

AN INVESTIGATION OF THE MILITARY APPLICATIONS OF COMMERCIAL PERSONAL SATELLITE-COMMUNICATIONS SYSTEMS

T. Mahoney, P. Kerr, DSTO, Salisbury Australia;
B. Felstead, CRC Ottawa, Canada, L. Wagner, DREO Ottawa, Canada;
P. Wells, M. Cunningham, DERA, Defford, UK; K. Ryden, DERA, Farnborough, UK;
G. Baumgartner, SPAWAR Systems Center, San Diego CA, USA; H. Demers, WL Dayton OH, USA;
L. Jeromin, MIT Lincoln Laboratory, Lexington MA, USA; B. Spink, RL Rome NY, USA.

ABSTRACT

Abstract: This paper provides a summary of the results of a four-nation workshop that investigated the military use of commercial satellite-based personal communications systems (SPCS). Military considerations and nine potential application areas are described. Of the fifteen vulnerabilities of SPCS examined in the workshop, six of the more important vulnerabilities (jamming, detection, position location, interception, communications security, and system and network control), and four limitations (capacity, coverage, user terminals, and regulatory) are discussed. A method for comparing and rating SPCS systems for military purposes is presented followed by an example comparing six planned or operational SPCS systems.

I. INTRODUCTION

Through The Technical Cooperation Program (TTCP), members of four nations joined in a working group to investigate the suitability of commercial satellite-based personal-communications systems (SPCS) for potential military applications. In this paper, a précis of the two-volume final report is presented. While it is not possible to publish in this paper the large amount of system information gathered for the final report, one can refer to the vast amount of literature on this subject including survey articles [1], [2], many Milcom papers, books [3], [4], and web sites.

Military considerations were examined under three categories: capabilities sought, issues affecting the use of SPCS by the military, and new capabilities. Nine potential military application areas are presented. Fifteen vulnerability types were studied and six of the more important (jamming, detection, position location, interception, communications security, and system and network control) are discussed along with some mitigation methods. Four limitations (capacity, coverage, user terminals, and regulatory) are discussed. Comparative scores were given to six current systems for each of the vulnerabilities and limitations. The systems were then compared for military applications by applying weights to each of the vulnerabilities and limitations for two example application areas, namely operations other than war (e.g. logistics, humanitarian), and stressed out-of-area operations (e.g. small conflict, peace keeping). With this approach, it is possible to take parameters of systems of interest, and calculate the performance for one's own particular application.

II. MILITARY CONSIDERATIONS IN THE USE OF COMMERCIAL SPCS

A. *Capabilities Sought*

The following capabilities would enhance the utility of any SPCS system for military use:

- a) Secure voice and low speed data capabilities using cryptographic equipment.
- b) Some control of the management sub-system to prevent compromise.
- c) Ease of use to allow SPCS to be used by a variety of other Forces and to reduce training.
- d) Special circuit features such as conference calls, preemption and priority.
- e) Mobility.
- f) Interoperability by use of common standards.

B. *Issues Affecting the Use of SPCS*

The following are some of the drivers for the use of SPCS.

- a) *Vulnerabilities and Limitations.* A clear understanding of the vulnerabilities and limitations is essential to assess the risk versus the operational benefits. Vulnerabilities and limitations are discussed in Secs. IV and V, respectively.
- b) *Cost.* Cost is always a key driver. Experience with Inmarsat in UN Peace Support Operations indicates that some terminals will be active for extended periods. Frequently the cost of calls and terminal maintenance far outweighs the cost of initial terminal procurement.
- c) *Control of Infrastructure.* Control of the infrastructure is a key issue to ensure that forces are not compromised, system availability is maintained, and there is assured access.
- d) *Common Operating Environment.* The SPCS and any associated terrestrial networks must provide a common operating environment, which also infers a level of standardization and interoperability.
- e) *Discipline.* Use of mobile phones by troops has proven to be a problem by eroding battlefield discipline, circumventing sound military tactics and compromising forces. The availability of SPCS from commercial suppliers and their worldwide capability makes SPCS even more of a problem. Control procedures and provisions must be set in place.
- f) *Third Party Users.* Other entities working within the theatre can use SPCS to accomplish their agenda. Some, such as the media, will be able to use SPCS to circumvent military controls.
- g) *Malevolent User Groups.* Groups such as smugglers, drug traffickers and terrorists can also take advantage of SPCS services. This usage may force government agencies to use SPCS just to ensure they are not at a disadvantage. There is a need for some government access to the commercial infrastructure to conduct analysis and disable communications in special cases.
- h) *Regulatory Issues.* The treaties governing the consortia supplying SPCS services may preclude their use in some circumstances including warlike activities. Conversely, use of systems endorsed under international agreements may offer the military user some protection against intentional disruption.

Military use of SPCS may place commercial assets at risk as they may be viewed as legitimate military targets.

i) *Assured Service*. The conventional civilian communications infrastructure may be disrupted as a result of natural disaster, armed conflict, and the like. SPCS could be a useful backup resource. An assured priority of service for the military above other potential resource competitors, such as the press, could be vital.

C. *New Capabilities*

SPCS may offer new capabilities such as: paging, global voice, facsimile and low-rate data, extension of facilities such as linking several local radio coverage areas into a virtual single radio net, extended coverage such as to polar and ocean regions, a common operating environment for connectivity between all organizations in an operation, and improved mobile platform capability.

III. MILITARY APPLICATIONS OF SPCS

Some potential military applications for SPCS are listed below in nine categories. Further applications will arise as SPCS become more commonly available.

A. *Observers*

Observers frequently operate in small groups and in isolated locations often widely dispersed throughout the theatre of operations. This low density makes it difficult to justify the deployment of major assets to support teams of observers.

B. *Humanitarian Deployments*

Disaster relief operations are normally conducted at short notice in areas where the indigenous communications infrastructure may be disrupted. Any surviving terrestrial communications infrastructure may be fully utilized by local aid teams. It is vital that any military humanitarian operations do not stress any surviving resources including communications. SPCS would offer a common operating system between other agencies.

C. *Interdepartmental Interoperability*

The ability of SPCS to offer a commonality between government departments overcomes many of the problems that often affect interdepartmental operations. SPCS also provides an off-the-shelf capability for those departments that do not require or cannot afford their own dedicated systems. Some examples are: law enforcement, VIPs, coast guards, non-governmental organizations such as Oxfam and the Red Cross, and fisheries protection.

D. *Logistics*

Certain parts of logistics might usefully be off loaded to SPCS such as: medical teleconference, transport control, vehicle and convoy tracking, and welfare telephone for military personnel in remote areas.

E. *Special Operations*

SPCS could be useful for a variety of special-operations purposes such as: advance forces, intelligence operations, counter terrorist, and combat search and rescue.

F. *Communications Engineering and Management*

Communications engineering and management applications might include: fallback engineering order wire, user request for broadcast data systems, remote switching and

control of sensors, links to indigenous systems, low rate alternate bearers for low priority traffic, combat radio expansion of coverage, and communications on the move.

G. *Small Platform Use*

During a crisis, commercial marine vessels that provide force transport, but are too small to warrant military satcom, can be fitted with SPCS. SPCS could be used on board commercial aircraft platforms allowing them to support military operations for example during a strategic air movement.

H. *Peace Support Operations and Operations Other Than War*

Lower intensity operations other than war allow a degree of controlled use of SPCS. Three of many potential applications are non-combatant evacuation operations, improved situation awareness, and safety communications for training of indigenous forces or training in challenging environments particularly for mobile platform operations.

I. *Out of Area Operations*

Some of the SPCS offer wider geographic coverage than many military communications systems, especially over the polar regions. SPCS may provide the only reliable form of long-range communications to and from these regions.

IV. VULNERABILITIES OF SPCS

In this study, 15 forms of vulnerability were identified. The ones considered of most concern were consolidated into 6 categories and discussed below. In some cases, methods of mitigating the vulnerabilities are given.

A. *Jamming*

Five links could be jammed: handset downlink (forward), gateway downlink (return), handset uplink (return), gateway uplink (forward), and inter-satellite links. Simple expressions for determining the jamming levels that can be tolerated are available [5], [6]. Handset downlink and uplink examples are presented below.

Fig. 1 illustrates the geometry for the handset uplink jamming, satellite uplink jamming, and detection of handset uplink. The subscripts h = 'handset', s = 'satellite', and i = 'intercept detector'. The subscripts are arranged so that G_{sj} is the gain of the satellite antenna in the direction of the jammer, and R_{jh} is the distance between the jammer and the handset, and so on. For handset jamming, the jammer has an EIRP in the direction of the handset of $EIRP_j$. Let SNR_{spec} be the specified signal to noise ratio at the handset, and $SNJR_{un}$ be the ratio of signal to noise plus jammer at the threshold of unacceptable error rate. The minimum jammer EIRP for unacceptable performance is

$$EIRP_j = \frac{SNR_{spec}}{SNJR_{un}} \frac{kTW_p (4\pi f / c)^2 R_{jh}^2}{G_{hj}} \quad (1)$$

where k is Boltzmann's constant, T is the noise temperature of the handset, f is the RF frequency, and c is the velocity of light. Against an unsophisticated jammer that jams the entire band, W_p occupied by all users, there is an AJ processing gain obtained from using *any* of the multiple access tech-

niques of $PG_{ma} \approx W_p / R_b$ [5] where R_b is the bit rate. This processing gain is akin to the one obtained from spread spectrum.

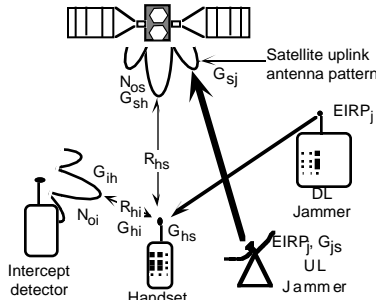


Fig. 1. The handset jamming geometry defining various parameters.

For uplink jamming of the satellite, the $EIRP_j$ that is necessary to make the bit-error rate (BER) in the transponder or the onboard processor of bandwidth, W_p , larger than the specification is

$$EIRP_j \geq EIRP_h \frac{PG_{ma} PG_{ant}}{SNR_{spec}} \left(\frac{SNR_{spec}}{SNR_{un}} - \frac{1}{M} \right) \quad (2)$$

where M is the link margin. The onboard antenna processing gain is $PG_{ant} = G_{sh} / G_{sj}$.

B. Detection

As the location of satellites, gateways, and control centers will likely be well known to an adversary, only detection of user uplinks was considered. A signal can be detected with simple specialized detectors such as radiometers and chip-rate detectors. The maximum handset-to-interceptor range R_{hi} , at which the signal can be detected is the "detection range". For handset-to-satellite range $R_{hs} \gg R_{hi}$, the interceptor has an advantage of many tens of dB over the legitimate onboard satellite receiver. Analysis of actual handsets showed that detection range is very large. This poor low probability of detection (LPD) performance may be improved by power control, limited message length and number, terrain shielding, and moving locality between communications. Since SPCS is intended for a mass market, non-military users could mask the military users and provide some detection anonymity.

C. Position Location

For SPCS, there are at least three means of undesired position location of handsets.

System Operator. The system operator, and any third party that is provided user position information, will know the location of any subscriber that is currently registered with the system to an accuracy to allow country borders to be determined. Countermeasures to prevent such exploitation would include not registering with the system (leaving the handset off), and through use of a military gateway and an enhanced service.

Line of Sight Direction Finding. If a handset transmission can be detected from two or more geographically separated ground- or air-based receivers, then direction finding is possible. Users should be aware that their terminals might

transmit at times other than when a call is being made in order to maintain registration with their networks. Location accuracy of hundreds of meters would be typical for a two-site ground-based DF system. Countermeasures would include: keeping the handset switched off when not in use, operating the handset from locations with many obstacles (natural and buildings), and keeping transmissions as short as possible.

Geolocation by Satellites. Two means of geolocation of handsets using satellites are single-satellite geolocation using Doppler tracking, and two-satellite methods using time or frequency difference methods. It was considered that neither method was of much concern in SPCS systems.

D. Interception

Under the category of interception, signal demodulation, traffic analysis and traceability were considered. Signal demodulation can be achieved by an interceptor with full knowledge of the transmission frequencies, waveform parameters and communications protocols. A significant amount of information about a particular user of a communication system can be obtained by monitoring traffic. This traffic analysis can be an indication that the terminal user is involved in a significant, or at least non-routine, operation.

E. Communications Security

The majority of military communications require some form of encryption. The planned systems have not been designed with full government encryption in mind but may have a form of privacy protection for business use. This privacy protection will usually allow access by the system provider and, also, by foreign governments with the appropriate capability. There is also a legal intercept requirement that the system operators must provide and agree with a host nation where the handsets will be used.

For military use, some form of government approved encryption is needed. It is preferred that the encryptor be built into the handset using some form of removable crypto key (e.g. smart card). However, this approach may not be a commercially acceptable option. The US is planning to use embedded encryption within a personal handset under their CONDOR program. This will allow them STU III interoperability via a gateway. An external encryptor could allow use of existing handsets if a suitable data interface was provided which would require two units to be carried along with their own battery and an interconnect cable.

F. System and Network Control

A number of methods to disrupt the system and network control are possible, and some are now discussed.

Network Saturation. For commercial reasons, system operators have a strong desire to maximize the utilization of the capacity of their system. Thus, there is a vulnerability to a deliberate saturation of the system by introducing additional callers into a specific region and gradually 'eating up' the capacity as soon as existing callers hang up.

User Control Channel Vulnerability. If the protocols of the system control channels are understood, an adversary could broadcast a deception version of the control channels to disrupt users within a region.

Denial of Specific Resources. Specific users could be targeted by a continuous stream of incoming calls which thus pre-

vents the placing of outgoing calls or reception of legitimate calls. The best mitigation to this type of attack is to maintain security of the telephone numbers allocated to individuals.

Sabotage and Hacking. Under this category is the attack of the control system databases and operations facilities to disrupt or monitor traffic. Such an attack could occur due to disgruntled employees, or 'planted' individuals. In addition, if any connections are made to external networks then the risk of outsiders hacking into the control system computers must be considered.

V. LIMITATIONS OF SPCS

In this study, four forms of limitations were examined.

A. Capacity Limitations

Capacity for commercial SPCS systems is usually quoted as the maximum number of equivalent voice or data circuits available worldwide from the entire constellation. In practice, this capacity cannot be totally utilized due to dynamic variations in the relative position of satellites in the constellation, and user traffic distribution. Dynamic changes in the constellation that affect capacity includes overlap of satellite footprints during the orbit, and variation or distortion in individual beams as satellites move over a fixed area. If traffic is concentrated in a limited geographic area, localized capacity of the SPCS system may not be able to accommodate the traffic load.

B. Coverage Limitations

Geographical coverage, user-to-satellite elevation angles and the degree of penetration of signals into buildings or other structures can limit the uses to which the networks may be put. The geographical coverage available varies considerably from system to system. The geostationary systems do not offer any polar region coverage and can be limited to specific regions of the world (e.g. ACeS will serve south-east Asia). Conversely, most of the LEO and MEO systems provide true global coverage including polar and oceanic regions. The notable exception is Globalstar that does not provide coverage above latitudes of 70° north or south, or mid-ocean coverage. One major advantage of the LEOs and MEOs is the high elevation angles available even in polar, mountainous or city regions, or when users wish to take advantage of terrain shielding. Since more than one satellite is often within view, the probability of blockage is further reduced.

C. User Terminal Limitations

Handheld. The handheld units have limited use within buildings and built-up urban areas. Body shielding effects are also factors.

Ground Vehicles. Use of an external antenna will reduce link margin problems. However, there can be a detrimental level of multipath and signal blockage while the vehicle is in motion.

Aircraft. A special approved installation is required for installation on aircraft including an external antenna. The EMC effects of using a satellite phone on board an aircraft would need to be determined individually for each installation.

Ships. An external antenna would be preferred.

Helicopters. Rotor blades can cause undesired modulations.

Battery Power. For military operations, the provision of additional batteries or access to daily re-charge facilities will be important.

Radiation Hazard. This is an emotive issue at present and is likely to become more of a concern as the acceptable level of radiation hazard is reduced in power level. The current limit of 10mW/cm² is already deemed too high in many countries. The handset providers are aiming to use the minimum amount of power for a satisfactory link and are now taking precautions to minimize exposure to RF radiation.

Multimode Capability. One of the longer term planned features of the personal satcom systems is the migration towards a multi-service handset covering terrestrial cellular and SPCS use with automatic selection of the cheapest method of making the call. Many of the vendors have adopted the route of dual- or even tri-mode units. By adopting cellular system protocol standards such as GSM, the design of the handset and network interoperability is simplified.

D. Regulatory Limitations

The subject of radio regulations for SPCS consumes enormous resources of potential system operators. Competition is fierce for allocations. Since SPCS is intended to be world wide, one of the biggest problems is that each of the proposed systems needs to seek approval from each country in which it intends to operate.

VI. SAMPLE VULNERABILITY & LIMITATIONS COMPARISONS

In the Workshop, 6 planned or operational SPCS systems were examined against 15 vulnerabilities and 4 limitations, some of which were discussed above. The detailed results are much too voluminous to present here. Instead, one example table, out of the large number of tables actually prepared, is given in Table I. The parameters in Table I were taken entirely from the open literature, mostly from [7]. Therefore, these parameters may not be accurate or up to date. Instead, they are merely used to illustrate a comparison approach. Beam-diameter coverage impact is rated relatively as small, medium and large. Since these systems vary widely in characteristics and types of service, it is difficult comparing them.

At the bottom of Table I are given relative scores chosen by group consensus opinion based upon the preceding data. Scores are relative to each other and not to a robust military system. Scores reflect military usefulness with a 1 being the worst and a 10 being the best. Other evaluators might come up with different scores. In order to use the scores for a comparison, weights were then chosen for each of the 15+4 items. The weights depend upon the application of the specific user group. We used two example applications and came up with the weights shown in Table II. The two applications considered were operations other than war such as logistics or humanitarian, and stressed out-of-area operations such as small conflicts or peace keeping. Again, other evaluators might arrive at quite different weights. Our weights are intended only to illustrate how one would proceed in one's own evaluation. The 'importance' values reflect both the probability of a threat occurring and its potential impact on the mission, should it occur.

The weights of Table II were then multiplied by the 15+4 sets of scores, summed, and, finally, normalized to a percentage of the maximum possible score for that mission. The resulting percentages give an overall comparison of the 6 systems in the two application areas. The results are shown in Table III.

The scoring and weighting values were chosen by consensus opinion within the working group to help reduce the subjectivity. Furthermore, a sensitivity analysis was done to examine the effect of variations of the individual scores on the final weighted scores. Random amounts between ±1 were added to the individual scores and the new total weighted score was computed for 100 trials, and statistics recorded and analyzed. The same procedure was repeated for a random amount of ±3. It was concluded that the analysis would not be sensitive to an error of ±1 on the individual scores, but the analysis would be questionable if there were a ±3 error. Hopefully, the consensus approach of the working group prevented such a large error. In retrospect, there should also have been a sensitivity analysis done on the weights.

VII. CONCLUSION AND RECOMMENDATIONS

A number of useful military applications for SPCS is given in Sec. III. Once such systems are fielded, even more applications will become apparent. Of the 15 vulnerabilities examined, 6 of the more important are discussed in Sec. IV and 4 limitation areas are discussed in Sec. V. Some examples of how SPCS used for military applications might be compared are given in Sec. VI along with a summary of comparison results for two application areas.

Based upon the above work, it was recommended that:

- a) Forces will use SPCS and there is a need to determine the current capability gaps that SPCS may fulfill to perform a vital function or complement existing communications capabilities.
- b) Develop a Concept of Operations for the use of SPCS across the full spectrum of operational intensities.
- c) Organizations procure sample equipment to further develop their Concept of Operations and cultivate the creation of some expertise within their Forces. TTCP is currently evaluating Iridium for military use and how interoperability may be achieved for the military.

Finally, there must be a willingness to accept that the operational use of SPCS will continually evolve as service providers offer greater functionality, and the military learn lessons from trials and earlier operations.

REFERENCES

[1] B. Miller, "Satellites free the mobile phone," IEEE Spectrum, vol. 35, pp. 26-35, March 98.
 [2] F. Ananasso and F.D. Priscoli, "The role of satellites in personal communication services," IEEE J. Selected Areas in Commun., vol. 13, pp. 180-196, Feb. 95.
 [3] B. Pattan, *Satellite-based Global Cellular Communications*, McGraw-Hill, New York, 1998.
 [4] A. Jamalipour, *Low earth orbital satellites for personal communications networks*, Artech House, Boston, 1998.
 [5] E.B. Felstead and R.J. Keightley, "Robustness capabilities of transponded commercial satellite communications," in Conf. Record, IEEE Milcom 95, pp. 783-787, San Diego CA, Nov. 6-8, 1995.

[6] J.W. Lee and V.A. Marshall, "Maximum capacity prediction and anti-jam performance analysis for commercial satellite communication systems," in Conf. Record of the IEEE Milcom '94, pp. 506-510, Fort Monmouth, NJ, October 1994.
 [7] K.G. Johannsen, "Mobile P-service satellite system comparison," Internat. J. Satellite Comm., vol. 13, pp. 453-471, 1995.

TABLE I. Vulnerability to user uplink jamming: EIRP and jammer type needed to disrupt channel, beam coverage impact, mitigation and score for 6 example systems.

System	LEOs			MEOs		GEOs	
	A	B	C	D	E	F	
Service	Messaging & paging	Handset voice services				Briefcase voice	
Main-beam jammer: EIRP/type	X dBW Low power	X + 9 dBW Medium power or sophisticated low power jammer required	X + 8 dBW	X + 12 dBW	X + 13 dBW	X + 30 dBW	
Sidelobe jammer EIRP & type	Y dBW Low eirp	Y + 32 dBW High eirp or sophist med. eirp	Y + 5 dBW	Y + 16 dBW	Y + 31 dBW	Y + 40 dBW High eirp or sophist med. eirp	
Beam dia impact	large	small	large*	medium	small	large	
Mitigation	Can only attempt to locate jammer and neutralize but could be as far away as the satellite foot print diameter.						
Score	3	6	4	5	5	6	

*The satellite diversity could make the effects of jamming worse.

TABLE II. Example importance weighting for two applications. Weighting: 0 = very low, 2 = high.

Vulnerabilities:	Other than war	Stressed out-of-area
	Importance Weightings	
Jamming-user UL	0	2
Jamming-user DL	0	2
Jamming-gateway UL	0	1
Jamming-gateway DL	0	1
Interference	1	1
Detection	0	2
Signal de-modulation	0	2
Comms security	1	2
Traffic analysis	1	2
Position location-LoS	1	2
Position location-sat	1	2
System disruption	1	1
Spoofing	1	1
Direct attack - ground	0	1
Direct attack - space	0	0
Limitations:		
Capacity	1	2
Coverage	2	2
User terminals	1	2
Regulatory	1	0

TABLE III. Relative Performance of SPCS for Two Example Military Applications

System	LEOs			MEOs		GEOs	
	A	B	C	D	E	F	
Service	Messaging & paging	Handset voice				Briefcase voice	
Operations other than war	53%	67%	62%	67%	56%*	54%	
Stressed out of area operations	45%	63%	57%	60%	51%*	47%	

*The geographical coverage of this system is comparatively very limited: these scores assume that the mission occurs within the coverage region.