities and audit processes to ensure the obligations conferred in the RCIED DB governance body are met.
Leadership	Strong strategic leadership is provided to ensure ECM against RCIED policy requirements and standards are embedded and enacted throughout the RCIED DB project.
Engagement	Key stakeholders are engaged to ensure broad ownership and a balanced approach to the delivery of the RCIED DB system.

Viability	The governance model is structured to ensure its information sharing focused and delivers benefits for all stakeholders.
Effectiveness	Designed to fit for purpose, balancing national with NATO Headquarters, National Commands Authorities, Agencies, the NATO ToE on ECM for RCIED and CREW communities' requirements without introducing unintended consequences.
Efficiency	Streamlined to ensure that it fits with the business practices of information sharing and delivery services and leverages existing and related capability package investments.
Integrity	Encompassing honesty, objectivity, high standards of propriety and probity in the stewardship of NATO funds and resources and in the management of the organisation.
Transparency	Ensuring stakeholders have visibility of status and can have confidence in the decision-making processes and actions of the governing body(s).
Sustainability	Flexibility to respond dynamically to changing requirements over the RCIED DB system lifecycle.

5. OPERATIONAL CONCEPTS

5.1 MISSION STATEMENT

The mission of the NATO RCIED DB is to provide for the exchange of RCIED technical exploitation data amongst participating nations.

The CONEMP document expresses what users want and envision in the proposed RCIED DB System. Scenarios convey these needs in simple non-technical language. Some of the scenarios overlap as a result of interaction between different users or due to similarity between different activities. The scenarios represented in the following sections describe how users may interact with the proposed RCIED DB system. Scenarios have purposely been made to be far reaching in an attempt to include all possible Users within a designated class (of users) but the scenarios are not intended to identify all possible situations for any given user class. Additionally, the steps in the scenarios should not be interpreted as a fixed sequence of events, but instead an illustration of capabilities the proposed RCIED DB system will offer (any user class).

A scenario is a step-by-step description of how RCIED DB should operate and interact with both its users and external interfaces under a given set of circumstances. Scenarios are described in a manner that enables readers to walk through them and gain an understanding of how all the principal parts of RCIED DB function and interact. The scenarios tie together parts of RCIED DB, the users and other entities by describing how they interact. Scenarios cover the user's concept of all the operational modes and all classes of users identified for the proposed RCIED DB System and illustrate all the business processes that RCIED DB will support.

For convenience, the scenarios are divided into four categories:

- User registration, log-in and interaction,
- Access to Information,
- Information management,
- System administration.

5.2 OPERATIONAL SCENARIOS

5.2.1 User Registration, Log-in and Interaction

5.2.1.1 Operational Scenario: Register with System

Actors: Unregistered User and Administrator.

Description: An Unregistered User wants to become a Registered User and have access to additional data and/or participate in the community resources provided by the RCIED DB. The Unregistered User registers on the site to become a Registered User. The Administrator reviews the Unregistered User's information to make sure the data is valid and requests authorisation from the relevant NPoC to add the user.

The Administrator creates the account in the RCIED DB and provides the access credentials to the requestor.

Preconditions: The Unregistered User has navigated to the system using BICES workstation (or NS WAN workstations – BICES enabled).

Steps:

1. The Unregistered User opens a web browser and navigates to the RCIED DB access page.
2. The Unregistered User reads and agrees the terms of use of the site.
3. The Unregistered User enters all mandatory information and, at their discretion, optional requested information. [Mandatory information is expected to include roles required, full name, organisation, organisation type, and country.]
4. Administrator forwardes the message to National PoC and receives confirmation the request is valid.
5. Administrator approves registration, provides email to user.

Notes: If user fails to authenticate (e.g., user provides an invalid email address or fails to respond to the registration email), Administrator rejects registration.

5.2.1.2 Operational Scenario: Log in to the System

Actors: Registered User and Administrator.

Description: The User wants to access the information available at his user level in addition to the open accessible information. The User inputs his log-in information and the system authenticates the User. The User then has access to the information available at his user level.

Preconditions: The User has registered with the System and has received log-in information.

Steps:

1. The User navigates to the log-in area.
2. The User enters his log-in information.
3. The subsequent steps happen when the User enters his information correctly:
4. The User is authenticated.
5. The User is given the ability to access data. If the User is a Registered User with Additional Roles (e.g. Creator), the User is also given access to the specific functions that he has been granted access to. If the User is an Administrator, the user also receives the ability to modify system information.

6. The subsequent steps happen when the User enters his information incorrectly:
7. The system does not authenticate the log-in information and displays an error message.
8. The Registered User re-enters his log-in information. Repeat from step 3 if the information is correct or from step 5 if it is incorrect.

Notes:

5.2.1.3 Operational Scenario: Contact the Application Administrator

Actors: Unregistered User, Registered User and Administrator.

Description: A User has a question about information in the RCIED DB or about the way the RCIED DB is working. The User sends a message to the Application Administrator, who answers the question or fixes the problem if necessary.

Preconditions: User has access to the System in the deployment network.

Steps:

1. The User navigates to the RCIED DB start page and retrieves the contact details of Administrator.
2. The User contacts the Administrator with his question.
3. The Administrator reads the question and sends a reply if necessary.

Notes:

5.2.1.4 Operational Scenario: Request a New Password

Actors: Registered User and Administrator.

Description: The User wants to log in to the system but has forgotten his password and so requests a new one. The User must provide identification information before the password is reset. The User then creates a new password and logs in.

Preconditions: The User has registered with the System and has received log-in information.

Steps:

1. The User navigates to the start page of RCIED DB and contacts the Administrator with the request for a new password.
2. The User provides identification information, including the email address they provided when originally registering.
3. The Administrator resets User password and sends the new password by e-mail.

4. The User is logged into the site.

Notes:

5.2.1.5 Operational Scenario: Review and Edit Profile

Actors: Registered User and Administrator.

Description: The User wants to change his or her user profile. The Administrator receives a confirmation from an authorised body (NPoC) to update the User profile.

Preconditions: User has navigated to the system using Bi-SC AIS (NS WAN) and retrieves Administrator’s contact details.

Steps:

1. Authorised User sends a request to Administrator with profile change request (e.g. add roles).
2. Administrator forwardes the message to National PoC and receives confirmation the request is valid.
3. Administrator changes User’s profile.

Notes:

5.2.2 Access to Information

5.2.2.1 Operational Scenario: View Accessible Content

Actors: Registered User or Administrator.

Description: A User reads RCIED DB accessible content including technical exploitation information, manufacturer specification information or event information.

Preconditions: The User has registered with the System and has received log-in information.

Steps:

1. User navigates to the RCIED DB accessible content of interest.
2. User views desired information.

Notes:

5.2.2.2 Operational Scenario: Search Accessible Content

Actors: Registered User or Administrator.

Description: A User is looking for certain information. The User inputs search criteria into the system to find the desired information. The User searches RCIED DB for information describing RCIED components and for actual content within the records. Such searching may be done at a variety of levels of aggregation (i.e., simple keyword search, structured query search, or full text search). Within the User's given access rights and privileges, the consumer may take advantage of available functions and features.

Preconditions: The User has registered with the System and has received log-in information.

Steps:

1. The User inputs the search criteria.
2. User views accessible information.

Notes:

5.2.2.3 *Operational Scenario: Unauthorised User Tries to View Content That is Not Publicly Accessible.*

Actors: Unregistered User.

Description: An Unregistered User tries to access information that is not available to the public using non-traditional means. The Unregistered User is denied access to the content.

Preconditions: User has access to the System deployment network.

Steps:

1. Unregistered User attempts to view content that is not publicly accessible by going directly to the URL of the content or accessing the page through non-traditional means (e.g. source page, TCP traffic etc.).
2. The Unregistered User is denied access to the content.

Notes:

5.2.2.4 *Operational Scenario: Download Data*

Actors: Registered User or Administrator.

Description: The User finds sample data and wants to download it. If required for the information in question, the user logs in to the system and his credentials and permissions are checked against those required for accessing the requested data. If there are no restrictions on access or the user is authenticated and has the required permissions, the user downloads the file and views the data.

Preconditions: User has navigated to the system using Bi-SC AIS (NS WAN) and is logged in to the system. User has found the information to be downloaded.

Steps:

1. User selects the data to be downloaded.
2. If the user is not logged in and login and/or additional permissions are required for the data in question, the user logs in to the system. The system checks the credentials and permissions of the user.
3. If the user is authenticated and has the appropriate permissions, they are granted access. If not, an error message is returned to the user. The system allows a limited number of attempts.
4. The User downloads the queried data.
5. The User views or stores the data.

Notes:

5.2.3 Information Management

This set of scenarios demonstrates the interaction of the data creators, approval and publish actors, data viewers and administrators. Note that some steps are performed by the system without the need for human intervention (e.g. automated e-mail notification), and some are a combination of system and human activities (e.g. approval of the dissemination of products).

Create, approve and publish roles are responsible for making decisions related to the records lifecycle management and processing activities and archival work as scheduled. Responsibility for the completion of archival tasks rests with the Content Managers (ToE Role). The Content Manager also interfaces with the Administrators (NCI Agency/BGX roles) when system problems disrupt the flow of work.

5.2.3.1 Operational Scenario: Add RCIED Exploitation Report

Actors: Registered User with Creator Role.

Description: The User needs to add new RCIED explotation information in the database. The User inputs the associated metadata and attaches relevant files and information. The User submit the database record for approval.

Preconditions: User has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. User created new Device.
2. User saves the Device in the database.
3. User link to other relevant elements in the RCIED DB (e.g. Manufacturer Specification or IED events).

4. User submits the device.
5. An e-mail message is sent automatically to the Approver for approval.

Notes:

5.2.3.2 Operational Scenario: Add Manufacturer Specification

Actors: Registered User with Creator Role.

Description: The User needs to add new Manufacturer Specifications in the database. The User inputs the associated metadata and attaches relevant files and information. The User submit the database record for approval.

Preconditions: User has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. User created new Manufacturer Specification report.
2. User saves the Manufacturer Specification in the database.
3. User submits the Manufacturer Specification.
4. An e-mail message is sent automatically to the Approver for approval.

Notes:

5.2.3.3 Operational Scenario: Add New IED Event

Actors: Registered User with Creator Role.

Description: The User needs to add new IED Event in the database. The User inputs the associated metadata and attaches relevant files and information. The User submit the database record for approval.

Preconditions: User has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. User created new IED Event report.
2. User saves the IED Event in the database.
3. User submits the IED Event.
4. An e-mail message is sent automatically to the Approver for approval.

Notes:

5.2.3.4 Operational Scenario: Approve new database record

Actors: Registered User with Approver Role.

Description: The User needs to Approve a new record (RCIED Report, Manufacturer Specification or IED Event) in the database. The User review the inputs and approve the record. Once the record is Approved it will be visible to all users of the database.

Preconditions: User has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. The Approver reviews the database record.
2. In case the report contains valid information the Approver approves the record.
3. In case corrections need to be made on the report the Approver reject the record, including a comment on why it has been rejected
4. The Creator updates the report and re-submit for approval.
5. The Approver approves the updated report.

Notes:

5.2.3.5 Operational Scenario: Publish new database record

Actors: Registered User with Publisher Role.

Description: The User needs to Publish a new record (RCIED Report, Manufacturer Specification or IED Event) in the database. The User reviews the inputs and publishes the record. Once the record is Published it will be disseminated to all channels created in the info server section of the database.

Preconditions: User has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. The Publisher reviews the approved records.
2. In case the report contains valid information the Publisher publishes the record.
3. If data is not releasable the Publisher will not publish the record, the Publisher may Archive the data.

Notes:

5.2.3.6 Operational Scenario: Export and Import Data

Actors: Registered User with Publisher Role.

Description: The User needs to export or import relevant information to or from a file (RCIED Report, Manufacturer Specification or IED Event).

Preconditions: User has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. The User selects the database record he wants to export to a file.
2. The User exports the information to a file.
3. The User navigates to export location and copy the file and disseminate the information as required (e.g. e-mail, manual).
4. For importing information the User selects the import option from the Application menu.
5. Navigates to the location of the import file.
6. Selects the import file and import into the system.

Notes:

5.2.3.7 Operational Scenario: Update Data

Actors: Registered User with Creator Role.

Description: The User needs to update a database record (RCIED Report, Manufacturer Specification or IED Event).

Preconditions: User has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. The User selects the record he wants to update.
2. The User enters the edit mode.
3. The User updates the record and submit.
4. An e-mail message is sent automatically to the Approver for approval.

Notes:

5.2.3.8 Operational Scenario: Delete Data

Actors: Registered User with Approver Role.

Description: The User needs to delete a database record (RCIED Report, Manufacturer Specification or IED Event).

Preconditions: User has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. The User selects the record he wants to delete.
2. The User deletes the record.
3. The record is moved into the Delete Items folder.

Notes:

5.2.3.9 Operational Scenario: Permanently Delete Data

Actors: Administrator.

Description: The Administrator needs to permanently delete a database record (RCIED Report, Manufacturer Specification or IED Event).

Preconditions: Administrator has navigated to the application using Bi-SC AIS (NS WAN) workstation and is logged into the system.

Steps:

1. The Administrator selects the record he wants to permanently delete from the Delete Items folder.
2. The Administrator permanently deletes the record.

Notes:

5.2.4 Application Administration

5.2.4.1 Operational Scenario: Promote Registered User to be Administrator

Actors: Registered User and Administrator

Description: There is a need for a User to be promoted to a system administrator. The User sends a message to current Administrator and request the profile change. The Administrator coordinates with the National PoC the approval of the request and implements the change.

Preconditions: The User has registered with the System and has received log-in information.

Steps:

1. User sends an e-mail message to Application administrator and requests profile change.
2. Administrator coordinates with the National PoC the approval of the request.
3. Administrator updates user's profile as requested.

Notes:

5.2.4.2 Operational Scenario: Restore System from Backup

Actors: Administrators

Description: There is a problem with the system which requires a system restore. The Administrators will coordinate to perform a system restore to a particular version from the backup.

Preconditions: The Administrator has access to the system.

Steps:

1. An Administrator requests system restoration.
2. The Administrator selects the version to which the system should restore.
3. The system stores the date, time, and description of the restoration event as part of the event log in the data store.
4. Administrator notifies all RCIED DB nations via email system status.

Notes:

5.2.4.3 Operational Scenario: Set Up Automated Synchronisation

Actors: Application Administrator.

Description: Multiple RCIED DB exists and need to be automatically synchronised.

Preconditions: The Administrator has access to the system.

Steps:

1. Application Administrator defines the synchronization architecture in the info Server section.
2. Application Adminstrator monitors system log to detect if synchronization problems exists.

Notes:

5.3 USE CASES

A serie of use cases covering the main functionalities of RCIED DB application are depicted in Figure 4. The key actors interacting with the RCIED DB are also illustrated in Figure 4.

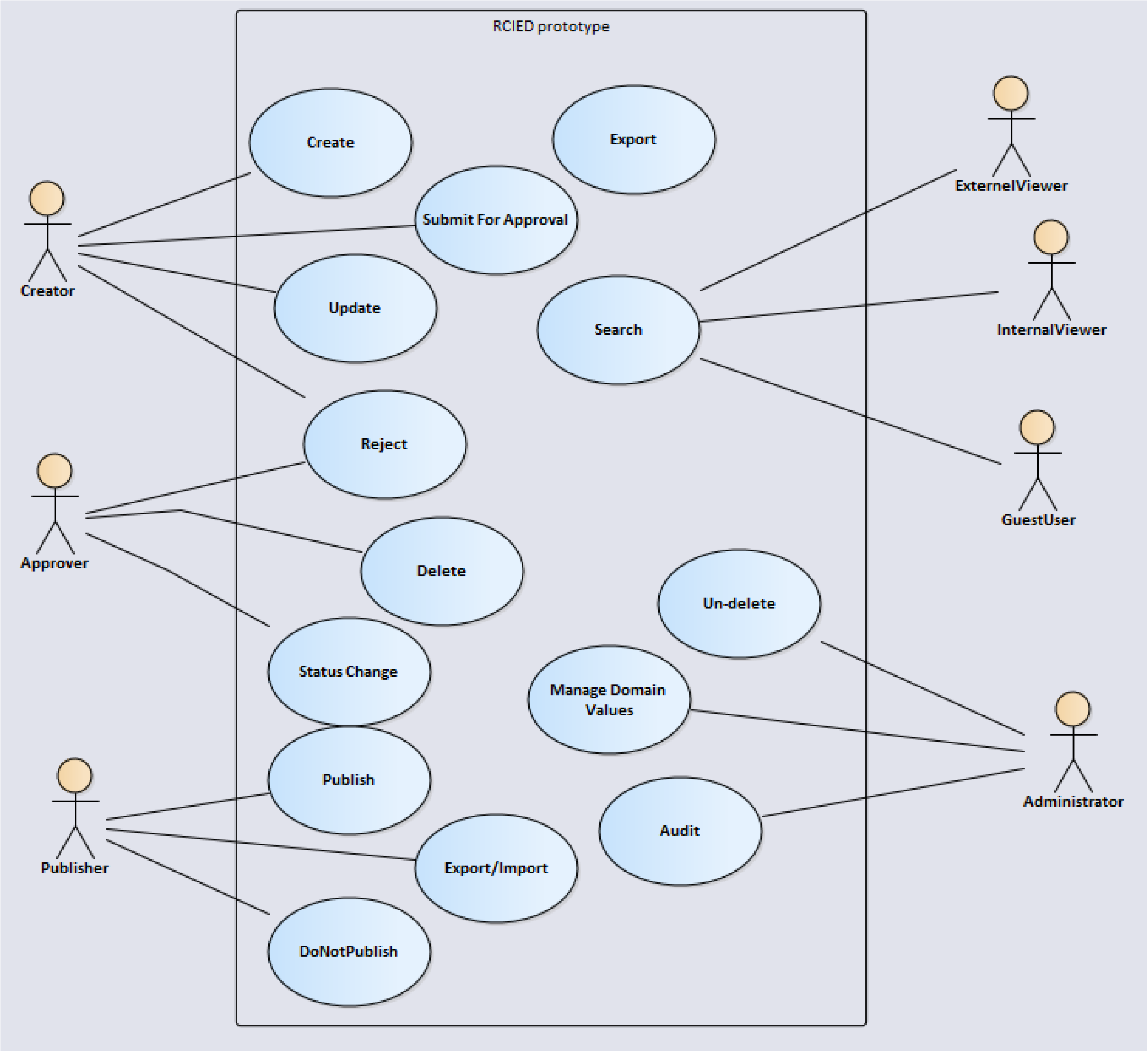


Figure 4 RCIED DB Use Cases.

5.3.1 Create

This use case covers the development of a record in the database. The Creator is the main actor interacting with this use case. Within this use case devices, Manufacturer Specifications or IED events are created.

5.3.2 Submit for approval

Once a record is created the Creator has the option to save this into the database and submit for approval. The record is not visible to the other users until the record is approved by approval authority (e.g. Approver).

5.3.3 Update

The creator of a record can update the information during the entire lifetime of the record from creation until permanently deleted from the database. if it is rejected from the publisher.

5.3.4 Reject

The approving authority can approve the records submitted for approval by creators or can request that changes are implemented in the record before approving.

5.3.5 Delete

There are two levels of delete in the RCIED DB application. A “soft delete” which will move a record from a Folder into the Delete Items folder. The records are still visible to Administrators, Approvers and Publishers, however Viewers will no longer see the record. A “hard delete” is also possible for records in the Deleted Items folder, which will remove the record from the database.

5.3.6 Status Change

A record can have different statuses during its lifetime: draft, approved, archived, rejected published, and delete. The approval authority can change the record status among some of these values.

5.3.7 Publish and Do Not Publish and Archive

The Publisher has the option to disseminate information to other RCIED DB instances in the network or through a file export/import mechanism to other systems outside of the deployment network. Information from the database can be exported and imported from xml files formatted in accordance with the datamodel format developed during the RCIED DB implementation project.

5.3.8 Search

Different types of search exist inside the RCIED DB application, which facilitate easy access to information. Simple keywords search, more complex structured search or free text search can be uses to identify the information of interest. Search queries can be saved in the system and folders are created for each os these queries where results are stored for easy access.

5.3.9 Undelete

When records are deleted from the folders they are first moved into the Deleted Items folder. The Administrator can restore these records such that they will be visible to all users again.

5.3.10 Manage domain values

To facilitate the data record a number of metadata fields have been restricted to a fix set of values. These values are stored in the RCIED DB application and an application administrator can update the value set if required.

5.3.11 Audit

The RCIED DB application records actions performed by the user in the system and this audite trail is available to the Application Administrator.

5.4 ROLES AND RESPONSIBILITIES

The success of the RCIED DB depends on cooperation and coordination among Actors (primarily in nations, but possibly including NATO commands or operational mission cells), RCIED Administrators and Users. Some national actors and users will, in fact, be the same people. However, from a database administration perspective, their responsibilities will differ slightly depending on the role they are in.

5.4.1 Actors

Actors (primarily in nations, but possibly including NATO commands or operational mission cells), work for and are responsible to their nation/organization only. They are responsible for producing datasets, approving datasets for publication and publishing datasets in the RCIED DB.

5.4.1.1 Creator

The Creator is an electronic exploitation analyst; one of the Creator's tasks is, to create new datasets or to update existing datasets if necessary. The Creator is responsible to submit that dataset for approval to the Approver.

5.4.1.2 Approver

The role of the Approver is to check the technical quality of a dataset from a data quality perspective. If the dataset is not ok, the Approver can reject it back to the creator or delete the whole dataset. If the Approver is satisfied with the data the Approver can change the status and raise the dataset up to the next level, the Publisher.

5.4.1.3 Publisher

The Publisher has three tasks. First the Publisher can decide to publish the dataset. That means he or she has to check the classification and releaseability markings and set all controls and flags for publishing and data sharing of the dataset. The Publisher can also decide to store the dataset in the database without publishing. The owner of the role "Publisher" can be either the exploitation manager in a laboratory or the National Point of Contact (NPoC). Finally, the Publisher must field reports about problems with his/her data that will be communicated to the Publisher from the RCIED DB Content Manager. Upon receipt of problem reports, the Publisher will have to unpublish/update/republish the corrected data, or possible delete uncorrectable data.

5.4.2 Users

Users include any person authorized to access the RCIED DB. Users can be located on any part of the network from where they can access the BICES server through a web browser.

A User may search only the published datasets in the database. Should a User find problems within any data he/she is viewing, the User should report the problem to the Content Manager.

5.4.3 RCIED DB Administrator and Content Manager

RCIED DB administrator, who may be a national contribution or NATO staff, works for the entire RCIED DB community. The Administrator supports by running the Database as a service within BICES, to build user accounts and control the access for national actors and users.

5.4.3.1 RCIED DB Application Administrator

The RCIED DB Application Administrator works for the benefit of the RCIED community and is responsible for keeping the Database running. He/she is responsible for backup and recovery (in coordination with BGX as a part of level 1 support) and for change management. He/she is also responsible for installing new users and their permissions in the system under the direction of the national point of contact. This role will be fullfilled by NCI Agency as part of the Level 2 and Level 3 O&M support respectively.

5.4.3.2 RCIED DB Content Manager

The RCIED DB Content Manager works for the benefit of the RCIED community and is responsible for the overall quality and consistency of the data in the database by being the central point of contact for resultion of quality issues. The Content Manager will receive reports from Users regarding data quality issues and alert Publishers of problems in the quality or consistency of published data. The Content Manager may set technical flags to highlight technical issues with data and/or administrative flags for problems with format. The function of the Content Manager will be fullfilled by nations on a voluntary basis and shall rotate every year among nations as shown in the table below under paragraph 6.4.

5.5 ACTIVITY DIAGRAM

A high level activity diagram for the RCIED DB is presented in Figure 5. Some of the common interactions with the systems are illustrated in this diagram. Detailed diagrams concerning interaction with core functionalities available in the software framework used by RCIED DB are not included in this activity diagram. Note that all of the Creat, Approve and Publish activities described below may take place either within an national “instance” of the RCIED DB or, at the discretion of the owner of the data, within the RCIED DB itself.

5.5.1 Create

A registered User can create a record in the database by using the interface accessible through a web browser. Once a record is created, it will be saved in the database on the server side.

5.5.2 Approve

The Approver will receive a notification that records are awaiting his attention in the database. The Approver will review the record and if updates are needed will send a notification message to the Creator to inform him/her that the current version of the report is rejected.

The Creator can update the record and re-submit for approval. If the content is valid the Approver can decide to approve the product. Once approved the record will be visible to all users of the database who have roles matching the respective data. A notification is also sent to the Publisher to inform him/her that new data is available in the system and can potentially be released to other RCIED databases.

5.5.3 Publish

The Publisher makes sure that releasable data is synchronised with other databases, if applicable.

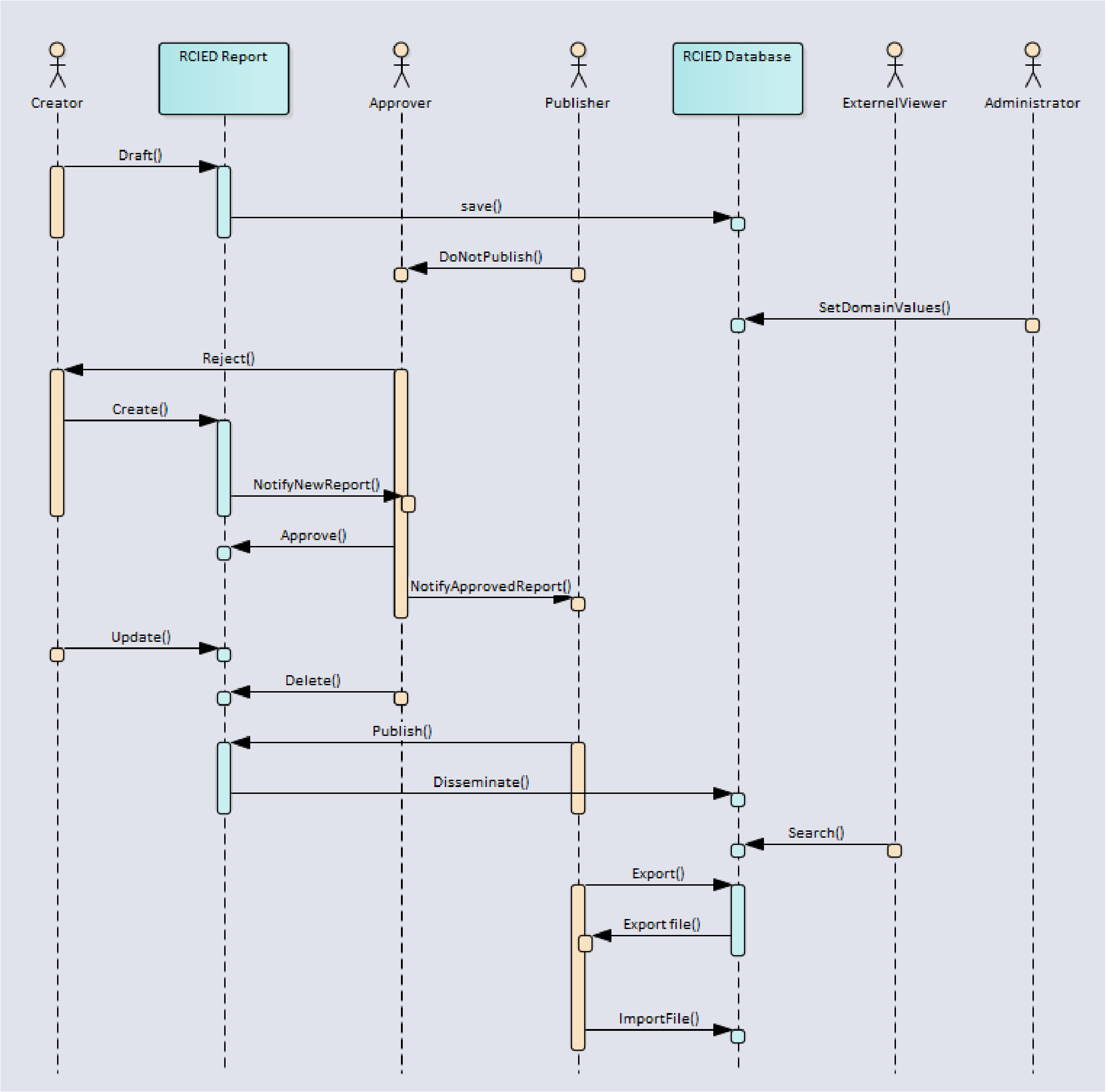


Figure 5 Activity diagram illustrating some of the common interactions of actors with the RCIED DB application.

6. RCIED DB MANAGEMENT PROCEDURES

6.1 RCIED DB COORDINATION MEETINGS

The NATO RCIED Database was developed under the program of work of the Team of Experts on Electronic Countermeasures for Radio-Controlled Improvised Explosive Devices (ToE on ECM for RCIED). A sub-working group of the ToE on ECM for RCIED is the Technical Working Group Electronic Exploitation (TWG ELEX) which will act as **Software Configuration Control Board** (SCCB) for the RCIED DB.

6.2 SOFTWARE CONFIGURATION CONTROL BOARD (SCCB)

The Software Configuration Control Board (SCCB) which will ensure Quality Control of RCIED DB software changes. The SCCB consists of ToE on ECM for RCIED nations, BGX and the NCI Agency staff. The TWG ELEX will provide leadership for the SCCB. The SCCB will:

a. Validate and prioritise Incident Reports and Software Change Proposals (SCPs),
b. Set timelines and responsibilities for implementation and testing,
c. Coordinate with NCI Agency and BGX the tests and the release of new software,
d. Provide regular reports to the ToE on ECM for RCIED (usually at each meeting).

6.3 SOFTWARE INCIDENT REPORTING AND SOFTWARE CHANGE PROPOSALS

6.3.1 Incident Reporting

The BICES service desk will often be the first point of contact for reporting indidents. BICES network related issues will be handled by the BICES system administrator.

Any RCIED DB issues will be reported by the BICES service desk to NCI Agency for resolution. NCI Agency will provide initial support to rectify issues that fall within the scope of RCIED DB O&M support. Any database issues requiring significant resource reallocation will be refered to the SCCB for development of a proposed solution to resolve the issue.

NCI Agency will report to the SCCB on the status of all issues addressed during the previous reporting period and the status of remaining O&M funding, in order to track incidents to burn-rate of funding.

Users will report through national representatives to the SCCB regarding any issues that have not been resolved by BICES or NCI Agency.

The SCCB will report notable issues to the ToE.

Nations are responsible for providing own reporting and support mechanisms for national instances of the RCIED database. Any national incidents that could require changes to the primary RCIED DB (on the BICES server), will be raised to the SCCB for consideration. National Instances may be updated by downloading a patch provided by NCI Agency.

6.3.2 Software Change Proposal (SCP)

Throughout the life and usage of the RCIED DB there will be occasions when improvements are identified, for example to enhance operational effectiveness. Such changes could range from a simple labelling change to a complex re-write of major sections of the RCIED DB application. In all cases, suggested changes to the format and function of the RCIED DB will be controlled and monitored by the SCCB by using the SCP procedure. The SCCB will act as Software Control Authority (SCA) on behalf of ToE on ECM for RCIED. SCPs raised within Nations should be submitted to National ToE on ECM for RCIED representative and SCPs raised by NATO Commands or other entities should be sent directly to the NCI Agency Staff.

6.3.2.1 SCP Procedures

6.3.2.1.1 Raising a new SCP

a) SCP received by SCCB.

b) SCP acknowledged.

c) SCP reviewed by SCCB and comments added, as required.

d) SCP sent to NCI Agency for evaluation of technical feasibility, time to complete and implications, including level of impact on the RCIED DB (including national instances) and resource implications,.

e) SCCB review comments from NCI Agency and, if further action is required, forwards a recommendation to the ToE for 30 day “under discussion” period.

6.3.2.1.2 Under Discussion

a) At any time during the 30-day under discussion period free text comments and attachments can be added to the SCP.

b) When any comment is added to the SCP all ToE on ECM for RCIED members will be informed by email.

c) SCCB review comments and action as required.

d) Any nation may reject the SCP at this stage. Rejections should contain a short justification statement. All ToE on ECM for RCIED members will be informed of a rejection by email.

e) After 30 days the SCP enters the 10-day “Ready for Approval” stage. All ToE on ECM for RCIED members are informed that the SCP has changed status.

6.3.2.1.3 Ready for Approval

a) At any time during the 10-day ready for approval stage free text comments and attachments can be added to the SCP.

b) When any comment is added to the SCP, all ToE on ECM for RCIED members are informed by email.

c) SCCB review comment and action as required.

d) This is the final stage where any nation may reject the SCP. Rejections should contain a short justification statement. All ToE on ECM for RCIED members will be informed of a rejection by email.

e) After 10 days the SCP is considered to be “Approved”. All ToE on ECM for RCIED members are informed that the SCP has changed status.

6.3.2.1.4 Approved

a) All ToE on ECM for RCIED members are informed that the SCP is approved.

b) SCCB will forward the SCP to NCI Agency for implementation.

c) NCI Agency implements the SCP into the relevant Beta version of the program and briefs the SCCB on the change and its implications. NCI Agency also includes the details of the change in the Help – Program Status display.

6.3.2.1.5 Implementation

a) Originator and SCCB review the program change to ensure that the SCP has been correctly interpreted and implemented.

b) When Beta version of the program has been approved by SCCB the SCP is closed. All ToE on ECM for RCIED members are informed by email.

c) Any nation submitting a SCP must also take responsibility for the reflective changes to the manuals.

d) National Instances may be updated by downloading a new release of the RCIED DB software provided by NCI Agency.

6.4 CONTENT MANAGEMENT HANDOVER

The function of the Content Manager rotates regularly. The rotation will be discussed in a TWG ELEX and will be decided in the ToE on ECM for RCIED Meeting each year. The rotation example is shown in the table below.

2019	2020	2021	2022	2023
Nation_1	Nation_2	Nation_3	Nation_4	Nation_5

6.5 USER MANAGEMENT

A User Role Concept is implemented in the RCIED DB. There are user roles with associated rights implemented. After a User has asked for a user account, and his need to have access to the database is approved by the National Point of Contact (NPoC), his user account will be created by the Application Administrator. Each nation has a NPoC for all user account requirements. The NPoC is the national head of delegation to the ToE on ECM for RCIED, although this duty may be delegated. Additional approving authorities will be recognized by the ToE on a case-by-case basis

6.6 DATA MANAGEMENT

A Data Management workflow is implemented in the RCIED DB. After a Dataset is edited or updated, the Creator can push the "Approve" button to send it to an Approver . Now the Dataset is only actionable for the Approver. The dataset is stored in the folder "to approve". The Approver can reject it by pushing the button "Reject" or the Approver can send it to the Publisher with the command "Publish". The Publisher is responsible to control the distribution of the information to the RCIED community depending on the releasability of the information .

6.7 QUALITY CONTROL

Quality control is made at all levels. The ultimate arbiter for quality is the Publisher.

6.8 DATA SHARING

Data sharing is controlled by the Publisher. The Publisher sets flags for the releasability of his or her dataset.

6.8.1 Access control at the application level

ToE on ECM for RCIED, through National and appointed PoCs, is the vetting agent. NCI Agency, the Application Administrator, will create the accounts.

6.8.2 Manual release to Non-NATO Entities

Nations own the data in the RCIED DB. Upon publication, the Publisher will set flags for releasability. Subsequent to publication, Users may manually export data in accordance with the releasabilty of the data.

6.9 DOMAIN VALUES MANAGEMENT

SCCB approves addition, alteration and/or removal of domain values for execution by NCI Agency as part of O&M.

7. ACRONYMS AND DEFINITIONS

AADE	Advanced Aggregate Data Extractor
AAP	Allied administrative publication
AEP	Allied engineering publication
AC	Atlantic Council
AIntP	Allied intelligence publication
AJP	Allied joint publication
APP	Allied procedural publication
AtN	Atack the Network
BGX	BICES Group Executive
BICES	Battlefield Information Collection and Exploitation System
BI-SC AIS	Bi Strategic Commands Automated Information Systems
BOD	Board of Directors
C2	command and control
C-IED	Countering Improvised Explosive Devices
CIS	Communication and Information System
COI	Communities of Interest
CONEMP	Concept of Employment
CREW	Counter RCIED Electronic Warfare
DB	database
ECM	electronic countermeasures
ELEX	electronic exploitation
EUMS	European Union Military Staff
EW	electronic warfare

HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IED	Improvised Explosive Device
ISAF	International Security Assistance Force
MC	Military Committee
MS4W	Map Server for Windows
MS IIS	Microsof Internet Information Services
NATO	North Atlantic Treaty Organisation
NCI Agency	NATO Communication and Information Agency
NNN	non-NATO partner nations
NPoC	National Point of Contact
NS	NATO Secre*
WAN	Wide Area Network
O&M	operation and maintenance
R&D	research and development
RCIED	Radio Controlled Improvised Explosive Device
RFT	Remote FOB Trigger
RSM	Resolute Support Mission
SCA	Software Control Authority
SCCB	Software Configuration Control Board
SCP	Software Change Proposal
SIR	Software Incident Report
SOP	standard operating procedure
SQL	Structured Query Language

SRS	Software Requirement Specification
STANAG	NATO standardization agreement
STANREC	NATO standardization recommendation
ToE	Team of Experts
TWG	Technical Working Group
VNCF	Voluntary National Contribution Fund
WEAT	Weapon Exploitation and Analysis Tool
WMS	Web Map Service
XML	Extensible Markup Language

AEP-4803.1(A)(2)