Chapter 1. Introduction

Verification has been called by the United States Arms Control and Disarmament Agency "the critical element of arms control";[1]† not *a* critical element, but *the* critical element. On the other hand an authoritative Soviet statement on verification states that "we are against giving absolute pre-eminence to verification and carrying it to absurd lengths; we are in favour of reasonable, balanced verification on the scale that is truly necessary – no more, no less".[2]

Both of these statements are highly abstract and both permit sufficient latitude in interpretation to allow either violent disputes or congenial agreements between the two sides. And the history of arms control negotiation between the USA and USSR has produced both kinds of result.

There is no logical contradiction between seeing verification as "the critical element" and still refusing to give it "absolute pre-eminence" or carry it to "absurd lengths". Yet there are differences in tone and emphasis in these statements which it is essential to elucidate and to analyse in order to understand why progress in arms control and/or disarmament has been so agonizingly difficult to achieve.

The problem becomes even more complex when it is realized that arms control and disarmament are not either ideally or practically bilateral concepts. Sooner or later all efforts to control or reduce armaments must involve *all* states and not just the few most powerful ones. The question must therefore be asked what role verification plays in existing international arms control agreements and how much it might be expanded and intensified in future agreements.

Given the great importance of verification in arms control it is unfortunate, but probably inevitable, that it is the subject most shrouded in secrecy, technical mystification and rhetorical distortion. On the one hand, over-enthusiastic arms control polemicists reassure us that all is well because satellites can read motor car licence plate numbers from an altitude of 200 kilometres. On the other hand, professional fear-mongers dream up bizarre evasion scenarios capable of defeating even the most sophisticated monitoring

†Superscript numbers refer to the notes and references at the end of each chapter.

devices and leading to ultimate 'victory' for the ruthless and imaginative cheater.

To say, as is so often said in such cases, that "the truth lies somewhere in between" may have a comforting and responsible tone, but it also misses the point. Even if there existed some kind of 'truth' in this deeply complex and subjective area, it would be neither accessible, comprehensible nor immutable.

Verification is intimately connected with the gathering of sensitive military intelligence, so a high level of secrecy is essential. Verification employs highly complex techniques and devices, so most people will never be able to assess for themselves the capabilities and limitations of most monitoring technologies, even if full information were made available. And rhetorical distortion is the very essence of political debate.

This book does not offer the 'truth' about verification. Instead, its purpose is to review the long record of arms control negotiations in order to identify some of the fundamental problems posed by verification and to derive a few general conclusions about the role that verification has played and is likely to play in the future.

There is a great danger in attempting to discuss verification on an abstract, theoretical level. It is understood by any student of arms control that negotiation of verification provisions only makes sense in the context of a given treaty or agreement. To an engineer, negotiator or political leader the tasks of designing, advocating or accepting a particular form of verification are intimately connected to the particular arms control objective to be achieved. General propositions are of little use in such practical questions.

But most people concerned about arms control are not engineers, negotiators or decision makers and have neither the desire nor the capability to influence detailed practical decisions on verification. Yet such people, for example teachers, journalists, diplomats or political activists, have an essential role to play in both informing and guiding public opinion. It is important that these groups have as clear as possible an overview of the problem of verification in order for them to deal constructively with the mass of arcane technical information and tendentious rhetoric that characterize the political debate over arms control. The question then becomes whether or not there exist some generalizations and propositions about verification which can be useful to such groups. This book is an attempt to derive such propositions using as a data base the history of arms control negotiations conducted and treaties signed since the end of World War II.

This data base is summarized in table 1, which has been organized chronologically to demonstrate the historical evolution of verification provisions in arms control treaties. Except for the first item all treaties listed are post-World War II, and the list includes treaties which, although signed, are still not in force, as well as three embryonic treaties which are in advanced stages of negotiation.

Several features of table 1 merit special attention. For example, the first

column of the table reflects the history of *détente* between the USA and USSR: its slow rise up to the late 1960s, its flourishing in the early and mid-1970s, and its rapid collapse at the onset of the 1980s. In particular, it can be seen that no significant arms control treaty has been signed since the SALT II Treaty of 1979.[3] The collapse can also be seen in the second column which shows that no bilateral US–Soviet treaty has entered into force since 1972 and no international treaty since the relatively insignificant (note only 47 signatories) Environmental Modification Convention in 1978.

The failure of recent bilateral US–Soviet treaties to enter into force is attributable entirely to the failure of the US Senate to ratify them. The blame for this must be shared by the Senate and Presidents Carter and Reagan who, since 1979, have not submitted any of the pending treaties for ratification. While it is important to emphasize that President Reagan has publicly committed the USA to abide by the terms of the pending treaties as long as the Soviet Union does so, it is still a very significant measure of the degree of tension and suspicion between the two states that these treaties remain unratified. This situation is also highly relevant for verification, since a number of important verification provisions in the Threshold Test Ban and Peaceful Nuclear Explosion Treaties cannot go into effect until the treaties are ratified. In particular the innovative and precedent-setting provisions for exchange of geological and seismic data, as well as observers for peaceful nuclear explosions, remain untested, even though much might be learned from them that would be relevant to verifying a comprehensive nuclear test ban treaty.

The final eight columns of table 1 list a variety of verification measures and whether they are included in a given treaty. There are five columns of monitoring techniques, which range from the remote-sensing techniques called 'national technical means' to unlimited on-site inspection, the most intrusive form of monitoring. The compliance procedures in the last three columns are means for dealing with ambiguities or disputes over implementation of the agreements and range from the weak injunction for the parties to "consult and co-operate" with each other to the more formal and well defined structures of a consultative commission or an international control organization.

No detailed analysis of the table entries is made in this introduction; such analyses are the subject of later chapters in which the treaties and their verification provisions are used to illustrate trends and general propositions in verification. Here it will suffice to point out the quite apparent increase over time in the variety and intensiveness of verification measures embodied in arms control treaties. This makes very clear the slow but steady increase in both the awareness of the importance of verification by some states and the efficacy and acceptability of a wider range of monitoring techniques and compliance procedures.

The trend to more thorough and effective verification measures is most evident in the last three treaties. The number of provisions already agreed to in principle is quite impressive. Yet these treaties remain unsigned, and by far

Table 1. The historical evolution of verification provisions in arms control treaties

Year signed	Years in force	Treaty and coverage	Review conference	Number of parties and type	Monitoring techniques: NTM[a]	Monitoring techniques: Information and observer exchange	Monitoring techniques: Black boxes or control posts	Monitoring techniques: Selective on-site inspection	Monitoring techniques: Unrestricted on-site inspection	Compliance procedures: Consult and co-operate	Compliance procedures: Consultative Commission	Compliance procedures: International control organization
Existing treaties												
1925	1928 ↓ ∞	Geneva Protocol Use of chemical and biological weapons	None	106 International								
1959	1961 ↓ ∞	Antarctic Treaty Military use of Antarctica	Possibly after 1991	31 Regional	Yes	Yes			Yes	Yes	Yes	
1963	1963 ↓ ∞	Partial Test Ban Treaty Nuclear weapon tests in outer space, the atmosphere and under water	None	112 International	Yes							
1967	1967 ↓ ∞	Outer Space Treaty Nuclear weapons in space	None	85 International		Yes		Yes	Yes			
1967	1968 ↓ ∞	Treaty of Tlatelolco Nuclear weapons in Latin America	None	23 Regional				Yes				Yes
1968	1970 ↓ 1995	Non-Proliferation Treaty Horizontal proliferation of nuclear weapons	Every 5 years	124 International			Yes	Yes				Yes
1971	1972 ↓ ∞	Sea-Bed Treaty Nuclear weapons on ocean floor	1977	75 International					Yes	Yes		
1972	1975 ↓ ∞	Biological Weapons Convention Production and stockpiling of biological and toxin weapons	1980	101 International						Yes		
1972	1972 ↓ ∞ / 1977	SALT I[b]: 5-year Interim Agreement (offensive strategic nuclear weapons) and ABM Treaty (anti-ballistic missiles)	Every 5 years (ABM)	2 Bilateral	Yes					Yes	Yes	

1974	—	Threshold Test Ban Treaty Nuclear weapon tests above 150 kt	None	2 Bilateral	Yes	Yes				Yes		
1975	1975 ↓ ∞	Document on confidence-building measures and certain aspects of security and disarmament (CSCE Final Act, Helsinki)	1978 1980–83 1984–86[c]	35 Regional		Yes				Yes		
1976	—	PNE Treaty Peaceful nuclear explosions above 150 kt	None	2 Bilateral	Yes	Yes		Yes			Yes	
1977	1978 ↓ ∞	Environmental Modification Convention Hostile use of environmental modification techniques	1984	47 International						Yes	Yes	Yes
1979	—	SALT II Treaty Strategic offensive weapons	None[b]	2 Bilateral	Yes	Yes				Yes		
Treaties under discussion												
—	—	Comprehensive Test Ban All nuclear weapon tests	—	— International	Yes	Yes	Yes	?			Yes	Yes
—	—	Chemical Weapons Treaty Development, production, stockpiling of chemical weapons	—	— International	Yes	Yes		Yes		Yes	Yes	Yes
—	—	M(B)FR Reduction of troops and weapons in Europe	—	— Regional	Yes	Yes	Yes	?		Yes	Yes	

[a] A 'yes' is inserted in this column only if the treaty contains an explicit provision on non-interference with NTM.
[b] The SALT I and II negotiations were originally assumed to be part of a continuing process of strategic arms limitation between the USA and the USSR. Continuation of this process (even under the new US designation of START and the present Geneva negotiations) serves many of the functions that review conferences serve under other treaties.
[c] While the Stockholm Conference is not a Review Conference it is part of the CSCE process.

Sources:
Goldblat, J., *Agreements for Arms Control: A Critical Survey* (Taylor & Francis, London, 1982) [a SIPRI book]; Crawford, A. *et al.*, *Compendium of Arms Control Verification Proposals*, 2nd. ed., ORAE Report R81 (Department of National Defence, Ottawa, 1982); Report of the *Ad Hoc* Working Group on Chemical Weapons, Committee on Disarmament document CD/416, 22 August 1983; SIPRI, *World Armaments and Disarmament, SIPRI Yearbook 1982* (Taylor & Francis, London, 1982), pp. 432-36; *Defense Monitor*, Vol. 11, No. 8, 1982.

the most common reason given (almost always by Western states) for not signing them is that they are not yet adequately verifiable. It seems that the perceived need for verifiability in some states has managed to stay well ahead of progress in finding technically feasible and politically acceptable verification methods. Why this gap remains so wide and what might be required to close it are discussed at length in subsequent chapters.

Terminology

Verification has developed a rich and varied vocabulary derived from the intimate historical connections between science, intelligence and diplomacy. Scientific terms have come from such diverse fields as seismology, electromagnetism, chemistry and biology. Technical terms flow in from photography, radar, computers, toxicology and space travel. The connection between verification and intelligence gathering has given words like 'monitoring' and 'surveillance' highly specific meanings, and diplomacy has produced such constructs as 'national technical means' and 'confidence-building measures'. Before moving ahead with the analysis of verification it is worth pausing to define some of these terms in the way they are used in the balance of the book.

Verification is defined by the Oxford English Dictionary as "the action of demonstrating or proving to be true or legitimate by means of evidence or testimony". When this abstract definition is applied to the particular field of arms control and disarmament, verification can be taken to be the action of *demonstrating compliance* with treaty obligations by means of evidence or information gathered by a variety of technical and institutional means.

The phrase 'demonstrating compliance' immediately raises the question 'demonstrating to whom?' The most straightforward answer to this is to assume that the parties to arms control agreements are unitary actors who demonstrate their compliance with treaties to one another. But in the real world, in which states are not unitary actors but complex political and bureaucratic entities, such an answer misses some essential aspects of the verification process, in particular its domestic political role. When the Soviet Union demonstrates compliance with SALT I does it do so for the US President or for the US Senate? And when the United States demonstrates compliance does it do so for the Soviet Politburo or the Soviet Army?

These are subtle and important questions which are analysed in detail in chapter 3. In the meantime the phrase 'demonstrating compliance' will be taken in the straightforward sense unless otherwise noted.

It is important at the outset to distinguish verification from two closely related concepts: *intelligence* and *espionage*. Intelligence is a general term for the full spectrum of methods by which one state acquires information about another. Intelligence gathering ranges all the way from reading the newspapers and recording the radio programmes of another state to infiltrating secret

agents into its most sensitive military, political or economic policy-making structures. Espionage occurs when these methods go beyond those sanctioned by "generally recognized principles of international law".

The last phrase has been placed in quotation marks because it has become a standard feature of the verification provisions of arms control treaties. It is used to distinguish those activities of such remote sensing devices as photographic satellites or radio antennas which qualify as *national technical means* (NTM) of verification from those which constitute illegal or improper intelligence gathering. Most recent arms control treaties contain non-interference provisions which prohibit any party both from interfering with the national technical means of verification of the other parties and from using deliberate concealment measures which impede verification by these means. These provisions explicitly recognize the legitimacy of NTM and make it a violation of the treaty to interfere with them or otherwise impede their use.

Such provisions make it extremely important to draw careful distinctions between legitimate NTM and other intelligence-gathering activities against which it remains legitimate to take countermeasures such as camouflage, deception, physical interference and so forth. But just where this line should be drawn has often been a matter of dispute and is strongly influenced by technological developments and the political atmosphere (see chapter 4).

In summary, intelligence can be seen as an umbrella term covering the full spectrum of information gathering activities, verification can be seen as those legal and proper intelligence activities which are carried out for the explicit purpose of demonstrating compliance with existing treaties and agreements, while espionage can be seen as those intelligence activities which are illegal or improper under generally accepted rules of international conduct. Even the combination of verification and espionage still leaves a vast area of the intelligence spectrum uncovered, and most of the intelligence activities of a state qualify as neither verification nor espionage.

While these definitions imply a satisfying precision of vocabulary, such precision should not be overrated. In the real world of military and political competition all information is potentially valuable, and it is rare that evidence for a possible violation of a treaty comes only from those devices or mechanisms devoted specifically to verification. Conversely, it is virtually impossible to design a device for monitoring compliance with a treaty which does not also pick up other information (often called *collateral* information) as well. And there is no question that espionage activity can help in the verification process and vice versa. So while the various terms have meaningful differences in international law, in practice the distinctions among them are much less important, and there are unavoidable limits to how precisely treaties can be worded or monitoring instruments designed to keep them separate.

The verification process itself consists of a number of activities which it is often useful to visualize as occurring in stages. The process begins with *monitoring*, which is the gathering of data, for example by reading the scien-

tific journals of another state or photographing its military installations from a satellite. Monitoring itself can be divided into two more or less distinct activities: *surveillance* and *reconnaissance*.[4] Surveillance is the systematic observation of some place or activity on a continuous or periodic basis. For example the International Atomic Energy Agency places tamper-proof cameras at sensitive locations in many nuclear facilities. These cameras take pictures on a continuous or periodic (or possibly random) schedule to watch for unauthorized or suspicious behaviour. In contrast, reconnaissance is carried out in the form of missions or *ad hoc* activities, generally aimed at a specific objective which for some reason has attracted attention. For example, high-resolution photographic satellites only take pictures when ordered or programmed to do so from the ground. The areas photographed are chosen for their particular interest at a particular time.

The monitoring step is accompanied or followed by an *information processing* step in which the data recorded by the monitoring device are assembled into some appropriate form. For example, the image of a missile exhaust plume recorded on the infra-red sensor of an early-warning satellite must be converted into digital data on temperature, speed, altitude, and so on, and transmitted back to a receiver on Earth where it is then put into a computer. Photographs taken from satellites or aircraft can be put through a wide variety of image processing techniques to make them more intelligible to photo interpreters (see chapter 2).

Once the data are processed they must be *analysed*. The digital or analog record of a seismograph must be studied by a trained seismologist (or by a computer that has been taught to 'think' like a trained seismologist) according to certain rules and procedures which seismology has evolved over many years of experience. Data taken from the bookkeeping records of a nuclear reprocessing plant must be analysed according to certain standard statistical methods and put into a form useful for subsequent stages of the safeguards process.

Following analysis comes the problem of *identification*; is the observed event a violation or is it not? At this stage it is common for information from other sources to be brought to bear on the problem, since it is rare that a violation can be unambiguously identified from a single source. For example, if a satellite sensor detects what appears to be the light flash from a nuclear weapon test in the atmosphere, it is possible to study various meterorological, seismological and radiological data to attempt to gain confirmatory or contradictory evidence.

One excellent, but all too infrequently used, means of gaining additional information is to consult with the party responsible for the observed event and ask for additional evidence or explanations. Encouragement of such cooperative behaviour is the basis for the creation of consultative commissions in many recent agreements, for example the Standing Consultative Commission of the SALT Treaties.

Most often the result of the best efforts at identification of a suspicious event will be some probability that the event represents a violation. For example, if one of the two parties to the SALT II Treaty tests a modified intercontinental ballistic missile (ICBM), the question may arise as to whether the throw-weight of the missile exceeds that of the earlier version by more than 5 per cent, a change forbidden by the Treaty. It may well be that existing verification techniques are only capable of determining a 5 per cent change to something like a 50 per cent confidence level. In such a case an indication of a violation would have to be treated with the same caution as any other variable subject to uncertainties in measurement.

A particularly important concept which should be introduced at this stage is the *false alarm*. This can be defined as an event which triggers any of the processes from monitoring to identification in a manner similar to a violation, even though it originates from some innocuous or irrelevant source. False alarms can be prevented from occurring at any stage of the process, but only by raising the threshold of sensitivity at that stage to real violations. For example, the monitoring of communications is usually designed to recognize certain key words or certain sending–receiving combinations and to ignore the rest. The more specific and limited this set is made, the easier it will be to spot relevant messages against the background of irrelevant ones, that is, the *signal to noise ratio* will be greater. But in doing this one risks missing possibly vital information in the huge volume that is ignored.

An alternative is to keep the monitors highly sensitive and to use special processing techniques to filter out false alarms or to set both monitoring and processing thresholds at a low level and count on analytical procedures to separate real from false events. But the higher in the sequence false alarms are allowed to propagate before being detected, the more technically sophisticated and time-consuming the filtering process becomes.

There is an unavoidable trade-off in verification between the demands for thoroughness and depth of coverage and the need to keep the false alarm rate at an acceptable level. The designers of any verification system must attempt to balance the military and political consequences of possibly missing some important events against the difficulties of trying to pick the real events out of the noisy background of false ones, as well as the political consequences of possibly responding to false alarms as if they were real.[5]

Once a violation has been identified, or a pattern of ambiguous and worrisome events established, there must ensue a process of *evaluation*. Decision makers and representatives of relevant agencies and political constituencies must decide how important this possible violation or pattern of behaviour is in the overall problem of national security.

It will be noticed that throughout all of the earlier stages leading up to this one, the degrees of professional judgement and political sensitivity have increased steadily. At the evaluation stage these assume full importance, and the evaluation of a possible violation is very much a political process. It will

generally be relatively easy for people to agree on what the evidence *says*, it will be far more difficult to get agreement on what it *means*.

The final stage of the process is *response*. Once a decision has been reached on the significance of a possible violation there are a wide variety of possible responses ranging from a decision to ignore the incident (possibly to protect intelligence sources) and hope it will not be repeated, or quiet diplomatic efforts to obtain a satisfactory explanation or a change of behaviour, to public accusations, the threat or actuality of retaliation, and even abrogation of the treaty. This decision on how to respond takes the process beyond what can accurately be called verification. It is better to use the term *compliance* to denote the full range of activities from monitoring to response. Since the problem of response will not be considered in any depth in this book, the term verification in the title is in fact the appropriate one.

The above description of the several steps of verification has emphasized the unilateral character of the process. National technical means are employed to monitor and process information; analysis and evaluation are carried out by national intelligence, military and foreign policy bureaucracies; and responses are determined by internal political processes. But verification is in fact an inherently *co-operative* process, and some elements of this co-operation have already been alluded to, for example the use of a consultative commission to resolve ambiguities and the agreement not to interfere with or impede NTM.

There are a number of other so-called *co-operative measures* which have been included in treaties or are under serious consideration for future treaties. These include arrangements for one party deploying monitoring devices or observation stations on the territory of another, for example seismographs in 'black boxes' which transmit data via satellite back to the state or international organization that controls them. Another increasingly common co-operative measure is the exchange of data by two or more states in order to establish an *agreed data base* for monitoring purposes. The creation of such a data base was an important achievement of the SALT II Treaty, and the failure to agree on such a base has for many years been a prominent obstacle to progress in the Mutual Force Reduction Talks in Vienna.

Another set of co-operative measures involves the prior notification by a party to a treaty of activities which might lead to misinterpretation or false alarms. For example, the Peaceful Nuclear Explosions Treaty requires prior notification of any planned peaceful nuclear explosion, and the Final Act of the 1975 Conference on Security and Co-operation in Europe (CSCE) requires prior notification of any military maneouvres in Europe involving more than 25000 troops.

This latter agreement is part of a group of provisions of the CSCE which have acquired the name *confidence-building measures* (CBMs), or, more recently, *confidence- and security-building measures* (CSBMs). It is worth dwelling on this name for a moment since the concept of a confidence-building measure has both a general and a particular meaning.[6] In its most general

sense the term confidence-building measure should encompass verification, since the purpose of the latter is to build confidence between parties to a treaty by demonstrating compliance. But this is not the way in which the term CBM is generally used. Instead it almost always is used in connection with the particular measures which have been created by the CSCE process to reduce political tensions and fears of surprise attack in Europe, that is the CSBM. That is how the phrase will be used in this book as well.

The final class of co-operative measures involves a variety of forms of *on-site inspection*, an activity which obviously requires the co-operation of the state on whose territory the inspection occurs. In this class can be included the regular inspections carried out by the International Atomic Energy Agency at commercial and research nuclear facilities under its safeguards programme. Other treaties, such as those covering the Antarctic, outer space and the sea bed, include provisions for unlimited on-site inspection by any party, and while such inspections do take place under the Antarctic Treaty they are of very limited military or political significance.

On-site inspection has been highly controversial throughout the history of arms control negotiations. It is generally seen as an *intrusive* form of verification as opposed to the supposedly *non-intrusive* national technical means, such as satellites and seismographs. But this distinction between intrusive and non-intrusive measures is a strange one, which grew out of historical and political conditions rather than from a strict interpretation of the usual meanings of these words.

One analysis has stated the paradox as follows:

> In practice all kinds of verification require some degree of access to the national affairs or to the territory of the state being verified. Even a report or questionnaire answered by a state in connection with the implementation of a treaty constitutes some form of access to a state's internal affairs. In addition their territories are constantly being photographed from outer space by high resolution cameras; radio and other telecommunications are monitored from abroad; movements of weapons and personnel are watched; levels of production are measured; the construction of fresh installations is established and so forth. All such monitoring encroaches deeply into a state's affairs and the information gained by it is extremely detailed and comprehensive. However, because such activities are not covered by any specific rules of international law, they cannot be prohibited by the states which are subjected to them. What is remarkable is that this type of verification is often termed 'non-intrusive'. The only explanation for the term is that direct personal access to sovereign territory, waters, or airspace is not required.[7]

An analogy might be helpful in appreciating the contradictions implied in the concept of 'non-intrusive' methods. The owner of a house could under the above definition have his property periodically photographed from the air, his

telephone and postal communications monitored, his visitors 'debriefed' at the end of their visits, his comings and goings closely watched and his financial transactions monitored. But as long as this was all achieved without physical encroachment on his property the process would be, according to customary verification usage, non-intrusive.

One study has recognized the fact that all forms of intelligence gathering are intrusive and has distinguished between *physical* intrusion and *cognitive* intrusion.[8] The former refers only to physical access by foreign inspectors to the territory of the state being monitored, while the latter encompasses all other measures by which foreigners acquire sensitive military or economic information. According to this study the distinction has some meaning because even though "cognitive intrusion usually implies some physical intrusion, it is possible to conceive of a system where no physical access is needed to acquire sensitive information".[9]

This distinction seems rather an academic one given the historical evolution of concepts of intrusion and the acceptance or rejection of the legitimacy of various forms of monitoring. This evolution is analysed in more detail in chapter 4, and here it is enough to say that intrusiveness has been and is likely to remain in the eye of the beholder. There is no monitoring technique, no matter how remote or purely 'cognitive' in nature, which cannot be interfered with or spoofed by a state unwilling to accept its legitimacy and willing to accept the costs and risks of such interference. States have agreed to accept or to tolerate certain forms of intrusion on their affairs for a variety of reasons, but this acceptance does not change the nature of the intrusion. For these reasons no attempt will be made in this study to distinguish instrusive from non-intrusive forms of verification, and the use of these words will be held to a minimum.

Overview

The basic organizing principle of this book is the treatment of verification as a complex and intimate interaction between technology and politics. In this sense it is similar to many modern problems in the fields of energy, health care, mass communications, information processing and so forth. Each of these problems has a technological dimension characterized by continual innovation, the demand for efficiency and an apparently endlessly expanding frontier of possible applications. Each problem also has a political dimension characterized by internal popular and bureaucratic conflicts, and external demands for international equity and co-operation, in conflict with national sovereignty and self-interest.

Verification displays all of these features, and much of the history and possible future evolution of this field can be analysed in terms of the interactions between these two aspects. It therefore seems appropriate to organize the analysis in the following way. Chapter 2 surveys the technological

developments which have so dramatically expanded the potential for effective verification over the years since the end of World War II. The descriptions focus on basic principles and, because they are intended to be understood by the general reader, excessive detail and technical jargon are avoided. The objective is to provide a simple, yet not over-simple, summary of the capabilities and limitations of these systems and the ways in which they can and might contribute to verification.

Chapter 3 considers the politics of verification both from an international and a domestic point of view. Because the international arms control arena has been effectively dominated by the United States and the Soviet Union, their political interaction with respect to verification issues is given primary attention. However, the political concerns of other states are also dealt with to demonstrate the growing pressures for internationalization of this field. Internal politics is divided into popular political concerns and bureaucratic dynamics. Here the focus is very much on the United States where verification plays a significant domestic political role and where far more information is available on the internal bureaucratic struggles on this issue.

Chapter 4 then combines technology and politics and focuses on four problems for which the interaction of these factors seems highly significant. These problems are the legitimacy of verification measures, the diagnosis and treatment of non-compliance, the role of co-operative measures and on-site inspection and the problems faced by efforts to make verification more international, both in scope and in control.

Finally, chapter 5 presents conclusions and propositions supported by the evidence and analysis of the preceding chapters. No attempt is made to deal systematically with the verification issues raised by particular treaties or negotiations. Instead, the treaties and negotiations are treated here as a data base from which to draw examples to illustrate particular propositions or generalizations. It is felt that these will be more useful to the general reader who needs some context in which to understand the almost overwhelming flood of information, whether relevant or irrelevant, accurate or inaccurate, sincere or disingenuous, which characterizes the present public discussion of verification.

References

1. ACDA, *Verification: The Critical Element of Arms Control,* US ACDA Publication No. 85 (US Arms Control and Disarmament Agency, Washington, DC, March 1976).
2. Issraelyan, V., quoted in Final Report of the 119th meeting of the Committee on Disarmament, Committee on Disarmament document CD/PV.119, Geneva, 31 March 1981, p. 17.
3. There have been three minor agreements signed since the SALT II Treaty in 1979. These are an agreement governing activities on the Moon, one on the physical protection of nuclear material, and one on the use of inhumane conventional

weapons (see Goldblat, J., *Agreements for Arms Control: A Critical Survey* (Taylor & Francis, London, 1982), pp. 286-302 [a SIPRI book]). However none of these agreements involves significant verification provisions and all are of very minor military and political significance. Their existence does not affect any of the analysis based on table 1.

4. Velocci, T., 'Strategic reconnaissance/surveillance', *Military Technology*, October 1983, p. 38.
5. Meyer, S.M., 'Verification and risk in arms control', *International Security*, Vol. 8, No. 4, Spring 1984, pp. 115-17.
6. Freedman, L., 'Assured detection: needs and dysfunctions of verification', in Nerlich, U. (ed.), *Soviet Power and Western Negotiating Policies*, Vol. 2 (Ballinger, Cambridge, MA, 1983), p. 249.
7. SIPRI, *Strategic Disarmament, Verification and National Security* (Taylor & Francis, London, 1977), pp. 22-23.
8. 'A conceptual working paper on arms control verification', Arms Control and Disarmament Division, Department of External Affairs, Department of National Defence, Ottawa, June 1981, pp. 30-33.
9. 'A conceptual working paper on arms control verification', (note 8), pp. 30-31.