# Concept of Operations for the Self-healing Autonomous Sensor Network

David Waller
*S&T OR Team*

*Ian Chapman*
*Land Concepts and Design OR Team*

*Capt. Max Michaud-Shields*
*Canadian Forces Land Advanced Warfare Centre*

DRDC CORA TM 2008–052
July 2009

**Defence R&D Canada**
**Centre for Operational Research and Analysis**

Science & Technology Operational Research Team
Director General Science and Technology Operations

National Defence Défense nationale

Canada

# Concept of Operations for the Self-healing Autonomous Sensor Network

D. Waller
Defence R&D Canada – CORA

I. Chapman
Defence R&D Canada – CORA

Capt. M. Michaud-Shields
Canadian Forces Land Advanced Warfare Centre

**Defence R&D Canada – CORA**
Technical Memorandum
DRDC CORA TM 2008-052
July 2009

Principal Author

*Original Signed by David Waller*

David Waller

DRDC CORA Defence Scientist

Approved by

*Original Signed by Thierry Gongora*

Thierry Gongora

S&T OR Team Leader

Approved for release by

*Original signed by Dale Reding*

Dale Reding

DRDC CORA Chief Scientist

Defence R&D Canada – Centre for Operational Research and Analysis (CORA)

# Abstract

The purpose of the Self-healing Autonomous Sensor Network (SASNet) Technology Demonstration (TD) project is to demonstrate an ad hoc wireless network of heterogenous, unattended ground sensors that can be rapidly deployed to perform remote surveillance for the Canadian Army. A concept of operations was developed for SASNet in order to have clear understanding of how the system might be used by the Army. This understanding should lead to the design of a successful surveillance system that meets the needs and constraints of the soldiers whose lives might depend on it.

# Résumé

Le projet de démonstration de technologie (PDT) du Réseau de capteurs autonomes à autorétablissement (SASNet) vise à faire la démonstration d'un réseau sans fil ad hoc de détecteurs au sol autonomes et hétérogènes, pouvant être déployé rapidement afin d'effectuer de la surveillance à distance pour l'Armée canadienne. Un concept des opérations du SASNet a été mis au point afin de bien comprendre la façon dont le système pourrait être utilisé par l'Armée. Cette compréhension devrait permettre de concevoir un système de surveillance fonctionnel, adapté aux besoins et aux contraintes des soldats dont les vies pourraient dépendre de son fonctionnement.

This page intentionally left blank.

# Executive summary

## Concept of Operations for the Self-healing Autonomous Sensor Network

D. Waller, I. Chapman, Capt. M. Michaud-Shields; DRDC CORA TM 2008-052; Defence R&D Canada – CORA; July 2009.

**Background:** The purpose of the Self-healing Autonomous Sensor Network (SASNet) Technology Demonstration (TD) project is to demonstrate an ad-hoc wireless network of heterogenous, unattended ground sensors that can be rapidly deployed to perform remote surveillance for the Canadian Army. In order to get a clear understanding of how SASNet might be used and real-life operational constraints, the SASNet project team held a workshop attended by Army subject matter experts to develop a Concept of Operations (CONOPS) for the system. This CONOPS is for a future operational system so some of the elements (e.g., logistics and inter-operability) will not be tested during the TD project.

**Concept of Operations:** The SASNet CONOPS is divided into two main parts: tactical and operational. The tactical CONOPS deals with the planning, deployment, employment and retrieval of the system. SASNet should be treated like any other surveillance asset used by the Army. As a result, planning its deployment should follow existing, standard procedures. Nodes in the SASNet network should be easy to deploy rapidly. This will minimize the expertise and training required of soldiers, and will reduce the risk to those who must deploy the system near hostile forces. SASNet should provide reliable and useful information in a timely manner so that soldiers have time to react to alarms indicating the detection of enemy targets. Finally, the retrieval of the system should also be easy and rapid, and in the event that nodes can not be recovered, they should be destroyed remotely to avoid capture by the enemy.

The operational CONOPS discusses command and control, interoperability, security, survivability, logistics and maintenance. SASNet's place in the command and control structure (likely controlled at the platoon or company level) is discussed, as are the inter-operability implications of its need to integrate with the existing command and control structure and systems. Both physical and electronic security are important for SASNet as the enemy must be denied the opportunity to use SASNet components against Canadian forces, and must not be able to hack into the SASNet (or higher) networks. As most SASNet nodes are envisioned to be disposable, their ability to survive kinetic weapons is limited; however, a more relevant survivability concern is their ability to manage their energy consumption in such a manner that their limited resources (i.e., batteries) last for long periods of time (at least two months in "quiet" areas). If SASNet will be used for surveillance as extensively as hoped, it will require significant thought from a logistics perspective as thousands of nodes could be

used by a battle group in a single month. Large quantities of equipment makes maintenance an issue as well, so care needs to be taken to ensure that problems can be fixed easily or that spares are readily available. Although some of these operational CONOPS topics will not be addressed during the limited time of the TD project, a final operational system will have to consider all these factors in order to be useful in the real world.

# Sommaire

## Concept of Operations for the Self-healing Autonomous Sensor Network

D. Waller, I. Chapman, Capt. M. Michaud-Shields ; DRDC CORA TM 2008-052 ;
R & D pour la défense Canada – CARO ; juillet 2009.

**Introduction :** Le projet de démonstration de technologie (PDT) du Réseau de capteurs autonomes à autorétablissement (SASNet) vise à faire la démonstration d'un réseau sans fil ad hoc de détecteurs au sol autonomes et hétérogènes, pouvant être déployé rapidement afin d'effectuer de la surveillance à distance pour l'Armée canadienne. Pour bien comprendre la façon dont le SASNet pourrait être utilisé et les contraintes opérationnelles réelles, l'équipe du projet SASNet a organisé un atelier réunissant des experts en la matière de l'Armée afin de mettre au point un concept des opérations (CONOPS) pour le système. Ce concept des opérations porte sur un système opérationnel futur. Par conséquent, certains éléments (comme la logistique et l'interopérabilité) ne seront pas mis à l'essai au cours du projet de démonstration de technologie.

**Concept des opérations :** Le concept des opérations du SASNet comporte deux principaux aspects : l'aspect tactique et l'aspect opérationnel. L'aspect tactique concerne la planification, le déploiement, l'utilisation et la récupération du système. Un SASNet devrait être traité comme n'importe quelle ressource de surveillance utilisée par l'Armée. La planification de son déploiement devrait donc se faire en respectant les procédures standard déjà établies. Les noeuds du réseau SASNet devraient être faciles à déployer rapidement, de sorte que les soldats puissent effectuer cette tâche avec un minimum d'instruction et de connaissances spécialisées. La rapidité de déploiement réduira également les risques encourus par les soldats chargés de déployer le système près de forces ennemies. Le SASNet devrait fournir rapidement de l'information fiable et utile afin que les soldats aient le temps de réagir aux alarmes indiquant la détection de cibles ennemies. Enfin, le système devrait pouvoir être récupéré facilement et rapidement. De plus, dans l'éventualité o des noeuds ne pourraient être récupérés, il devrait être possible de les détruire à distance afin d'éviter que l'ennemi ne s'en empare.

L'aspect opérationnel du concept des opérations concerne le commandement et le contrôle, l'interopérabilité, la sécurité, la surviabilité, la logistique et la maintenance. La place du SASNet dans la structure de commandement et de contrôle (le contrôle serait probablement effectué au niveau du peloton ou de la compagnie) a été étudiée, tout comme les conséquences en matière d'interopérabilité de la nécessité d'intégrer le système à la structure et aux systèmes de commandement et de contrôle. La sécurité du SASNet, tant physique qu'électronique, revêt une importance particulière, car il faut empêcher l'ennemi

d'utiliser les éléments du SASNet contre les Forces canadiennes ou de pénétrer les réseaux SASNet ou les autres réseaux militaires (supérieurs). La plupart des noeuds SASNet envisagés seront des dispositifs à utilisation unique ; leur résistance aux armes cinétiques sera donc limitée. Il existe cependant une préoccupation plus pressante à l'égard de la surviabilité des noeuds : leur capacité à gérer leur consommation d'énergie de façon à faire durer leurs ressources limitées (leurs batteries) pendant de longues périodes (au moins deux mois dans les zones "calmes"). Si le SASNet est employé pour la surveillance aussi largement que nous l'espérons, une réflexion poussée sur la logistique sera nécessaire : un groupement tactique pourrait utiliser des milliers de noeuds en un seul mois. Ces grandes quantités de matériel soulèvent également des problèmes de maintenance : il faut veiller à ce que les problèmes puissent être réglés facilement ou s'assurer que des pièces de rechange sont disponibles et facilement utilisables. Il ne sera pas possible d'aborder certains de ces sujets opérationnels liés au concept des opérations au cours de la durée limitée du projet de démonstration de technologie. Toutefois, le système opérationnel final devra tenir compte de tous ces facteurs pour être réellement utile.

# Table of contents

# List of figures



# List of tables

# Acknowledgements

The authors are very grateful to the many people who helped us to produce this report. This CONOPS would not have been created without the enthusiastic involvement of all the people from the CF, DND, DRDC and the Communications Research Centre who took part in the CONOPS workshop and survey. Thank you to Thierry Gongora and Fred Cameron for reviewing, editing and ultimately improving this document. And finally, we would like to thank everyone from the SASNet team lead by Shawn Hoag, formely of DSTL, Louise Lamont and Luc Boucher from CRC, and Benoit Ricard from DRDC Valcartier. We greatly appreciate their support of this work and we hope it influences the development of SASNet in the years ahead.

This page intentionally left blank.

# 1 Introduction

The purpose of the Self-healing Autonomous Sensor Network (SASNet) Technology Demonstration (TD) project is to demonstrate an ad hoc wireless network of heterogenous, unattended ground sensors that can be rapidly deployed to perform remote surveillance for the Canadian Army. Although this concept of operations does not include applications in the air and maritime domains, SASNet could also be used in the defence of harbours, airfields and other, similar facilities that might require improved perimeter security. Designing an effective unattended ground sensor system (UGS) requires accurate knowledge of how the system is likely to be used by the military. For this reason, the design of SASNet must take into consideration realistic constraints imposed on the Army for surveillance operations. In order to get a clear understanding of how SASNet might be used and the operational constraints, the SASNet project team decided to write a detailed Concept of Operations (CONOPS) for the system. The CONOPS that is presented in this report is not expected to be the final word on how SASNet will be used; the CONOPS will evolve as experience is gained from annual trials with users. This report provides the first iteration of SASNet's CONOPS. It is important also to note that since this CONOPS is for a future operational system, some of the elements (e.g. concealment of nodes, logistics and inter-operability) are beyond the scope of what will be investigated during the TD project.

A CONOPS for a system is a user-focussed document that describes the use of the system from the users' perspective [1]. It is not a document that provides details on the design of engineering; however, the users' information on how it will be used strongly influences the design and engineering of the system. A CONOPS should be written from the users' perspective, but it should be easily understood by all of the people involved in the project: scientists, engineers, technicians, project managers, and future users. As a result, it should contain neither military nor technical jargon[2].

After a brief overview of SASNet (Section 2.1) and the surveillance scenarios that are being considered for the project (Section 2.2), the development of the SASNet CONOPS will be reviewed. The rest of this memorandum consists of the tactical (Section 3) and operational (Section 4) CONOPS for SASNet.

# 2 Background

Before presenting the CONOPS for SASNet, some background is required. First, an overview of how SASNet works is presented. After this, the three scenarios that will be demonstrated in SASNet are described. The background section concludes with a description of how the SASNet CONOPS was developed.

## 2.1 SASNet Overview

SASNet is an ad hoc wireless network of unattended ground sensors that can be rapidly deployed to perform remote surveillance for the Canadian Army. The system can be divided into four main types of components. The hierarchy of these components is shown in Figure 1. At the lowest level are numerous inexpensive sensor nodes that are disposable. Each of these nodes has an antenna for radio communications, a small computing platform, batteries for power, and a variety of acoustic, seismic, magnetic, and passive infra-red sensors. The ranges of these different sensors vary from a few metres (magnetic detection

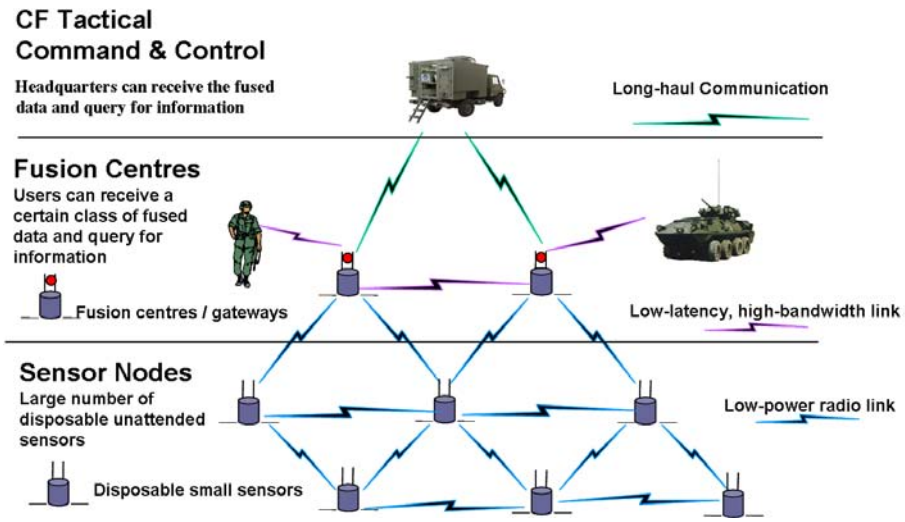


***Figure 1:*** *Hierarchy of nodes in SASNet.*

of dismounted soldier with rifle) to hundreds of metres (seismic detection of large vehicles). Each sensor node can have many different types of sensors on it. The sensor nodes can communicate with each other and higher-level nodes via low-power radio links. The range of the radio links is typically tens of metres and the bandwidth is tens of kilobits per second. The radio communications will involve an authorization and authentication mechanism which will prevent unauthorized access to the network.

The second level of the SASNet network consists of nodes that perform fusion or aggregation of the data collected by the low-level sensor nodes. These second-level nodes are called fusion nodes (or fusion centres on Figure 1). These nodes have more computing resources, higher power and bandwidth (hundreds of kilobits per second) radio links. The range of these links can be hundreds of metres. The fusion nodes are more expensive and therefore should be retrieved if the operational conditions permit. They also consume power more quickly than low-level nodes, so should only be drawing power when necessary.

Additionally, more sophisticated sensors can be deployed with SASNet, either as part of a fusion node, or as separate "second-level" sensor nodes. These nodes are not shown in Figure 1. These sensors include electro-optical infra-red (EO-IR) sensors and acoustic arrays used for sniper detection. Other sensors, such as chemical, biological, and radiological sensors, could also be included on second level nodes. Because of their much higher cost than the first level sensor nodes, these sensor nodes will be deployed in much smaller numbers and will not be considered disposable. However, their long ranges, hundreds of metres for EO-IR cameras and acoustic detectors, mean that fewer of these sensors are required to cover a large area. Because of the large amounts of data produced by these sensors, they will require high-bandwidth links like those of the fusion nodes.

The fused data and alarms from the fusion nodes can be sent either to a personal digital assistant (PDA) carried by a soldier in the field, or to the highest (third) level of SASNet: the management node. The PDA requires a specific application on it for communicating with SASNet. The management node is a computer running SASNet software in a static headquarters or a vehicle. Besides providing an interface for monitoring SASNet, a PDA or management node will allow a user to control SASNet by tasking the nodes.

SASNet will be a self-healing network as it will be able to re-configure its network without operator intervention if some nodes cease working. Its ability to self-heal depends on the availability of redundant wireless communication links; if too many nodes cease working, the network will eventually lose its ability to re-configure. Self-healing is an important feature as the large number of nodes would make manual repair of the system extremely onerous. Also, since the number of nodes can be large, the likelihood that a single node will stop working at some point in time is high. In order for SASNet to be self-healing, the network protocols will have to be flexible to adapt to changing conditions.

SASNet will be autonomous so that it requires minimal intervention or monitoring by a soldier. Soldiers in the field are already extremely busy, so SASNet must not add extra tasks for them. Instead, it should make their jobs (particularly surveillance) easier. In order to be autonomous, SASNet must be able to fuse data from many different sensors automatically. This will be done at the fusion nodes. Fusing multiple sources of data should lead to lower false-alarm rates and a higher degree of confidence in detections of real targets. Fusion nodes will also be able to cue second level sensors nodes (e.g. an EO-IR camera) automatically so that detailed information about a target can be captured and relayed to a

PDA or the management node for further analysis by software or a soldier.

If SASNet is successful, it will replace the current UGS used by the Canadian Forces (CF): the Thales UK's Classic 2000. Although CF users have found it somewhat effective at performing remote ground-based surveillance, it is hoped that SASNet will provide a significant improvement. Areas that SASNet hopes to improve on are system cost, size and weight, robustness, and performance.

Currently, off-the-shelf UGSs are very costly (tens of thousands of dollars per sensor node) and heavy (one kilogram or more per sensor unit), so it is not economically feasible to instrument large areas, nor is it feasible for dismounted soldiers to carry large numbers of sensors. Demonstrating a system with nodes that are much cheaper (hundreds of dollars) and smaller (hundreds of grams), makes it realistic to consider instrumenting much larger areas. Another important advantage that SASNet should have over existing UGSs will be its ability to analyze aggregated data from multiple sensors autonomously. The Classic 2000 does not aggregate data from multiple sensors, so each individual alarm must be considered in isolation. By combining information from multiple sensors with overlapping sensor footprints, SASNet should be able to reduce the rate of false alarms, increase the confidence in detections, and improve the ability to classify targets. Finally, some of the sensor nodes in SASNet will be EO-IR cameras that can be cued by the cheaper and more numerous low-level sensor nodes. SASNet's ability to capture images and send them to a remote operator further improves the system's ability to reduce false alarms and classify targets, and provides the possibility of identifying targets.

## 2.2 SASNet Scenarios

Although SASNet could be used in a large number of different scenarios, time constraints limit the project to three demonstration scenarios. Fortunately, these scenarios cover a broad range of the types of applications that SASNet might have. These three scenarios were considered during the development of the CONOPS. Further scenarios where SASNet could be used are shown in Figure 2.

The three scenarios provide illustrations within land operations. SASNet could also have applications in support of maritime or air operations. SASNet nodes could be deployed around the perimeter of a port, forward area refuelling point or airfield to provide early warning detection.

The first scenario will demonstrate the effectiveness of SASNet for barrier surveillance. A covert soldier will use a hand-held PDA to monitor an area that is approximately 100 m by 50 m. The area will be instrumented with tens of lower-level sensor nodes and possibly one or more second level sensor nodes. The monitoring soldier will be 30 m from the deployed sensors. Figure 3 shows what the layout will look like.

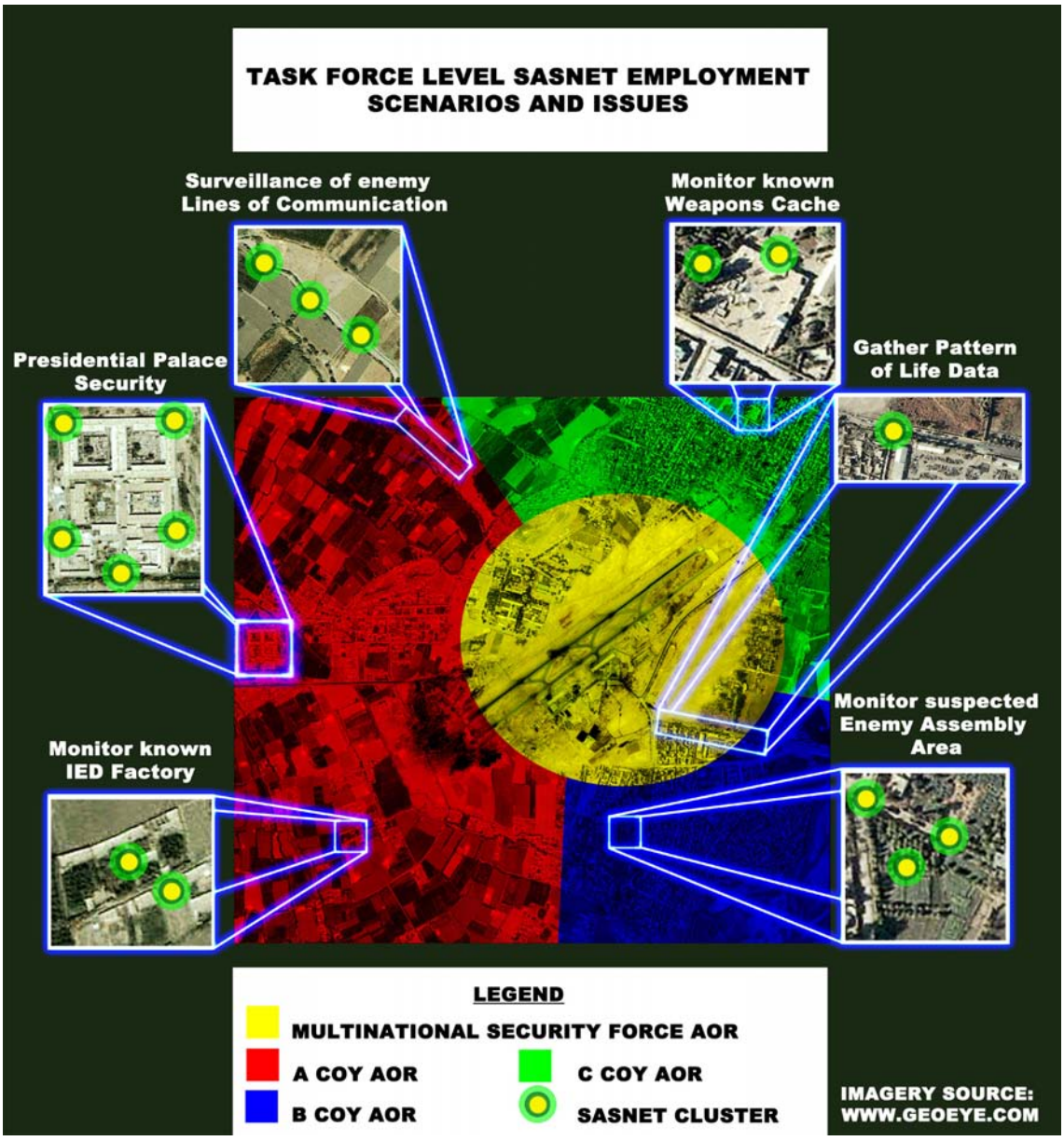


***Figure 2:*** *Example of Task Force level SASNet employment scenarios. Kandahar Air Field is used for illustrative purposes to show how and where SASNet might be used. The specific locations indicated on the map are arbitrary, and so do not represent tactically relevant information. The colour-coding indicates hypothetical Areas of Operation (AORs) of different army companies (COY).*

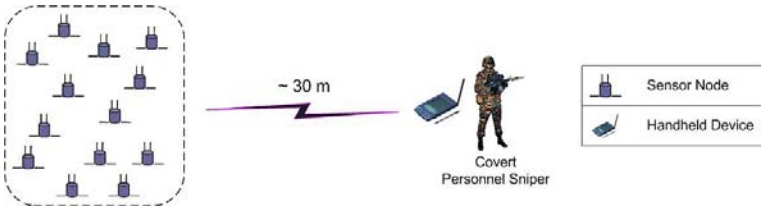


***Figure 3:*** *First scenario to be demonstrated by SASNet.*

The second scenario will demonstrate SASNet's effectiveness for monitoring a choke point (e.g. a mountain pass with a narrow road). The terrain that will be instrumented will be more irregular than in the first scenario. This makes the placement of the sensors more challenging for detection and communications purposes. Also, the scenario will include several fusion nodes which will communicate with a management node and a PDA over a long distance (500 m). Figure 4 shows the set-up for this scenario.

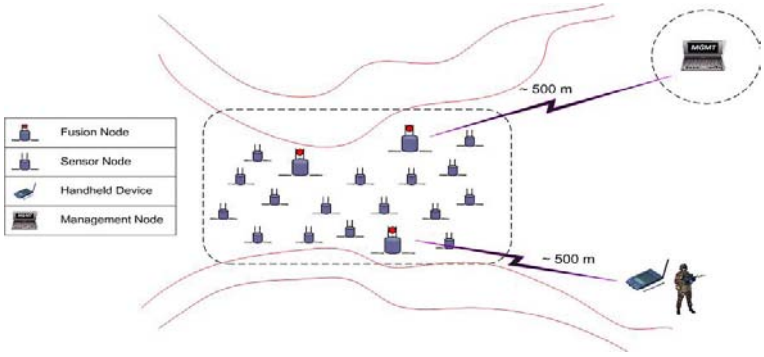


***Figure 4:*** *Second scenario to be demonstrated by SASNet.*

The third and final scenario demonstrates SASNet's ability to monitor a road junction. Figure 5 shows the set-up. Both low- and second-level sensor nodes will instrument the roads within tens of metres of the intersection, and each of the four incoming roads 500 m from the junction. The fusion nodes that are deployed will communicate with each other up to 500 m apart, a soldier-held PDA (1000 m from the junction), and the management node (10,000 m away). This final demonstration will demonstrate the full functionality of SASNet.

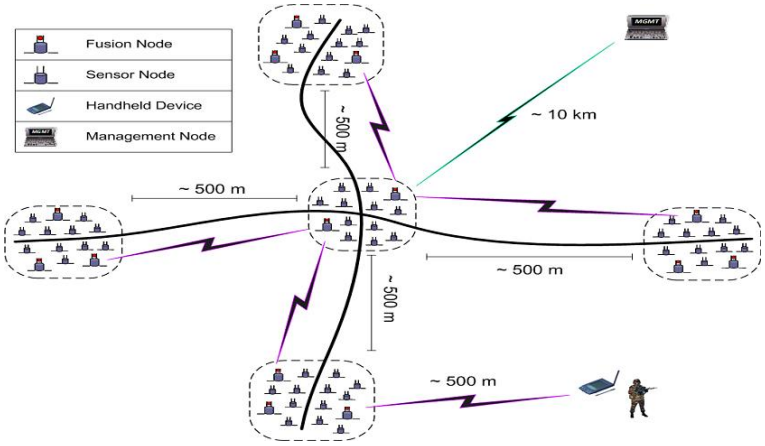


***Figure 5:*** *Third scenario to be demonstrated by SASNet.*

## 2.3 CONOPS Workshop

It was decided that the most efficient way to obtain the necessary input for the CONOPS was by holding a short workshop where military personnel with experience using UGSs could offer their insight into how these types of systems are used in the field. Originally, the CONOPS workshop was scheduled for two days, with two days afterward for a follow-on workshop dedicated to Functional Task Analysis (FTA) for SASNet; for a description of a FTA see Reference [3]. Due to the very limited availability of Canadian Army subject matter experts (SMEs), the CONOPS and FTA workshops were compressed into one day each.

The one-day CONOPS workshop was not long enough to collect all the required user information. Although the tactical aspects of the CONOPS were covered, information for the operational aspects had to be collected after the workshop by questionnaires distributed to the Army SMEs. The questionnaires that were distributed for the operational CONOPS are provided in Annex A.

The Army SMEs were carefully selected for the workshop so that they represented a relevant cross-section of the user community. A warrant officer who had recent operational experience with a mechanized reconnaissance platoon was chosen to give the perspective of an experienced non-commissioned member of the Army. A captain (one of the authors) who had recent operational experience in a dismounted reconnaissance platoon and is a very experienced user of the Classic 2000 UGS provided invaluable information based on his recent experience in Afghanistan. The exploitation manager for SASNet, a major from the Directorate of Land Requirements, represented the viewpoint of Army requirements.

An operational research analyst (also, one of the authors) with the Directorate of Land Concepts and Designs provided the perspective of the Army of Tomorrow: the vision of the Canadian Army in the future. A major with recent experience as a combat team commander was unable to attend as he was re-tasked at the last minute; however, he provided input for the CONOPS via email.

In addition to the Army SMEs, defence scientists and engineers from the Communications Research Centre Canada (CRC), Defence Research and Development Canada (DRDC) Valcartier, and DRDC Centre for Operational Research and Analysis (CORA) took part in the workshop. The scientists and engineers contributed to the CONOPS workshop by providing technical expertise on the capabilities and limitations of SASNet.

The morning of the CONOPS workshop was devoted to briefings that provided all the participants with common background information. The briefings covered (1) recent CF experience with UGSs in Afghanistan, (2) an overview of how SASNet works, and (3) a summary of the Army of Tomorrow. The afternoon was devoted to developing a tactical CONOPS.

The afternoon's tactical CONOPS sessions were organized so that each of the four tactical elements (planning, deployment, employment, retrieval) was dealt with in a separate one-hour session. Due to the relatively small number of Army SMEs, all the workshop sessions were plenary.

Each element of the tactical CONOPS was addressed first by distributing a preliminary, draft list of tasks that might be required for each element. The preliminary lists for planning, deployment, employment, and retrieval are given in Annex B. These lists were used as a starting point for developing a more complete and detailed list of tasks for each element of the tactical CONOPS. During the session for each element, each workshop participant was given ten minutes to read and critique the task list. Participants were encouraged to write notes on their lists; all the participants' lists were collected at the end of each session as part of the record of the workshop.

After the participants had finished reading and thinking about the lists individually, they were grouped in pairs. The pairs were directed to discuss their thoughts about the tactical CONOPS element for ten minutes. The intra-pair discussion allowed the participants to refine or change their thoughts about the tactical CONOPS element. These discussions were followed by a group discussion involving all the workshop participants. This method of progressively increasing the size of the discussion groups is referred to as a "pyramid" activity.

At the beginning of each whole-group discussion, the Army SMEs with recent operational experience shared their thoughts about the draft task list. The majority of the group discussion focussed on the comments of these SMEs. The discussions were organized in this way to ensure that the CONOPS focussed on the military users. After the SMEs finished

giving their feedback on a draft task list, the other workshop participants were given an opportunity to provide further comment.

The draft task lists were edited on a projected screen during the group discussion to ensure that the recorded changes properly reflected the comments of the participants. After the workshop, the authors used the edited task lists and participants' written notes to develop the tactical CONOPS described in Section 3 of this memorandum.

# 3 Tactical CONOPS

The tactical CONOPS for SASNet was developed by following the procedure outlined in Section 2.3. It assumes that SASNet will be employed in the scenarios described in Section 2.2. The tactical CONOPS for SASNet can be broken down into four main elements: planning, deployment, employment and retrieval. The details of the tasks that make up these elements are elaborated on in the Sections 3.1 to 3.4.

## 3.1 Planning

The first step in using SASNet is planning when, where and how it will be used. The following two sections outline the details of the planning element of the CONOPS.

### 3.1.1 ISTAR planning process

Planning to use SASNet should be part of the standard Battle Group Level (BGL) Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) planning process. During this process, many sources of information are synthesized to produce planning documents that indicate the areas of interest (Named Areas of Interest and Targeted Areas of Interest) to which surveillance assets are designated. SASNet should be treated like any another asset that can be employed. In the BGL ISTAR process the following tasks must be performed:

1. determine the surveillance requirements;
2. determine the availability of surveillance assets (SASNet included);
3. assess the terrain; and,
4. determine the types, numbers and locations of sensors that satisfy the surveillance requirements.

To determine the surveillance requirements, a planner first needs to decide what type of information needs to be collected. As a minimum, targets must be detected when they traverse a sensor field. Ideally, imagery should be made available that makes it possible to determine whether a target is friendly or hostile; although, imagery alone may not be sufficient to distinguish friend from foe. The type of targets to be detected must be decided at the planning stage as some sensors might be effective for one type of target but poor for another.

The second decision is where to collect surveillance data. The highest priority areas for SASNet will be in locations that are beyond-line-of-sight (BLOS). There are few systems that provide BLOS surveillance for land (electronic warfare and signals intelligence systems, or sensors mounted on uninhabited aerial vehicles or satellites) so this is an important

niche for SASNet. If resources permit, SASNet would also be valuable in areas with line-of-sight (LOS), as it would reduce the surveillance burden on soldiers.

When large deployments are planned for SASNet, the order that the nodes will be deployed will not necessarily be the order that minimizes the deployment time. Instead, the areas that have the greatest tactical importance will be instrumented first. This includes approaches, paths, and known launch sites of enemy attacks. As time progresses, the gaps can be filled. The most important gaps to fill will be those that are BLOS. The last gaps to be filled are those which can be monitored directly (i.e. areas with LOS from a base or outpost).

The ISTAR planner must also decide when to collect the surveillance information. In general, persistent surveillance is preferable. This means that SASNet must operate without interruption. The longer it can stay active (i.e., have adequate power), the more flexible it will be. As a minimum, SASNet should stay active for several days; however, it should stay active for at least one month to be a valuable surveillance resource. Some applications might require that nodes have power for many months, but these applications usually assume that the system can lie dormant for months before becoming active. An example of this type of application is where one wants to monitor a mountain pass that is passable during summer months only, but one wants to deploy the sensors at the end of one summer so that they lay dormant until the following summer. Deployments of a month or more also make it more likely that buried SASNet nodes might become submerged in water for extended periods of time. Consequently, the nodes should be able to withstand extended exposure to water.

The final consideration for the surveillance requirements is deciding to whom the surveillance information should be distributed. The distribution of information will be mission-specific and will depend on who is responsible for planning the deployment of SASNet. If a lower-echelon group (e.g., section) will be deploying SASNet, they may not have any reason to distribute raw SASNet information to higher-level echelons. However, if a section has been tasked from above to deploy SASNet, it is possible that the information will be desired by a higher echelon.

Before surveillance resources can be allocated to meet the requirements, the availability of surveillance assets must be assessed. As far as SASNet is concerned, this requires an up-to-date inventory of functioning equipment. This information can be arranged so that the number of complete “kits” of SASNet equipment is known, or alternatively, the numbers of different components can be tracked (e.g., numbers of sensor nodes of different types, number of fusion nodes, relays, EO-IR cameras, etc.).

The terrain needs to be assessed so that its effect on radio-frequency wireless communications between SASNet nodes, and sensor detection ranges can be estimated. Terrain can have a large effect on the range of inter-node communications, so this can affect the spacing of nodes that ensures a reliable, contiguous network of sensor and fusion nodes. Terrain

can also have a large effect on the range of detection for different sensors types. For example, the firmness of the soil can affect the detection range of seismic detectors. Either the detection or communications range is the limiting factor that determines the inter-node spacing. Some expertise is required to assess the impact of terrain accurately. As a result, the person who plans the use of SASNet should have sufficient training or experience to do this properly.

Once the surveillance requirements and asset availability are known, the planner can determine the best mix of sensors (subject to terrain constraints) to achieve the surveillance goals. SASNet software that runs on a section-level PDA or standard Army computer (in a land vehicle or headquarters) should be available to help determine the best mix of SASNet sensor nodes. The software must run on this diverse range of computing platforms to allow both ISTAR planners and lower-level echelon commanders to determine how to deploy SASNet optimally. The software should be intuitive and easy to use, with minimal data entry. In order that terrain information be accounted for properly, the SASNet software should be integrated with a geographical information system (GIS) that is already running on the Army computing platforms (e.g., Situational Awareness System (SAS) terminals in Coyote reconnaissance vehicles).

In principle, there could be a variety of different types of sensor nodes for SASNet. Each type could have a different combination of sensors on it. In reality, having a large number of node types could make planning and deployment more confusing for soldiers in the field. It would be simpler to have a single type of lower level sensor node that incorporates all the different types of sensors (acoustic, seismic, magnetic, and passive infra-red) on a single node. The cost per node would not be increased significantly due to the "economy of scale" of having multiple transducers on the same computing platform (all sharing the same wireless communication system). Unless there are significant costs or technical issues with having multi-sensor nodes, it will probably be preferable to have a single type of multi-sensor node.

If all SASNet low-level sensor nodes have multiple sensors, then there will usually be multiple sensors monitoring each point in an instrumented area. This redundancy is highly desirable as it will increase the probability of detecting targets, while reducing the rate of false alarms [4]. If resources permit, redundancy in the number of nodes covering the same area (so that there are multiple sensors of the same type covering the same area) has an additional, important advantage: when a node fails (e.g., due to loss of power or communications), the instrumented area will still be covered. The wireless network will also be less susceptible to becoming partitioned.

When the SASNet software determines the suggested number and mix of nodes, the ISTAR surveillance plan should have sufficient flexibility to allow modifications during deployment. During deployment, it might be realized that the number and/or type of sensors should be adjusted. This could be due to incomplete knowledge of the terrain during plan-

ning, or a last minute change to the surveillance requirements. The CF has found that the Classic 2000 UGS is limited due to its lack of flexibility, so it is important that SASNet avoid this problem.

A decision must be made whether a node needs to be deployed on the ground, buried, or placed elsewhere. This decision will depend on the intended purpose of the SASNet deployment. If the intention is to perform covert surveillance, then the nodes must be well concealed (usually by burying). If the intention is to deter people from entering an area or let them know they are being monitored, then the nodes should be clearly visible. The design of the nodes should take both of these possibilities into consideration. However, if a choice must be made between overt or covert use of SASNet, and there are no overwhelming reasons to select an overt deployment, then covert is the preferred option.

The first iteration of the ISTAR surveillance plan generated by the ISTAR process determines which areas of interest will be covered with specific surveillance assets during specific times. The initial plan results in the production of an ISTAR "trace" that guides the deployment of surveillance assets and aids in subsequent iterations of the planning cycle. The ISTAR trace is not final after this first iteration of planning: it is frequently updated as more information becomes available or operational conditions change.

The trace and its lower-echelon equivalents are distributed to those who will deploy the surveillance assets in the field. Following the concept of "mission command" [1], it is up to the subordinate commanders who are responsible for the deployments to determine the exact locations of sensors and the tactics employed. A platoon-level trace (called a range card) may show a surveillance hole that can be covered by SASNet. In this case, a platoon commander can decide himself to deploy SASNet if he has access to SASNet equipment.

After the system has been deployed and gaps have been identified (and possibly filled), this detailed information is pushed back up the chain of command. Subsequent planning cycles use this more detailed information to refine the ISTAR planning and to produce more detailed traces.

### 3.1.2 Additional planning tasks

There are some planning tasks that should be performed for SASNet that are not usually part of the ISTAR planning process. The first extra task is to assess the radio environment of the entire operational area (not just the area under surveillance). This information will likely only be available from a brigade-level expert in radio communications. The assessment of the radio environment includes consideration of the susceptibility to jamming (by friend and foe). Another consideration is the possible use of weapons that can damage electronics from long range.

1. Mission command is defined as "the philosophy of command that promotes unity of effort, the duty and authority to act, and initiative to subordinate commanders."[5]

The surveillance planning for SASNet must also account for the method of node localization that is employed. In order for SASNet alarms to be most useful, accurate target locations are required. Since large numbers of nodes will be deployed, it is challenging to determine the locations of all nodes with high accuracy and precision. As a result, careful thought needs to be given at the planning stage.

SASNet will perform node localization while the system is deployed by using a PDA that is equipped with a Global Positioning System (GPS) and an ultrasound transmitter [6]. The PDA will send "beacons" containing its current position along with ultrasound and RF signals. The Time Difference Of Arrival (TDOA) between the ultrasound and RF signals will be used by each node to calculate its distance from the PDA. As the soldier who carries the PDA moves around, many beacons are sent so each node gets multiple distance measurements to different reference points (GPS locations). Once at least three beacons have been received, the sensor node can perform a multilateration calculation to determine its position. The accuracy of the node position estimates, relative to each other, should be tens of centimetres [2]. The advantages of this approach compared to other localization methods are

– it is distributed (no single point of failure other than the PDA);
– no precise synchronization of clocks on different nodes is required;
– there is a better chance of getting LOS readings (compared to using fixed anchor points); and,
– improved accuracy.

If nodes are concealed before the beacons are sent, the localization method could be adversely affected if the RF or ultra-sound signals are not received by the nodes. If this is a problem, then the localization procedure will have to be carried out before the nodes are concealed.

As soldiers must deploy the SASNet nodes by hand, it is imperative to secure the surveillance area. The terrain and perceived threat will determine how large an area needs to be secured during deployment.

The eventual retrieval of SASNet nodes must be considered during the planning process. Some of SASNet's nodes are very expensive (fusion and second level sensor nodes) so they should be retrieved for re-use if the tactical situation allows it. Retrieving nodes requires relocating them. This requires precise location information if the nodes are well-concealed, otherwise it might take too long to retrieve the nodes from the field. Knowing the relative locations of nodes (with respect to a landmark or a "reference" node) within one metre is highly desirable to shorten the retrieval phase.

It is important to note that surveillance plans are revised throughout an operation as neces-

2. The accuracy of each GPS estimate is on the order of metres, but the relative positions are known much better if the measurements are taken within minutes of each other. This is due to systematic biases in the GPS estimates.

sary. Revisions can result from a changing operational environment or feedback from the field. As a result, SASNet must be able to cope with modifications during its use. These modification could include moving nodes, removing or adding nodes, or re-tasking nodes. This requirement should not be a problem for SASNet as one of its main abilities is to self-heal; this means that its network can re-configure autonomously.

The person who plans a SASNet deployment is determined by who is using it. The planning could take place at the battalion, company, platoon, or section level. This depends both on the specifics of the mission and the level of echelon that is equipped with SASNet.

Since the number of SASNet nodes being deployed could be large (hundreds of nodes or more), it is important to consider the volume and weight of nodes for transport purposes. When planning the deployment of SASNet, it is important to realize that space in or on vehicles and on soldiers is limited. How many nodes a vehicle or soldier can carry will depend on the final specifications of SASNet, but the smaller and lighter the nodes are, the easier the deployment process will be.

Finally, the thoroughness of planning will depend on the size of deployment and who is carrying out the planning. If SASNet planning is carried out at the section-level in a hostile environment in the field, the section commander might not go through all the steps. On the other hand, a surveillance planner at a static headquarters should have adequate time and resources to complete all the steps.

## 3.2 Deployment

After planning a SASNet deployment a few additional tasks should be performed before soldiers deploy the system. First, nodes are checked to verify they are functioning. Second, the management node (MN) should be set-up if it is required. If it is not required then the PDA(s) that will connect to SASNet should be checked to make sure it is functioning properly. The final preliminary step is to ensure that all the fusion nodes that will be used can communicate with MN and/or PDA. This step might not be required if this happens automatically during the deployment; however, if the technical solution for fusion node to management node communications requires this to be done manually, it should be done before the nodes are deployed. This allows any problems to be addressed at the base or outpost instead of in potentially hostile territory. Naturally, any or all of these preliminary steps can be skipped if there is not sufficient time. The consequence of skipping any of these steps is increased risk of deploying nodes that do not function properly.

After the preliminary steps are taken, the soldiers who will be deploying the nodes should travel to the deployment area with all the nodes that are required if possible. The necessity for return trips will depend on how much room is available on the vehicles, how many nodes each soldier can carry, how large the nodes are, and how many are required. Obviously, small nodes are desirable as this will make transport and deployment easier and faster.

Currently, there is little extra space in CF land vehicles and the space on the vehicles is extremely limited. As a result, SASNet components should be rugged enough to withstand being carried on the exterior of vehicles.

Before the SASNet nodes can be deployed, the deployment area must be secured. The extent of this area should have been determined in the planning phase. After the deployment area has been adequately secured, it is important that security is maintained throughout the deployment process. Depending on the threat environment, up to half the soldiers who travel from the base/outpost for deployment will be involved exclusively in maintaining security. This means that the number of soldiers required for a deployment can be significant. When there is a possibility of encountering hostile forces, the group of soldiers that goes "outside the wire" will usually have at least six people. These soldiers will always remain in view of each other during the deployment process.

In order to lower the risk to personnel and increase the covertness of deployment, SASNet is likely to be deployed at night or with a smoke screen. For this reason, it is important that the nodes be easily identifiable to those who are deploying them in these conditions. Also, it must be possible to check whether or not they are functioning properly in poor visibility conditions.

SASNet nodes should be "rapidly" deployable. How rapid depends on the scenario: for a hasty retreat, rapid means a few seconds per node; however, for an extensive perimeter around a forward operating base [3] (FOB), rapid could mean five minutes per node. If only a few seconds are available per node (for example, during a hasty retreat where the nodes are deployed to cover the route of a withdrawing force), then there will be inadequate time to check the functioning of nodes, or to conceal all of them carefully. Nodes could also be deployed overtly to serve as a deterrent to entering an area.

If soldiers have a few minutes per node, then there should be adequate time to conceal nodes at least partially and test whether they are functioning properly. In populated areas, a deployment team will arouse suspicion if they stay in the same location for an extended time. This makes a rapidly deployable system desirable. For example, in Afghanistan, it is difficult to stay for 45 minutes in an area without someone taking interest in you. Attracting attention could compromise a covert deployment, so this reinforces the need to be able to deploy SASNet quickly.

The nodes will be emplaced by dismounted soldiers, so they will need to be able to carry as many nodes as possible when they are outside of their vehicles. Some type of carrying device that attaches to the hip, thigh or chest would be useful for carrying a sufficient number of nodes. It is important to keep in mind that dismounted soldiers typically carry at least 30 kg of equipment (in addition to any SASNet nodes during deployment). However, if a deployment occurs very close (300 m or less) to a base, then the soldiers might not

3. It can take months to build a forward operating base.

have to carry their full load of equipment. This would allow them to carry more SASNet equipment during deployment.

When SASNet nodes are deployed, at least one soldier in the deployment group should have a copy of the deployment plan on a PDA. The separation between nodes can be estimated by pacing off the distance between them. Obtaining more accurate location estimates of the nodes will require the TDOA localization scheme described in the previous section. The node locations relative to each other should be known to a few metres at worst, and ideally to a metre or less. The more restrictive location constraint is imposed by the desire to recover the nodes rapidly if possible. If the position is not known to better than one metre, it can take a very long time to find a well-concealed node.

As each node is deployed it needs to be powered-on. There must be some type of indicator for verifying that a node has been turned on (e.g. light emitting diode (LED), audible signal, vibration). Once the node is on, it should be possible to check whether it is functioning properly. For example the node should be able to run some low-level self-checks automatically, or after a button or switch is set. Again some type of indicator is required to show that the node has passed the self-check.

After the self-check, the node should be emplaced. This may include concealment if desired. Once the node is emplaced (and concealed), its communications with its nearest neighbours should be checked. Communications should be checked *after* a node is emplaced since concealment might affect the radio range. Since a node might be completely buried, a communications indicator that is on the node might not be helpful. Instead, a PDA will have to be used to check the communications links [4]. This process should be quick and easy so that little time is used and minimal expertise is required. If time is not a factor, then each node's sensing capability can also be tested after emplacement. This could involve walking near a node at various distances to verify that it is capable of detecting dismounted targets at the assumed ranges. It is valuable to know the actual detection ranges of the different sensors (especially the shortest range sensor) after deployment in different locations as this can affect the optimal spacing between nodes.

Due to the nature of SASNet's sensing transducers, all of SASNet's low-level sensors are omni-directional except for the passive infra-red (PIR) sensors. As a result, care needs to be taken to ensure that a PIR is oriented in the desired direction. This requires that (a) the desired direction of a PIR's field-of-view is clearly indicated in the surveillance plan, and (b) the PIR sensors clearly indicate their fields-of-view.

After all the nodes in a cluster (low-level and second-level sensor nodes, and the fusion node) have been deployed, the network formation of the cluster should be checked. Either the deployment team responsible for the cluster, or a remote operator (e.g., soldier at the

4. The PDA must be able to query a sensor node directly or via a fusion node to obtain information about how many neighbours the sensor node can communicate with.

management node in a forward operating base) should be able to perform this check. This means that the cluster check can be done from a PDA or the management node. Any problems that are identified should be fixed immediately, either by deploying more nodes or replacing malfunctioning nodes.

Once all the SASNet clusters have been deployed, the network for the whole (global) network should be checked. As with the cluster-level check, either a PDA-carrying soldier on a deployment team or a remote operator should be able to check the global network formation. Again, problems with the global network should be fixed immediately by deploying more nodes or replacing malfunctioning nodes. At the same time as the global network check, the network should be analyzed to identify likely single points of failure. A likely single point of failure might exist where there are few communications links to a key node (e.g., a fusion node). If any weak points are identified, the risk to the system should be mitigated by deploying more nodes (if more are available) to provide alternate, redundant network routes.

Once all the nodes have been deployed and their locations have been calculated or measured, it is desirable to know whether adequate sensor coverage has been obtained. The SASNet software will do this calculation if it is provided with the node locations, node types and performance of each sensor. Unfortunately, this may be very difficult to assess reliably as sensing coverage will depend on local conditions such as the properties of the ground, micro-topography, and the quantity, location and type of vegetation cover. Unless there is sufficient time to test the performance of each sensor (with the results recorded on the PDA or MN), the estimation of the sensor coverage will depend on the assumptions of the sensor models in the SASNet software. If these challenges can be overcome, then the deployment team(s) should be alerted of any instrumented areas that do not meet the tactical requirements for sensor coverage. More sensor nodes should be deployed to fill the gaps.

Each SASNet node should have an anti-tamper device. This device should be engaged as soon as the deployment team is confident that it is functioning properly (i.e., the node has power, passes its self-test, can communicate with its neighbours, and joins the sensor network). This is necessary to ensure that no one steals or hacks into nodes on the network. If someone does attempt to tamper with a node, the node should automatically disable or destroy itself so that it is unusable [5]. This includes erasing any on-board memory and destroying all of the node's electronics. Just in case the deployment teams are overwhelmed by enemy forces during deployment, it must be possible to enable the anti-tamper device rapidly either locally or remotely. This way, the enemy will be denied the use of all SASNet components.

5. The extent to which the node should be disabled or destroyed is not currently known. For the remainder of this document, we shall refer to the (self-)destruction of the nodes, but this could also mean a less severe "disabling" of the node.

After all the SASNet nodes have been deployed, the nodes must be tasked by an operator. Either a soldier on the deployment team with a PDA, or an operator at the management node can do this. The tasking of the nodes will follow the surveillance plan that was developed earlier. The tasking should take place as soon as the proper functioning of the system has been verified. The tasking should be completed before the deployment team returns to base, just in case there are any problems. Tasking the nodes should be a straightforward process that does not require extensive training.

At the end of the deployment, the deployment teams will return to base without leaving any evidence of having deployed the nodes (this is a requirement for covert surveillance). This means that no equipment can be left behind, and any disturbances to the ground should be concealed.

## 3.3 Employment

The main purpose of SASNet is to detect, count and classify [6] targets. Identification [7] of targets may be possible if clear, high-resolution images can be obtained with EO-IR cameras. However, a soldier will likely be required to identify a target. When SASNet detects a target, the MN and/or PDA must produce an alarm that alerts the operators. The alarms should be provided in a number of different ways: a visual alarm on a PDA or computer screen, an audible alarm, and a vibrating alarm. An operator should be able to pick which types of alarms are given depending on the operational constraints (e.g. in some circumstances a visual or audible alarm might give away the position of a soldier who is monitoring SASNet, so only a sub-sonic vibrating alarm should be provided). It is important that alarms be differentiated from non-urgent messages (e.g., warnings about a small change in the health of the system). Alarms require immediate attention while warnings do not. Warnings can be dealt with when time permits. The MN and PDA will record all the alarm and warning data in a database for later retrieval or analysis.

Alarms should be easy to understand and provide enough information to be useful. Important information to convey includes the location, number and classification of targets. The type of alarm (visual, audible, vibration) will affect how much information can be conveyed, but a user should be able to access additional information quickly and easily if desired. For example, it will be difficult to encode and interpret much information in a vibration alarm; however, once a vibration alarm is received, a soldier should be able to access additional alarm information quickly.

It is important to bear in mind that few of the soldiers who use SASNet are likely to receive formal training in its use. Instead they might receive second-hand instruction from a soldier who has received some limited training (e.g., a few hours of instruction). This second-hand

6. Classifying a target means that the target type is determined (e.g. person, animal, car, truck, tank).
7. Identification is the process of determining whether a detected target is friendly or hostile.

instruction could be as short as five minutes. Consequently, it is imperative that SASNet's alarm and warning messages be as clear as possible. Similarly, the SASNet software must be very simple to use.

For some applications (e.g., monitoring a road junction) SASNet will be used to determine the velocity of a target. To do this, SASNet must track a target while it is in the sensor field. Consequently, the velocity data must be associated with the correct target(s). These calculations and associations will most likely be carried out at a fusion node due to its greater computation resources (compared to the sensor nodes).

While SASNet is operational it must self-monitor and self-heal if necessary. This is necessary to ensure that SASNet can meet its surveillance requirements with minimal demand on personnel. If a problem is identified, a message should automatically be sent to the operator. As mentioned previously, the message should indicate whether the problem is urgent. SASNet should be able to diagnose the problem so that useful information is sent to the operator. If SASNet is not able to self-heal (due to limited network resources or technical difficulties), then an alarm must be sent to the operator informing him of the loss of surveillance capability. If possible, more nodes can be deployed to fill the gap left by non-functioning nodes. When the network self-heals or new nodes are added, the global connectivity must be re-checked to ensure that the system is functioning effectively. Also, the sensor coverage should be re-calculated to ensure adequate sensor coverage.

Part of the self-monitoring includes testing the state of the node power supplies. If a battery is running low and is expected to be depleted in the next week, a warning should be sent to the operator so that the battery can be swapped. A low-level node is unlikely to have its battery swapped as there should be redundant coverage; however, a fusion node, second-level sensor node, or relay should have its battery swapped if possible as these are higher value nodes with less (if any) redundancy. One of the challenges of self-monitoring is to be robust against temporary communications problems. This is important so that temporary problems do not distract the operator. Also, unnecessary re-deployments of nodes should be avoided, especially if there are hostile forces nearby.

To ensure that the sensor nodes are performing well, a periodic self-calibration should be conducted. As environmental conditions change, the nodes must re-calibrate to avoid missing targets or causing high false alarm rates. Consequently, the frequency of the calibrations should be determined by the rate of change of the relevant environmental conditions (e.g., ambient sunlight, temperature, wind, precipitation). If a node is not able to calibrate itself, a message should be sent to the operator that the system is not functioning optimally. If resources permit, more nodes can be deployed if necessary.

Besides receiving automated warnings and alarms, the SASNet operator should be able to monitor the system himself via a PDA or the MN. Monitoring should be made easy by having a user-friendy and flexible interface for querying the system. An operator should

be able to determine system-wide, cluster-level and node-level properties. The SASNet diagnostics should be available quickly (a few seconds or less).

Like SASNet, the Classic 2000 can also send information to or be controlled by a hand-held monitor or a laptop (with the hand-held monitor plugged into it). Unfortunately, the limited display on the hand-held monitor (only four lines of text) provides limited information to a soldier. Also, soldiers find it difficult to use as the information had to be decoded. The PDA that will be used with SASNet will not be a SASNet-dedicated PDA, but will be a multi-purpose device. However, the SASNet software that runs on it must avoid the pitfalls identified in the current system: the SASNet program (or service) should provide more information (e.g. graphics to display maps), but remain concise and easy to understand. The Classic 2000's laptop was deemed to be more useful than the hand-held monitor, as it was easier to use. However, there were problems with new laptops as they allowed only USB inputs. The older UGS equipment uses only serial connectors, so this caused compatibility problems. If possible, SASNet should be designed so that it will be adaptable to future changes in computer hardware.

## 3.4 Retrieval

Although a preliminary retrieval plan will have been formulated during the initial planning for the deployment of SASNet, the retrieval plan that is implemented will be entirely dictated by the tactical situation when the retrieval begins. The risk to personnel has paramount importance in determining if and how many nodes are retrieved. The plan must be flexible as the tactical situation might change during retrieval. The availability of personnel to conduct a retrieval operation will also affect how many nodes are retrieved. The higher level nodes such as the second-level sensor nodes and the fusion nodes will be given priority for retrieval due to their significantly higher cost and importance to the system. The low-level sensor nodes will be retrieved only if there is very low risk to soldiers, and there are no other missions to accomplish.

The retrieval operation begins with the soldiers traveling to the areas where the nodes have been deployed. The retrieval team will bring equipment with them for locating, retrieving and carrying back the nodes. A detailed plan of the locations of the nodes will be required for retrieval. This plan can be on a PDA or an adequately detailed map with the node locations recorded on it. Depending on the available technology for locating the SASNet nodes, additional equipment can be used to find the concealed nodes. This technology could aid the soldiers in finding the precise location of the nodes by communicating with the nodes to give their relative range and/or bearing information. The nodes will be recovered by dismounted soldiers who may or may not be traveling to the instrumented area by vehicle. Consequently, the soldiers will have to carry appropriate equipment for stowing the nodes securely until they return to their base. If the soldiers travel to the retrieval area in vehicles, the equipment for carrying the nodes must be securely stowed on or in their vehicles.

Upon arrival at the instrumented area, the area will have to be secured again. Security will be augmented by leaving the portions of SASNet which will not be retrieved active as long as possible, so that these nodes can alert the retrieval teams of possible danger. However, any nodes that are nearby and might produce alarms due to the activities of the retrieval team need to be de-activated. Either a PDA in the field or an operator at the MN should be able to de-activate the required nodes.

Before the nodes are retrieved, they must have their anti-tamper function de-activated. This will likely be done at the same time as the nodes' abilities to sense targets are disabled.

Locating the nodes can be performed in a two-step process. First the retrieval plan (on PDA or paper map) should guide the team to within a few metres of each node. If the retrieval plan does not provide greater precision than this, a second locating stage should enable the team to know where the nodes are to at most one metre. The second stage could involve the retrieving soldier sending signals to the nodes asking them to provide audible or visual signals.

If any nodes are buried, the retrieval team will require tools to dig the nodes out carefully. Once a node is recovered, it must be stowed in some type of bag or other carrying equipment so that the soldier can carry the nodes back to his base (directly or via a vehicle).

Before the retrieval team leaves an area, a self-destruct command must be sent to any remaining nodes in the area. The retrieval team might have to leave before the planned retrieval mission is complete due to nearby hostile forces or a limited time window. Destroying the remaining nodes ensures that the enemy is denied all material. Otherwise, the SASNet components could be used by the enemy (e.g. building improvised explosive devices). Depending on the expected network topology after the retrieval is completed, it might be necessary to send the self-destruct command to nodes *before* any nodes are retrieved. This might be the case if a cluster's network is partitioned by removing the fusion node or other nodes. Note that fusion nodes and second-level sensor nodes are more likely to be recovered than lower-level sensor nodes due to their much greater cost and smaller numbers. The order that nodes are instructed to self-destruct should also ensure that no partitions are created before all the desired nodes are destroyed. In general, it is expected either all or none of the lower-level sensor nodes will be retrieved; the tactical conditions will dictate what happens.

The self-destruct command makes a node inoperable. For obvious security reasons, it is especially important that any cryptographic material (if it is present) be completely destroyed. Also, all its electronics should be degraded to a state that they could not possibly be used by hostile forces. This means that not only do all memory modules need erasing, but the electronics needs to be damaged to the extent that no components can be re-used. The self-destruction should not harm a person who is holding a node when it self-destructs. This ensures that non-combatants who inadvertently disturb or pick up a node are not hurt. There may also be environmental considerations related to the abandonment of destroyed

nodes. It is important that SASNet conform to the most recent CF regulations that govern what types of materials or equipment can be left in theatre.

After a node is ordered to destroy itself, a quick low-level check of the self-destruction should be performed. The only simple test is to verify that the node is incapable of communication. Clearly, if its communications are still functioning, it is not destroyed. Of course, its other systems might still be functioning. This limitation will have to be accepted. As a consequence, the dud-rate for self-destruction must be very low. If a node has not carried out a remote self-destruct command, it should still be able to self-destruct (a) when its power is almost depleted, or (b) when it is tampered with.

A node needs to be able to self-destruct when its power is almost depleted, otherwise it cannot be destroyed remotely. For example, if it is allowed to run out of power under the assumption that it will be possible to swap a battery later, the tactical situation could change so that it is no longer possible to return to the node. This would make it easy for the enemy to capture it and employ its technology to the maximum extent possible. This must be avoided. The nodes do not have to self-destruct as soon as they are no longer capable of sensing and communicating regularly due to a lack of power; instead, they should go into an "energy conservation mode" when their power gets very low, so that they do nothing but guard against tampering and are capable of receiving and carrying out a self-destruct instruction. This should extend the time that the nodes last before destroying themselves.

After all nodes are either retrieved or destroyed, the retrieval team returns to base. When they return all SASNet components will have their batteries swapped for batteries with full charges. All mission-specific settings should also be reset to their defaults (alternately, this could be done as soon as a node is retrieved if it is technically and operationally easy to implement). The nodes should be cleaned and any routine maintenance should be performed as soon as possible. Finally, the nodes should be stored in standard SASNet kits for future use.

# 4 Operational CONOPS

As discussed in Section 2.3, it was not possible to discuss the operational portion of the CONOPS as a panel during the workshop, owing to the time restrictions imposed. Instead, a number of questionnaires were passed out to the subject matter experts, seeking their insights on the topics of command and control, interoperability, security, survivability, logistics, and maintenance. The following sections are compiled from the received responses, and represent the assessment of the subject matter experts.

## 4.1 Command and Control

An important consideration for SASNet is its relationship with the Command and Control (C2) structure of the Canadian Forces. SASNet will be a new tool in the commander's toolbox, one that represents an incremental improvement to CF capabilities rather than a revolutionary technology that requires a paradigm shift in the C2 structure. The following sections discuss several C2 considerations in relation to SASNet.

### 4.1.1 Integration of SASNet in the Command and Control Structure

The current C2 structure of the CF is unlikely to change in order to incorporate a new tool like SASNet. Rather, it is preferred that SASNet is incorporated into the existing C2 structure with minimal accommodation required by the system that is already in place. Flexibility must be built into the SASNet system, in order to allow for any changes in the C2 system in the future.

SASNet will function best if it is seen as an additional element that can fit into the ISTAR plan. Likely a platoon-level asset, SASNet provides platoon commanders with a tool that can fill gaps in the Platoon Range Cards. Should the platoon commander use SASNet to cover otherwise unobservable terrain, he can do so at his discretion, with information appearing on the battle group's (BG's) C4ISR network for reference. It is also possible that a BG commander could order a surveillance task (e.g., on a route he intends to advance along in three days) which would fall on the reconnaissance/ISTAR squadron/company to accomplish. The commander could implicitly task the deployment of SASNet by ordering continuous surveillance be established on a route, or he could explicitly direct that the ISTAR unit instrument an area with SASNet clusters.

SASNet is designed such that it sends alarms to an operator, which can then be reported over the platoon/company/battle group command networks as appropriate. As currently envisioned, it is the responsibility of the operator to provide Situational Reports (SITREPs) and give notice of alarms to his immediate commander. This chain of reporting is the same

for other ISTAR assets, and there is no need to change the system if SASNet is seen as "just another tool" in the ISTAR toolbox.

### 4.1.2 Command and Control of SASNet Deployment

The decision to deploy SASNet depends on the ISTAR assessment of an area to be monitored, a standard practice known as "Information Preparation of the Battlefield" (IPB) that is fully described in Reference [7]. An obvious use for the SASNet system is to cover gaps that cannot be covered with the conventional sensor suites available on current CF land vehicles (e.g., Light Armoured Vehicles (LAVs) and Coyotes). The decision to use SASNet in such a situation is at the discretion of the commander in charge of the given tasking, possibly ranging from a section to a brigade commander. Depending on the length of the deployment and the estimated likelihood of retrieval of the system, the commander should report this deployment to a higher commander so that he is aware of the unavailability of the asset until it is replenished.

At the CONOPS workshop, much discussion centred on the use of SASNet as a type of sophisticated trip-flare. Trip-flares are frequently used by low-level units at their discretion. SASNet clusters, which may be held at the platoon level, may be deployed in a similar fashion. However, should a higher commander wish to use the SASNet clusters for a larger mission (e.g., covering a large, mountainous area), he could feasibly direct his subordinate commands to withhold the use of SASNet in order to preserve these resources for the larger task.

The deployment of SASNet as described above is very similar to the deployment of any other ISTAR asset. Thus, the decision to deploy SASNet closely resembles the decisions that are currently made with existing ISTAR tools.

### 4.1.3 SASNet Information Flow

Once a SASNet system has been deployed, information begins to flow through the SASNet and higher C2 network. It is important to determine how this information flows through the C2 networks, and who sees what information.

The main issue of how information flows through the network revolves around whether information is "pushed" or "pulled". Part of this issue is associated with the design of SASNet itself. SASNet can be tasked to monitor an area for certain types of events, sending alarms, data, and images once appropriate detections have been made. This type of operation is called a "push" since the information is sent to the user at the system's discretion. It is also possible that SASNet could be set up to store data gathered by the sensors, allowing a user to request data from memory that fits a given query. This type of operation is a "pull" and could require the SASNet nodes to transmit large amounts of data to a central repository

(possibly collocated with the SASNet management node). The ability of SASNet to operate in both push and pull modes is a basic feature of the system.

An additional question revolves around who should receive information generated by the SASNet system. The SASNet operator who is responsible for monitoring the system should be the first person to receive information. This operator holds a PDA device or has access to a computer terminal (SASNet management node) that allows him to perform special setup functions on SASNet. As the *i*n situ operator of the SASNet system, all alarms, warnings and notifications from the system must be sent to him.

An important secondary group to receive information are soldiers within a pre-defined radius of the SASNet nodes. If warnings are sent to this group, they can be alerted to a possible enemy attack, and thus be ready with a quick reaction. The ability to notify soldiers in the area of a SASNet cluster should be a capability that the SASNet operator can activate, and would require SASNet to be able to connect to individual soldiers through their personal "Blue" Situational Awareness systems. [8]

In addition to the soldiers in the area of a SASNet deployment, alerts should be sent from the SASNet network to higher level Canadian Army networks. At present, SASNet information would flow to the Land Command Support System (LCSS). This would allow SASNet information to be incorporated into the main Common Operating Picture (COP). Since there is the potential for a lot of data to be sent from each SASNet that is deployed, each local SASNet operator needs to define and activate a filter so that only important alerts are sent. Since SASNet should be able to make complex assessments of the targets it detects, filters can be defined fairly simply (e.g., "Send an alert to higher if a group of three or more men pass by the cluster on an Easterly heading"). These filters will prevent information overload at higher levels.

The last issue in the area of information flow has to do with what information should be passed or made available through the SASNet network. The alerts sent out by SASNet should be structured as "contact" reports with the following information:
– Grid (location)
– Nature of contact
– Target size
– Target activity
– Direction and speed of target
– Time of contact
– Own action (e.g., continuing to monitor, activating cameras, going dormant, self-destruct, etc.)

The SASNet operator should be able to customize the alerts as desired. Beyond this basic information, SASNet should allow users to query the network or allow them to task SASNet

8. Friendly forces are referred to as "blue" forces. Personal Blue Situational Awareness systems are expected to be available by 2020.

to acquire further information.

Aside from traditional target contact reports, SASNet should also pass alerts to all levels if physical or electronic tampering is detected. A networked sensor like SASNet is a potential gateway for attackers to exploit, and requires special monitoring to prevent this from happening. If electronic tampering is detected, the SASNet operator and higher-level C4ISR operators should get urgent alarms as this may represent a significant threat to the system.

Other information, such as system health, should be passed to the SASNet operator when a major change occurs (e.g., loss of a number of sensors in the cluster). Other system health issues, such as battery life, should be available for query, with the possibility to automatically send messages to the local operator when failure of a sensor node becomes imminent. Messages requesting battery changes or the deployment of additional nodes could also be sent to those responsible for the logistics chain, in order for the proper supplies to be included with future shipments.

## 4.2 Interoperability

Since SASNet will be a new tool added to the CF ISTAR toolbox, it is important to examine the interoperability issues associated with making this new tool work in the existing structure. The main focus areas for this discussion include communication standards and hardware considerations

### 4.2.1 Interoperability and Data Communication

The obvious first step toward interoperability is to ensure that SASNet can communicate with Canadian C4ISR systems both at the time of fielding and in the future. This would include the ability for SASNet to post notifications directly or indirectly onto the electronic situational awareness maps that are used (currently in the ATHENE system). The communication and data standards of SASNet need to remain flexible after fielding, since they may need to be changed as the CF acquires newer systems. Connection to allied information systems will be through higher level Canadian C2 systems so no special consideration is required for SASNet's interoperability with these allied systems.

As was discussed in Section 4.1, a SASNet network should have the ability to communicate with the higher C4ISR network. Filters need to be defined such that only detections of significance are sent to the higher network, thus reducing the potential for information overload.

An issue associated with communication interoperability is the type of data that will be passed amongst the systems. The most useful data on the detections are contact time and location, contact nature, target speed and heading, imagery, and target infrared signatures.

The format of the files that contain this information and the units in which the data are measured must adhere to the standards of the C4ISR systems.

### 4.2.2 Hardware Considerations for Interoperability

Although hardware interoperability is not a large concern for SASNet (owing to the lack of physical interaction amongst the nodes), there are several considerations to take into account. The first among these concerns involves the device which will be used by the local SASNet controllers to manipulate the SASNet clusters. This device is envisioned as a PDA or tablet-type computer that will allow the controller to activate the cluster, set filters and options, and perform other setup and maintenance operations. The device will also function as the operator's main method of receiving SASNet messages. It is preferable that the device chosen be based on a Commercial-Off-The-Shelf (COTS) product, perhaps a ruggedized COTS PDA, with specialized SASNet software installed on it. This way, SASNet management software is installed on a standard operating system, and may be easily installed on future PDAs. This PDA may also be interfaced with the Commander's situational awareness software (currently the Situational Awareness Module) on the computer in a land vehicle, and thus a standard communications protocol could be used to transfer data.

Another hardware consideration for SASNet has to do with perhaps its only hardware-hardware interaction: transportation on the battlefield. While the system itself will not require special care during transportation, the currently cramped rear compartment of the LAV does not offer much in the way of space to store SASNet. There may be a requirement for SASNet to come with its own container system that can either be fitted into the back of a LAV or easily strapped to the outside of the vehicle. Ideally, this container system could also serve as a node carriage and dispenser system for dismounted soldiers.

The final hardware consideration for interoperability has to do with the sensor nodes themselves. The CF has a tendency to field equipment for decades, and if successful, SASNet will likely follow this pattern. With the potential for a long period of fielding, and since the lower-level SASNet nodes are designed to be essentially disposable, there will likely be numerous replenishment orders to replace depleting sensor node stocks. Since technological development will also continue during the SASNet fielding, new sensor nodes may eventually be manufactured and used to replenish stocks. As an example, a new development in nanotechnology could allow for extreme miniaturization of the sensor nodes. The new nodes must be able to interact with sensor nodes of the previous generations, as well as with the SASNet management modules.

## 4.3 Security

The security of SASNet is one of the most important operational considerations for this new system. Since SASNet will likely be deployed into areas that are not directly observed by other sensors, it is possible that the clusters could become targets for attack and exploitation. This section discusses the vulnerabilities and precautions associated with the security of the SASNet system.

### 4.3.1 Vulnerabilities

SASNet clusters will likely be deployed into areas that are not directly observable by other sensors, and thus may present an attractive target for attack by enemies. For example, insurgents in Afghanistan are quite adept at detecting new items in their environment, such as trip flares, and either removing them, or using them against the Canadian or allied unit in the area. This suggests SASNet sensor nodes would be targeted if they are detected.

The obvious first concern for the SASNet nodes is their physical security. It is possible that the nodes could be tampered with to render them inoperable or possibly made to do harm to soldiers returning to the area to perform maintenance or retrieval operations on the system. Other concerns are that the nodes could be stolen or that the electronic components inside could be used in the manufacturing of improvised explosive devices (IEDs).

Another concern with SASNet is its vulnerability to electronic attack. While the current conflict in Afghanistan is against relatively low-technology insurgents, other operations in the future could involve hostile forces with comparable or even superior technological prowess. Since SASNet communicates wirelessly, it is possible that a sophisticated enemy could carry out a number of types of attacks on the system of varying degrees of severity. At the low end of the severity scale, sensor nodes could be made to shut down, rendering the system useless. It is possible that SASNet would be vulnerable to "phishing" attacks and made to reveal the location of other nodes, clusters, or even the SASNet operator. This leads to the possibility of attack against the operator or the cluster itself. Other severe attacks could focus on duping the system to make false reports, or even hacking into the higher C4ISR networks, depending on the level of integration of SASNet into the overall network structure.

When an attack occurs, whether it is physical or electronic, an alarm should be sent to the SASNet operator's PDA or management node. The alert should take the form of a contact report, giving the location(s) of the node(s) that are affected by the attack, the nature of the attack, and present the operator(s) with several options to counter the attack. While less severe attacks could be handled by the local SASNet operators, severe attacks, such as hacking attempts, will likely require a response from a higher level. This tiered approach will make the physical security of SASNet a local responsibility, while electronic security will be handled at a higher level where experts in computer warfare are more likely to be

available.

### 4.3.2 Precautions

The primary precaution to take is to monitor the SASNet system continuously for signs of an attack, be it physical or electronic. This should primarily be done autonomously by SASNet, as it would be able to react faster than a human at the first signs of tampering. In addition to taking initial countermeasures for the attack, SASNet should send alerts to the SASNet operator(s) (and higher levels if it is an electronic attack). The operator(s) could then decide what further actions to initiate, or refer the alert to a computer-warfare expert.

In the event of physical tampering, there are a limited number of precautions that could be taken to preserve the security of the system. If the SASNet cluster is within the reach of a Quick Reaction Force (QRF), the force could be dispatched to investigate the tampering. However, if the security situation does not allow for a QRF to be dispatched, the system would need to be able to protect itself. This could be accomplished by designing each sensor to be able to self-destruct. Since physical tampering may not be the result of hostile actions (i.e., a child could find a sensor node and play with it), the self-destruction should not impact beyond the sensor node itself. At the same time, the sensor node cannot just be rendered inoperable as it could be scavenged for parts that, for example, could then be used for bomb-making. A self-destruct mechanism that would completely destroy the electronics inside, without injuring anyone holding the node, would be ideal. A further investigation of this mechanism is warranted, with particular attention on the environmental safety of this destruction mechanism.

A node should also self-destruct if its power is almost completely depleted. If it runs out of power before self-destructing, there is no way of denying the node to the enemy. [9]

Should electronic tampering be detected, a number of precautions could be taken, depending on the nature of the attack. The primary response should be to erect a firewall around the affected node(s) from the network, such that an electronic attack can go no further. If the attack is some form of a “phishing expedition”, deceptive information could be sent back in order to frustrate or draw out the attacker. If the nature of the attack permits, a counter-hack could be enacted to attempt to attack or learn more about the enemy. The implication of these suggestions is that the CF may need to employ computer-warfare specialists who would be able to “fight” in the cyber domain.

9. Note that the self-destruct mechanism can be disabled remotely if it is determined that there is no threat to the nodes but they will not be retrieved until after they lose power. This is a particularly useful feature for more expensive nodes like the second-level sensor and fusion nodes.

## 4.4 Survivability

The survivability of SASNet refers to the amount of abuse that the system should be able to absorb, whether during transport, deployment or employment. While it is desirable for SASNet to be highly survivable in all conditions, this will drive up the costs of the nodes and may result in heavier casings. From an economic and a soldier-loading standpoint, more expensive, heavier sensors would make SASNet less attractive for use on the battlefield. Consequently, there are trade-offs amongst survivability, cost, number of nodes and ease of transport/deployment.

### 4.4.1 Survivability in Transport and Deployment

In the current operating environment, SASNet will likely be employed forward of the main operating base, and this has ramifications in terms of the transportation of SASNet equipment to forward units. Currently, the CF faces a difficult security environment, where logistics vehicles are threatened with attack by improvised explosive devices, rocket-propelled grenades, and small arms fire with little protection for the cargo. As a consequence to this threat, small cargo loads may be air-dropped to more remote outposts, using pallets with parachutes to deliver the loads.

SASNet must be designed to be able to survive transport by ground and by air. When transported on the ground, SASNet kits will likely be strapped to the outside of a vehicle, so will need to be able to withstand the shocks and jostling of traveling over rough terrain. SASNet nodes should also be required to survive the shock of an air drop. While the load would be parachuted to its objective, there is still an appreciable shock associated with hitting the ground.

As was discussed earlier (Section 4.2.2), the best solution for ground transportation would be if SASNet nodes were packed into a durable container/dispenser that could be fastened to a land vehicle (either inside or outside). These containers should be designed to help cushion any impacts. If the containers provide enough cushioning, the casing of the SASNet nodes would not have to be designed to be as hardy, thus reducing the production cost per node.

### 4.4.2 Mission Survivability

Once the SASNet nodes have been transported forward and deployed into areas of interest, they will then need to survive the conditions on the ground. The sensor nodes will be exposed to a number of challenging conditions, and the system must be robust enough to survive in order to be useful to the units deploying the nodes.

A major consideration for a deployed node's survivability is the environment. In the current theatre of operations in Afghanistan, the nodes will be exposed to extreme temperatures and

extreme weather. This will likely be true in any operational environment, and thus these factors must be designed against. In the summer time, nodes in Afghanistan will regularly experience daytime temperatures greater that $40^{o}$ C, and may endure rapid temperature drops to near freezing at night. These temperature swings can be particularly challenging for the nodes, as repeated expansion and contraction of components could potentially lead to system failure.

Weather events such as sandstorms or severe rain or snow occur frequently, and can lead to foreign elements getting inside of the nodes. Some specific challenges that the nodes will be expected to survive include long term burial by sand or snow and periodic submersion under water. Thus, SASNet nodes should be cased in weatherproof shells that will allow the nodes to continue or resume operation after an extreme weather event. In addition to weather considerations, extreme temperatures, such as the extreme cold of the Arctic, may result in poor battery performance. The degradation of SASNet power modules under these conditions should be studied and other methods of powering the nodes or recharging drained batteries should be investigated.

Another critical mission survivability issue is power. The environments that SASNet will be deployed into will range from extremely quiet, remote areas to extremely busy urban areas. These factors will impact SASNet's power and energy requirements. In quiet areas, fewer detections means that the nodes will lay dormant for longer periods of time, while in busy areas, the nodes could potentially be making detections constantly and thus be constantly powered up. Under quiet conditions, SASNet should be capable of operating for at least 60 days; this benchmark was achieved with the Classic 2000 UGS system. It is believed that an operational capability shorter than this would not make the personnel, cost and time commitments to deploying SASNet worthwhile. In a busy environment, the system would likely be employed for short-term tasks like covering temporary observation posts, covert hides (e.g., sniper nest), and ingress/egress routes from key locations. For these short-term tasks, a SASNet node life of 72 hours (operating constantly) would be acceptable.

Beyond environmental and activity considerations for SASNet survivability, it is also possible that combat could take place where the systems will be placed. Small arms fire is not likely to be a concern, as the SASNet nodes would be widely scattered and camouflaged when deployed. However, SASNet clusters may be engaged (intentionally or not) by indirect fire, such as artillery or heavy bombs. An indirect fire attack such as this would subject the nodes to extreme concussion and overpressure effects. It may be infeasible to harden the nodes against these effects, but it would be useful to provide commanders with an estimate of the expected percentage loss of SASNet nodes that are within a given radius of an indirect fire attack. This would also give the commanders information relevant to the use of indirect fire of their own to engage enemies within the SASNet observation area.

## 4.5 Logistics

A number of logistical issues are centred on the deployment of SASNet with the CF. Since SASNet is a new set of equipment for the CF, and ideally it could be heavily used, the logistical implications of introducing this new tool need careful consideration. The issues dealt with in the logistics operational CONOPS include transportation to and within a theatre of operations and inventory control.

### 4.5.1 Transportation

The transportation of SASNet begins in Canada, where the asset will be held until an operational commander decides that SASNet should be brought to theatre. The decision to bring SASNet to theatre would be made as early as possible in the commander's plan, when an operational requirement for SASNet is identified. Early inclusion of SASNet in the commander's plan allows stocks of the system components to be made ready for transportation, with sufficient stocks shipped to cope with the expected high rate of consumption of the disposable nodes.

SASNet's priority level for entering theatre will depend on the commander's plan. Of course, top priority for supplies is given to ammunition, fuel, and rations, but if SASNet represents an essential part of the Canadian ISTAR plan, it will also have a high priority for transportation.

Once in theatre, the deployment of SASNet will depend on the level at which it is held. If SASNet is held at the platoon level, then a basic SASNet kit, with its requisite packaging system, should be included in the planning of what land vehicles carry. If vehicles in the platoon require non-SASNet payloads in order to complete certain missions, the SASNet kits would be left behind with the Company Quartermaster (CQ).

For "light" or "dismounted" companies, the soldiers would be required to obtain SASNet systems from their CQs and bring them to the staging area before departure. Assuming that the sensor nodes are about the same size, shape, and weight as a hockey puck (approximately 250 g per node), an efficient packing of the system will be essential. For example, a tube-like dispenser that could be strapped to the outside of a soldier's pack could be used. For future consideration, a transportation/storage solution should be easily adaptable to carriage by pack robots that may be present on the battlefield of the future.

The main issue that is driving transportation considerations is weight. Both vehicles and individual soldiers are heavily burdened with supplies essential to their missions. Sensor packs must be able to fit into current cargo racking systems, and broken down into subcontainers for each soldier to carry on foot.

### 4.5.2 SASNet Inventory Control

Since the operational concept of SASNet includes a layer of sensor nodes that are essentially disposable, SASNet should be treated as a consumable supply. Although SASNet nodes will be consumed at a much slower rate than other consumables (food, water, etc.), they will still require constant replenishment.

To control the inventory, the CQ will be required to maintain an up-to-date manifest of the SASNet nodes that he is holding. The CQ staff will be required to perform routine verification of the SASNet systems, ensuring that they have not expired and are in good working order. As SASNet nodes are returned from the field (second level nodes would likely not be considered disposable) the CQ would perform routine maintenance on them to return them to service where possible, and send the remainder further up the maintenance chain for further repairs or back to Canada for recycling.

In addition to the systems themselves, supporting tools will also need to be kept in stock. There should be little or no need for first line maintenance tools, as the system should be designed to be compatible with the soldier's usual tools. At least a 10% reserve of batteries, repair, and cleaning parts should be held with the CQ for the second-level nodes (e.g., fusion and camera nodes). Maintenance beyond this should be done at a higher level, and thus would not require specialized tools to be deployed forward with the system.

### 4.5.3 Consumption Estimate

It is difficult to predict precisely the rate at which nodes will be consumed, but a typical SASNet scenario, defence of a FOB, is analyzed to provide a consumption estimate. A FOB is typically defended by a platoon or company-sized group of soldiers. It was estimated that a company located at a FOB could consume around 1,000 sensor nodes per month. Consequently, a battle group-sized task force might consume more than 3,000 sensor nodes per month. If each sensor node (plus packaging) weighs 0.5 kg, that means 1,500 kg of SASNet cargo is required each month.

## 4.6 Maintenance

In spite of the operational concept of being a "disposable" system, SASNet includes a number of components that are either too expensive or too sensitive to be left in the field once their usefulness has come to an end. When a tasking ends, or a more sophisticated component fails, these nodes will need to be collected and returned for maintenance. The issues discussed in this section include the equipment that will be maintained as well as what levels maintenance will be performed by whom.

### 4.6.1 Equipment to be Maintained

As discussed previously, some of the components of SASNet are too expensive or too sensitive to leave in place upon the completion of a task or failure of the equipment. This equipment will need to be collected and maintained so that it can be returned to service. The camera and fusion nodes in the SASNet architecture will obviously need to be maintained, due to their expense and possible accumulation of sensitive data.

Failure of the second-level nodes in the field could potentially create single-point failures of the SASNet clusters themselves, and thus this could be a very significant issue. This risk could be mitigated by including spares with every SASNet kit. If spare nodes are immediately available, these can be deployed at the same time the inoperable nodes are being removed for maintenance, thus maintaining the integrity of the SASNet cluster without waiting for resupply.

Other equipment that will require maintenance is the PDA device to be used by the local SASNet operator to setup and interact with their clusters. It is expected that the majority of the maintenance to be performed on this device is regular updating of the firmware/software. It is possible that the SASNet PDA will be the same as other PDAs supported by the Army G6, and thus the maintenance burden could be reduced.

An acceptable schedule of regular maintenance, including updates to the PDA and basic work on the sensor nodes (e.g., cleaning lenses and other components), should occur no more frequently than twice per year. This minimizes the burden to the operators, and indicates that SASNet hardware should be designed to be highly robust. A minimum sensor node reliability rate [10] of 90 - 95% should be realized in the disposable sensor nodes, and a higher rate in the higher level nodes.

### 4.6.2 Maintenance Lines

An examination of the types of maintenance tasks that will be performed has shown that these tasks can be grouped into several “maintenance lines”. First-line maintenance is made up of the simplest tasks. As each SASNet node is unpacked and readied for deployment, it should have its battery checked and a self-test should be run. If the batteries are low, they should be replaced. If the node fails the self-test, it should be sent to second-line maintenance (see paragraph below). Additionally, any sensor nodes that are retrieved from the field should receive first-line maintenance before being repacked for their next use. These tasks can be performed by the local SASNet operators using their standard equipment (e.g., Gerber multi-tool, bayonette) in the field.

Should a part in a sensor node fail, resulting in the loss of the node, or a malfunction occur

10. Here, “reliability rate” is defined as the probability that a node will operate for a fixed duration of time (e.g. two months) without encountering problems that affect its effectiveness.

in a higher-level node, these nodes should be sent for second-line maintenance. It will likely require a Land Force Computer Information Systems (LFCIS) technician to perform tasks in this line of maintenance. They should be able to perform these tasks with their normal tools set, although they may require specialized diagnostic software to determine what systems are malfunctioning. Second-line maintenance will be performed inside a FOB or Main Operating Base.

The final, third-line of maintenance will take care of any systems that cannot be fixed at the second line. Third-line maintenance will be performed in Canada by the company that will be contracted to manufacture and maintain SASNet sensor nodes. They will use whatever specialized tools are necessary for the repairs, and may elect simply to replace and recycle the returned sensor nodes.

# 5 Conclusion and Recommendations

The CONOPS for SASNet has been presented in this paper. It was developed after extensive consultation with Canadian Army personnel with expertise in UGSs, and scientists and engineers involved in the development of SASNet. The Army experts provided insight on how an operational SASNet might be used. Based on their experience they highlighted the real-world constraints that exist when conducting military operations. The SASNet scientists and engineers provided expertise on the technologies that will be used in the sensor network. This expertise is vital for understanding what is possible with today's state-of-the-art technology.

The SASNet CONOPS is dealt with in two parts: tactical and operational. The tactical CONOPS deals with the planning, deployment, employment and retrieval of the system. SASNet should be treated like any other surveillance asset used by the Army. As a result, planning its deployment should follow standard procedures. Nodes in the SASNet network should be easy to deploy rapidly. This will minimize the expertise and training required of soldiers, and will reduce the risk to those who must deploy the system near hostile forces. SASNet should provide reliable and useful information in a timely manner so that soldiers have enough time to react to the detection of enemy targets. Finally, the retrieval of the system should also be rapid, and in the event that nodes can not be recovered, they should be destroyed remotely to avoid capture by the enemy.

The operational CONOPS discusses command and control, interoperability, security, survivability, logistics and maintenance. SASNet's place in the command and control structure (likely controlled at the platoon or company level) is discussed, as are the interoperability implications of its need to integrate with the existing command and control structure and systems. Both physical and electronic security are important for SASNet as it is vital that an enemy be denied the opportunity to use SASNet components against Canadian forces, or be able to hack into the SASNet (or higher-level) network. As most SASNet nodes are envisioned to be disposable, their ability to survive kinetic weapons is limited; however, a more relevant survivability concern is their ability to manage their energy consumption in such a manner that their limited resources (i.e., batteries) last for long periods of time (at least two months in "quiet" areas). If SASNet will be used for surveillance as extensively as hoped, it will require significant planning from a logistics perspective as thousands of nodes could be used by a battle group in a single month. Large quantities of equipment make maintenance an issue as well, so care needs to be taken to ensure that problems can be diagnosed and fixed easily, or that spares are readily available.

## 5.1 Recommendations

We recommend that the SASNet CONOPS should guide the development of the system over the course of the TD project, bearing in mind that the CONOPS is likely to evolve as

new insights are obtained during successive field trials. This guidance should ensure that the system is designed with the intended users and operational realities in mind. Ultimately this should lead to a more successful sensor network that is trusted by the soldiers who rely on it for their safety.

During the development of this CONOPS, several areas were identified where further operational research studies could help to refine the CONOPS for SASNet. These are mainly trade-off studies which would provide a better understanding of the relationships amongst several key variables. Trade-off studies between cost and performance would give valuable insight into the optimal design and employment of the system. There are also trade-offs to consider between power usage, sensor performance, and node weight and volume. Additionally, an important assumption to test is whether a single type of multi-sensor node is preferable to multiple single-sensor nodes. We recommend that these studies be performed, resources permitting, by operational research analysts to ensure that the effectiveness of SASNet is maximized.

# References


[1] Institute of Electrical and Electronics Engineers (1998), *IEEE guide for information technology - system definition - Concept of Operations (ConOps) document*, Technical Report Institute of Electrical and Electronics Engineers. IEEE Standard 1362-1998.

[2] Vorthman, R.G. and Holt, S.M. (2006), Towards a Rational Approach to Standards for Integrated Ocean Observing Systems (IOOS) Development, In *OCEANS 2006*, pp. 1 – 7, Institute of Electrical and Electronics Engineers.

[3] Diaper, Dan and Stanton, Neville (2003), *The Handbook of Task Analysis for Human-Computer Interaction*, Lawrence Erlbaum Associates.

[4] Waller, David (2008), Suitability of the SASNet Wireless Sensor Network for Early Warning Detection, In *CORS/Optimization Days 2008 Joint Conference*, Canadian Operational Research Society.

[5] Defence Terminology Bank (online), Assistant Deputy Minister, Information Management, http://terminology.mil.ca
(Access Date: November 2007).

[6] Zhou, Yifeng and Lamont, Louise (2008), An Optimal Local Map Registration Technique for Wireless Sensor Network Localization Problems, In *International Conference on Information Fusion (FUSION08)*, International Society of Information Fusion.

[7] Directorate of Army Doctrine (2000), *Land Force Information Operations - Intelligence Field Manual*, B-GL-357-001/FP-001 ed, Chief of the Land Staff.

[8] Communications Research Centre Canada (2006), Self-healing Autonomous Sensor Network (SASNet) Requirement Document - Version 15. unpublished.

[9] U.S. Marine Corps (2004), Remote Sensor Operations (including errata), MCRP 2-24B ed, U.S. Marine Corps.

This page intentionally left blank.

# Annex A: Operational CONOPS Questionnaires

## A.1 Command and Control questionnaire

1. Address how the system will integrate into the existing command and control structure. Identify clear lines of communications to meet the proper command and control requirement.
2. Where does this system fit in current C2 structure?
3. Could its place in C2 structure change in the future?
4. Who makes decision to deploy the system?
5. Who plans the deployment?
6. Information/warnings/alarms from the system are accessible by or flow to whom?
7. What information is provided to or accessible by different people?
8. When should information be pushed from the system to other systems/people?

## A.2 Inter-operability questionnaire

1. Address how the system will be standardized and inter-operate with existing infrastructure. Identify procedural and technical interface standards to be incorporated into the system design to ensure the required degree of inter-operability. A system should be designed to conduct normalized operations and maintenance consistent with the mission and responsibilities delegated to it. Areas to address may include how standard commercial-off-the-shelf (COTS) hardware/software may be utilized for mission execution and for enhancing commonality of replacement parts with other like units. This commonality of hardware/software will enable systems with compatible and/or similar missions to share the same resources.
2. What part(s) of system should be able to inter-operate with existing (or future) systems? (e.g. Does software need to run on specific computing platform?)
3. Can system run entirely stand-alone?
4. Will system be pushing data to other systems? Pulling data from other systems?
5. What data need to be shared between this system and other systems?
6. Are there physical interfaces between this system and existing equipment? (To pass data, supply power, secure during transport, etc.)
7. What standards does system have to comply with?

## A.3 Security questionnaire

1. Discuss the security aspects and requirements necessary to maintain the effectiveness of the system.
2. What must be done to ensure the system is secure?
3. Who is responsible for the security of the system?
4. How frequently is the security of the system checked?
5. Where can you verify the integrity of the security from?
6. How are security breaches identified?
7. Who is notified about security breaches?
8. What security measures (automatic and manual) are in place in the event of a security breach?

## A.4 Survivability questionnaire

1. Address the level of conflict the system will survive/endure to assure mission accomplishment.
2. What must be done to the system to render it inoperable?
3. For how long should the system operate? (days, weeks, months?)
   (a) under “quiet” conditions
   (b) in busy urban environment
4. How robust do components have to be to survive transportation, deployment, and retrieval?
5. Is camouflage of components required? How good should camouflage be?
6. In what type of weather conditions should system be able to operate?
7. What degree of node failure rate should the system be able to absorb?

## A.5 Logistics questionnaire

1. Describe the concept of support for this system. Discuss issues regarding replenishment and reconstitution of the system during all periods of conflict. Include software configuration control, transportation and supply issues where applicable.
2. What needs to be transported with the system to support it? (e.g. spare batteries, tools for repair)
3. Are there any special considerations for the transportation of this system?
4. How much volume/weight should a single "unit" of the system take up?
5. How is hardware or software updated in theatre?
6. Are special services required to support the system?
7. When will system be transported (with respect to soldiers who will employ the system)?
8. How will inventory of system components be maintained?
9. Who decides that the system will be transported into theatre?
10. When will the decision to transport to theatre be made?
11. How will non-functional components be dealt with? (Who decides to fix or dispose? How, where, when to dispose?)

## A.6 Maintenance questionnaire

1. Address any maintenance issues which may include single point failures, common maintenance support, and operation & maintenance (O&M) or life-cycle costs.
2. What system components need to be maintained?
3. What is an acceptable frequency of maintenance?
4. When should maintenance be performed (with respect to employment of system).
5. Who should do the maintenance?
6. Where should one be able to do the maintenance (in field? at base? in Canada only?)
7. What tools are required to perform maintenance? (hardware and software)
8. What is a realistic expectation for system reliability?
9. What fraction of components are considered spares?

# Annex B: Tactical CONOPS elements - task lists

The task lists that were used to prompt discussion at the SASNet CONOPS workshop were derived from an analysis of the SASNet Requirements document [8] and a United States Marine Corps document for “Remote Sensor Operations”[9].

## B.1 Planning task list

1. Determine surveillance requirements.
   (a) What information to collect
   (b) Where to collect it
   (c) When to collect it
2. Determine availability of surveillance assets (SASNet included).
3. Assess terrain (and its effect on comms, detection range, etc. of surveillance assets).
4. Determine specific types of sensor nodes required to meet surveillance requirements.
5. Assess radio environment of surveillance area.
6. Determine approximate number and locations of nodes (sensor, fusion, EO cameras, relays).
7. Determine taskings for all nodes.

## B.2 Deployment task list

1. Secure area where SASNet will be deployed.
   (a) Determine extent of area to secure.
   (b) Travel to area.
   (c) Secure area.
   (d) Maintain security while SASNet is deployed.
2. Deploy nodes ”rapidly”.
   (a) Verify nodes are functional before transport to deployment area.
   (b) Transport nodes to deployment area.
   (c) Place nodes with required positional accuracy.
   (d) Power-up/initialize nodes.
   (e) Verify nodes are functioning.
   (f) Conceal nodes (optional).
   (g) Check communications between neighbouring nodes.
3. Check cluster-level and global network formation.
   (a) Check that each cluster has its network properly formed.
   (b) Check that the global network is properly formed.
   (c) Identify any likely single points of failure (due to few comms links).
   (d) Ensure all nodes are appropriately tasked.
4. Localize nodes. (This may happen during task 2. depending on the localization scheme)
   (a) Estimate inter-node distances if possible/required.
   (b) Calculate node positions and uncertainties.
5. Determine whether adequate coverage has been obtained.
   (a) Calculate coverage for detection and classification (including uncertainties).
   (b) Alert user if minimum coverage is not satisfied.
6. Deploy more nodes if required and operationally feasible.
   (a) Repeat tasks 2 to 5.

## B.3 Employment task list

1. Detect and classify targets.
   (a) MN and/or PDA alerts user if target class has been pre-selected to be of interest.
   (b) MN and/or PDA records all data for later retrieval.
2. Determine velocity of target.
   (a) At MN or PDA, velocity data must be associated with correct target(s).
3. Self-monitor and self-heal if necessary.
   (a) Periodic self-calibration of nodes.
   (b) Diagnose problems (must be robust against temporary comms problems).
   (c) Autonomously fix problem if possible.
   (d) Ensure network is reconfigured successfully (no partitions).
   (e) Recalculate coverage if nodes lost/gained.
   (f) Inform user about any change in coverage.
4. User monitors system (through fusion nodes with PDA or via management node).
   (a) Monitoring software should run on machine already used by soldier (just another application/service).
   (b) Flexible and easy-to-use interface for querying (at system- or node-level).
   (c) System diagnostics available quickly.
5. User understands and reacts to alarms/messages generated by SASNet.
   (a) System effectively alerts user of all alarms and problems.
   (b) Alarms and problems must be articulated concisely to minimize the time spent interpreting them.

## B.4 Retrieval task list

1. Disable/destroy nodes that will not be retrieved.
   (a) Assess risk to personnel for recovery of nodes.
   (b) Determine which nodes, if any, warrant recovery given risk to personnel and time constraints.
   (c) Send “self-destruct” message to nodes that do not warrant recovery.
   (d) Verify that destroyed/disabled nodes are really disabled.
2. Recover some or all nodes (if reasonable and able) after mission complete.
   (a) Verify list of nodes to recover; determined in 1.2. (Include nodes that could not be successfully destroyed/disabled.)
   (b) Formulate schedule/plan for recovery of nodes.
   (c) Travel to and secure appropriate area.
   (d) Recover desired nodes.
   (e) Return to base.

# List of Abbreviations

| | |
|---|---|
| AOR | Area of Operation |
| BG | Battle Group |
| BGL | Battle Group Level |
| BLOS | Beyond-Line-of-Sight |
| C2 | Command and Control |
| C4ISR | Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance |
| CF | Canadian Forces |
| CONOPS | Concept of Operations |
| CORA | Centre for Operational Research and Analysis |
| COTS | Commercial-Off-The-Shelf |
| COY | Company |
| CQ | Company Quartermaster |
| CRC | Communications Research Centre |
| DND | Department of National Defence |
| DRDC | Defence Research and Development Canada |
| EO-IR | Electo-optical infra-red |
| FOB | Forward Operating Base |
| FTA | Functional Task Analysis |
| GIS | Geographical Information System |
| GPS | Global Positioning System |
| IED | Improvised Explosive Device |
| ISR | Intelligence, Surveillance and Reconnaissance |
| ISTAR | Intelligence, Surveillance, Target Acquisition and Reconnaissance |
| LAV | Light Armoured Vehicle |
| LED | Light Emitting Diode |
| LOS | Line-of-Sight |
| PDA | Personal Digital Assistant |
| PIR | Passive Infra-red |
| QRF | Quick Reaction Force |
| R&D | Research and Development |
| SAS | Situational Awareness System |
| SASNet | Self-healing Autonomous Sensor Network |
| SITREP | Situational Report |
| SME | Subject Matter Expert |
| TD | Technology Demonstration |
| TDOA | Time Difference Of Arrival |
| UGS | Unattended Ground Sensor System |
| UOR | Unforeseen Operational Requirement |

This page intentionally left blank.

# Distribution list

DRDC CORA TM 2008-052

## Internal distribution

### DRDC CORA

1 Lise Arseneau

1 Abderrahmane Sokri

1 Ian Chapman

1 Thierry Gongora, Team Leader, Science and Technology Operational Research Team

4 Library DRDC-CORA

### DRDC Valcartier

### DRDC Ottawa

1 David Waller

1 Director of Science and Technology Land

### DRDC Valcartier

1 Benoit Ricard, SASNet Scientific Advisor

**Total internal copies: 11**

## External distribution

### Department of National Defence

1 Capt Max Michaud-Shields, Canadian Forces Land Advanced Warfare Centre

1 Maj Keith Laughton, SASNet Exploitation Manager, Directorate Land Requirements

1 Maj Thomas Burke, Directorate Land Concepts and Designs

1 Maj Ruff, Directorate Land Concepts and Designs, Gagetown Detachment

1 WO Berrigan, Directorate Land Concepts and Designs, Gagetown Detachment

1 Shawn Hoag, Directorate Land Command and Information

### Communications Research Centre, Industry Canada

1 Louise Lamont, Research Manager, Mobile Ad hoc and Sensor Network Systems, 3701 Carling Avenue, Ottawa, Ontario, K2H 8S2

1 Luc Boucher, Program Manager, Wireless Applications and Systems Research, 3701 Carling Avenue, Ottawa, Ontario, K2H 8S2

## Newtrax Technologies Inc.

1 Alexandre Cervinka, 3674 St-Hubert, Montreal, Quebec, H2L 4A2

**Total external copies: 9**

**Total copies: 20**

## DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

   Defence R&D Canada – CORA
   Dept. of National Defence, MGen G.R. Pearkes Bldg., 101 Colonel By Drive, Ottawa, Ontario, Canada K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

   UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

   Concept of Operations for the Self-healing Autonomous Sensor Network

4. AUTHORS (Last name, followed by initials – ranks, titles, etc. not to be used.)

   Waller, D.; Chapman, I.; Michaud-Shields, C.M.

5. DATE OF PUBLICATION (Month and year of publication of document.)

   July 2009

6a. NO. OF PAGES (Total containing information. Include Annexes, Appendices, etc.)

   72

6b. NO. OF REFS (Total cited in document.)

   9

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

   Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

   Defence R&D Canada – CORA
   Dept. of National Defence, MGen G.R. Pearkes Bldg., 101 Colonel By Drive, Ottawa, Ontario, Canada K1A 0K2

9a. PROJECT NO. (The applicable research and development project number under which the document was written. Please specify whether project or grant.)

   12pk

9b. GRANT OR CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

   DRDC CORA TM 2008-052

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

   (X) Unlimited distribution
   ( ) Defence departments and defence contractors; further distribution only as approved
   ( ) Defence departments and Canadian defence contractors; further distribution only as approved
   ( ) Government departments and agencies; further distribution only as approved
   ( ) Defence departments; further distribution only as approved
   ( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11)) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

The purpose of the Self-healing Autonomous Sensor Network (SASNet) Technology Demonstration (TD) project is to demonstrate an ad hoc wireless network of heterogenous, unattended ground sensors that can be rapidly deployed to perform remote surveillance for the Canadian Army. A concept of operations was developed for SASNet in order to have clear understanding of how the system might be used by the Army. This understanding should lead to the design of a successful surveillance system that meets the needs and constraints of the soldiers whose lives might depend on it.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

unattended ground sensor
remote ground sensor
wireless sensor network
surveillance
ISR
C4ISR
operational research
CONOPS
concept of operations


DRDC CORA

www.drdc-rddc.gc.ca