

Coordinating National Research

Geir Hallingstad

NATO C3 Agency
P.O. Box 174, 2501 CD, The Hague
The Netherlands

Geir.Hallingstad@nc3a.nato.int

Jim Obal

HQ SACT
7857 Blandy Road #100, Norfolk, VA 23551
United States

Jim.Obal@act.nato.int

Marko Jahnke

Research Institute for Communication,
Information Processing and Ergonomics (FGAN-FKIE)
Neuenahrer Str. 20, D-53343 Wachtberg
Germany

jahnke@fgan.de

ABSTRACT

Many nations are currently initiating information assurance related research and product development activities. As the objectives of these activities are more or less overlapping, the potential gain by multi-national cooperation is large. This paper mentions some of the traditional problems of such cooperation, and looks at how cooperation can be performed and how the nations can achieve shared awareness of research activities. With proper multi-national cooperation in the area of information assurance, the path to a network enabled capability will be quicker and easier for all parties.

1.0 INTRODUCTION

With the advent of the concept of Network Enabled Capability (NEC), many nations are currently looking at how to further technology in order to best support this military concept. As a result, the research objectives for many different nations will more or less overlap, and the potential gain from well coordinated activities between nations is large. However, this requires some form of cooperation between the nations and shared awareness of research activities to a higher degree than today.

There are numerous information security and information assurance (IA) related research initiatives that are in process within different nations, their technical research organisations, commercial industries and subordinate government organisations. Information pertaining to these initiatives is sometimes provided by briefings and documented updates from the nations but there is no common repository for such information making it difficult to find. Further, the information is often not complete and presentations are often non-uniform in structure, content, and terminology, making it difficult to fully utilise the information.

Regarding IA related products, an increasing number of products are emerging. High assurance products are frequently initiated by government hosted programmes, either by acquisition or by being the launching customer for a security product for wider use. However, the resultant high-assurance security solutions are subsequently often held in close control by those sponsoring nations. The resulting lack of high-assurance solutions on a global basis often blocks the introduction of new information and

Coordinating National Research

communications systems in coalitions.

Many national projects that depend on research initiatives are managed by programme managers who are not subject matter experts in IA related disciplines. It is not unusual for these managers to focus on the broader aspects of their project's functional areas rather than to recognise the criticality of the IA function with regards to their respective project. This typically minimises or marginalises the importance of IA related products, and often both lengthens the time to achieve proper assurance as well as limits functionality. Proper awareness of the role of IA in NEC and the research activities might aid in this situation.

This paper considers how nations can cooperate and how shared awareness of research activities can be improved. Section 2 and 3 looks at multiple ways to cooperate, section 4 addresses shared awareness, section 5 looks at the problem of terminology and understanding, and sections 6 and 7 concludes and gives recommendations.

2.0 PARALLEL EFFORT VERSUS SINGLE EFFORT

In order to advance technology and knowledge, and to be able to properly support an NEC environment, research collaboration will be required in general, also including computer security. While the most common modus operandi is that each nation performs its own research independent of other nations, this is unlikely the most efficient way of advancing technology. Taking advantage of common interest among nations to advance quicker or achieve higher quality should be a goal.

2.1 Multiple Single Efforts

Having multiple single efforts without any coordination or sharing of results has been the traditional way of doing military research. Each nation would do their own research tailored to their own requirements, which usually were unique to the nation. Little information sharing took place, with the possible exception of publication of the results after project completion.

2.2 Combined Effort

In a combined effort, multiple participants join forces to research and develop technologies or prototypes according to a common need. Even though the objectives of the effort might not be perfectly aligned, the commonality of the work is large enough for the work to be beneficial to all parties. Such common effort ensures that no duplicate work is taking place and that the solution can be applied by all the participants involved.

2.3 Parallel Effort – Common result

In a parallel effort, duplicate work is performed by multiple participants. This might seem like inefficient use of resources, but if the result is common amongst participants this approach can yield great advances both in technology and knowledge.

This approach has been used successfully in several different scenarios. DARPA's Grand Challenge [6] is one example where multiple participants have competed to create different kinds of autonomous vehicles. While not looking for a particular solution, the Grand Challenges have greatly advanced the research within robotics and autonomous control. In the Advanced Encryption Standard (AES, [5]) competition hosted by the National Institute for Standards and Technology (NIST) in the USA, multiple participants competed to find the best encryption algorithm. This was both beneficial for the cryptologic research, as well as producing a result that would have great impact – The AES algorithm currently used in many

modern encryption products. NIST is currently organising a similar competition to replace today's hash algorithms.

Parallel effort can be a great driver for technology in that it creates a community working on solving the same problem, and at the same time awakes the competitive spirit. There is however a need for creating a shared setting or a common problem in order to coordinate the activities, such as has been done by the competitions previously mentioned.

3.0 COORDINATION VERSUS INTEGRATION

When similar research activities are undertaken in multiple nations, there is a potential benefit in co-operation. Such cooperation can take place through coordination or through integration. In a coordination approach, each nation retains its own objective and works with the other participants who might have similar objectives. In an integrated approach, each participant commits resources and one common objective is created by and for the participants.

3.1 Research Coordination

When coordinating research the participants work with other participants who have somewhat aligned objectives, even though they are not identical. The benefit of such coordination can be related to how aligned the objectives of the participants are. If the objectives are very divergent, the coordination is less likely to succeed as the work performed for coordination has to be done in addition to the primary work load.

RTO is based on research coordination, where each nation participates in technical activities based on its own funding. While the topics can have interest for several nations, the ability to actively contribute to the activity varies depending on national funding. With some activities spanning multiple years, it is also possible that the objectives were originally aligned, but as time moves on, the national objectives change. This makes it difficult to keep the active contributions.

In order to effectively coordinate between individually funded activities, it is necessary that the activities are aligned. Alignment of national program can be done if there is sufficient time from a technical proposal to the start of the activity. This would give interested nations time to plan and fund such activities with basis in the proposed technical activity. The interested participants could then ensure that their own programs are aligned with the primary objectives, and the likelihood of a highly fruitful coordination activity is increased.

3.2 Multi-national projects

Whereas coordinated activities are nationally funded, multi-national projects are typically formed by funding commitments from the nations. Either the nation just commits contractually to put a given amount of resources in a project, or a separate project organisation is set up to handle the project including funding. In this case, all the participants in the project work towards the same objective, and there is no problem of misaligned objectives among the participants. INSC , STP, and the NNEC Feasibility Study, are examples of such multi-national programs.

A drawback of a multi-national program is that they usually require a long setup time due to the requirement of multi-national contracts, memorandums of understanding between governments, and possible separate project organisations and reporting lines.

During the execution phase of a multi-national project, the resources are committed to the project. The

Coordinating National Research

drawback compared to a coordination approach is the longer setup time necessary. Aligned and coordinated approaches also have longer setup time, but does not require the contractual agreements between participants making it slightly more flexible but prone to changes in objectives.

4.0 ACHIEVING SHARED AWARENESS

There exist many independent nationally funded research and development organisations that could assist in the resolution of NEC security related issues. Similar capabilities exist within international organisations like NATO that are focused on the development of InfoSec/IA related products. If information pertaining to these national and organisational specific project initiatives was shared during the conceptual stage, significant time and cost savings could be gained by forming co-operative ventures minimising the opportunity for duplication of effort.

4.1 Willingness to share

Availability of technical specifications pertaining to high assurance and cryptographic related products is often limited by national trade agreements and technology transfer regulations, effectively delaying the fielding of high assurance products in coalitions and multi-national organisations. Similarly, relevant product information for many reasons is not shared with other programme managers and subject matter experts outside of the national project sphere which expands the security product technical gap further.

Knowledge of emerging security products is generally withheld by nations until confidence in the product is attained prior to official release. The emergence of similar competing products from other national sources is not unusual during this lull. This reduces the effective availability of security products that may have otherwise contributed to the resolution and minimisation of the current international security dilemma confronting NEC and other related cross domain requirements. Proper sharing of information would enable quicker availability and better interoperability in the NEC environment.

4.2 Difficulties of sharing

Even if the willingness to share is in place, it is not always easy to achieve proper information sharing. The reasons include differences in the nature of the exchanged information such as:

- The amount, structure and detailedness of relevant information that is releasable from nations differ. This is due to the heterogeneity of the information exchange policies and is not expected to change in the future.
- People who participate in the coordinating initiatives have different educational and professional backgrounds and often do not share the terminology. On one hand, this makes it difficult to harmonize activities; on the other hand, different points of view may contribute to more substantial output. For a more detailed view on terminology, see sect. 6.0 of this contribution.
- If the topic to be discussed is as broad as the whole area of IA, it is almost impossible that all participants are equally experienced in each of the relevant aspects of the topic. For instance, some persons have a fairly good knowledge in cryptography where others are specialized in using network management measures to prevent attacks. Again, this has the advantage of different view angles, but may impair common understanding.
- The participants' connection to their national military, public administrative and scientific communities differs largely. For some persons it is easy to obtain the requested information; for others it seems almost impossible – especially if a common structure and degree of details is needed.

- Although there is a might be a commonly agreed minimum amount of working effort for contribution, the working plans of the different persons differ and may lead to synchronization problems. Again, contributing to an information sharing effort while being responsible for other activities on the national side helps to broaden the view angle but might reduce the amount of work that goes into sharing efforts.

4.3 Information sharing approaches

A framework for sharing information about national and coalition research activities, deployment campaigns, events (conferences, symposia, workshops, etc.) and relevant literature is warranted. Such a framework can rely on different approaches, from unstructured to structured and from informal to formal.

A formal and structured approach to increase shared awareness is to maintain centralized or synchronized databases which hold the available information and allow features like extensive searching and cross-reference capabilities. A good civilian example for such a database is the Community Research & Development Information Service (CORDIS) of the European Union [1]. Civilian literature and event databases already exist and may be adapted for military research coordination efforts (e.g. Computer Science Bibliographies [1], CiteSeer [2], Secorvo IT Security Event Database [3]). Clearly, formal restrictions on who may have access to the information need to be established.

Before joining a coordination initiative, each nation must commit itself that it is willing to provide information with the agreed structure, sensitivity and detailedness. An example for a record in a research activities database might look as shown in Figure 1. Note that an extensive usage of hyperlinks makes information retrieval easier and may also help in generating a high-level picture of inter-dependencies between activities, projects, organizations, publications and so on.

Identification	10
Short Name	MITE
Objective	MANET Intrusion Detection for Tactical Environments
Nation	DEU
R&D Organization	FGAN/FKIE; FhG IGD; German Universities
International Relations	DRDC-RDDC Ottawa, CA, NIO section
POC	Marko Jahnke <jahnke@fgan.de>
Sponsoring Organization	German Federal Office for Information Management and Information Technology (IT-AmtBw)
Time-frame	2005-2008
Size (persons/year)	~5
Short Abstract	Scenario based threat analysis for small-scaled tactical MANETs; development of algorithms and supporting IDS components to detect attacks against tactical MANETs
Types Of Activity	Study, Experiments, Prototype
Categories	Traditional Cyber Defence, Defense Measures for New Network Technologies
Available int'l Literature	M. Jahnke, S. Lettgen, J. Tölle, M. Bussmann, U. Weddige. A Robust SNMP based Infrastructure for Intrusion Detection and Response in Tactical MANETs. In: Proceedings of the GI/IEEE Conference on „Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA2006), Berlin, pp. 164-180, jul. 2006. ...
Available nat'l Literature	...
Appearances on conferences	DIMVA 2006, Berlin, Germany. D-A-CH Mobility 2006, Ottobrunn/Munich, Germany. MILCOM 2006, Washington D.C. USA. ...
Cross references to other projects	Cooperative Intrusion Detection in Dynamic Coalitions, FGAN/FKIE, DEU Security for MANETs, DRDC-RDDC Ottawa ...

Figure 1 – A Research Activity Database Record

Coordinating National Research

A computer aided but informal approach to information sharing would be to create an online information and discussion board, similar to Wikipedia [4]. A so-called wiki can be a web site where visitors can enter information in either free form or with some structure. In a research coordination setting, this would mean that the participants of a certain project in a given nation would present the project, give its relevance and objectives and the participants would also update the wiki as to the project progressed. Figure 2 shows an example of what a wiki page for a project could look like.

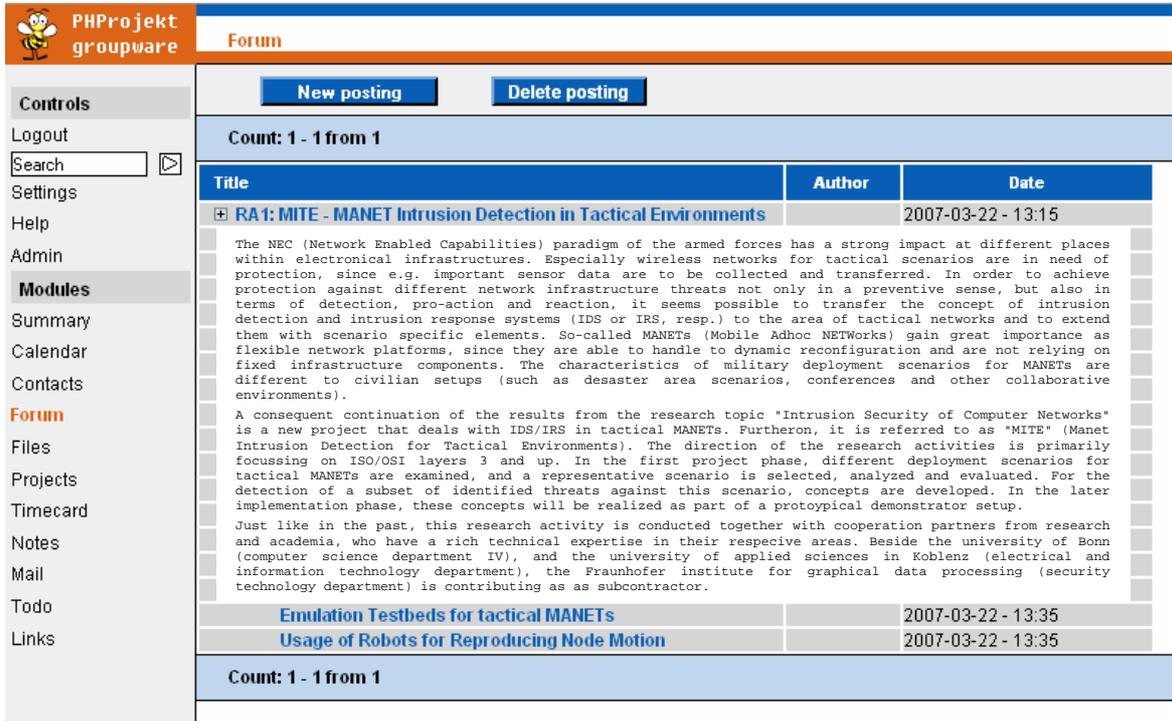


Figure 2 – A Wiki Page for a Research Activity

With powerful search capabilities, a wiki approach could be beneficial in both a structured and unstructured approach. However, a semi-structured approach, for example one where the setup of a wiki page has some mandatory sections, could make it easier to find information quickly.

5.0 THE ROLE OF A COMMON TERMINOLOGY

Unsurprisingly, a common terminology has a key role in the process of sharing information in order to establish coordinated research activities. In many initiatives, the process of establishing a common understanding of the keywords takes a long time and shortens the available time for conducting the program of work itself. Unfortunately, it is a common understanding in linguistic sciences that establishing a common terminology takes its time, and no general framework or technical support system is known that shortens this process. Clearly, seeing things from different angles may enrich a discussion and may also help to understand potential difficulties. But as long as the coordination of research is the main focus of the initiative, terminology discussions are a potential stumbling block.

A potential solution on this might be to establish a basic terminology prior to the working period of an initiative or during a limited time period. This terminology (including a reference case and/or a taxonomy of the terms, wherever possible) needs to be agreed by all initiative members as a discussion basis for the rest of the working period. A list of the relevant terms and their relationships might be a part of a “Terms of Reference” document. All individual differences in understanding terms might be written down in

dedicated, continuously updated documents (e.g. as supplements to the “Terms of Reference”), rather than being discussed repeatedly. This allows to honour individual points of views without hampering the working process of the initiative.

An alternative might be the usage of an according online discussion board (as suggested for the information sharing process, see above) that records the terms and potential differences in understanding. This might also help to reconstruct discussions and to retrace chains of discussion arguments.

6.0 CONCLUSIONS

The common vision of NEC is shared between numerous nations. It is commonly agreed that the implementation of the NEC paradigm is only feasible in a cooperative and synchronous manner. Since a lot of research and scientific work is needed in order to accomplish this vision, strategies and procedures to bundle the existing and planned activities are more than welcome. Obviously, coordinating national and NATO research activities is one way to leverage existing efforts, since all participating entities have the same objective. Aligning national programs to common research strategy may also help to avoid multiple single efforts and to place investments more effective.

Obviously, national and NATO information sharing policies urgently need to be revised in order to respect the benefits that can be achieved by existing and future coordination initiatives. Whatever may be useful to share (under proper access restrictions as mentioned above) may support the coordination process and thus help to save resources. A strong commitment of the participating nations and NATO bodies to give input to the strategy is inescapable.

The quantity and the internal structure of the information about past, current and planned research activities that the nations are willing to contribute, differs largely. A common terminology has a key role in the coordination process, but unfortunately, supporting technical or procedural measures for establishing a common terminology quicker are not visible on the horizon. A common agreement on terminology, quantity and structure of the exchanged research activity information would ease the process of developing a research strategy.

The way of exchanging information can either be formal or informal. Both extremes have their advantages. The formal way – combined with the strong commitment mentioned earlier – will support the strategy development process efficiently. The informal way potentially enables more contributors to feed information into the process, since also incomplete or vague pieces of information would fit there. A semi-formal approach with the support of online systems might be the most promising solution for this.

7.0 RECOMMENDATIONS

The following recommendations can aid in improving national research coordination:

1. That the RTO sets out objectives to be achieved within a number of areas 1-2 years before the task is started in order to allow nations to individually fund these activities. This also fits in the current approval cycle of the RTO.
2. That the nations and NATO define their activities as much in the direction set forth by the RTO as possible in order to reap the highest benefits. NEC is about making an effective collaborative environment, not perfect individual solutions.
3. That nations and RTO agree on structure and amount of exchangeable information about current and planned research activities in the area of information and communication systems (an example

Coordinating National Research

was given within this paper).

4. That the RTO be tasked to set up and administer a Research-Wiki where the nations and NATO can share information on their research activities in a fairly informal and semi-structured way.

8.0 REFERENCES

- [1] Community Research & Development Information Service (CORDIS). Online available at <http://cordis.europa.eu>.
- [2] The Collection of Computer Science Bibliographies. Online available at <http://iinwww.ira.uka.de/bibliography/index.html>.
- [3] CiteSeer – Scientific Literature Digital Library. <http://citeseer.ist.psu.edu/citeseer.html>.
- [4] Secorvo IT Security Events Database (in German). Online available at <http://www.veranstaltungen-it-sicherheit.de>.
- [5] Homepage of the Wikipedia Project. Online available at <http://www.wikipedia.org>.
- [6] AES – Advanced Encryption Standard. FIPS Publication 197.
- [7] The DARPA Grand Challenge Homepage. Online available at <http://www.darpa.mil/grandchallenge/index.asp>.