The Weapon of Openness

by Arthur Kantrowitz
Dartmouth College

Foresight Background No. 4, Rev. 0

Introduction | The SDI Example
Strength of Openness | The Cryptography Case
Secrecy and Corruption | Openness and the Future

"The best weapon of a dictatorship is secrecy,
but the best weapon of a democracy
should be the weapon of openness."

—Niels Bohr

Introduction

What is the "weapon of openness" and why is it the best weapon of a democracy? Openness here means public access to the information needed for the making of public decisions. Increased public access (*i.e.* less secrecy) also gives information to adversaries, thereby increasing their strength. The "weapon of openness" is the net contribution that increased openness (*i.e.* less secrecy) makes to the survival of a society. Bohr believed that the gain in strength from openness in a democracy exceeded the gains of its adversaries, and thus openness was a weapon.

Technology developed most vigorously
in precisely those times and places
where the greatest openness existed

This is made plausible by a Darwinian argument. Open societies evolved as fittest to survive and to reproduce themselves in an international jungle. Thus the strength of the weapon of openness has been tested and proven in battle and in imitation. Technology developed most vigorously in precisely those times, *i.e.* the industrial

revolution, and precisely those places, western Europe and America, where the greatest openness existed. Gorbachev's *glasnost* is recognition that this correlation is alive and well today.

Let us note immediately that secrecy and surprise are clearly essential weapons of war and that even countries like the U.S.—which justifiably prided itself on its openness—have made great and frequently successful efforts to use secrecy as a wartime weapon. Bohr's phrase was coined following WWII when his primary concern was with living with nuclear weapons. This paper is concerned with the impact of secrecy vs. openness policy on the development of military technology in a long duration peacetime rivalry.

Let us also immediately note that publication is *the* route to all rewards in academic science and technology. When publication is denied, the culture changes toward the standard hierarchical culture where rewards are dependent on finding favor with superiors. Reward through publication has been remarkably successful in stimulating independent thinking. However, in assessing openness *vs.* secrecy policy it must be borne in mind that research workers (including the present author) start with strong biases favoring openness.

In contrast, secrecy insiders come from a culture where access to deeper secrets conveys higher status. Those who "get ahead" in the culture of secrecy understand its uses for personal advancement. Knowledge is power, and for many insiders access to classified information is the chief source of their power. It is not surprising that secrecy insiders see the publication of technological information as endangering national security. On the other hand, to what degree can we accept insiders' assurances that operations not subject to public scrutiny or to free marketplace control will strengthen our democracy?

My own experience relates only to secrecy in technology. Therefore I will not discuss such secrets as submarine positions (which seem perfectly justifiable to me in the sense that they clearly add to our strength) or activities which are kept secret to avoid the difficulties of explaining policy choices to the public (which seem disastrously divisive to me).

First, we offer some clues to understanding the historical military strength of openness in long duration competition with secrecy.

Second, we suggest a procedure for the utilization of more openness to increase our strength.

The Strength of Openness

An important source of support for secrecy in technology is the ancient confusion between magic and science. In many communications addressed to laymen the terms are used almost interchangeably. Magic depends on secrecy to create its illusions while science depends on openness for its progress. A major part of the "educated" public and the media have not adequately understood this profound difference between magic and science. This important failure in our educational

system is one source of the lack of general appreciation of the power of openness as a source of military strength. A more general understanding of the power of openness would bolster our faith that open societies would continue to be fittest to survive.

Openness is necessary for the processes of trial and the elimination of error, Sir Karl Popper's beautiful description of the mechanism of progress in science. Let's try to understand what happens to each of these processes in a secret project and perhaps we can shed some light on how the peacetime military was able to justly acquire its reputation for resistance to novelty.

Trial in Popper's language means receptivity to the unexpected conjecture. There is the tradition of the young outsider challenging the conventional wisdom. However in real life it is always difficult for really new ideas to be heard. Such a victory is almost impossible in a hierarchical structure. The usual way a new idea can be heard is for it to be sold first outside the hierarchy. When the project is secret this is much more difficult, whether the inventor is inside or outside the project.

Impediments to the elimination of errors will determine the pace of progress in science as they do in many other matters. It is important here to distinguish between two types of error which I will call ordinary and cherished errors. Ordinary errors can be corrected without embarrassment to powerful people. The elimination of errors which are cherished by powerful people for prestige, political, or financial reasons is an adversary process. In open science this adversary process is conducted in open meetings or in scientific journals. In a secret project it almost inevitably becomes a political battle and the outcome depends on political strength, although the rhetoric will usually employ much scientific jargon.

Advances in technology incorporate a planning process in addition to the trial and elimination of error which is basic to all life. When the planned advance is small the planning can be dominant, in the sense that little new knowledge is required and no significant errors must be anticipated. When the planned advance is large it will usually involve research and invention, and the processes of trial and the elimination of error discussed above will determine the rate of progress. In these cases the advantages of openness will be especially important. The familiar disappointments in meeting schedules and budgets are frequently related to the fact that, in selling new programs, the importance of these unpredictable processes is not sufficiently emphasized. More openness would reduce these disappointments.

Trial and the elimination of error is essential to significant progress in military technology, and thus both aspects of the process by which significant progress is made in military technology are sharply decelerated when secrecy is widespread in peacetime. Openness accelerates progress. In peacetime military technology, openness is a weapon. It is one clue to the survival of open societies in an international jungle.

Secrecy as an Instrument of Corruption

The other side of the coin is the weakness which secrecy fosters as an instrument of corruption. This is well illustrated in Reagan's 1982 Executive Order #12356 on National Security (alarmingly tightening secrecy) which states {Sec. 1.6(a)};

"In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security."

This section orders criminals not to conceal their crimes and the inefficient not to conceal their inefficiency. But beyond that it provides an abbreviated guide to the crucial roles of secrecy in the processes whereby power corrupts and absolute power corrupts absolutely. Corruption by secrecy is an important clue to the strength of openness.

Corruption by secrecy is an important clue to the strength of openness

---

One of the most important impacts of corruption from secrecy is on the making of major technical decisions. Any federally sponsored project and especially a project so hotly contested as the Strategic Defense Initiative must always keep all its constituencies in mind when making such decisions. Thus the leadership must ask itself whether its continual search for allies will be served by making a purely technical decision one way or the other. (A purely technical decision might determine whether money flows to Ohio or to Texas. Worse yet, revealing technical weaknesses could impact the project budget.)

When this search for allies occurs in an unclassified project, technical criticisms, which will come from the scientific community outside the project, must be considered. Consideration of these criticisms can improve the decision making process dramatically by bringing a measure of the power of the scientific method to the making of major technical decisions.

In a classified project, the vested interests which grow around a decision can frequently prevent the questioning of authority necessary for the elimination of error. Peacetime classified projects have a very bad record of rejecting imaginative suggestions which frequently are very threatening to the existing political power structure.

When technical information is classified, public technical criticism will inevitably degrade to a media contest between competing authorities

When technical information is classified, public technical criticism will inevitably degrade to a media contest between competing authorities and, in the competition for attention, it will never be clear whether politics or science is speaking. We then lose both the power of science and the credibility of democratic process.

Corruption is a progressive disease. It diffuses from person to person across society by direct observations of its efficacy and its safety. The efficacy of the abuse of secrecy for interagency rivalry and for personal advancement is well illustrated by the array of abuses listed in Sec. 1.6(a). The safety of the abuse of secrecy for the abuser is dependent upon the enforcement of the Section. As abuses spread and become the norm, enforcibility declines and corruption diffuses more rapidly.

However, diffusive processes take time to spread through an organization, and this makes it possible for secrecy to make a significant contribution to national strength during a crisis. When a new organization is created to respond to an emergency, as for example the scientific organizations created at the start of WWII, the behavior norms of the group recruited may not tolerate the abuse of secrecy for personal advancement or interagency rivalry. In such cases, and for a short time, secrecy may be an effective tactic. The general belief that there is strength in secrecy rests partially on its short-term successes. If we had entered WWII with a well-developed secrecy system and the corruption which would have developed with time, I am convinced that the results would have been quite different.

Secrecy Exacerbates Divisiveness: the SDI Example

Reagan's Executive Order, previously referred to, provides another clue to the power of openness. The preamble states;

" It [this order] recognizes that it is essential that the public be informed concerning the activities of its Government, but that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure."

The tension in this statement is not resolved in the order. It may be informative to attempt a resolution by considering a concrete example, namely the Strategic Defense Initiative. SDI symbolizes one of the conflicts, clearly exacerbated by secrecy, which currently divide us.

I would assert that there are unilateral steps toward openness which we could take, and which would leave us more unified and stronger, even if no reciprocal steps were taken by the Soviets. I propose that we start unclassified research programs designed to provide scientific information needed for making public policy. If these programs are uncoupled from classified programs, their emphases would not compromise classified information. Their purpose would be to provide a knowledge base for public policy discussions. These programs would not reveal the decisions taken secretly, but a public knowledge base would reduce the debilitating divisiveness fostered by secrecy.

The Strategic Defense Initiative provides a classic example of debilitating divisiveness. Countermeasures to SDI are deeply classified. The deadly game of countermeasures and countercountermeasures will probably determine whether SDI is successful or a large-scale Maginot Line. At the present time, classification of the countermeasure area trivializes the public debate to a media battle between opposed authorities offering conflicting interpretations of secret information.

An example of this game is decoying vs. discrimination. If the offense can proliferate a multitude of decoys which cannot be discriminated from warheads by the defense, SDI will not succeed. Knowing a decoy design would of course make it easier for an adversary to discriminate it from a warhead. It is therefore very important that such designs be carefully guarded. On the other hand, maintaining secrecy over the scientific and engineering research basic to the decoying-discrimination technology would, for the reasons discussed earlier, make it much more difficult to provide assurance to the public that all avenues had been explored. Indeed, a substantial part of the criticism of the feasibility of SDI turns on the possibility that an adversary would invent a countermeasure for which we would be unprepared.

The Cryptography Case: Uncoupled Open Programs

We can learn something about the efficiency of secret *vs.* open programs in peacetime from the objections raised by Adm. Bobby R. Inman, former director of the National Security Agency, to open programs in cryptography. NSA, which is a very large and very secret agency, claimed that open programs conducted by a handful of matheticians around the world, who had no access to NSA secrets, would reveal to other countries that their codes were insecure and that such research might lead to codes that even NSA could not break. These objections exhibit NSA's assessment that the best secret efforts, that other countries could mount, would miss techniques which would be revealed by even a small open uncoupled program. If this is true for *other* countries is it not possible that it also applies to us?

Inman (1985) asserted that

""There is an overlap between technical information and national security which inevitably produces tension. This tension results from the scientists' desire for unrestrained research and publication on the one hand, and the Federal Government's need to protect certain information from potential foreign adversaries who might use that information against this nation.""

I would assert that uncoupled open programs (UOP) in cryptography make America stronger. They provide early warning of the capabilities an adversary might have in breaking our codes. There are many instances where secret bureaucracies have disastrously overestimated the invulnerability of their codes. In this case I see no tension between the national interest and openness. The cryptographers have provided a fine case study in strengthening the weapon of openness.

Consider then the value of starting unclassified, relatively cheap, academic research programs uncoupled from the classified programs. These UOP could provide the more solid information on countermeasures needed for an informed political decision on SDI, just as the open cryptography research has taught us something about the

security of our codes. If indeed SDI's critics are right about the opportunities for the invention of countermeasures, then the UOP would provide an opportunity to make a conclusive case. On the other hand if the open programs exhibited that SDI could deal with all the countermeasures suggested and retain its effectiveness, its case would be strengthened.

More openness will do more

to increase our military strength

than it could possibly do to increase

the military strength of our enemies

These open programs would indeed be shared with the world. They would strengthen the U.S. even if there were no response from the USSR by reducing corruption by secrecy, by improving our decision making, and by reducing our divisiveness. Undertaking such programs would exhibit our commitment to strengthening the weapon of openness. Making that commitment would enable democratic control of military technology. More openness, reducing suspicions in areas where Americans are divided, will do more to increase our military strength by unifying the country and its allies than it could possibly do to increase the military strength of its enemies.

The Weapon of Openness and the Future

Bohr's phrase which was the keynote of this article was invented in an effort to adapt to the demands for social change required to live with advancing military technology. Unfortunately Bohr's effort, to persuade FDR and Churchhill of the desirability of more openness in living with nuclear weapons, was a complete failure. There can be no doubt that the future will bring even more rapid rates of progress in science-based technology. Let's just mention three possibilities, noting that these are only foreseeable developments and that there will be surprises which, if the past is any guide, will be still more important.

Artificial Intelligence is advancing, driven by its enormous economic potential and its challenge in understanding brain function.

Molecular biology and genetic engineering are creating powers beyond our ability to forecast limits.

Feynman some years ago wrote a paper entitled **"There's Plenty of Room at the Bottom"** pointing out that miniaturization could aspire to the huge advances possible with the controlled assembly of individual atoms. When the possibility of the construction of assemblers which could reproduce themselves was added by Eric Drexler in his book ***Engines of Creation***, a very large expansion of the opportunities in atomic scale assembly were opened up. This pursuit, today known as

nanotechnology, will also be driven by the enormous advantages it affords for health and for human welfare.

But each of these has possible military uses comparable in impact to that of nuclear weapons. With the aid of the openness provided by satellites and arms control treaties, we have been able to live with nuclear weapons. We will need much more openness to live with the science-based technologies that lie ahead.

Dr. Kantrowitz *is a professor at the Thayer School of Engineering at Dartmouth, and former Chairman of Avco-Everett Research Lab. He serves as an Advisor to the Foresight Institute.*