ARMS CONTROL VERIFICATION OCCASIONAL PAPERS No. 7

# Satellites Harming Other Satellites

by Peter C. Hughes

Dynacon Enterprises Ltd.

prepared for The Arms Control and Disarmament Division
External Affairs and International Trade Canada, Ottawa, Ontario, Canada

Canada

External Affairs and International Trade Canada

The cover graphic is based on an ancient Egyptian hieroglyph representing the all-seeing eye of the powerful sky god, Horus. Segments of this "eye in the sky" became hieroglyphic signs for measuring fractions in ancient Egypt. Intriguingly, however, the sum of the physical segments adds up to only 63/64 and, thus, never reaches the equivalent of the whole, or perfection. Similarly, verification is unlikely to be perfect.

Today, a core element in the multilateral arms control verification process is likely to be the unintrusive "eye in the sky," represented by a space-based or an airborne remote sensing system. These overhead imaging techniques will have to be supplemented by a package of other methods of verification including ground-based sensors and some form of on-site inspection and observations. All these physical techniques add together, just as the fractions of the eye of Horus do, to form the "eye" of verification. Physical verification, however, will not necessarily be conclusive, and there is likely to remain a degree of uncertainty in the process. Adequate and effective verification, therefore, will still require the additional, non-physical, element of judgement, represented by the unseen fraction of the eye of Horus.

Arms Control Verification Occasional Papers

Arms Control Verification Occasional Papers are issued periodically by the Arms Control and Disarmament Division of External Affairs and International Trade Canada (EAITC). Their purpose is to disseminate the results of selected independent research undertaken for EAITC as part of ongoing work by the Department in this area.

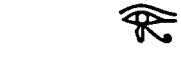
**THE VIEWS EXPRESSED IN THESE REPORTS ARE THOSE OF THE AUTHORS AND DO NOT NECESSARILY REPRESENT THOSE OF EXTERNAL AFFAIRS AND INTERNATIONAL TRADE CANADA OR OF THE GOVERNMENT OF CANADA.**

On peut se procurer une version française de cette étude en écrivant à l'adresse suivante :

Direction du contrôle des armements et du désarmement
Affaires extérieures et Commerce extérieur Canada
Tour A
125, promenade Sussex
Ottawa (Ontario)
Canada
K1A 0G2

External Affairs and International Trade Canada
Cat. No. E54-8/7-1991E
ISBN 0-662-18863-2
ISSN 0840-772X

July 1991



# Satellites Harming Other Satellites

by Peter C. Hughes

Dynacon Enterprises Ltd.

prepared for

The Arms Control and Disarmament Division

External Affairs and International Trade Canada

Ottawa, Ontario, Canada

**Canadian Cataloguing in Publication Data**

Hughes, Peter C. (Peter Carlisle), 1940-

Satellites harming other satellites

(Arms control verification occasional papers ; ISSN 0840-772X ; no. 7)
Includes an abstract in French.
ISBN 0-662-18863-2
DSS cat. no. E54-8/7-1991E

1. Space weapons. 2. Anti-satellite weapons. 3. Artificial satellites — Tracking. 4. Arms control — Verification. I. Canada. Arms Control and Disarmament Division. II. Title. III. Series.

UA12.5H84 1991 35'8.8 C91-098648-7

# *Table of Contents*

# *List of Tables*

# *List of Figures*

## *Abstract*

A strategy is developed for assessing the harm that one satellite can do to another. A total of 29 modes are identified through which this harm can transpire, and the parameters and characteristics of each are explained. An overall, quantitative index of harm can be calculated (with respect to a nominal target satellite) for any satellite. A detailed verification strategy for each of these harm modes is also worked out. Peaceful space operations for the next 20-year period are surveyed and possible ambiguities noted. Confidence-building measures are also evaluated. The notion of "keep-out zones" is explored and traditional ideas for such zones are shown to be simplistic and unworkable. A new, "free space" keep-out zone is proposed. The technical means for verification of a keep-out zone treaty include the well-established practices of satellite tracking and orbit prediction.



## *Résumé*

L'auteur élabore une stratégie de vérification pour évaluer les dommages qu'un satellite peut causer à un autre. Il définit vingt-neuf façons dont ces dommages peuvent être infligés et il explique les paramètres et les caractéristiques propres à chacune. Il est ainsi en mesure d'établir un index global et quantitatif des dommages (en fonction d'un satellite-cible type) pour n'importe quel satellite. L'auteur élabore également une stratégie détaillée de vérification pour chacun des vingt-neuf moyens susceptibles d'être employés pour infliger des dommages à un autre satellite. Il examine les opérations spatiales à buts pacifiques qui auront lieu au cours des vingt prochaines années et relève ainsi plusieurs ambiguïtés relatives à leur usage réel. L'auteur analyse aussi quelques mesures propres à accroître la confiance dans ce domaine. Il s'interroge sur la notion de "zones interdites" et montre que les idées traditionnelles concernant ces dernières sont simplistes et impraticables. Il propose un nouveau concept : une zone protégée dans l'espace libre. Parmi les moyens techniques de vérification d'un traité sur les zones interdites, l'auteur mentionne les méthodes bien établies servant à suivre les satellites et à prédire leur orbite.

# *Preface*

This study is a distillation of four technical reports prepared by Dynacon Enterprises Ltd. for the Verification Research Program of External Affairs and International Trade Canada over the period 1 April 1987–31 March 1991.

The author is the founder and chairman of Dynacon Enterprises Ltd.

# *Acknowledgements*

The genesis of this line of inquiry, in which the vexed issue of international agreements on control and verification of space "weapons" is approached rationally by a quantitative analysis of the potential harm one satellite can wreak on another, first occurred in the mind of Peter Stibrany, while on secondment in 1987 from Spar Aerospace Ltd. to External Affairs. The idea was further enhanced by Gabriele D'Eleuterio (who wrote the winning technical proposal) and by Kieran Carroll, both of Dynacon Enterprises Ltd.

Subsequent technical contributions at Dynacon have also been made by Wayne Sincarsin, Donald McTavish, and the present author. The new keep-out zone concept featured in this paper is due to Don McTavish. The primary managerial responsibility at Dynacon has fallen to its president, Glen Sincarsin.

The energizing force behind this work, and the keeper of the purse, was Lt Col F.R. (Ron) Cleminson, Head of the Verification Research Unit within the Arms Control and Disarmament Division of External Affairs and International Trade Canada. He was ably assisted in the technical monitoring of this work by Jeffrey Tracey. Alan Crawford's many editorial suggestions were also very helpful.

# *List of Abbreviations*

| | |
|---|---|
| **ABM** | Anti-Ballistic Missile |
| **ASat** | Anti-satellite Satellite |
| **DSat** | Defensive Satellite (including anti-ASats) |
| **GEO** | Geostationary (or Geosynchronous) Earth Orbit |
| HARMDEX | Computer software to calculate the Harm Index for a satellite (see Chapter 9) |
| **ICBM** | Intercontinental Ballistic Missile |
| **IR** | Infra-Red (range in the electromagnetic spectrum) |
| **KOZ** | Keep-Out Zone (particularly the type introduced in Chapter 11) |
| **LEO** | Low (altitude) Earth Orbit |
| **NORAD** | North American Aerospace Defense Command |
| **SALT** | Strategic Arms Limitation Treaty |
| **SDI** | Strategic Defense Initiative (USA program popularly known as "Star Wars") |
| **UN** | United Nations |
| **USA** | United States of America |
| **UV** | Ultraviolet (range in the electromagnetic spectrum) |

# Chapter 1: Introduction

The problem of arms control and verification for space systems has many unique challenges. Developed nations, notably the superpowers, have come to rely on spaced-based systems for communications, surveillance, navigation, and many other uses. Satellite assets that provide or support strategic military functions are vulnerable to attack; as a consequence, anti-satellite (ASat) technology has been developed and demonstrated, and continues to progress. The real possibility of ASat spacecraft threatening valuable space assets further encourages the development of ASat technology for the purpose of active defense against attack; hence defensive anti-ASats or DSats.

To date, certain international agreements have attempted to limit the proliferation of weapons in space. The *Outer Space Treaty* of 1967 forbids the placing of weapons of mass destruction in space; this outlaws such space weapons as orbiting nuclear bombs. The *Anti-Ballistic Missile Treaty* (ABM Treaty) of 1972 restricts the development by the superpowers of both space-based and ground-based ABM systems — and bans their deployment. As many of the modern ASat technologies are nearly identical to ABM technologies, this treaty has effectively limited ASat development. At this moment, fortunately, space remains relatively weapon-free, due partly to these treaty impediments, and partly to the historical nondeployment of space-based ASat weapons and to their enormous development costs. The present challenge is not to control an arms race in space — it is to avoid one.

This paper is divided into three principle parts. Part I reviews the broad spectrum of space operations in which current satellites are engaged and extrapolates to the much broader spectrum of operations that could conceivably be carried out by satellites of the early twenty-first century. Some of these involve "critical capabilities" that could potentially enable harm to be done to other satellites; others do not. Some of these (conceivable) future operations will, by definition, have harmful intent; others will not. When this multitude of possibilities is examined, it is found that, while certain space operations are clearly "weapon" and others are clearly "nonweapon," there is a substantial number that tend to be ambiguous: they may or may not be weapon operations. Twelve specific examples are given, and suggestions for disambiguating these operations are offered.

Part II contains a rigorous quantitative analysis of the harm that one particular satellite can do to another (at least potentially) once its key parameters and characteristics have been specified. A large number of methods (or "modes") of harm are defined. The potential harm from each is quantified; then, by superposition, the total possible harmfulness for that particular satellite can be calculated.

It is explained how each of the constituent parameters and characteristics on which the calculation is based can be verified, thus lending practicality to the analysis and credibility to its results.

Finally, Part III describes a set of initiatives that should help to deal with the problems raised in Part I, based on the technical analysis of Part II. These ideas include a new keep-out zone concept, autonomous monitoring, verification beacons, and — if there must be weapons in space — their international regulation.

# PART I: SATELLITE OPERATIONS

## Chapter 2: Satellite Operations, Current and Planned

The following chapters focus on the work done by Dynacon concerning long-term space operations that could be perceived as space weapon research. In this chapter, projections of nonweapon space operations over the next 20 years will be compared with similar projections for weapon space operations. Then, in the following chapter, special attention will be given to cases where nonweapon operations could be confused, accidentally or deliberately, with weapon research or deployment.

Experience in previous rounds of arms-control agreements teaches that success hinges on careful definition of the objects to be regulated. Moreover, the discussion below is intended to be sufficiently broad to encompass not only those space systems that have already been developed, but also those that might be developed. On the other hand, the definition should be restrictive enough that desirable nonweapon space activities can avoid becoming entangled in the resulting agreements. The line of demarcation between ambiguous operations must be drawn with great care.

### 2.1 What Is a Space Weapon?

Before proceeding further, a definition of "space weapon" is in order. Though many definitions are possible, we shall, for the purposes of this paper, define a space weapon to be a satellite that has the following two key properties:

(a) it is capable of inflicting major harm on other satellites; and

(b) its owners intend it to inflict major harm on other satellites, if "sufficiently provoked."

This definition raises many additional questions, many of which are addressed in this paper. Most noteworthy is that Property (a) is essentially a technical one — complex, but susceptible[1] to engineering analysis — while Property (b) implies knowledge of the intentions of nations and their leaders — thus requiring judgements that are almost impenetrably complicated.

It is especially important to note that just because a satellite *can* harm another satellite does not mean that it *will*. Moreover, while intent can never be fully verified, it does help to be knowledgeable concerning possible space operations, both current and planned (the subject of this chapter), so as to be able to identify (and hopefully remove) any ambiguities that may arise (the subject of the next two chapters).

## 2.2 Methodology

Nonweapon space operations will first be surveyed, followed by weapon space operations. Then (next chapter) these two surveys will be categorized and cross-referenced to identify operations in one list that could be confused with operations in the other. Because the discussion is centered on space weapons operations, ICBMs, for example, are outside scope, as are Earth-launched ASat weapons, and weapons threatening lunar targets.

Issues that frequently arise in the specification of space weapon operations include questions relating to research, development, testing, and deployment. The precise definition of these activities, especially in the business of arms treaty negotiation and interpretation, is a matter of poignant debate. For example, it has been claimed that the much publicized Strategic Defence Initiative Program of the 1980's is in direct violation of the 1972 *Anti-Ballistic Missile Treaty* which forbids, among other activities, the "development" of ABM systems, unless it is "basic research." No explicit distinction will be made here between these subclassifications of space weapon operations. In fact, given that projections are to be made for *possible* operations, with the implication that research could lead to future deployment, this distinction is not helpful.

## 2.3 Nonweapon Space Operations

Existing satellites carry out a wide range of activities. A list of current *non*-weapon space operations is shown in Table 1. Capabilities can be grouped into classes such as these, based on the main function of each type of spacecraft, because with satellites form tends to follow function. Thus, all spacecraft carrying out a specified function will tend to look much the same. Conversely, much can be inferred about a satellite's functions from its observable characteristics.

In addition to these current operations, several new space activities are planned for the future, including satellite repair, lunar exploration, space power generation and transmission, lunar mining, Mars exploration, and asteroid mining. These activities must be supported, in turn, by a number of new (nonweapon) space operations, such as those listed in Table 2. These operations are often most conveniently identified in terms of the types of space vehicle required to carry

- Geodesy
- Astronomy
- Navigation
- Surveillance
- Meteorology
- Space Stations
- Communications
- Lunar Exploration
- Earth Observation
- Search and Rescue
- Manned Orbital Shuttles
- Space Physics Research
- Interplanetary Exploration
- Microgravity Experimentation

**Table 1**

**Current Nonweapon Space Operations**

them out. Some of these satellites are currently available — for example, transport of astronauts into orbit in support of a manned lunar base will likely be carried out, at least initially, by currently-available manned orbital shuttles using currently operational or soon-to-be-operational space stations as stopping points — others are new. The operations vehicles listed in Table 2 are in addition to those currently available.

- Lunar Bases
- Lunar Orbiters
- Mass Catchers
- Microspacecraft
- Orbital Factories
- Interplanetary Bases
- Antimatter Propulsion
- Lunar Ferries/Landers
- Solar Power Satellites
- Telerobotic Spacecraft
- Interstellar Exploration
- Lunar Shuttling Stations
- Orbital Debris Sweepers
- Orbital Transfer Vehicles
- Interplanetary Ferries/Landers
- Interplanetary Shuttling Stations

**Table 2**

**Future Nonweapon Space Operations (Planned)**

## 2.4 Weapon Space Operations

Current known *weapon* space operations are listed in Table 3. Notably, there are few current "space weapons": of the five types listed, only two are "space-to-space weapons"; the remainder are ground-launched direct-ascent weapons, without orbiting capabilities. Also, two have been cancelled and another two are still under development. The current scarcity of weapons in space bodes well for potential treaties. The space weapon genie has not yet been let out of the bottle: once loosed, it will not easily be put back in.

**Table 3**

**Current Weapon Space Operations**

- USA F-15 ASat
- USA Nuclear ASat
- USSR Nuclear ASat
- USA ERIS/SBI ASat
- USSR Co-Orbital ASat

Although only a small number of ASat weapons had been developed in the past, the 1980's saw a marked increase in interest in such concepts, primarily under the aegis of the Strategic Defense Initiative (SDI) in the USA and its mirror-image programs in the USSR.[2] Indeed, several programs have been spawned to develop operational systems, notably Lawrence Livermore Lab's "Brilliant Pebbles." While these were promoted as being means to destroy ballistic missiles (which are not satellites by our definition, being suborbital), some observers have noted that these weapons could also be effective against space targets. These and other future possibilities are listed in Table 4.

**Table 4**

**Future Weapon Space Operations (Possibilities)**

- Rail Guns
- Space Mines
- X-Ray Lasers
- Lunar Catapult
- Sabotage Satellites
- RF Beam Weapons
- Laser Battle Stations
- Orbiting Laser Mirrors
- Orbiting Nuclear Bombs
- Antimatter Beams/Clouds
- Smart Rocks, Brilliant Pebbles
- Neutral Particle Beam Weapons
- Defensive Weapons on Satellites
- Tracking-Satellite Component of Space Weapons Systems

# Chapter 3: Ambiguous Space Operations

By comparing the lists of "weapon" and "nonweapon" space operations, ambiguities can be identified. This process is the central issue towards which the discussion in the last chapter has been building. The following questions are especially discriminating in identifying ambiguities:

(a) How could space weapons be camouflaged?

(b) How could spacecraft originally intended for use in nonweapon roles be misused as weapons?

(c) To what nonweapon uses could a space weapon be put?

(d) What characteristics would make a satellite unambiguously a weapon?

(e) What characteristics would make a satellite unambiguously a nonweapon?

The limited space available does not permit an exhaustive categorization of all possible entries and their cross-references; representative results will be presented here.

## 3.1 Criteria for Discrimination

Three criteria for distinguishing between weapon and nonweapon operations will be used in the following discussion:

- critical capabilities;[3]
- supporting technologies; and
- observables.

Using these criteria, similarities between entries in the two lists can be identified. If a nonweapon and a weapon share even one criterion, they will be judged ambiguous.

Among the *supporting technologies* judged to be critical are these: antimatter generation/storage, mass-drivers, nuclear reactors pulse-nuclear rockets, antimatter rockets, large-aperture mirrors, ion rockets, large-aperture high-power lasers, or particle accelerators. For the most part, *observables* include visible[4] characteristics: large power source, large fuel/oxidizer tanks, long, slender structure, large-aperture optics, radioactive emissions, or large constellations.

Based on the foregoing analysis, there are twelve space operations that could be ambiguous, either now or in the foreseeable future. In the remainder of this chapter, each of these will be considered briefly.

## 3.2 Brilliant Pebbles: Ballistic Missile Defence or ASAT System?

Brilliant Pebbles are billed as SDI defense weapons against suborbital targets (ballistic missiles) and thus are not "space weapons" in the narrow definition used here. In fact, however, they are designed to attack not only ballistic-missile booster rockets, but also the missile bus carried by those rockets, in case they don't reach the rocket booster prior to burnout. This means they also have the inherent ability to target most satellites; hence this putative "ballistic-missile-defense weapon" could easily be used as an ASat weapon.

Brilliant Pebbles are especially dangerous as space weapons because they have enough fuel to attack every Earth satellite — no matter how high the orbit. This would be the first ASat weapon capable of threatening GEO satellites.

Another important characteristic is the economy of these space weapons. The plan is to launch 4,164 of them in the initial procurement phase. Development funding is in the multi-hundred-million-dollar range, and orbital testing against target vehicles is planned for late 1991, indicating that this system could be in orbit within three years. With such a system in place, the USA would have the capability to disable all currently operational Earth satellites, and have enough capacity left over to interdict space launching by other nations.

The main aspects of "ambiguity" for Brilliant Pebbles are the observables of a large constellation (making this very effective as a first-strike-support ASat), the very large fuel/oxidizer tanks (allowing all Earth satellites to be threatened), and the critical capabilities of tracking, intercept, communications and control.

## 3.3 What Might Radioactive Emissions Mean?

Detected radioactive emissions (an observable) might cause confusion between a nonweapon space nuclear reactor and orbiting nuclear bombs. Similar confusion might arise between these and the operation of a nonweapon (physics research) particle accelerator in space, or the use of antimatter in nonweapon space propulsion, or the use of antimatter for space weapons; all of these operations can generate radioactive emissions.

## 3.4 Solar Power Satellite or Microwave Beam Weapon?

Solar power satellites would be effective as a directed-energy weapon against other satellites by depositing intense microwave beams, by overloading

target receivers, or through thermal overload. Both satellites share the observable of high-power sources, the critical capability of tracking, and the ability to focus a high-power beam of microwave energy.

## 3.5 Lunar Mass Driver: Materials Transporter or Bombardment Catapult?

A lunar mass driver for launching mined material into orbit for processing could be confused with a lunar bombardment catapult weapon. Both share the observables of a long, slender structure (the accelerator section), the supporting technology of mass drivers, and a large high-power energy delivery system. Indeed, a lunar mass driver could in principle be used as a bombardment weapon.

## 3.6 Large Aperture Optics: Astronomy Telescope or Space Laser?

Development of large astronomy telescopes in orbit could be confused with the optics of either a space-weapon laser or a weapon targeting system. They share the supporting technology of large aperture mirrors. Even if not confused with operational weapons, research into large reflectors for orbital astronomy could contribute to the development of the optical components of these systems. Historically, on the other hand, things have gone the other way; one hears that the most recent civilian space optics technology — the Hubble Space Telescope — drew on military optics for surveillance applications.

## 3.7 Earth Observation: Means of Verification or Weapons Tracking System?

Civilian Earth-observation satellites and nonweapon military surveillance satellites could be confused with the tracking component of a space weapon system. These spacecraft types share the observable characteristic of large aperture optics, the supporting technology of large mirrors, and the critical capability of performing extremely accurate tracking of targets.

## 3.8 Particle Beams: Ion Rocket or Neutral Particle Beam Weapon?

Satellites using ion rockets could be confused with research into neutral particle beams. Both share some technologies: a high-power energy source and an ion acceleration and neutralization device. An ion engine, however, is not likely to be confused with an operational neutral particle beam weapon, because the former should not have the pointing or focusing capabilities of the latter.

## 3.9 Particle Acceleration: Physics Research or Particle Beam Weapon?

Space physics particle accelerators could be confused with technology development of neutral particle beam weapons or of antimatter beam weapons. There is little difference between the acceleration equipment for these three devices. An orbital physics particle accelerator could be confused with operational weapons based on the observables of a long, slender structure, a large power source, and possibly of radioactive emissions.

## 3.10 Microsatellite Constellations: Nonweapons or Brilliant Pebbles?

Microsatellites deployed in large constellations could be mistaken for a constellation of weapons. In the case of Brilliant Pebbles, a constellation of Pebbles could be effective against an attempted massive ICBM first strike by an enemy.

Microsatellites could also be mistaken as technology development for smart rocks or Brilliant Pebbles. Launchers for microspacecraft, such as laser launcher systems or mass drivers, could be interpreted as being a launch system for Brilliant Pebbles, microsatellite-based space mines, or a sabotage satellite.

## 3.11 Orbital Laser: Communications Device or Beam Weapon?

A large orbiting communications laser (say, for communicating with the Thousand Astronomical Unit mission proposed by the Jet Propulsion Laboratory) could be mistaken either for an operational laser battle station or as development of technology in support of a laser space weapon. A laser-based orbital debris sweeper could be similarly mistaken for a weapon, although such a debris sweeper might not need the focusing ability of a weapon; however, it might still be mistaken for technology development towards space laser weapons.

## 3.12 Telerobotic Satellites: Satellite Repair or Sabotage?

Telerobotic orbital transfer vehicles could be mistaken for sabotage satellites. Indeed, the same spacecraft could be used either for purely peaceful purposes or for sabotage/weapons purposes.

## 3.13 Satellite Constellation: Debris Sweepers or Space Mines?

A constellation of debris-collecting satellites (e.g., orbital debris sweepers) could be mistaken for a constellation of space weapons, (e.g., space mines). The observable they have in common is the constellation.

# Chapter 4: Removal of Ambiguities

The discussion in this chapter centers on spacebased weapons — orbiting satellites that might be used in either space-to-space or space-to-ground direct weapons operations. Suborbital objects (such as ICBMs and air-launched ASats) are excluded. Moreover, the space operations discussed are those foreseeable in the immediate future (less than 10 years). More exotic operations in the farther future (e.g., lunar-based operations) are not considered.

## 4.1 Ambiguity Identification

The basis of ambiguity in spacecraft operations *is the question of intent and purpose, given known information.* In the absence of any space-use treaty or agreement and its verification mechanisms, the true intent of space operations by one nation is completely privy to that nation. In an environment of military competition — the race to control the "high ground" — a guess at the intent will tend conservatively toward a worst case scenario. If a space-use treaty is in effect and the purported intent disclosed but unverified, then the question of honesty arises, potentially creating suspicion.

Conventional monitoring of space operations is often not adequate to fully resolve key details, and hence the purpose, of the satellite involved. A set of detectable ambiguous operations is shown in Table 5. For each, there are both peaceful and weapon interpretations. For example, the first item in the list, "pursuit of, and/or rendezvous with, satellites," could be associated with peaceful operations like intersatellite resupply or personnel transfer, manned satellite maintenance, or telerobotic satellite maintenance. On the other hand, it could equally be associated with weapon testing or operations like target acquisition within weapon range.

**Table 5**

**Detectable, Ambiguous Space Operations**

- Pursuit of, and/or rendezvous with, satellites
- Deployment of large space structures
- Satellite breakup or fragmentation
- Radioactive debris or emissions
- Excessive orbital maneuvering of unmanned satellite
- High-power RF transmissions
- Flyby interception of satellite
- Blasts (especially nuclear)
- Constellation deployment
- Particle beam emissions
- Satellite without a cause
- Laser emissions

In some cases the ambiguities regarding a space operation can be cleared up with a minimum of basic information, i.e., through unilateral monitoring — at least to the extent where it can be established that some operation is inconsistent with a hostile objective. In the absence of more direct knowledge of the hardware used in such space-based operations, it is difficult or impossible to rule out direct space weapon research operations and/or deployment.

## 4.2 Ambiguity Removal

It is here that international treaties and agreements can play a key role. A United Nations agreement, the 1975 *Convention on the Registration of Objects Launched into Outer Space*, requires participating states to maintain national registries of space objects launched into orbit and beyond. This information is submitted to the Secretary General for the purpose of international registration. States are required to provide information such as the date and place of launch, the launching party, a designation of the space object, basic orbital parameters, and the general function of the object.

A major function of this *Registration Convention* is to support the 1972 *Liability Convention* which, with regard to outer space, assigns responsibility for damage caused by a space object to the nation who has ownership of that object. Frequently noted deficiencies in the *Registration Convention* are the lack of requirement for a more specific description of spacecraft function and the absence of a set timetable for notification.

Greater exchange of satellite information could play an important support role in virtually any space weapon treaty. The essential purpose of such an exchange would be openness and timely disclosure. To this end, the mentioned shortcomings of the current *Registration Convention* could be corrected through an upgraded convention, a separate agreement, or by imbedding data exchanges within the space weapons treaty to be supported. A more specific description of the spacecraft function should be required and advance notification given of orbital status provided. For example, a pre-launch notification of the nominal mission timetable could be required.

These improvements are an integral and practical corequisite to any on-site or on-orbit verification procedure. Thus, the verification of the payload of a satellite not constituting an illegal weapon system involves verifying both what the payload is not and what the payload is purported to be.

The pre-launch disclosure of on-station orbital parameters is relevant to the management of any sort of keep-out zone treaty. This would allow participating states to preemptively evaluate the new satellite orbit with regard to possible keep-out zone violations and to initiate a grievance procedure if required.

Improved international registration and licensing address the issue of ambiguous space operations by openly assigning purposes to satellites in orbit. If the observable characteristics and operations of a satellite are consistent with its advertised purpose, confidence is generated in support of that claim. The possibility of an illegal space weapon system masquerading as a peaceful spacecraft can only be diminished through comprehensive data exchanges and direct verification procedures.

# PART II: SATELLITE HARM ANALYSIS

## Chapter 5: Modes of Harm

It is much too simplistic to divide satellites into "bad" and "good," or "harmful" and "harmless." If one reflects on the wide range of possible space operations enumerated in Part I, it becomes apparent that one satellite can harm another, at least potentially, in a large number of ways. In this chapter we shall examine these modes of harm in some detail.

A modern spacecraft is a triumph of engineering. Within its compact structure are arranged a number of sophisticated subsystems, each operating in complex and reliable collaboration with the others, to execute the spacecraft mission — usually over a period of several years. These subsystems are many in number and diverse in character, and have implications for the potential harm that one satellite can do to another.

### 5.1 Classes of Harm Modes

The number of possible spacecraft designs, the current variety of mission requirements, and the range of orbital altitudes and inclinations all make the assignment of a harmfulness rating — or, as we shall call it, a "harm index" — very difficult indeed for any specific spacecraft. Only with the aid of a carefully crafted methodology[5] can such an analysis be carried out. This chapter represents the first step in this methodology: defining *harm modes*.

A spacecraft must cause harm in a specific manner, using specific means. Some satellites may have only a few such harm modes, while others may have many harm modes, falling into five general *classes*:

| | |
|---|---|
| Kinetic Energy | *K* |
| Directed Energy | *D* |
| Nuclear | *N* |
| Electronic/Optical Interference | *I* |
| Sabotage | *S* |

Not surprisingly, harm modes belonging to a single class have key features in common, most notably, the manner in which the "target satellite" (or *target*, for brevity) is damaged. See Table 6.

| | |
|---|---|
| **Kinetic Energy:** | Energy flux deposition. |
| **Directed Energy:** | Energy flux deposition (most); penetrating radiation deposition (some). |
| **Nuclear:** | Energy flux deposition (most); penetrating radiation deposition (some). |
| **Electronic/Optical Interference:** | Harm caused by the target itself after its sensors or control systems are jammed, spoofed, blocked, or taken over. |
| **Sabotage:** | Performing acts of mischief, vandalism or sabotage, usually after rendezvous. |

**Table 6**

**Harm Mode Classes**

Twenty-nine harm modes (Table 7) are identified below. While this list is not claimed to be exhaustive, one can reasonably claim that any additional modes would be of a highly unusual and specialized nature.

| | | |
|---|---|---|
| **Kinetic Energy:** | 4 | Ramming, shooting, mining, torpedoing |
| **Directed Energy:** | 7 | Blinding, shocking, beaming, heating, overloading, blasting, irradiating |
| **Nuclear:** | 4 | Pulsing, blasting, irradiating, heating |
| **E/O Interference:** | 4 | Blocking, jamming, spoofing, takeover |
| **Sabotage:** | 10 | Breaking, coating, spraying, torching, shading, gassing, shocking, grappling, limpet mining, masking |

**Table 7**

**Twenty-Nine Harm Modes Studied**

## 5.2 Kinetic Energy Modes of Harm

Four harm modes in the Kinetic Energy class are now briefly described. In the following discussion, "the threat" is short for "the threat satellite," and "the target" is short for "the target satellite." Note that all these harm modes involve energy flux deposition.

*Ramming [K1]:* The threat collides with the target at high speed; damage is caused by impact.

*Shooting [K2]:* The threat projects one or more passive projectiles (e.g., bullets, mass-driver, rail-gun slugs) toward collision with the target; damage is caused by impact.

*Mining [K3]:* The threat carries an explosive device, triggering it in such a way that shrapnel impinges on the the target; damage is caused by impact.

*Torpedoing [K4]:* The threat releases subsatellite(s) having autonomous capability at low (relative) speed, which employ harm modes K1, K2 or K3.

## 5.3 Directed Energy Modes of Harm

Seven harm modes in the Directed Energy class can be cited. In brief, these are as follows:

*Ramming [D1]:* The threat directs a concentrated beam of light toward the target, causing damage to light-sensitive components in the target.

*Shocking [D2]:* The threat applies a differential electric field to the target via electron or ion beam, damaging the target by electrical discharges.

*Beaming [D3]:* The threat deposits energy onto the target via laser beam, ion beam, particle beam, reflected sunlight, or other nonpenetrating radiation, at a power level sufficiently high to damage the target by heating.

*Heating [D4]:* The threat radiates heat onto the the target, causing damage to heat-sensitive components.

*Overloading [D5]:* The threat deposits excessive electromagnetic energy into an EM receiver on the target, damaging the receiver.

*Blasting [D6]:* The threat deposits energy onto the target via laser beam, ion beam, particle beam, etc., at a very high power level, causing structural damage to the target from the resulting mechanical shock wave.

*Irradiating [D7]:* The threat applies a beam of penetrating radiation to the target, damaging sensitive electronic or other components.

## 5.4 Nuclear Modes of Harm

Four harm modes in the Nuclear class can be identified. Briefly, these are as follows:

*Pulsing [N1]:* The threat generates an electromagnetic pulse by detonating a nuclear explosive device; the target is harmed by the resulting transient electrical potential field.

*Blasting [N2]:* The threat explodes a nuclear device to damage the target by the resulting shock-wave.

*Irradiating [N3]:* The threat explodes a nuclear device to damage the target by the resulting nuclear radiation (rays and neutrons).

*Heating [N4]:* The threat explodes a nuclear device to damage the target through the resulting heat-pulse.

## 5.5 Electronic/Optical Modes of Harm

Four harm modes in the Electronic/Optical class can also be identified. The ideas behind these modes are, briefly, as follows:

*Blocking [I1]:* The threat physically blocks the line of sight between the target and its operators, interfering with communications between the operator and the target.

*Jamming [I2]:* The threat jams the target's communications uplink by transmitting noise at the appropriate band in the electromagnetic spectrum.

*Spoofing [I3]:* The threat spoofs the target by transmitting deceptive signals into one of the target's sensors in order to mislead the target into behaving in a manner undesirable to its operators.

*Takeover [I4]:* The threat takes control of the target by invading the target's command-uplink channel and impersonating the target's operators.

## 5.6 Sabotage Modes of Harm

Finally, one can identify a Sabotage class of harm mode. The ten principal modes in this class are briefly as follows:

*Breaking [S1]:* The threat draws up to the target and executes manipulative damage (e.g., wire snipping).

*Coating [S2]:* The threat sprays the target with a coating substance; the harm comes from obscuring the sensors.

*Spraying [S3]:* The threat sprays target with a heat-absorbent, reflective, corrosive, conductive or otherwise harmful substance.

*Torching [S4]:* The threat fires a thruster or similar device so that its plume impinges on the target in order to interfere with or damage the target.

*Shading [S5]:* The threat physically blocks the line of sight between the target and another point in space towards which the target must look, interfering with the target's operation.

*Gassing [S6]:* The threat releases a cloud of gas, damaging the target.

*Shocking [S7]:* The threat applies on electrical potential difference across the target, by direct electrical connection, damaging the target by the resulting electrical discharge.

*Grappling [S8]:* The threat draws up to the target, grapples it, then alters its attitude or its orbit, in order to interfere with its operation.

*Limpet Mining [S9]:* The threat attaches an explosive device to the target, to be detonated at a later time.

*Masking [S10]:* The threat jams the target's communications downlink, by physically approaching and then transmitting on the downlink frequency; the target's operators are thus denied information.

## 5.7 Summary Thus Far

The long list of "harm modes" makes it amply evident that the general question of how one satellite can harm another cannot be answered in a simple, straightforward manner. In view of this complexity, a careful methodology is called for.

Although the methodology recommended in the next chapter could have been presented at the outset, the magnitude of the problem is best first appreciated. Thus, while the most logical presentation may be strictly deductive and analytical, the most readable presentation is likely to be inductive and synthetical. Here a middle ground has been chosen: the underlying methodology will be presented, not at the beginning (when motivation would be lacking), nor at the end (when its benefit as a roadmap would be lost), but next.

# Chapter 6: Analysis of Intersatellite Harm

The intersatellite harm modes described in the previous chapter form the framework for an analysis of intersatellite harm. This process of analysis has two major levels, as shown in Figure 1. Level A, in which a single satellite is analyzed in terms of its potential harm modes, was the subject of the last chapter. At Level B, the topic for the present chapter, each harm mode is analyzed in detail: the parameters, characteristics, and critical capabilities (words defined precisely in a moment) of each mode of harm are identified and characterized.

There are also two general themes upon which the development of this methodology rests:

(a) wherever possible, properties or features of a harm mode should be defined in a manner that makes them, in principle, verifiable;

(b) wherever possible, properties or features of a harm mode should be defined in a manner that makes them, in principle, quantifiable and measurable.

The reasons for these two themes are self-evident: to the extent that properties are quantifiable and measurable, to the extent that a more precise mathematical analysis can be used to assess potential intersatellite harm. And, verifiability follows the well-known maxim: "Trust, but verify."

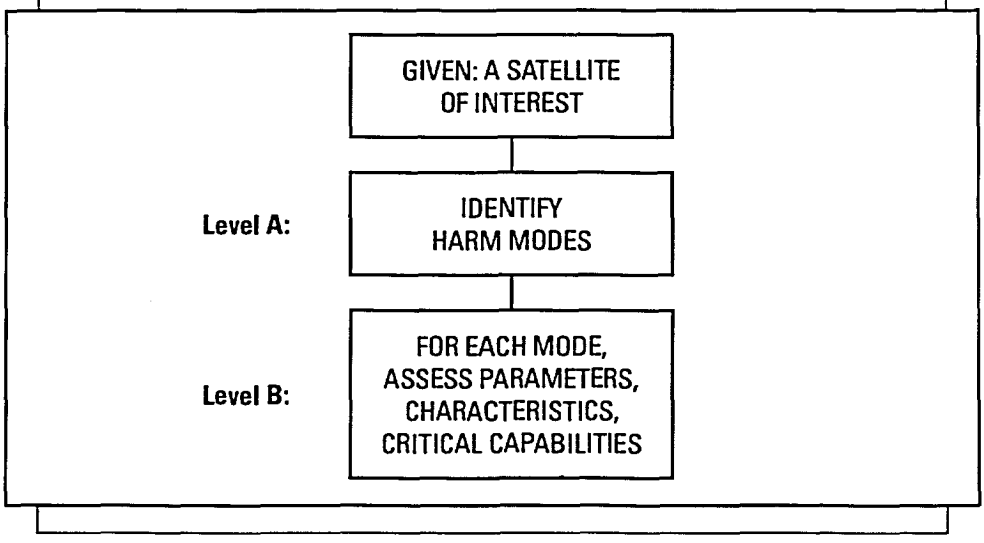
## 6.1 Harm Mode Parameters

Whenever a harm mode feature is *quantifiable* — that is, if a number or set of numbers can be assigned to it — this feature will be called a *parameter.* This is the ideal circumstance, since a harm mode characterized entirely by such parameters can be discussed in quantitative, mathematical terms, rather than in merely qualitative terms.

The relative importance of the several parameters that characterize a particular harm mode can then be assessed in quantitative — and therefore definitive — terms. If one moves back up to Level A (see Figure 1), one can compare the relative importance of the various harm modes possessed by a specific satellite on a quantitative basis.

Last, and not least important, the process of verification (Chapter 7) can be conducted using quantitatively defensible protocols. In summary, harm mode features that are quantifiable will be referred to as *harm mode parameters.*

*Figure 1. Analysis Methodology*




## 6.2 Harm Mode Characteristics

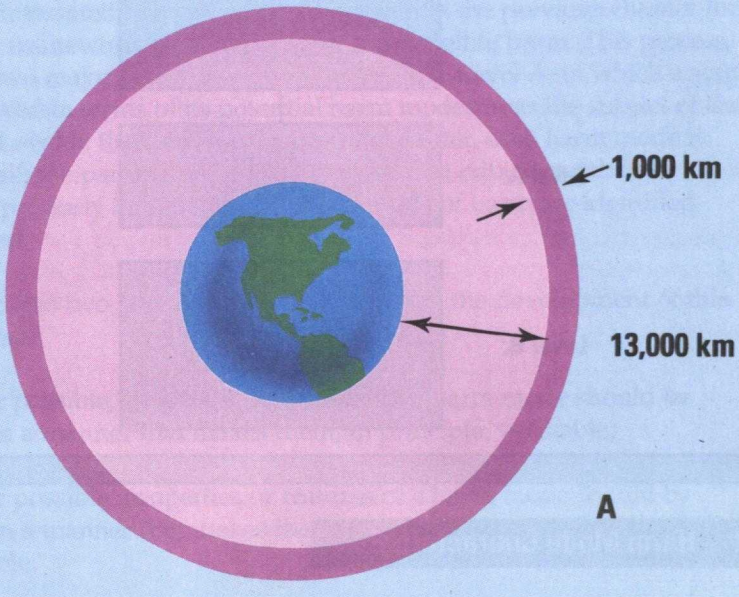
Alas, not all harm mode features are quantifiable on a continuous numerical scale. This tends to be due primarily to the intrinsic nature of the feature involved. For example, no one would argue the importance for harm mode analysis of whether an Earth sensor is on board. Yet one cannot characterize this presence or absence quantitatively over a continuous range. One can only note that this significant device is, or is not, on board the satellite of interest. In summary, harm mode features that are not quantifiable will be referred to as *harm mode* characteristics.

## 6.3 Harm Mode Critical Capabilities

In the course of identifying the important parameters and characteristics of the harm modes, one comes to observe that certain "bundles" or "clusters" of these parameters and characteristics recur again and again. Moreover, one can discern that the reason for this multiple recurrence is that each such bundle of parameters and characteristics corresponds to a *critical capability*, as a result of which the "threat" satellite can harm another satellite (Table 9).

*Figure 2 Two Types of Keep-Out Zone*

**TRADITIONAL CONCEPT**

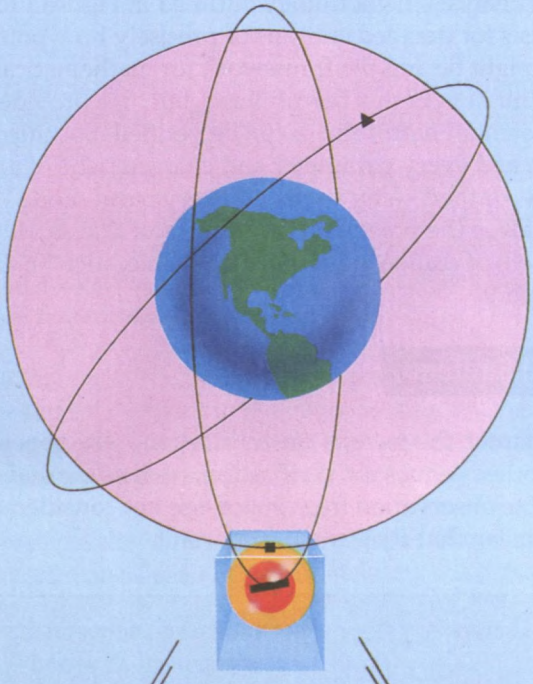



## TWO TYPES OF KEEP-OUT ZONES

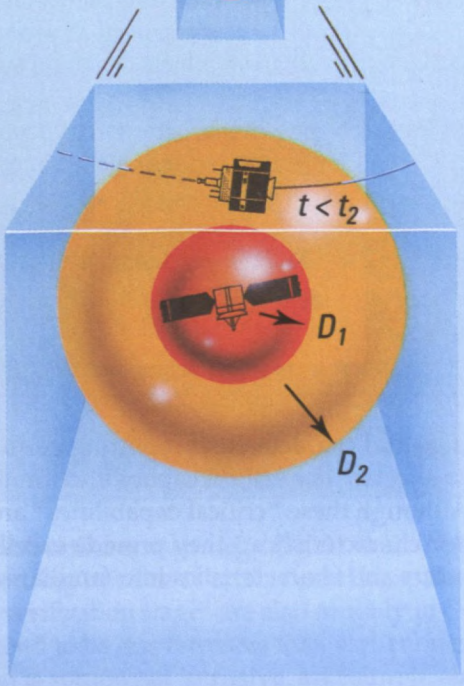
Past suggestions for keep-out zones have focussed on establishing protected volumes in space such as the concentric spherical shells illustrated in (A); essentially "space fences".

The "free space" keep-out zone suggested in Chapter 11 and illustrated in (B) and (C) here involves two stipulations: satellites must remain outside the minimum keep away distance ($D_1$) at all times and satellites may remain within the flyby distance ($D_2$) for a period of time ($t$) no longer than the maximum flyby time ($t_2$).

B



C



# Chapter 7: Verification

The analysis methodology outlined in Figure 1 forms not only the basis for detailed analysis of precisely how potentially harmful a given satellite might be and the framework for mathematical modeling of the quantitative estimation of this harmfulness, but also provides a roadmap for how the satellite's potential harmfulness can be verified. Specifically, if in the ideal circumstance each and every parameter and characteristic of a "threat" satellite were incontrovertibly verified — for each and every harm mode — then all the data necessary to analyze the potential harmfulness of that satellite would be available. The analysis itself, of course, must also be reliable; such an analysis is the subject of Chapters 8 and 9.

## 7.1 General Strategy

In this chapter, the focus is on verification.[6] The general strategy is shown in Table 8. Still other venues for verification, such as ground observation from space and satellite observation from space, are not considered here, which should not be taken to mean that they are unimportant.

*Table 8*

**Verification Strategy**

| | |
|---|---|
| **In Factory:** | 1. Inspect and test components.<br>2. Observe component-level and system-level testing.<br>3. Observe vehicle integration and testing. |
| **Launch Pad:** | 1. Pre-launch satellite inspection.<br>2. Test fluids/gases loaded into tanks.<br>3. Observe fueling operations. |
| **In Orbit:** | 1. Observe (from ground) in-orbit checkout, repair and refurbishment.<br>2. Monitor satellite orbit.<br>3. Observe satellite in orbit. |

The parameters and characteristics requiring verification are tabulated in harm mode "data sheets." The critical capabilities identified in this study are shown in Table 9. Although these "critical capabilities" are not features additional to "parameters" and "characteristics," they provide excellent algorithms for organizing these parameters and characteristics into familiar sets.

**Table 9**

**Critical Capabilities**

| | |
|---|---|
| **Approach:** | Satellites in similar orbits may naturally pass closely. Here, however, the threat alters its neighboring orbit slightly, using small thrust, to approach within 100 km of the target. |
| **Flyby:** | More accurate than "approach," but not as accurate as an "intercept." A "flyby" uses larger thrust to maneuver within 1 km of the target. |
| **Intercept:** | More accurate than "flyby," but produces intersatellite distances within a few meters, based on control of thrust magnitude and direction. Special sensors and thrust control required. |
| **Rendezvous:** | Like "intercept," but with the much more demanding requirement that not only the target position, but the target velocity also, be matched. At least two thrusting maneuvers are required. |
| **Manipulation:** | Carried out after rendezvous, and requires an on-board robotics/manipulation capability, including computer power and/or extensive communications capability. |
| **Communications:** | One looks for high bandwidth which might permit ground control during complex maneuvers. Uninterrupted access (many ground stations or a constellation of satellites) is also critical. |
| **Attitude Tracking:** | Threat can sense and control its attitude relative to target. This implies major sensors based on infra-red (IR) or ultraviolet (UV) measurements, or perhaps tracking telescopes. Tracking may be on a separate appendage. |
| **Control:** | On-board ability to orbit-identify, and rendezvous with, the target. Also needed: control computer, software, sensors, actuators. Latest computers create many new possibilities. |

Three aspects of the verification strategy (Table 8) are noteworthy: first, the strategy is organized according to where verification takes place; second, by the nature of the process, the verification stages are also roughly in chronological order; and third, later methods tend to be less intrusive than earlier ones (e.g., testing is quite intrusive, inspection is somewhat intrusive, and simple observation is rather

passive). Certain nontechnical issues — that a country might not permit inspection, or that a satellite manufacturer may attempt deception — are beyond the scope of this report. It can be pointed out, however, that there is frequently some redundancy in the verification process, so that if one avenue for verification is closed, or if further confidence is wanted, a second possibility may be used.

**Table 10**

**Harm Mode Data Sheet (Sample)**

**Harm Mode Data Sheet**

***Mining — [K3]***

**Brief Description:**
- The threat carries an explosive device, triggering it so that shrapnel impinges on the traget.
- Damage to the target is caused by impact.

**Discussion:**
This harm mode will usually require the threat to assume a near-collision orbit with the target. If the threat carries several mines, it would have to avoid striking the target itself in order to be reused. The mine's harmfulness arises either from the kinetic energy added to the shrapnel in the mine's explosion or from the increased volume of space threatened by a cloud of shrapnel (as opposed to a nearly point-like satellite). An example of the use of this mode of harm can be found in the current USSR "co-orbital interceptor" ASat weapon.

**Critical Capabilities:**
√ Interception accuracy [C3, C4].
√ Velocity relative to target on interception [C3, C4].
√ Pointing accuracy [C7].
√ Ability to calculate where to point, and when to fire the mine [C6, C8].

**Parameters:**
1. Quantity of explosive material on the threat.
2. Expected number of pieces of shrapnel.
3. Expected velocity distribution of shrapnel.
4. Expected mass-distribution of shrapnel.
5. Expected kinetic-energy distribution of shrapnel.
6. Expected directional distribution of shrapnel.

**Characteristics:**
1. Presence of explosive devices on the threat.
2. Presence of shrapnel-generating structures on the threat — hand-grenade type structures, explosives surrounded by pellets, etc.

**Table 11**

**Verification Checklist (Sample)**

| Harm Mode Verification Checklist | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| *Mining — [K3]* | | | | | | | | | |
| | In Factory | | | Launch Pad | | | In Orbit | | |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| *PARAMETERS* | | | | | | | | | |
| 1 | √ | | √ | √ | √ | √ | √ | | |
| 2 | √ | | | | | | | | |
| 3 | √ | | | | | | | | |
| 4 | √ | | | | | | | | |
| 5 | √ | | | | | | | | |
| 6 | √ | | | | | | | | |
| *CHARACTERISTICS* | | | | | | | | | |
| 1 | √ | √ | √ | √ | | | √ | | |
| 2 | √ | √ | √ | √ | | | √ | | |

To reiterate, the *columns* (1,2,...) in Table 11 refer to the verification methods listed in Table 8, while the *rows* (1,2,...) in Table 11 refer to the particular parameters and characteristics listed on the data sheet — Table 10, in this case.

## 7.2 Mode Verification Checklist

Verification Checklists for all 29 harm modes identified in Chapter 5 have been designed using the methods listed in Table 8. A sample data sheet and corresponding Checklist, for "Mining" are shown in Tables 10 and 11, respectively. A checkmark (√) indicates that a particular method (the column) can be used to verify the particular parameter or characteristic (the row). The parameter "number" or characteristic "number" refers to the harm mode data sheets mentioned above.

Through this process, then, properties or features of every harm mode needed for the quantitative calculation (Chapter 8) of harmfulness for a particular satellite have been defined in a manner that makes them in principle verifiable, and an appropriate procedure for such verification has also been identified.

# Chapter 8: Quantitative Indices of Harm

In Chapter 6 it was stated that two general themes underlie the methodology for analyzing rigorously the potential harm one satellite can do to another. These two themes are as follows:

(a) wherever possible, properties or features of a harm mode should be defined in a manner that makes them, in principle, verifiable;

(b) wherever possible, properties or features of a harm mode should be defined in a manner that makes them, in principle, quantifiable and measurable;

The first of these themes — verifiability — has now been addressed in Chapter 7. The focus now turns to the second theme — quantifiability.

## 8.1 Modal Harm Index

The harm modes identified in Chapter 5 are now each assigned a mathematical measure, or index, of harm — the *modal harm index*. Wherever possible, this index is simply a positive number. In fact, if a harm mode were specified entirely by parameters (i.e., quantitative characteristics), a completely quantitative modal harm index would be within reach, although not necessarily trivial to calculate. The reader is also reminded once again that, in all cases, the harm under discussion is only potential harm. The focus here is on what a satellite *can* do (a technical question) not what it *will* do (includes nontechnical questions).

This document is not the proper place to go into the analytical complexities of the indices for each of the 29 harm modes. Such an analysis unfortunately requires many pages of rather technical material and makes nontrivial demands on the mathematics and physics training of the reader.

The logic is once again as depicted in Figure 1, only in reverse: one first forms an index of harm at the mode level and then combines these (see next section) to form an index of harm for the satellite as a whole.

A general discussion of the *concept* of modal harm index is possible, however. For example, it should have certain properties that can be discussed in generic terms. First, a harm mode index should be an arithmetic *scalar*: although many modal parameters may be used in its calculation, the harm attributable to mode $i$ should be represented by a single positive number, which will be denoted by the symbol $H_i$. Second, as already mentioned, the modal harm index should depend on *identifiable parameters and characteristics*. Third, its calculation should be

*computationally tractable* using state-of-the-art computers. Fourth and last, it should be *selective*: it should be sensitive only to parameters corresponding to which the true potential harm changes drastically as that parameter changes.

## 8.2 Satellite Harm Index

Having developed the *modal* harm indices $H_i$ for all the harm modes of a specific satellite, the next step is to combine them, if possible, to form a *satellite* harm index, denoted $H_\Sigma$ for that satellite. Slightly different processes of aggregation correspond to somewhat different definitions of modal harm index, but these processes can all be written symbolically thus:

$$H_\Sigma = H_1 \oplus H_2 \oplus H_3 \oplus \ldots \oplus H_N$$

where $N$ is the number of harm modes attributed to the satellite, and $\oplus$ just means "added to" in a general sense.

Although the mathematical details of this "summation" will not be gone into here (there is more than one useful definition of the "sum," in fact), certain simple observations can be made that are pertinent and that give the flavour of the process. If a satellite had no harm modes — only a theoretical possibility — then $H_\Sigma = 0$. If a satellite had only one harm mode — highly unlikely — with index $H_1$, then $H_\Sigma = H_1$. When a satellite has $N$ harm modes, then evidently its harm index is greater than the harm indices of any of its individual harm modes: $H_\Sigma > H_i$ for $i = 1,2,3,\ldots,N$.

Using this methodology, one can calculate for any satellite of interest, a quantitative index of the harm it can potentially do to other satellites.

# Chapter 9: Automated Harm Calculation: The HARMDEX Software

As part of this study, a computer software package called HARMDEX was developed based on the methodology outlined in Chapters 5–8. This permits the quantitative estimation of the potential harmfulness of any given satellite, given appropriate input data. Intersatellite harm analysis can thus now be conducted on a more automated basis. The HARMDEX code includes all 29 harm modes in the five classes described in Table 6: kinetic energy, directed energy, nuclear, electronic/optical interference, and sabotage.

Although a detailed description of this software is not appropriate here, two brief examples will perhaps suffice to indicate its general style. The first example shows how the satellite harm index can be used to analyze the threat posed by an unintentional "weapon." In the second, more sinister, example, the threat satellite is in fact an ASat weapon, an intentionally hostile satellite.

## 9.1 Example 1: A Fragment Threatens *Anik*

Harm mode analysis shows that harm may be caused even by a satellite never intended by its launchers to do so. Awareness has been increasing in recent years regarding the hazards of space debris. In addition to natural debris such as micrometeorites, man-made debris also represents a considerable risk through high-speed collisions. A recent study[7] cites damage to the U.S. space shuttle window. An impact pit 4 mm in diameter was thought to have been caused by a fleck of white paint about 0.2 mm in size! The impact speed was estimated to be 3–6 km/sec.

In the present example, the harmfulness posed by a seemingly innocuous threat will be considered. A small, benign debris fragment, weighing 5 gm and generally having the properties of a piece of chalk, and moving in a counter-geostationary orbit, collides with one of Canada's communications satellites, *Anik*.[8] Only the [K1] harm mode, *ramming*, is relevant in this example.

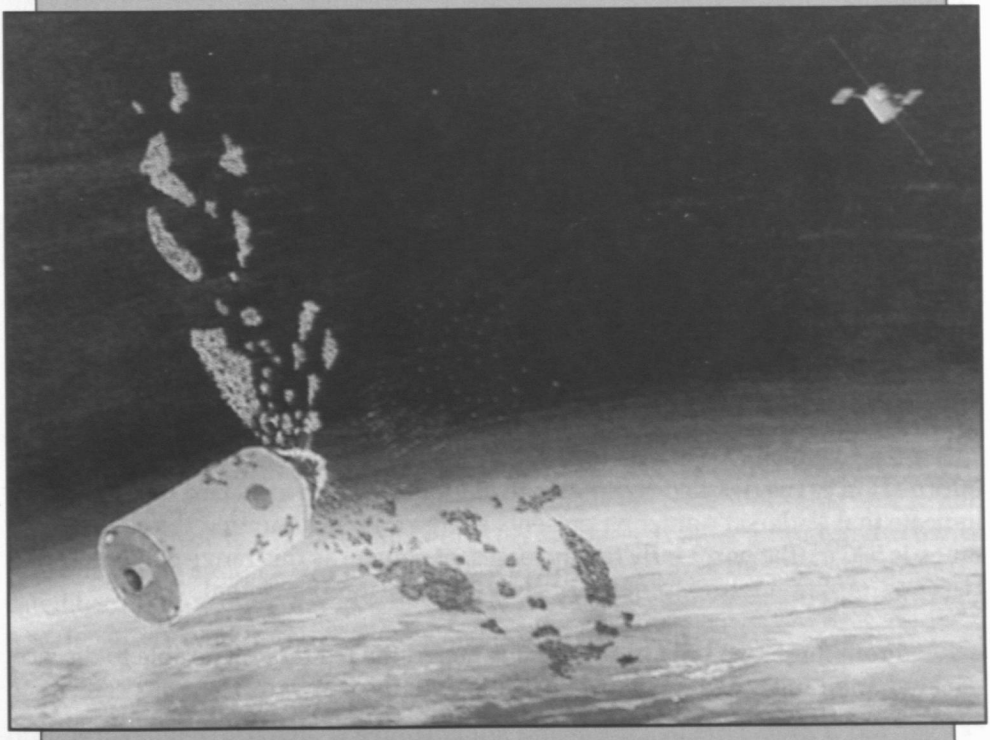
Under assumptions most favorable to the threatening fragment, the HARMDEX software returns a value of $H_\Sigma$ of approximately $5 \times 10^{-5}$, showing that the expected harm caused by the fragment is 0.005% of the critical[9] value — small, but not zero.

This example may seem somewhat trivial in a discussion of the potential harmfulness of full-sized satellites, and the real purpose of HARMDEX is, of course, to facilitate these latter calculations. However, it does show that the software is useful even at the lowest end of the "harm spectrum." (Example 2 will be at the other end of that spectrum.) Furthermore, although a small piece of debris was used here as the threat, the methodology and software can equally be applied to a "normal" (full-sized) satellite of benign intent — such as a domestic weather or communications satellite.

## 9.2 Example 2: An ASat Threatens *Radarsat*

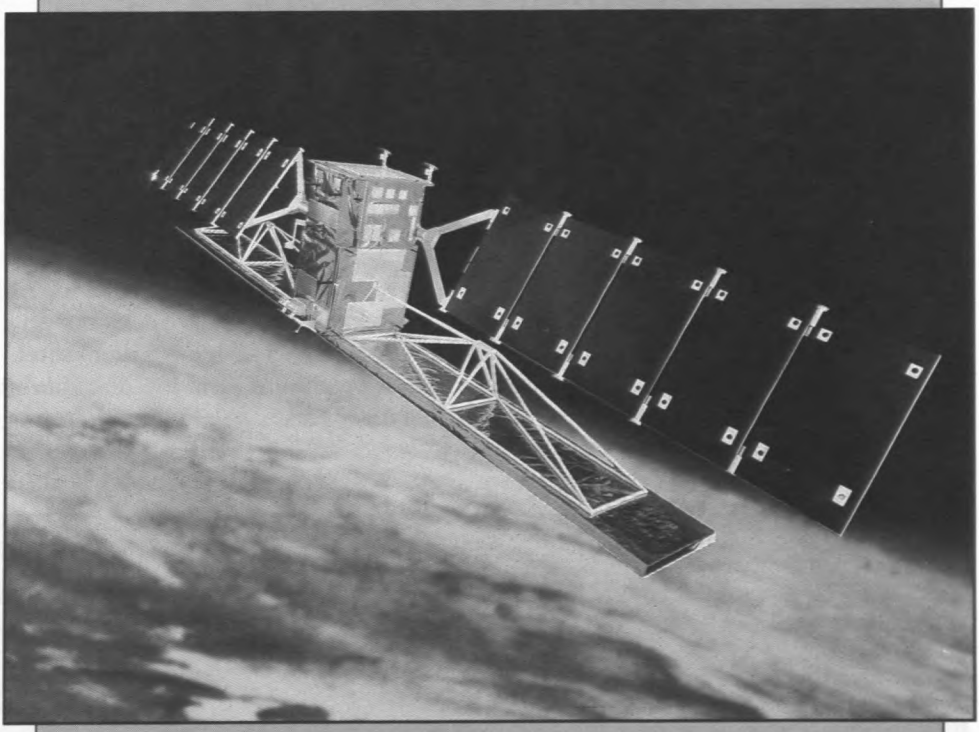
At the other end of the spectrum of intended harmfulness we consider an ASat: a model of a known anti-satellite system, the Soviet co-orbital "killer" satellite (Figure 3), is pitted against a large surveillance-type satellite in low-Earth orbit — such as Canada's planned remote sensing satellite, *Radarsat*[10] (Figure 4). In this example the primary harm mode is *mining* [K3].

***Figure 3. A Soviet ASat Spacecraft***



Source: United States, Department of Defence, *Soviet Military Power*, Washington, D.C.: March 1987, p. 52. Used with permission.

*Figure 4.* Radarsat — *A Canadian Earth-Resources Satellite*



Courtesy of the Canadian Space Agency

The existence of Soviet ASat's has been known for several years. The technique used is to achieve either a rendezvous or moderate-accuracy flyby of the target satellite and detonate a conventional mine device at close range. Shrapnel from the explosion can then strike the target satellite to inflict harm through kinetic energy deposition.

The detailed characteristics of the ASat can be estimated using unclassified information.[11] The detailed technical calculations performed as part of this project indicate that Radarsat's antenna presents a large target. Assuming the closest range is 500 m (the harm inflicted increases, of course, as this range decreases), the HARMDEX program returns a value of $H_{\Sigma} = 1.88$, greater than lethal.

From these two brief examples it is hoped the reader will be able to discern the kind and range of calculations available with the software. HARMDEX can be applied in a similar manner to any other satellite to give a quantitative measure of its potential harmfulness.

# PART III: CONFIDENCE-BUILDING MEASURES

## Chapter 10: Range of Harm

The idea of agreeing on a formula for measuring the *range of harm* for each satellite has great intuitive appeal. This concept is especially attractive here because a satellite's range of harm is in principle quantitative and therefore fits well within the present scheme.

In terms of the analysis methodology illustrated earlier in Figure 1, each of the harm modes associated with a particular satellite would be assigned a characteristic harm-versus-range graph. The harm-versus-range graph for Satellite X's Harm Mode Y would specify the harm (i.e., quantitative harm index) that Satellite X could potentially inflict, through Mode Y, on a target at a specified distance (range) from Satellite X.

The overall "satellite harm index" for Satellite X could then be calculated, at each given range, by combining, in the manner prescribed in Chapter 8, the modal harm-versus-range characteristics for all of Satellite X's harm modes. In particular, the distance from Satellite X at which its "satellite harm index" equals 1.0 can reasonably be called the *range of lethality* for Satellite X.

### 10.1 Maneuverability Is Critical

It is not difficult to realize that the harm that one satellite might visit on another will depend on their mutual distance. Complexities arise, however, from the myriad orbital characteristics that satellites may have. These vehicles are not lined up in a static row: their orbits fill a vast three-dimensional spherical space; their altitudes range from the near-Earth to the geostationary; their orbital inclinations vary from zero (geostationary satellites) to near-polar (Earth resources satellites); and, if large, their orbital eccentricities confer the benefit of being able to get occasionally close to a large number of other satellites at other altitudes. It is therefore difficult to assign a single "range of lethality" to each of these thousands of satellites, all travelling in excess of 1,600 km/hour and whizzing around Earth in a wide variety of altitudes, latitudes and orbital ellipticities.

Even greater complexity arises when the ability of a satellite to change its orbit is taken into account. If a threatening satellite is maneuverable, it can approach its targets more closely, thus expanding its range of lethality.

Virtually all satellites have some maneuvering capability — for initial orbit adjustment, for initiating long-term drifts to new orbital configurations, and for stationkeeping. This capability does extend their range of potential harm. But any satellite that possesses a significant maneuvering capability (e.g., large fuel tanks in orbit) can reasonably be concluded to pose at least a potential hazard to a large number of orbiting space systems.

## 10.2 Range of Lethality

It can be seen that two factors contribute to the range of lethality of a particular satellite: the intrinsic range of its potential modes of harm, and its maneuverability. These two factors can be combined geometrically, as depicted in Figure 5.

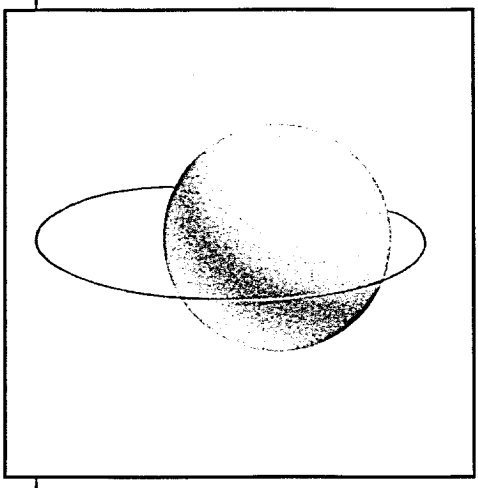
As explained in the full report on this project, one can geometrically superpose the (roughly toroidal) domains of harm associated with a given threat satellite. Thus, if one begins (as in Figure 5a) with the nominal orbit of a threat satellite that has two critical capabilities, (i) a space weapon, and (ii) maneuvering capability, one can construct two "domains of lethality" surrounding this nominal orbit: the toroidal domain within which its weapon is lethal (Figure 5b), and the toroidal domain defined by all the orbits that the threat satellite can, by maneuvering, occupy (Figure 5c). If the threat satellite were to first maneuver, and then use, its weapon, the domain of lethality would be expanded to the toroidal domain shown in Figure 5d.

The average radius of this latter torus, whose cross-sectional size is, in general, a superposition of the intrinsic range of the satellite's harm modes and the set of orbits into which by maneuvering it can reposition itself, is a quantitative measure of its range of lethality. A target satellite whose orbit intersects this summed toroidal volume can be considered to be within the range of lethality of the threat satellite.

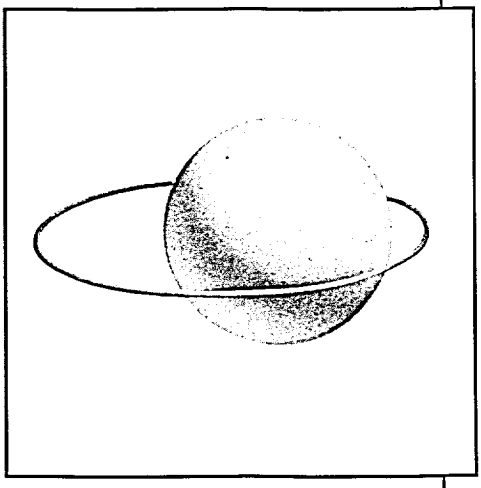
An important distinction between the two contributing factors (intrinsic harm-mode range, and maneuvering range) is their temporal immediacy. Within the "intrinsic harm-mode range," damage can be inflicted relatively quickly. Any maneuvering required to achieve that range, however, would take time. Moreover, such pre-attack orbital changes would be observable.

It must also be observed that any harmful interaction between a *specific* threat satellite and a *specific* target satellite will depend equally on the parameters and characteristics of *both* satellites. The presentation here has emphasized harm modes, harm mode indices, satellite harm indices, ranges of harm, ranges of lethality, etc. — that is, it has treated each satellite in terms of the *harm* it can

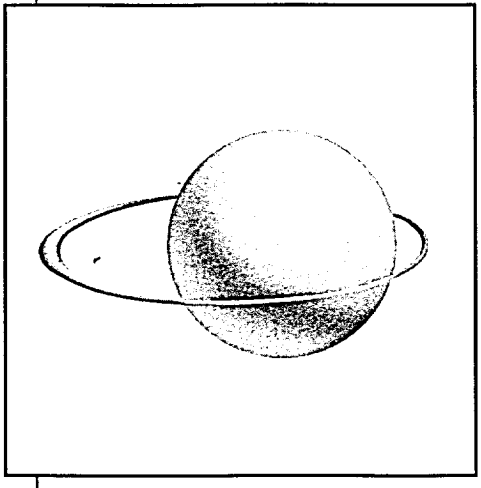
**Figure 5. Toroidal Domains of Potential Lethality**



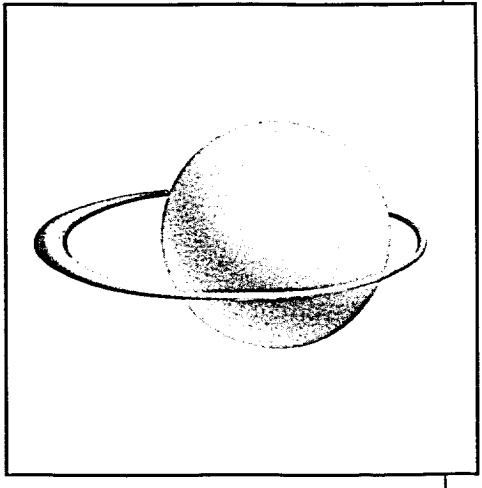
(a) Nominal Orbit of Threat Satellite



(b) Weapon Range



(c) Maneuvering Range (Flyby)



(d) Combined Toroid of Lethality (Weapon + Maneuvering)

Virtually all satellites have some maneuvering capability — for initial orbit adjustment, for initiating long-term drifts to new orbital configurations, and for stationkeeping. This capability does extend their range of potential harm. But any satellite that possesses a significant maneuvering capability (e.g., large fuel tanks in orbit) can reasonably be concluded to pose at least a potential hazard to a large number of orbiting space systems.

## 10.2 Range of Lethality

It can be seen that two factors contribute to the range of lethality of a particular satellite: the intrinsic range of its potential modes of harm, and its maneuverability. These two factors can be combined geometrically, as depicted in Figure 5.

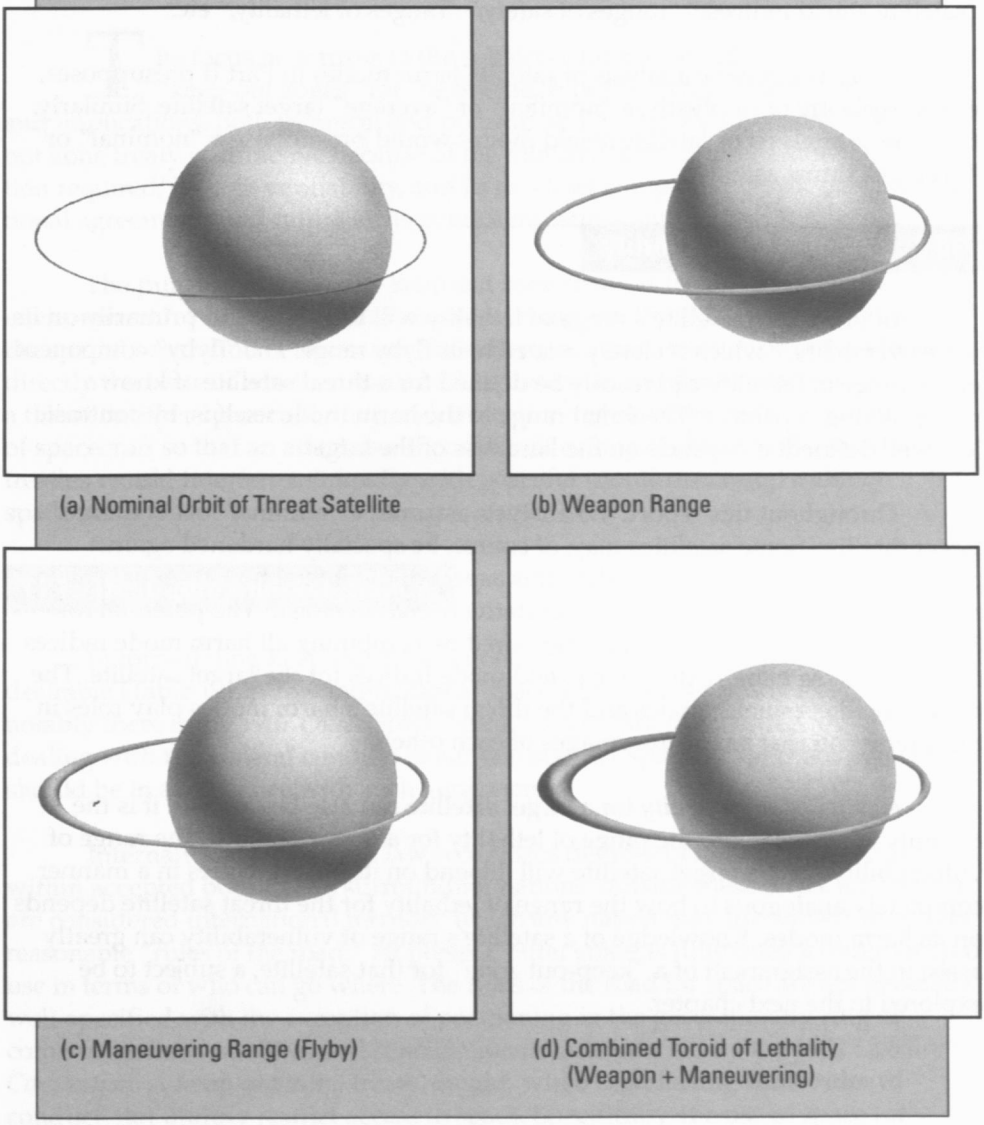
As explained in the full report on this project, one can geometrically superpose the (roughly toroidal) domains of harm associated with a given threat satellite. Thus, if one begins (as in Figure 5a) with the nominal orbit of a threat satellite that has two critical capabilities, (i) a space weapon, and (ii) maneuvering capability, one can construct two "domains of lethality" surrounding this nominal orbit: the toroidal domain within which its weapon is lethal (Figure 5b), and the toroidal domain defined by all the orbits that the threat satellite can, by maneuvering, occupy (Figure 5c). If the threat satellite were to first maneuver, and then use, its weapon, the domain of lethality would be expanded to the toroidal domain shown in Figure 5d.

The average radius of this latter torus, whose cross-sectional size is, in general, a superposition of the intrinsic range of the satellite's harm modes and the set of orbits into which by maneuvering it can reposition itself, is a quantitative measure of its range of lethality. A target satellite whose orbit intersects this summed toroidal volume can be considered to be within the range of lethality of the threat satellite.

An important distinction between the two contributing factors (intrinsic harm-mode range, and maneuvering range) is their temporal immediacy. Within the "intrinsic harm-mode range," damage can be inflicted relatively quickly. Any maneuvering required to achieve that range, however, would take time. Moreover, such pre-attack orbital changes would be observable.

It must also be observed that any harmful interaction between a *specific* threat satellite and a *specific* target satellite will depend equally on the parameters and characteristics of *both* satellites. The presentation here has emphasized harm modes, harm mode indices, satellite harm indices, ranges of harm, ranges of lethality, etc. — that is, it has treated each satellite in terms of the *harm* it can

***Figure 5. Toroidal Domains of Potential Lethality***



(a) Nominal Orbit of Threat Satellite

(b) Weapon Range

(c) Maneuvering Range (Flyby)

(d) Combined Toroid of Lethality (Weapon + Maneuvering)

potentially do. There is also a completely symmetrical, or dual, viewpoint,[12] which would emphasize, respectively, "shield modes," "shield mode indices," "satellite shield indices," "ranges of safety," "ranges of lethality," etc.

Thus, the generic analysis of satellite harm modes in Part II presupposes, either explicitly or implicitly, a "nominal" or "average" target satellite. Similarly, the generic analysis of satellite shield modes would presuppose a "nominal" or "average" threat satellite.

## 10.3 Range of Vulnerability

In practice, a satellite's range of lethality will likely depend primarily on its maneuverability,[13] which is closely related to its flyby range. The "flyby" component of the range of lethality can readily be defined for a threat satellite of known maneuvering capability. The lethal range of the harm mode itself is, by contrast, less well defined: it depends on the hardness of the target.

Throughout this report, the analysis assumes a "nominal" or "standard" target satellite. Some satellites may, of course, be specially hardened against potential damage. To accommodate this aspect of the interaction, a set of "shield modes" could be identified and quantitatively characterized. The potential for intersatellite harm would then be measured by combining all harm mode indices for the threat satellite with all the shield mode indices for the target satellite. The target satellite's shield modes and the threat satellite's harm modes play roles in the interaction that are mirror images of each other.

A *range of vulnerability* for a target satellite can also be defined: it is the quantity symmetrical to the range of lethality for a threat satellite. The range of vulnerability for the target satellite will depend on its shield modes in a manner completely analogous to how the range of lethality for the threat satellite depends on its harm modes. Knowledge of a satellite's range of vulnerability can greatly assist in the assignment of a "keep-out zone" for that satellite, a subject to be explored in the next chapter.

# Chapter 11: Keep-Out Zones

The focus now turns to the subject of internationally agreed-upon "keep-out zones" for the operation of spacecraft. Their usefulness and implications, both technical and political, will be briefly discussed. A keep-out zone treaty is attractive because of the minimal level of international cooperation required, its high verifiability, and its excellent compatibilty with past international agreements and future arms-control measures with respect to space.

The purpose of a satellite keep-out zone treaty is to provide a secure environment for the operation of nonthreatening satellites through regulation of the spatial separation between satellites. Keep-out zone treaties do not address directly the issue of whether spacecraft represent, either deliberately or otherwise, a threat to other spacecraft; they seek instead to regulate the relative proximity of spacecraft so that an attack is either difficult or impossible. Ideally such treaties would interfere minimally with peaceful (nonthreatening) military space activities.

## 11.1 Desirable Characteristics

In formulating keep-out zone agreements, several characteristics are desirable (Table 12). A few international space agreements already exist. Most notably there is the 1967 *Outer Space Treaty*, a set of broadly worded articles dealing with the general conduct of nations in outer space. A keep-out zone treaty should be in accordance with such agreements.

International air and sea law recognizes degrees of national sovereignty within accepted boundaries surrounding nations; outside these areas, air and sea are considered international territory which any nation may use subject to certain reasonable "rules of the road." At present, outer space is fully open to international use in terms of who can go where. The rules of the road for space are not generally well-specified with the exception of positioning in the geostationary ring of communications satellites and sensible constraints inferred by the 1972 *Liability Convention*. A keep-out zone treaty should, while establishing some rules of conduct, not unduly restrict access to space. Specifically, the use of space for peaceful purposes, including "national technical means" for the verification of controls on weapons activities, should not be restricted by keep-out zones. A new treaty should be applicable to all regimes of satellite operation; that is, it must somehow cope with the three-dimensional reality of spacecraft operations.

**Table 12**

**Desirable Characteristics for Keep-Out Zones**

- Definability, Tractability, Verifiability.
- Compatibility with future space law.
- Compatibility with existing space law.
- Applicability to all satellite operations.
- Minimal impact on the operation of nonweapon military satellites.

## 11.2 Traditional Concepts — The 'Space Fence'

Past suggestions in the literature for keep-out zones consider the establishment of protected volumes in space in which one nation's satellites would operate. The unwarranted intrusion into these zones by a satellite of an unfriendly country would be considered a hostile act. One such proposal[14] would partition space into some 360 concentric spherical shells, each 1,000 km thick, starting at 13,000 km altitude and ranging out to the Moon's orbit.

While this idea (illustrated in Figure 2) has the advantage of being easily understood, it has severe shortcomings: it is restrictive to many orbits, including low Earth orbits (LEO) and elliptical orbits; it contravenes the spirit of existing space agreements; it is inherently territorial; and it encourages the establishment of armed camps in space.

It has been pointed out[15] that such effectively sovereign territories in space violate existing agreements, specifically the 1967 *Outer Space Treaty*, Article II, which reads:

> *"Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means."*

Keep-out zones as traditionally conceived could well lead to an increased militarization of space as nations strive to monitor and defend their respective "territories" in space. Keep-out volumes are very often proposed by military interests to protect military satellite systems. In the same breath the use of ASat countermeasures (anti-antisatellites or DSats) is mentioned to actively defend the zone by attacking intruding spacecraft. Hence, traditional keep-out zone ideas appear to be regressive to the purposes of deweaponization, demilitarization, and the use of space for peaceful purposes.

## 11.3 A 'Free Space' Keep-Out Zone

A more practical "free space" keep-out zone can be developed based on the range of harm and range of lethality concepts developed in Chapter 10.

Illustrated in Figure 2, the zone has three associated parameters:

$D_1$ — minimum keep-away distance,

$D_2$ — flyby distance,

$t_2$ — maximum flyby time.

These parameters quantify the two stipulations that underlie the meaning of this free space keep-out zone: satellites must remain outside the minimum keep-away distance $D_1$ at all times; and satellites may remain within the flyby distance $D_2$ for a period of time no longer than the maximum flyby time $t_2$.

The minimum keep-away distance reflects the range of vulnerability and should be selected to ensure that a nominal threat satellite will have difficulty inflicting significant harm upon its target. At the same time, this distance should not be so large as to be impractical. In the most general analysis, the keep-away distance would depend on both satellites involved — that is, on both the threat satellite and the target satellite.[16]

The maximum flyby time accepts the fact that satellites must occasionally come close to each other, but restricts the duration for such a pass. This limits the opportunity for hostile action: there would not be time to acquire and attack the target. Using this framework, a threat satellite could not easily stalk a target.

For this system to work, there must be international communication. Against this "disadvantage," however, consider these advantages:

(a) it permits great freedom for peaceful space activity;

(b) it is applicable to all orbiting spacecraft (GEO, LEO, elliptical,...);

(c) it is flexible (each satellite could have its own keep-out zone specifications);

(d) it avoids territories to be defended; and

(e) it complies with, even enhances, existing space law.

In summary, the proposed free space keep-out zone does not put up fences in space or establish territories to be defended. Instead, it establishes zones surrounding individual satellites — zones that move with them, protecting only them, the national assets, not the space in which they operate.

## 11.4 Preliminary Parameter Estimates

Choices for keep-out zone parameters would be points for treaty negotiation; however, estimates for these values can be given. One recalls that each satellite can have its own custom-tailored zone. In practice, a satellite would likely be classified as belonging to one of a limited number of broad classes. For example, one such classification might be "manned orbiting space stations," for which a generous zone would be appropriate, emphasizing the minimum keep-away distance.

The following keep-out zone parameter estimates are reasonable for *un*manned satellites: $D_1$, 5–20 km; $D_2$, 100–500 km; $t_2$, 20–90 sec.

Any keep-out zone strategy must also be tractable and verifiable in practice. There must be a straightforward procedure to establish compliance with, or violation of, the zones. It is possible using the tools of orbital mechanics to establish the interaction of two spacecraft with respect to the above free space keep-out zones.

# Chapter 12: Autonomous Monitoring, Verification Beacons

In this chapter, the term "keep-out zone" (KOZ) will refer exclusively to the concept developed in the last chapter and illustrated in Figure 2b and c. Chief among the attractive features of this KOZ definition is its practicality. Attention will now be directed to two specific aspects of this practical viability: autonomous monitoring and verification beacons.

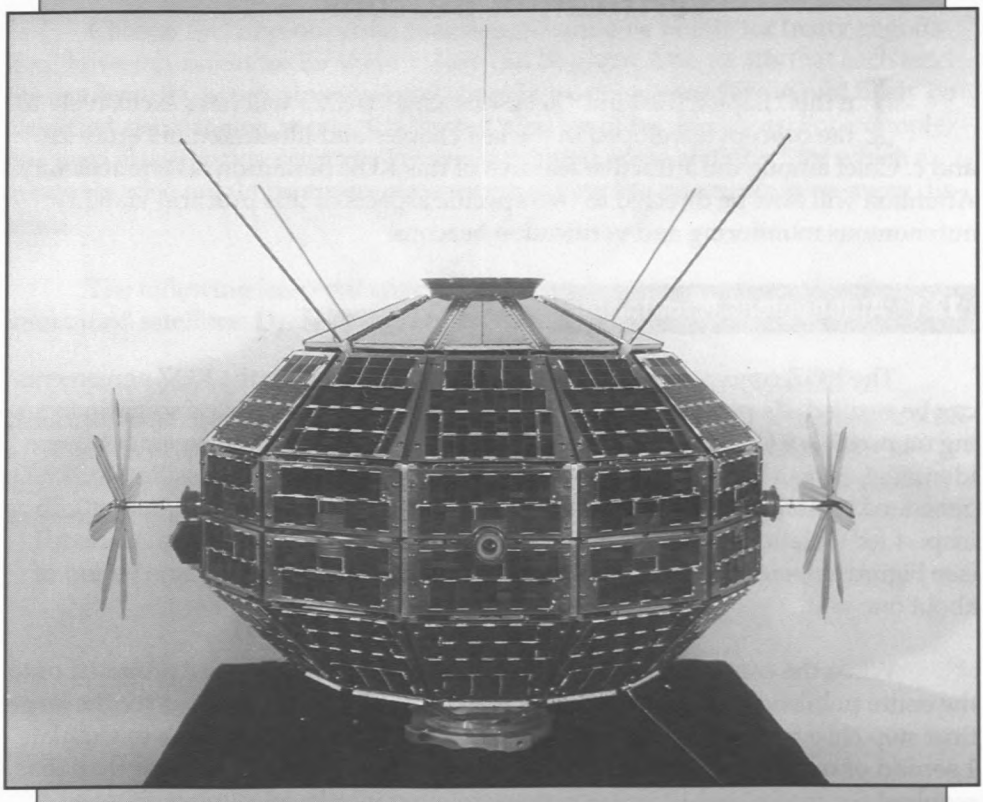
## 12.1 Autonomous Monitoring

The KOZ concept is workable only if compliance with the KOZ agreements can be verified. As part of this research project, therefore, a test-case scenario focusing on possible KOZ violations was computed in detail. KOZ infringements were identified using a group of 137 "threat" satellites (defined by unclassified NORAD-generated orbital elements) and Canada's Alouette I satellite[17] as the "target". To inspect for violations, the minimum distances between the threats and Alouette I (see Figure 6) were compared against a specified KOZ range, for a time period of about one year.

When the computer times observed in this trial situation are projected onto the entire published NORAD database, they indicate that, on average, for the large time step chosen, it will take a large mainframe computer 3.2 seconds to simulate 1 second of real motion for the 46 million threat-target pairs. This is less than that required for accelerated-time predictions; in other words, encounters must be computed fast enough to predict the future faster than the future is happening.

This preliminary computer study thus suggests that this technique is not feasible at present for producing the accelerated-time simulations needed to predict KOZ violations, even though such predictions are necessary to make the KOZ concept a viable confidence-building measure. However, this limitation will tend to disappear as new generations of computers become available. Moreover, unless altered, the threat satellite's orbit will remain relatively constant for weeks. Therefore, most violations can be predicted well in advance. Several other methods for reducing the amount of computer time required to test for KOZ violations also show promise.

*Figure 6. Alouette I*



Courtesy of the Department of Communications

## 12.2 Verification Beacons

Another approach to the task of verifiying KOZ agreements is to place beacons on board spacecraft. To investigate this approach, a strawman preliminary design for a beacon-based KOZ monitoring system was developed. The system as envisaged involves five components:

- a Treaty;
- a Satellite Monitoring Agency;
- beacons;
- tracking station(s); and
- a Control Centre.

Each beacon in this system would transmit a unique identification signal in response to a request from a tracking station. Beacon masses of less than 10 kg, power requirements of less than 20 watts, and lifetimes of 20 years seem achievable, based on radio frequency transponder-based beacons operating at approximately 1 GHz.

Such a system of beacons is technically feasible and could be used to monitor and verify KOZ agreements. Dollar costs of such a system could be substantial, though they could be offset in part by using components of the system as a satellite tracking service for treaty parties. There would, in addition, be potential economies of scale from using standardized beacons instead of national ones. Ultimately, the KOZ system could be integrated into a future space-traffic control system.

# Chapter 13: Regulating Space Weapons

The research reported here was motivated by the need to lay a practical, quantitative foundation for an examination of the feasibility of restricting or regulating weapons in space. Two main approaches to such regulation have been probed:

(a) regulation of spacecraft based on a rigorous evaluation of their potential harmfulness; and

(b) enforcement of keep-out zones, based on the target satellite's vulnerability.

In Article VI of the 1967 *Outer Space Treaty*, all space-faring nations agreed to *bear international responsibility for national activities in outer space*, including the activities of all nongovernmental entities and international organizations in which they participate. Any future regulations governing weapons in space will necessarily be codified in the form of a treaty between nations.

## 13.1 Current Space-Related Treaties

Future space treaties will have to fit within the framework of existing international space law. The *Outer Space Treaty* is the parent document for all subsequent international space agreements. A number of relevant treaties are reviewed in Table 13. Examination of these treaties shows that, of all the methods that one spacecraft can use to harm another (Chapter 5), current space law addresses only one: nuclear explosions in space. The relevant treaties, whose object was to slow down the nuclear arms race on Earth, addressed separately the testing and deployment of nuclear weapons in space in order to curtail their development and proliferation, respectively. These approaches may also be applied to non-nuclear space weapons.

## 13.2 Verification of Space Weapon Treaties

The acceptability of any arms control agreement hinges on the means chosen for verification of compliance with its terms. Several possible verification techniques for space weapons treaties have been examined in earlier chapters. These are summarized in Table 14, where a T or D indicates the method is well suited for verification of testing, or deployment, respectively.

Three possible types of treaties regulating space weapons seem feasible based on the precedents set by past arms control agreements, and on the verification techniques discussed above. These are introduced in the remaining three sections in this chapter.



**Table 13**

**Brief Review of Relevant Treaties**

| | |
|---|---|
| ***Limited Test Ban Treaty*** (1963): | Prohibits nuclear explosions in space. |
| ***Outer Space Treaty*** (1967): | Prohibits space-based nuclear weapons and other weapons of mass destruction. |
| ***Anti-Ballistic Missile Treaty*** (1972): | Prohibits development and testing of space-based ABM systems by the two superpowers. |
| ***SALT I*** (1972): | Prohibits interference with arms-control verification satellites of the two superpowers.* |
| ***Liability Convention*** (1972): | Governs national liability for damage caused by their spacecraft. |
| ***Registration Convention*** (1975): | Requires nations to notify the UN of spacecraft they launch. |
| ***Environmental Modification Convention*** (1977): | Prohibits deliberate hostile manipulation of natural processes from outer space. |
| ***SALT II*** (1979): | Prohibits space-based deployment of weapons of nuclear weapons or other weapons of mass destruction, and the interference with verification satellites. |

* This bilateral prohibition has been reinforced between the two superpowers by several subsequent arms control agreements. It has been extended to include the satellites of some other countries by the Conventional Forces in Europe (CFE) Treaty of November 1990. The CFE Treaty also includes within the scope of this prohibition, interference with "multinational technical means".

**Table 14**

**Relevant Verification Techniques**

| | |
|---|---|
| Conventional Surveillance: | *D* |
| Factory Inspection: | *T, D* |
| Launch-Site Inspection: | *T, D* |
| On-Orbit Inspection: | *D* |
| On-Board Monitoring: | *D* |

*T* = Testing; *D* = Deployment

## 13.3 A Satellite Keep-Out Zone Treaty

Article III of the *Outer Space Treaty* clearly provides a starting point for such agreements when it states that,

> *"States... shall carry on activities in the exploration and use of outer space... in the interest of maintaining international peace and security, and promoting international cooperation and understanding."*

Article IX further enjoins nations thus:

> *"If a State... has reason to believe that an activity or experiment planned by it or its nationals in outer space... would cause potentially harmful interference with activities of other[s]... in the peaceful exploration and use of outer space... it shall undertake appropriate international consultations before proceeding with any such activity or experiment."*

and furthermore,

> *"A State party to the Treaty which has reason to believe that an activity... planned by another... in outer space... would cause potentially harmful interference with activities in the peaceful exploration and use of outer space... may request consultation concerning the activity or experiment."*

A treaty requiring nations to agree upon certain satellite keep-out zones would operate within the same principles. If well-defined, such an agreement would preclude one nation's satellites from interfering with the satellite activities of another nation. Such a treaty would generally provide a secure environment for the routine nonhostile operation of satellites.

While a keep-out zone treaty would not address space-based weapon research and testing, it would restrict the threatening deployment of many space-to-space weapon systems. By regulating the proximity of spacecraft, even the perception of threatening deployment can be avoided.

The verification requirements for a properly conceived keep-out zone treaty are attractive. Verification of compliance could be accomplished fairly reliably using existing remote surveillance techniques, without requiring intrusive inspection of spacecraft, which some nations may find objectionable. Such a treaty can be made anticipatory by requiring pre-launch notification of intended orbital parameters. The Registration Convention provides a precedent for the international disclosure of the necessary information. Reliability can be increased even further at a moderate cost, through the use of identification and tracking beacons aboard spacecraft, as discussed in the last chapter.

## 13.4 Space Weapon Test Ban

Several past treaties — the 1963 *Limited Test Ban*, the 1972 *ABM Treaty*, and the (now expired) 1979 *SALT II Treaty* — prohibited the testing of nuclear weapons in space, in order to impede the development of space-based nuclear weapon systems. These provide models for a possible future treaty banning the testing of other types of space weapons, perhaps even of space weapons of all types. Tests of ASat weapons have been carried out in the past by both the USA and the USSR; such a treaty would have been a barrier to such testing.

The main tool for verifying such a treaty would be the Satellite Harm Analysis presented in Part II of this paper. Testing of equipment that contributes to the "critical capabilities" of harm modes would be monitored, regulated, or restricted. This would involve inspection of spacecraft, likely prior to launch, as well as on-orbit.

A significant difficulty is that past treaties did not ban research into ABM systems, partly because the line between "research" testing and "development" testing of space weapons can be contentious. Another difficulty is that many of the critical capabilities required by space weapons are equally critical to the peaceful use of outer space. For these reasons, such a space weapon treaty might, in order to be effective, have to be draconian: in promoting the "peace and security" goal of the *Outer Space Treaty*, it would undermine the "exploration and use of outer space" goals. If developed in conjunction with other treaties that compensate for its weaknesses, however, this type of treaty may be of benefit. Furthermore, the harm-mode analysis of Part II (in combination with its mirror image, shield-mode analysis) could shed light on how to make these critical distinctions.

## 13.5 Space Weapon Deployment Ban

A number of past treaties prohibit the deployment of nuclear weapons in space, providing a model for future treaties regulating the deployment of other types of space weapons. These include the *Outer Space Treaty*, the *ABM Treaty*, and the *SALT I* and *SALT II* treaties. Such a treaty would have to draw a distinction between offensive weapons (to be prohibited or regulated) and defensive weapons (likely permitted under the *Outer Space Treaty*).

Verification of a deployment ban for space weapons would be technically easier than for a test ban. The verification tools would be the same in both cases, primarily spacecraft inspection. However, while a test ban could be circumvented by testing technologies useful to weapons piecemeal on otherwise peaceful satellites, recognition of many types of space weapons should be possible by applying Satellite Harm Analysis to the results of pre-launch inspections.

# Chapter 14: Concluding Remarks

This paper has summarized several research projects undertaken by Dynacon Enterprises Ltd. for the Verification Research Program of External Affairs and International Trade Canada.

Many peaceful space operations for the next twenty-year period have been reviewed. Of the current nonweapon spacecraft, very few are "ambiguous." In fact, within the definition used here (see Section 2.1), there are few current space weapons. (Ground-based direct ascent weapons were excluded from discussion.) A number of proposed future space operations could, however, be misconstrued as, or used to camouflage, space weapon development.

Under the SDI program, the USA is researching several technologies that could be applied to space weapons operations. Similar research is undoubtedly being undertaken in the USSR, though less is known about this. At least one of these technologies, the "Brilliant Pebbles" concept, would give the USA an extremely effective ASat capability. The extremely high maneuverability of these kinetic-kill microspacecraft allows each one access to all of orbital space from any initial altitude. Under current plans, this system could be deployed within four years.

Ambiguities in space operations can arise in several ways. First, there is a commonality of critical capabilities and characteristics between weapons spacecraft and ostensibly peaceful spacecraft. Second, a spacecraft that is advertised as a weapon has applications beyond its advertised strategic purpose. The aforementioned "Brilliant Pebbles," an SDI concept, is intended as an ABM defense weapon; however, it also appears to have some potential in the ASat field.

A number of ambiguous operations have been identified in terms of their observability by space monitoring. Specific space activities have been noted that, when observed, could be interpreted as weapon-related. Since such ambiguities exist even with conventional remote monitoring, the need for more direct verification is clear: to regulate weapons in space, it must be possible to tell whether a "satellite" is, or contains, a "weapon."

Considerable effort has been devoted to the development of an appropriate strategy for the assessment of the harm that one satellite can do to another, towards the goal of regulating weapons in space. A total of 29 harm modes have been identified and their parameters and characteristics explained. A quantitative "index" of harm can be calculated (with respect to a nominal target) for any satellite. Both the mathematical tools and the software to implement the method have been completed, and a detailed verification strategy worked out.

Differing concepts for keep-out zones can have drastically different implications for the international use of space. The simplistic "traditional" keep-out zone referred to briefly in Chapter 11 is tantamount to a formal militarization of orbital space, eliminating free access to space by setting up permanent encompassing national boundaries. To overcome these drawbacks, Dynacon has proposed and developed a new type of keep-out zone; illustrative examples have also been provided.

The technical means for verification of a keep-out zone treaty is the well-established practice of satellite tracking and orbit prediction. Moreover, although a keep-out zone treaty does not directly contribute to the deweaponization of space, it does promote confidence in its peaceful use by impeding the threatening deployment of space weapons. This kind of treaty, by avoiding the control of spacecraft payloads, does not require the intrusive inspection protocols associated with other, more direct, space weapon verification measures.

Various confidence-building measures have been evaluated, including various kinds of inspection, keep-out zones (if properly defined), autonomous remote monitoring, and verification beacons. These measures offer a practical foundation on which to build future international agreements for the regulation of space weapons. Past space and arms-control treaties have been used here as a starting point for examining possible future space weapon agreements. Different verification measures do, however, vary somewhat in their cooperation requirements — a fact that impinges greatly on their feasibility.

## NOTES

1. The meaning of intersatellite "harm" is examined in Part II (Chapters 5–9) of this paper, where a graduated scale is developed for measuring satellite harm, ranging from negligible harm to lethality (satellite death). The important circumstance of *intersatellite range* (distance) is discussed in Chapter 10, becoming the basis for *keep-out zones* in Chapter 11.

2. Since most USSR space weapon research is hidden, this paper tends to focus on USA programs, for which more information is available.

3. A satellite's *critical capabilities* will be discussed in Chapter 6.

4. This is significant in light of the possibilities for on-site or on-orbit close-up inspection.

5. The methodology presented in this chapter was first conceived by Peter Stibrany (seconded from Spar Aerospace Ltd. to External Affairs and International Trade Canada) and Kieran Carroll (of Dynacon Enterprises Ltd.).

6. General verification concepts have been examined by F.R. Cleminson and E. Gilman in *A Conceptual Working Paper on Arms Control Verification*, Ottawa: Department of External Affairs, Arms Control Verification Study No. 1 (January 1986).

7. See Loftus, Tilton and Temple, "Decision Time on Orbital Debris," *Aerospace America* (June 1988).

8. The *Anik* satellites are members of an ongoing series of Canadian communications satellites, beginning with *Anik A* in 1972, and continuing with the ninth in the series, *Anik E*, launched on *Ariane* as this is being written. (More than one satellite in the *Anik* series has the same alphabetical label.)

9. When the harm index of the threat satellite attains the critical value, chosen through normalization to be unity, the target satellite is harmed to the extent that it can no longer function. It has, in the vernacular, been "killed."

10. *Radarsat*, scheduled for launch in the mid-1990's, is Canada's latest Earth-resources satellite and features synthetic-aperture-radar technology.

11. Such information has been compiled from the U.S. Department of Defense and the Congressional Office of Technology Assessment in *Anti-Missile and Anti-Satellite Technologies and Programs*, Noyes Publications, Park Ridge, NJ (1986).

12. Detailed analysis of this viewpoint is beyond the scope of this report.

13. Consider a threat satellite in an elliptical orbit with a perigee height of 200 km and an apogee halfway to geostationary altitude. If 20% of its mass is fuel for maneuvering, a forward thrust at perigee will raise the apogee more than 20,000 km toward to geosynchronous radius. This distance is greater than the range of most potential weapons.

14. For further details on this unworkable kind of keep-out zone, see S. Fetter, M. May in "Protecting U.S. Space Assets from Antisatellite Weapons," in *The High Technologies and Reducing the Risk of War*, Annals of The New York Academy of Sciences, Vol. 489, pp. 18–37, New York (1986).

15. By I. Vlasic, in "Preventing Weaponization of Outer Space in the Period of "'Glasnost" and 'Perestroika'," in *Arms Control and Disarmament in Outer Space: Towards Open Skies*, Vol. 3, pp. 147–166, Centre for Research in Air and Space Law, McGill University, Montreal (1989).

16. Refer to the discussion in section 10.2.

17. *Alouette I* was launched on 29 September 1962 to investigate aspects of the ionosphere. With its launch Canada became the third country, after the USSR and USA, to operate a satellite in space.


**Arms Control Verification Occasional Papers**

No. 1 International Atomic Energy Safeguards: Observations on Lessons for Verifying a Chemical Weapons Convention, by James F. Keeley, November 1988

No. 2 Verification of a Central American Peace Accord, by H.P. Klepak, February 1989

No. 3 International Atomic Energy Agency Safeguards as a Model for Verification of a Chemical Weapons Convention, H. Bruno Schiefer and James F. Keeley, ed., July 1989

No. 4 Conventional Arms Control and Disarmament in Europe: A Model of Verification System Effectiveness, by James W. Moore, March 1990

No. 5 Security Considerations and Verification of A Central American Arms Control Regime, by H.P. Klepak, August 1990

No. 6 Overhead Imaging for Verification and Peacekeeping: Three Studies, by Allen V. Banner, March 1991

External Affairs and International Trade Canada
Affaires extérieures et Commerce extérieur Canada