
Finnish Defence Forces – Network-Centric Operations

A Problem and an Opportunity ¹

Disaster can strike at a moment's notice, and an ineffective response can cost thousands of lives. But only rarely do crises fit in neat boxes, perfectly suited to the capabilities of one organization. Like other military organizations facing crises or conflicts – such as Hurricane Katrina, the SARS epidemic, or the war in Iraq – the Finnish Defence Forces (FDF) are increasingly being asked to assemble or participate in networked coalitions with diverse military and civilian organizations. Critical scenarios might require coordination between the Air Force, Navy, police, hospitals, and other military and civilian groups.

To operate effectively in such environments, the groups involved must quickly agree on a method of working together in what are often extremely stressful and unpredictable situations. Technological incompatibility can complicate coordination, particularly when groups operate under different technical architectures and communication protocols. After the September 11 attacks on New York City's World Trade Center, for example, the police and fire departments were not able to communicate with each other because their radio systems were incompatible.² Consequently, the police weren't able to warn fire fighters that the building they were in was likely to collapse.

In a similar fashion, the FDF's "silo-ed" organization and technology make emergency response coordination difficult. Their command, control, communications and computing (C4) systems were each developed to support only one branch of the military, as were many of their business processes. Major General Markku Koli, the FDF's Chief of Operations, states, "Most of our current C4 systems are stove-piped systems to support Army, Navy or Air Force operations. We face the same challenge as most of today's militaries. We cannot afford to develop future systems on top of old systems by patching and bridging gaps and trying to maintain old technology. ... Technical, data, and application integration can take us only so far."³

Fortunately, the FDF has begun to uncover opportunities that could be achieved through operational, technical and cultural changes. A few small FDF initiatives have revealed promising new ways of conducting business. For example, in 2004, the Finnish Kosovo Peacekeeping Force deployed, tested, and implemented a Deployable COTS Network (DCN) that integrated military and non-military voice communications (previously run under separate networks and protocols) for daily command and control operations. The FDF realized that different groups, such as the police, military, fire, and rescue services, could use this capability to cooperate during a crisis at both the tactical and strategic levels, and without compromising security.

This case was written by Karianne Gaede, Research Affiliate, Leadership for a Networked World Program, under the supervision of Jerry Mechling, Lecturer in Public Policy at the John F. Kennedy School of Government, and Faculty Chair of the Leadership for a Networked World Program.

© 2007 by the President and Fellows of Harvard College. No part of this publication may be re-produced, revised, translated, stored in a retrieval system, used in a spreadsheet, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the written permission of the John F. Kennedy School of Government.

FiNED: Transforming the Military

Major General Koli knew that network-centric operations would require a major transformation of technology, organization, and process. Because only a small window of opportunity was available, the FDF needed to act decisively, boldly, and proactively.

Koli and his team had reviewed a substantial amount of research on network-centric operations. They knew about the promise of networking in the military, but they needed more direction. Where should they begin? Would the changes they needed take two years or ten? They studied a number of private sector companies, benchmarking their successes and analyzing their challenges. These studies convinced the FDF that the potential value was real. A Nokia study was particularly persuasive. Like the FDF, Nokia needed to break down a “stovepipe” structure. They began to implement network-centric operations in 1999, and completed the work approximately 5 years later. Koli and his team were convinced that they could achieve similar results in similar ways, but in a slightly longer timeframe.

In 2003 the FDF team, led by Koli, proposed a new program, called Finnish Network-Enabled Defence (FiNED), aimed at achieving network-centric operations within a decade. FiNED aims to transform Finland’s homeland security and crisis management infrastructure through greater and more flexible interagency and international collaboration. This includes collaboration with groups such as Customs, Border Guard, Police, Fire and Rescue, state ministries and industry, and international organisations such as NATO and the European Union. According to Admiral Juhani Kaskeala, Finnish Defence Chief: “It is not alone about technical change. We need to educate leadership and train organizations to make functional change happen. We have to learn to do better things as well as to do things better. We cannot use service-specific processes to carry out joint planning. We must create a single joint process to link the respective planning processes.”⁴

FiNED is planned to result in a new kind of partnership and a co-operative culture between information technology, organizational, and process structures. Together these structures will improve and will integrate data and weapon systems to support command and control of joint and territorial operations. Key requirements include interoperability with NATO; the integration of weapons systems; implementation of intelligence, surveillance and reconnaissance (ISR) capabilities; and the transfer of expertise in mission command, planning, task delegation, and information technology to a central program.⁵

FiNED will also result in a significant reduction in the number of systems to maintain. According to the FDF’s CIS Chief Architect, Mika Hyytiäinen, the FDF currently has over 300 legacy IT systems, mainly weapons systems and associated infrastructure. Many of these systems perform the same functions but in different locations or different divisions. During FiNED, many of these systems will be consolidated onto a common service, reducing the number of systems to tens, instead of hundreds.

The FiNED program is divided into five phases that must be complete by 2012:

- C4ISR:¹ Upgrading the technical infrastructure. The FiNED team will perform technical and data integration of selected legacy systems plus some new technology. Non-strategic legacy systems will be retired, but selected strategic legacy systems will be decomposed and reused.
- (i)C4ISR [initial integrated C4ISR]: Integration of existing stovepiped systems into a common network accessed via a common portal. The administration network (AdminNet) will be separated (decoupled) from the operations network (OpNet). By consolidating and simplifying AdminNet, the FDF’s technology staff will be able to focus more attention on the complex and sensitive operational components.
- iC4ISR [integrated C4ISR]: Eliminating the “stovepipes” so that users within and outside the FDF can rapidly reorganize organizational boundaries and flexibly share information. This requires significant process innovation and changes in capability. This stage will bring about the implementation of Service-Oriented Architecture (see Appendix C: Service-Oriented Architecture) and the retirement of all non-strategic legacy systems.

¹ Command, Control, Communications, Computing, Intelligence, Surveillance and Reconnaissance

- Architecture: Changing the “business case” approach to IT governance. This work will be done simultaneously with the first three phases.
- Business Process: Enhancing business processes so that the FDF can gain the maximum benefit from the new technology. This will occur in two stages: the first enhancements will occur alongside the (i)C4ISR phase, with a second set after the iC4ISR phase. The second set of enhancements, which will occur after 2010, will be the “true” rollout of network-centric operations.

In addition to technology integration, the FDF must ensure that the organizational culture adapts to the new, networked way of doing business. Once the cultural change takes place, the organization must improve its capabilities, which will take place when the new applications and business processes are implemented.

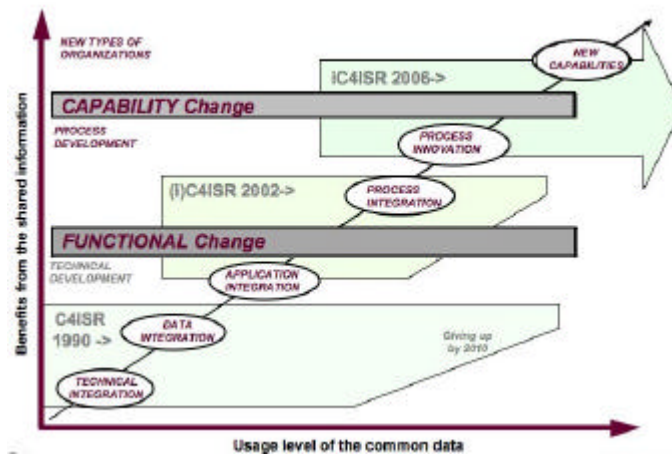


Figure 1 -- FiNED Roadmap⁶

The FiNED project consists of a core FDF technology team plus representatives from each FDF division and from IBM, the FDF’s technology partner [IBM participates only in the core (i)C4ISR phase]. The FDF selected IBM largely because they offered a competitive price and because they had the capability to serve a dual role as a) system integrator (developing and implementing hardware and software) and b) technology provider (COTS software). After selecting IBM, the FDF expanded the relationship to include the European Network-Centric Operations Centre of Excellence. IBM and the FDF have established a joint integration office to coordinate and plan the technical and project work.

The FiNED team chose to implement a Service-Oriented Architecture because they wished to reduce redundancy and facilitate technology reuse. They chose to rely on COTS packages such as Oracle, SAP, Tivoli, and Lotus Notes because of economics: Finland is a small country and would like to avoid the expense of custom development unless absolutely necessary. The new FDF architecture will focus on a core “common services” platform including all areas of the military. Specific functions will be implemented on top of this platform.

Building Support for Change

Many high-level Finnish leaders, such as Finland’s Chief of Defence, Admiral Juhani Kaskeala, and Permanent Secretary of Defence Mr. Matti Ahola, supported the FiNED proposal because their military experience and discussions with international colleagues convinced them that the FDF needed to take action.

Even with high-level sponsorship, however, gaining the support of service chiefs (Army, Navy, Air Force) proved difficult. Defence spending in Finland has been slowly increasing, but not as rapidly as operations and maintenance costs. Therefore, all branches of the military were being asked to do more with less money. The Ministry of Defence was hesitant of the FiNED proposal, mindful of the costs, priorities, and risks. They stipulated that FiNED must be achieved under existing FDF funding levels, even though FiNED is expected to eventually consume 20% of the procurement budget (€800 million by 2012).⁷

Koli knew that gaining the divisions' and funders' support was crucial. Most people in the FDF realized that they could not continue with "business as usual" if costs rose but funding did not. But why should they support FiNED, when the money to pay for it would have to be taken from their other programs? How could Koli and his team secure and assure their commitment to the needed organizational and technical change?

As Koli recalls, he "used a stick to drive people toward the carrot." To free up money to fund the central FiNED program, the FiNED team reviewed all existing technology platforms, and then froze spending on all work that did not contribute to the strategic vision. Simultaneously, they promised the branches that, once FiNED was complete, the cost savings it generated would increase their future funding.

Koli's team also performed some short-term Return on Investment (ROI) calculations to define the major components of the payback. These consisted mainly in reduced maintenance costs for non-strategic and duplicate systems and productivity through more efficient business processes. The FiNED team found that the relatively small 2004 outlay would be paid back in approximately one year. Although post-2004 paybacks would take longer, these initial ROI calculations were instrumental in building support.

Koli's team also needed a "quick win" to illustrate their value proposition. In response, they chose to centralize mobile phone procurement. The FDF's previously fragmented approach to phone purchasing was expensive and resulted in using an extremely large number of models. Koli and his team centralized the procurement process and reduced the number of approved models to three. This saved a significant amount of time and money. Although the phone project was simple and straightforward, it proved to division staff that they could indeed benefit by working together.

Finnish culture was also key in developing support: the Finns are very IT-literate and, as a society, have a great appreciation for the benefits that technology can bring.

The FiNED program kicked off in December 2005.

Sustaining Support

To sustain political support, the FiNED team decided on an incremental approach to implementation, proving the benefits of one stage before moving to the next. This was also necessary because of the criticality of the military's IT systems: the FDF could not risk national security by compromising operational readiness through ill-fated implementations. Moreover, the incremental approach was a good cultural fit, consistent with the pragmatic Finnish mentality.

Although the C4ISR, (i)C4ISR, and iC4ISR phases are scheduled sequentially, in reality some of the work will be done simultaneously. The FiNED team is currently working on aspects of all phases other than iC4ISR, and plans to release new or improved capabilities at least twice a year. Most of the work is on schedule, with the exception of the AdminNet restructuring, which has been delayed due to unanticipated complexity.

The FDF must report progress on the business case to the Ministry of Defence 2-3 times per year. To date, the key stakeholders (the Chief of Defence and the service chiefs) remain committed because the team is delivering results. The real test will come at the end of the decade, however, when the old information systems are dismantled and replaced with new ones. Koli said, "In change, it's easy to accept and support the principles but more difficult to keep support when the actual changes are made."

The FiNED team also hopes to sustain support via incentives emerging from the project's division of labor. They have assigned some responsibilities (such as the cross-functional governance board) to be jointly held among all divisions, but other responsibilities to the FDF division with the most interest. For example,

- The intelligence division handles data security and information assurance
- The Air Force tackles real-time situational awareness and bandwidth issues
- The Army addresses interoperability with international groups.

Because of Finland's small size, the experts involved (within and outside the FDF) know one another from previous experience and continue to meet regularly. To help break up the silos, the FDF has begun to implement joint

programs made up of staff from all military branches and, in the case of the Maritime joint program, civilian organizations. Other joint programs will also soon begin to work with civilians.

Leveraging Innovation

Although FiNED's technical architecture offers great potential, it also comes with great risk from complexity and continuing technology change. It requires a degree of experimentation, something that is often difficult within a structured government environment.

To address these issues, IBM proposed that the joint IBM/FDF team set up a European Network-Centric Operations Centre of Excellence (NCO CoE) at IBM's headquarters in Helsinki. According to Dr. Lawrence Sellin of IBM, who suggested the concept, "It was a potential win-win situation. The FDF would get access to some of IBM's innovation capabilities and IBM would be able to work closely with the customer to understand and test concepts directly related to NCO projects and which might have applicability in other defense engagements."

The NCO CoE, based on IBM's Innovation Hub model (see Appendix D: Innovation Hubs), has two main goals: (1) to jointly gain experience by testing potential innovations via short, focused Proofs of Concept and (2) to leverage innovations so other organizations can learn from this experience. It includes a software lab, test environment, and capabilities for live demonstrations.

The NCO CoE is now the focal point for developing and enhancing both military and civilian network-centric operations practices, processes, and technologies. Since opening in January 2006, it has completed three Proofs of Concept:

- Child Architecture: Scaling SOA down to the laptop level with the ability to continue to function in disconnected mode and to rapidly establish the current common operational picture once reconnected.
- NATO Integration: Mapping NATO's NC3TA Core Enterprise Services to the IBM SOA down to the application level to help Finland integrate with NATO standards.
- Cross-Organization Integration: Proving that legacy systems, proprietary systems, and other government/third party systems can successfully interconnect during crisis situations.

The Proofs of Concept have removed many uncertainties and risks posed by the technical architecture. The FiNED team expects to draw upon the CoE's innovations throughout the FiNED program.

International Crisis Management

FDF is clearly not the only military organization implementing network-centric operations: the US, UK, Singapore, Sweden, Germany, Norway and The Netherlands are also pursuing such changes. Finland has placed a great priority on contributing internationally by leveraging its strengths:

- A strong history of interagency cooperation
- A sophisticated IT infrastructure and comfort with new technologies
- 50 years of peacekeeping experience
- A comprehensive crisis management initiative backed by the former Finnish President, Mr. Martti Ahtisaari.

Finland's experience has taught them that they could be an information service provider to international crisis responders, a service in some cases just as valuable as the provision of food and water. According to Koli, "Everybody needs information, and if you look at the crisis areas today ... the situations are dangerous for everybody and the information is still not shared."

Encouraged by the former President Ahtisaari, the FDF have begun to develop tools to facilitate information sharing and encourage people to cooperate (many groups are reluctant to share data and intelligence). To date, however, their progress has been slow because of an inability to find trusted partners to work with. They were able to set up a

dialogue with their initial preferred partners, the United Nations and the European Union, but these partners could not assume responsibility for further development of the concept: their structures and priorities simply didn't match the need.

The FDF, however, still believes it is possible to develop a solid command structure and information sharing during crises like the Pakistani earthquake. They are optimistic that they can make progress by cooperating with the United States military on Multinational Experiment 5 (MNE5), one of a series of tests aimed at developing integrated planning, communication, and assessment capabilities for civilian crisis management.⁸

What's Next for FiNED?

FiNED is an ambitious program to increase the FDF's effectiveness in both military action and civilian crisis management. Progress to date has been extremely encouraging. But great risks and challenges remain to be negotiated. General Koli understands that "We still define our world by things that can be measured and felt – artillery fire, close air support, movement of troops via ship, rail, or road. There are very few people who really understand the change that is taking place and who can implement the change. Many people in Finland get vertigo when FiNED is described, especially with the price tag associated with it."⁹

The FiNED team is particularly concerned about the skill levels of the FDF. The success of the project depends on a handful of people, which poses a risk. Moreover, the FDF overall must develop advanced analytical skills to take advantage of the new information they will be getting, skills to combine information rather than just gather and analyze it in silos. Recruiting and retaining qualified staff when the private sector offers higher wages may be difficult.

Because NCO requires collaboration with a wide variety of groups, the FiNED team must develop solutions that reflect the priorities of these groups. This could obviously be challenging if priorities diverge.

With respect to international crisis management, the team must also consider that:

- Organizations must trust each other if they are to achieve proper collaboration. Will these groups be able to overcome their different responsibilities and cultures to establish the necessary levels of familiarity and trust?
- Each external organization has its own information policy and security needs. Can the new system and processes accommodate these differing security levels?
- Many operations will occur in areas where there is little or no connectivity. Can SOA be successful in bandwidth-constrained environments?

To solve these and other challenges, the FDF is counting on its firm commitment to technological innovation and its pragmatic approach to implementation.

Appendix A

Finnish Defence Forces¹⁰

The 17,000 employees of the FDF, part of Finland's Ministry of Defence, are responsible for "territorial surveillance, safeguarding territorial integrity and defending national sovereignty in all situations."¹¹ Defence Staff, who handle national defence planning and leadership, report to Chief of Defence Admiral Juhani Kaskeala, who is a direct report to the Finnish President. The FDF are divided into three branches:

- Army (infantry, field artillery, anti-aircraft artillery, engineers, signals and materiel)
- Navy (naval and coastal defence)
- Air Force (air commands and the forces that support them).

Finland's three commands (western, eastern and northern) are each responsible for defence and planning in their own area. Each of the 12 military provinces is responsible for conscription, gathering wartime troops, organizing local defence, and supporting soldiers. Finland's current wartime strength of about 520,000 troops (385,000 Army, 35,000 Air Force, 43,000 Navy) will be reduced to 430,000 by 2008. All men over 18 years of age must participate in mandatory military service.

According to the FDF's CIS Chief Architect, Mika Hyytiainen, the FDF is responsible for four major functions:

- Strategic planning and goal setting: tasks such as determining the type and number of forces required or defining military doctrine.
- Building up the force in both war and peacetime: operational tasks such as buying and storing materiel or training the troops. This work is mainly handled by the FDF's SAP system.
- The execution of military missions: Planning and directing troops and operational functions to successfully establish a common operational picture (a single display that contains important information from a number of different command sources)¹² and complete a mission. The IBM technology takes the lead on this work.
- Support functions such as technology.

For over 50 years, the FDF have adhered to the concept of Total Defence. According to Major General Markku Koli, "A long tradition in total defence – or Homeland Security – means that Finnish ministries and interagency elements already have established cooperation practices and initial capabilities... Our operational art is based on mission command. In command we always emphasize 'the what' needs to be accomplished and we leave 'the how' to our subordinates – centralized planning and distributed execution was reality for us."¹³

In addition to defence and domestic crisis management, the FDF are also committed to international peacekeeping as a part of NATO's Partnership for Peace program.

Total FDF expenditure in 2006 was €2.1 billion (\$2.8 billion), less than 2% of GDP.¹⁴

Appendix B

Network-Centric Warfare¹⁵

Pioneered by the United States Department of Defense, network-centric warfare (NCW) aims to achieve a competitive advantage in wartime through better networking and information sharing among forces that are geographically dispersed. For NCW to be effective, organizations must be able to create cross-agency task forces to quickly mobilize to deal with a crisis. The need for NCW became especially acute after the September 11, 2001 attacks.

According to NCW theories: better networking facilitates better information sharing leading to enhanced situational awareness, greater collaboration, and more effective missions. To achieve this, NCW relies heavily on information technology. According to the book "Power to the Edge," modern military environments are too complex to be understood by any one group or person; technology can facilitate information-sharing to such a degree that "edge entities" (those who conduct the missions) should be able to "pull" information rather than having centralized agencies try to anticipate their needs and "push" it to them.¹⁶ U.S. Major General Dale W. Meyerrose describes a compelling example of how NCW could also be used in a crisis management scenario:

"On the first of February 2003, a space shuttle falls out of the sky. Within 90 minutes, we had to set up a critical information exchange environment with 15 organizations that we had not even so much as made a phone call to. What elements of planning can you do when you don't even know who your partners are on an event-driven basis? You have to figure out how to dynamically create trusted information exchange environments, dynamically merge them, and have them go away when no longer required."¹⁷

The creation of and transformation to this environment requires structural and cultural change across a number of elements:

- Military doctrine must stimulate innovation and change by moving from "need to know" to "need to share".
- Organizations can no longer assume that they will only collaborate with groups that have similar structures and are well known to them.
- People must build trust and become more comfortable with risk and uncertainty. This can be difficult in conservative military environments.
- Technology must become more flexible to accommodate unpredicted and rapid changes in organizational processes
- Leaders must exhibit transformational leadership as well as operational leadership.

NCW has a great deal in common with the network-centric operations (NCO) performed in a number of private sector industries and civilian crisis management. The terms are sometimes used interchangeably.

Appendix C

Service-Oriented Architecture

Service-Oriented Architecture (SOA) is a technological approach to designing and building information systems. In SOA, applications are dissolved into sets of separate “services” that are then made available to users, or “consumers”. Services can be consumed independently of each other or linked together (choreographed) in different ways to support a variety of business processes. Services are also implemented to be independent of the computing platforms on which they run.

SOA is extremely flexible because it provides the ability to plug services together, to easily add new services to meet particular operational needs, and to retire those services that are no longer needed. Prior to SOA, technology teams would integrate data and processing into one complete system. This led to information “stovepipes” that could not easily be integrated to support information sharing or broken down for reuse. In environments requiring rapid change, the stovepipe approach is far more costly and difficult to build and maintain than the more open and agile SOA approach.

In SOA, data is passed between individual services by means of a standards-based messaging facility called the enterprise service bus (ESB). The ESB, an event-driven messaging engine, makes it easier to implement a large-scale SOA because it reduces the complexity of application integration (architects can implement messaging without having to write code).

For example, military personnel in the field would act in an SOA model as “service consumers”, who might make requests for specific intelligence data.¹⁸ Depending upon the chosen Enterprise Service Model being used, one or more “service producers” would provide the required information – making use of the transportation services of the ESB to deliver the service. Depending on the request, the flexible nature of SOA architecture would give each service producer the ability to access a variety of data and legacy applications with which to build their specific service. Flexibility leads to the provision of a diverse and changing portfolio of highly usable, information-rich services.

SOA appeals to defence establishments for several reasons:¹⁹

- SOA applications can be integrated more easily than the often-monolithic non-SOA applications. This makes it easier and cheaper for defence systems to share critical information and for disparate organisational groupings to collaborate with each other.
- SOA software components are “location transparent”: the services can be provided by any system and aren’t tied to a specific server. This makes it easier for organizations to deploy or attach themselves to different command structures.
- SOA is very standardized and requires fewer components and less code. This reduces maintenance expense and operational risk. The environment is more predictable because changes to the system can be isolated and minimized.
- Services can be developed and rolled out incrementally, which is compatible with the defence realities (mission-critical activities, budget pressures, large-scale organizational change).
- Because the services are usually defined in business terms, the system users must take an active role in defining them. This increases the likelihood that the technology will meet their needs.

The North Atlantic Treaty Organization’s (NATO’s) C3 Agency is currently planning a networking and information infrastructure (NII) that features SOA and a multinational federation-of-systems approach.²⁰

Appendix D Innovation Hubs

IBM Innovation Hubs are "windows" to IBM's research and innovation pipeline, and provide access to the following kinds of work:

- Science and basic research (vision and invention)
- Horizon/bleeding edge (first of a kind Proof of Concept, or PoC)
- Leading edge (tomorrow's technology today)
- Standard solutions (business as usual)

Each Hub is dedicated to researching and testing promising new technical and business solutions. Hub staff generate new ideas by analyzing market / technology trends and considering a client's particular "pain points." Once ideas have been generated, the Hub team jointly prioritizes them to determine which ones to take into the Proof of Concept, or pilot, stage. Once PoCs are complete, findings are captured in a technical white paper. They are also incorporated into client and (with client permission) IBM presentations and sales collateral globally. Successful PoCs can be migrated into implementation projects.

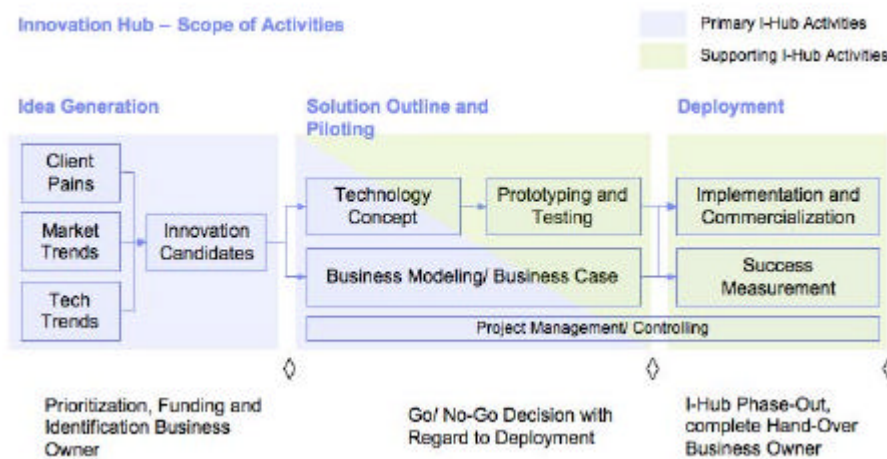


Figure 2 -- Innovation Hub Scope of Activities²¹

End Notes -----

- ¹ Much of the data for this case was obtained through interviews with managers within the Finnish Defence Forces and IBM.
- ² Paul Davidson, "Compatible radio systems would cost billions," *USA Today*, 28 December 2005.
- ³ Markku Koli, "Experiences and Challenges in Implementing Network Enabled Defence," presentation given to Network Centric Warfare Europe 2006, 7 June 2006.
- ⁴ Gerard O'Dwyer, "Finland Overhauling Communications Systems," DefenseNews.com, <<http://www.defensenews.com/story.php?F=1662787&C=europe>>, Last Updated 17 April 2006.
- ⁵ Gerard O'Dwyer, "Finland Overhauling Communications Systems," DefenseNews.com, <<http://www.defensenews.com/story.php?F=1662787&C=europe>>, Last Updated 17 April 2006.
- ⁶ Source: "Experiences and Challenges in Implementing Network Enabled Defence," presentation given to Network Centric Warfare Europe 2006, 7 June 2006.
- ⁷ Markku Koli, "Experiences and Challenges in Implementing Network Enabled Defence," presentation given to Network Centric Warfare Europe 2006, 7 June 2006.
- ⁸ United States Joint Forces Command, "Multinational Experiment 5" <<http://www.jfcom.mil/about/experiments/mne5.html>> (cited 26 April 2007).
- ⁹ Markku Koli, "Experiences and Challenges in Implementing Network Enabled Defence," presentation given to Network Centric Warfare Europe 2006, 7 June 2006.
- ¹⁰ Heavily based on Overview of the Finnish Defence Forces, <http://www.mil.fi/perustietoa/esittely/index_en.dsp>, Last updated 26 Jan 2004.
- ¹¹ Overview of the Finnish Defence Forces, <http://www.mil.fi/perustietoa/esittely/index_en.dsp>, Last updated 26 Jan 2004.
- ¹² United States Joint Forces Command Glossary, <<http://www.jfcom.mil/about/glossary.htm>> (cited 3 May 2007).
- ¹³ Markku Koli, "Experiences and Challenges in Implementing Network Enabled Defence," presentation given to Network Centric Warfare Europe 2006, 7 June 2006.
- ¹⁴ Wikipedia, "Finnish Defence Forces", <http://en.wikipedia.org/wiki/Finnish_Defence_Forces>, Last Updated 5 Mar 2007.
- ¹⁵ Heavily based on Wikipedia, "Network-centric Warfare", <http://en.wikipedia.org/wiki/Network-centric_warfare>, Last Updated 22 Feb 2007.
- ¹⁶ "Power to the Edge," an open-source book published by the Command and Control Research Program (CCRP) within the Office of the Assistant Secretary of Defense (NII), United States Department of Defense.
- ¹⁷ Major General Dale W. Meyerrose, statement to JWID final planning conference in Chesapeake, VA, 30 March 2004. Quoted in Lex Bubbers, "Transforming homeland defense through Network Centric Operations," IBM Business Consulting Services, April 2005.
- ¹⁸ Gartner, "Planning the Shift to SOA in Defense Establishments Involves More than Technology," ID Number: G00144549, 21 November 2006.
- ¹⁹ Bullet points heavily based on Gartner, "Planning the Shift to SOA in Defense Establishments Involves More than Technology," ID Number: G00144549, 21 November 2006.

²⁰ Gartner, “Planning the Shift to SOA in Defense Establishments Involves More than Technology,” ID Number: G00144549, 21 November 2006.

²¹ IBM On-Demand Innovation Services, “Collaborative Innovation – Introduction to the Innovation Hub concept,” presentation given in Zurich, 15 April 2004.