

Chapter 7 – RECOMMENDATIONS

7.1 DYNAMIC RISK ANALYSIS

With the new concept of operations outlined in the NNEC or NCW concepts there is a need for dynamic risk assessment. Dynamic risk assessment refers to a risk assessment that can be updated quickly as the system being assessed changes. These changes for example may be due to:

- The operational threat level;
- The mission type (peace support operation, humanitarian operation, high intensity fight, ...);
- The incremental system development; and
- The deployment phase.

In the current and near-term situation, the mission network is centrally managed, with the participating nations bringing their own equipment not attached to their own national networks. In the transition to the NEC, the mission networks will become less centralized and more of a federation of networks – with consequent impact on responsibility for dynamic risk assessment and deployment of tools supporting dynamic risk assessment.

Another aspect of dynamic risk analysis concerns the feedback between vulnerabilities detection tools and the results of the initial risk analysis which identified potential and generally high level vulnerabilities.

7.2 INFORMATION EXCHANGE REQUIREMENTS

7.2.1 For Systems Interconnections

When two CIS are required to be interconnected to exchange information, an SISRS (or national equivalent(s)) should be formulated, which forms the basis of a security agreement between the two CIS operating authorities (or between the two system managers) and the two security approval or accreditation authorities. SISRS, relies on risk analysis performed by one party, and is approved by both parties.

It is then of major importance that the results of risk analysis can be exchanged and understood by both parties.

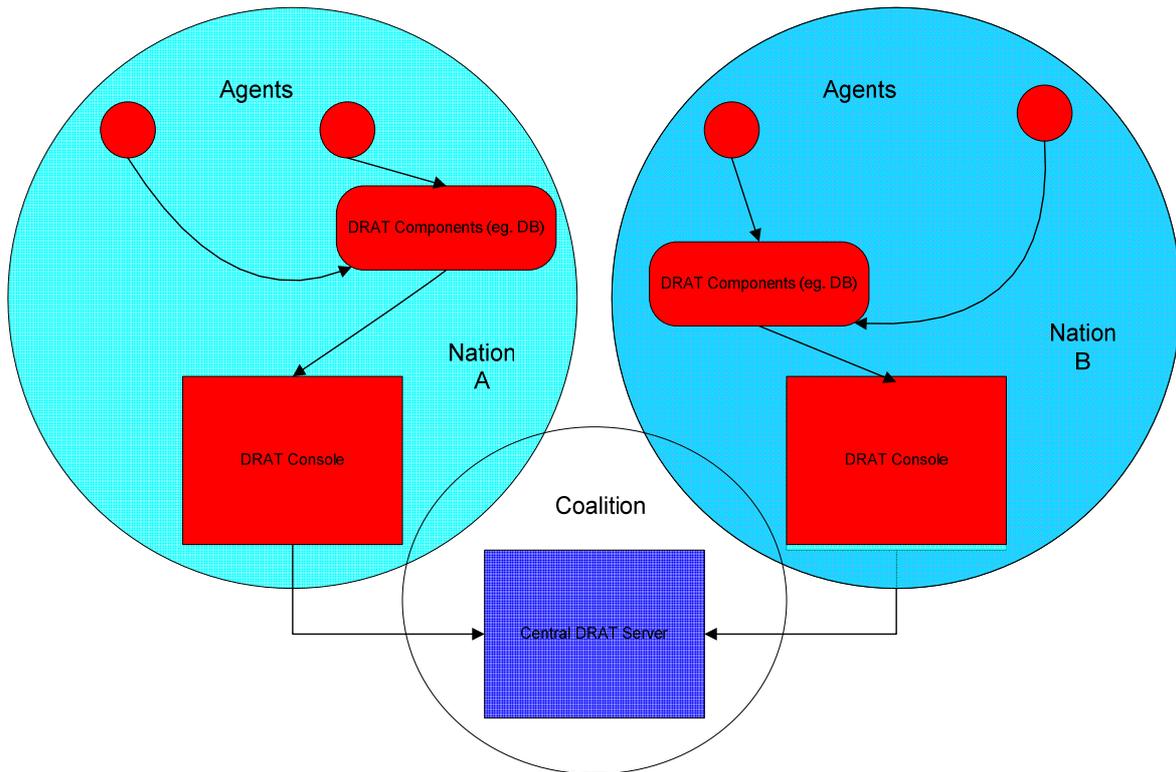
7.2.2 To Update a Common Threat and Vulnerability Repository

Having common profiles for system assets, threats and vulnerabilities will greatly facilitate the sharing of this information and could permit the creation of a common and shared threat and vulnerability repository. Annex B and C give examples of such profiles for threats and assets.

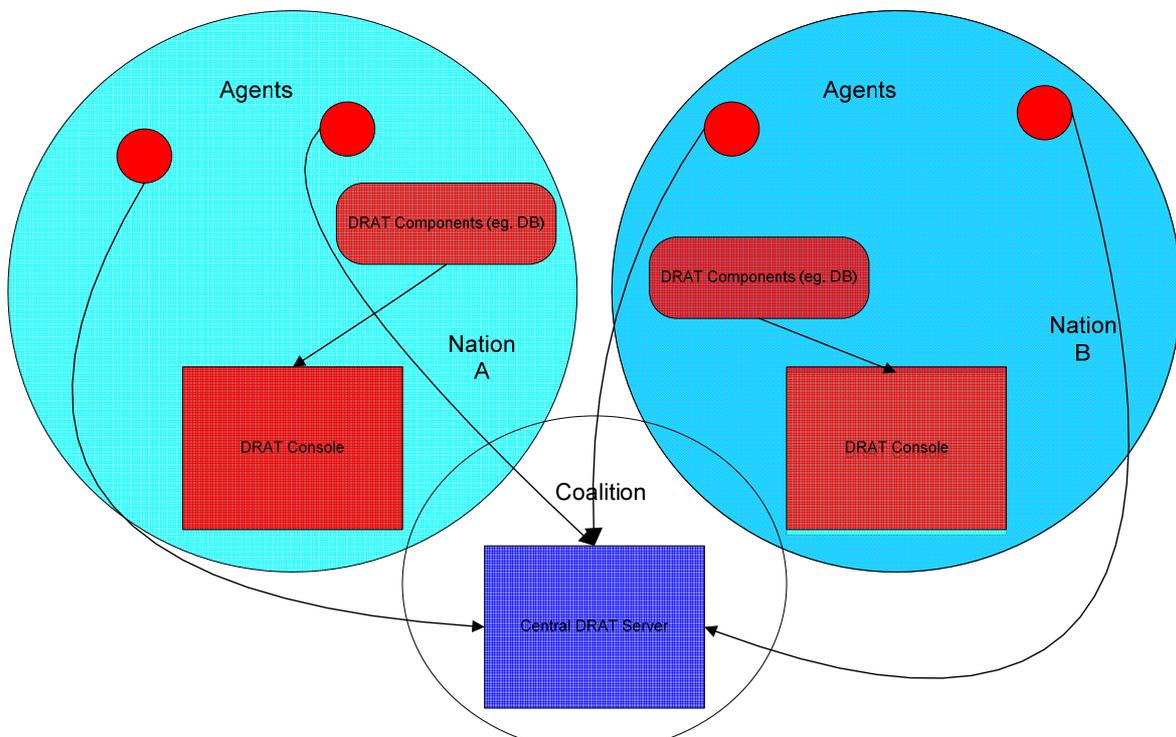
7.2.3 Within a Coalition

In attached coalition networks, a nation can maintain and control the scope of the dynamic risk assessment on their domain of control. This would allow them to limit network information disclosure if necessary by national policy.

The NNEC foresees all dynamic risk assessment tools under national control only. In that scenario and in the phases leading up to it, national systems can run their own dynamic risk assessments and pass the output to be correlated with a central tool, or to the tool of another partner, as illustrated in the below figures. Alternatively or in parallel, the components could send information straight to another partner's tool depending on the architecture or policy.



Logical Reporting Case – Consolidation of Multiple DRA



Logical Report Flow – Agents Report Directly To Central Server

Figure 7-1: DRA, Alternative Architectures for Coalitions.

The final objective is to obtain a “Consolidated Information Assurance Picture”. The features of this CIAP as well as the nature of the exchanges between the different components are still to be defined by the Nations.

7.3 PROPOSED EVOLUTIONS OF EXISTING METHODS AND TOOLS

To help interoperability between risk analysis performed using different methods and to help the TRA users a set of additional functionalities have been identified.

- Methods should be based on documented models (e.g. impact model, risk model, threat model, threat agent model, entity model, entity relationship model, vulnerabilities model). It should be possible for a user to improve or to replace these models. This implies the modularity of the methods.
- Methods should use a technical repository for assets, threats and vulnerabilities. The mid term objective should be to use the common repository described in 7.2.2.
- Methods should be quantitative instead of qualitative.
- Methods should use the principle of refinement (more depth) to reuse and improve TRAs.
- Methods should allow reusability: it should be possible to reuse the result of a previous risk analysis on a system, sub system or component and to include these results in a new analysis.
- Methods should allow to reuse of the vulnerabilities analysis done during a product evaluation (CC, FIPS 140-1) or a system security testing.(vulnerabilities scan, IDS, ...).
- Tools should be able to implement accurately the methods, to interface with external repositories, and to offer a user friendly interface.
- When performing risk assessment or when identifying countermeasures, tools shall be able to take into account the standard NATO security measures (physical, procedural) and the NATO technical security requirements.
- Tools should offer functionalities to conduct high level risk analysis in a time frame coherent with the new needs for system deployment and accreditation. Detailed risk analysis should be refined from these high levels ones if necessary.
- Tools should offer simulation capabilities or at a minimum extended “What if” functions, in order, for example, to select the most appropriate countermeasure or to identify the impact of a change in threat level, in system architecture / configuration.

7.4 FOLLOW ON ACTIVITIES

7.4.1 Within RTO/IST

An IST workgroup should streamline the Consolidated Information Assurance Picture and Dynamic Risk Assessment concepts, which are two key capabilities listed in the NATO Network Enable Capability (NNEC) Information Assurance roadmap to be published in early 2007 by ACT.

The Consolidated Information Assurance Picture can be seen as a first step in Cyber Command and Control giving operators visibility on what is currently going on in the Communications Information System (CIS). This will enable the operators to make proper decisions on what actions to take.

The Dynamic Risk Assessment (DRA) is to an additional component in the Cyber Command and Control Capability. The DRA tool will be able to feedback to the sensors based on threat levels and policy.

RECOMMENDATIONS

Actually no formal concept is recognized, no clear methods are formalised and no empiric or commercial tools seem to exist. Nevertheless, these two needs are explicitly identified and required insomuch capabilities at mid and long term for the NATO Network Enable Capability.

7.4.2 Within Other NATO Entities

This IST report should then be transmitted to the NATO Computer Incident Response Capability (NCIRC) and the NATO Security Accreditation Board (NSAB), in support of their current missions.

The output of this group and more precisely the 7.3 should be used for the selection and procurement of risk analysis tools in support of the Capability Package CP0A0155 for Electronic Information Security Services (called INFOSEC CP 155).

NC3A, implementing the ACT Experimental and Scientific Program of Work (EPOW and SPOW) should consider this report and take inspiration in its production. Moreover, NC3A is encouraged to continue its effort to liaise with IST forums on following activities in this area and to report back (on behave ACT) on the progress done within the EPOw and SPOW.

The INFOSEC Subcommittee (number 4), belonging to the NATO C3 Board Substructure, should be presented some IST results to raise the awareness of the operational and technical INFOSEC community, on the work done by scientific INFOSEC community.