Classification and compartmentation

Protecting Satellite Reconnaissance Photographs

(b)(3)(c)

A powerful intelligence organization can develop sources of information of a value utterly beyond price. . . .

The revelation of such sources or even a hint of their identity will cause their extinction. . . .

Security is like armor. You can pile on the armor until the man inside is absolutely safe and absolutely useless.

Sherman Kent, 1949

Sherman Kent anticipated the dilemma that the imagery intelligence community has faced over the past 30 years: how to protect a space reconnaissance capability that has proved its value beyond price, yet avoid becoming so secretive about this capability that it becomes useless?

The community has struggled with this problem since 1960, when President Eisenhower directed establishment of the TK System as a Sensitive Compartmented Information (SCI) control system for the protection of intelligence and mapping products acquired by imaging reconnaissance satellites. This SCI "armor of security" has been maintained for more than three decades because the investment in satellite reconnaissance has been high, the benefits enormous, and the community has been convinced that wide dissemination of the intelligence product would increase the probability of a compromise that could result in neutralizing the investment.

The SCI control system for satellite imagery grew out of a mind-set in the 1960s and 1970s that saw all aspects of the US imaging satellite reconnaissance program as representing the state of the art. The view of satellite reconnaissance as a fragile collection capability was reinforced by evidence of Soviet countermeasures against US imaging operations.

The strict need-to-know criteria for imaging satellite reconnaissance products was given its first relief in January 1966, when the DCI's Committee on Overhead Reconnaissance published guidelines for the non-SCI dissemination of sanitized intelligence and mapping products. But it was not until November 1973, when President Nixon downgraded the "fact of" an imaging satellite reconnaissance program to Secret, that attributable imagery and related intelligence products could be disseminated at the Secret level outside of SCI control. Even though most of the intelligence products were eligible for Secret-level dissemination, the focus was on meeting specifically identified high-priority military and intelligence requirements. As a result, most of the imagery-derived intelligence remained under SCI control.

In 1978 President Carter authorized unclassified acknowledgment of the "fact of" photo satellite reconnaissance activities. This created an environment within the community that was open to development of further policy modifications. These modifications, which were implemented in 1982, resulted in making almost 98 percent of the imagery-derived products eligible for decompartmentation and subsequent dissemination at the Secret level. Continued SCI control, however, was mandated for the imagery used for intelligence analysis, the Primary Imaging Record (PIR). This resulted in maintaining a rather robust SCI infrastructure for much of the product, as well as this basic PIR and all its full-format reproductions.

In 1992 the Department of Defense publicly acknowledged the existence of the National Reconnaissance Office and its role in developing and operating US reconnaissance satellites. This was followed by an extensive review of compartmentation under a DCI Classification Review Task Force. The CRTF considered a series of proposals focused on making fundamental changes to the security policy for protecting and handling imaging satellite reconnaissance products. As a result of this effort, the Central Imagery Office (CIO) has been preparing a series of proposals for the DCI. On 2 February 1994 the DCI approved the first of these, which recommended the automatic decompartmentation and Secret-level dissemination of almost all satellite reconnaissance imagery. The DCI is now considering other CIO proposals that would further liberalize the security controls over satellite reconnaissance imagery and its products.

The findings of the CRTF, along with other pressures, make it only a matter of time before the White House authorizes the DCI to declassify much of the early reconnaissance imagery in the archives. A fundamental finding of the CRTF is that the technologies and capabilities associated with many of these older imagery programs no longer exceed today's unclassified state of the art. At the same time, the environmental community has concluded that classified imagery offers data "of unparalleled significance to environmental issues." Additionally, the industrial sector is looking to older classified technology as a marketing opportunity. Finally, the findings of the National Performance Review, along with the Intelligence Community's new openness with Cold War records, has created a public expectation for declassification of older reconnaissance imagery, information that is seen as a primary source for scholarly research.

The Nature of Imagery

The task of determining the sensitivity of satellite reconnaissance imagery is difficult because of the unique nature of a picture—a medium that has both high information content and high ambiguity. A photographic image is a complete record of a scene, and it reflects a wealth of information about what is depicted in it. In addition to information about the scene, an image contains unique information about the imaging system that acquired the picture. The image actually is a record of complex data that requires experienced analysts to extract the full range of embedded information. As a first step to understand why the imagery intelligence (IMINT) community has maintained a conservative approach to the classification and compartmentation of imaging satellite reconnaissance products, it is useful to examine the nature of the embedded information, its ambiguity, and the uncertainty of its sensitivity.

Content Information

Satellite pictures can record an enormous amount of information about a significant portion of the Earth's surface, over 1,000 nautical miles in a single frame. This extensive data record of a large geographic area is preserved and displayed on a small piece of acetate film (or, alternatively, on a comparatively small cathode ray tube). Imaging systems can capture and display more information on a single piece of acetate or its equivalent than the human brain can extract from a comparable display on the retina. At 0.6 mile the eye is limited to seeing a small area of high-contrast objects that are spaced no closer than 8 inches.

(b)(1)
(b)(3)(n)

Imaging freezes time for a particular event, stops motion for a particular activity, and captures virtually the totality of information within a particular field of view. The image comes close to becoming a complete reproduction of that reality. In stereoscopic imaging, even the three dimensions of reality can be replicated. The picture is constrained in its information content only by the limits of the optics and recording medium. Other visual information records, like a drawing, sketch, or the written word, are constrained in their information content by the discrete symbols that represent the information being depicted. The photographic record can capture a view of reality with its full information content. An image, then, becomes as sensitive as the information in the scene being imaged. Sometimes the mere fact that the observer is aware of an activity in a scene is, by itself, sensitive. In this way, both the image of the scene, as well as a textual description of the scene content, can be sensitive.

The content information in an image can have a wide range of sensitivity. A particular scene can include information with both high-content sensitivity and information with low-content sensitivity. For example, a sensitive, clandestine, terrorist staging area can be imaged adjacent to a known, nonsensitive rail line. To

(b)(1)
(b)(3)(n)

Technical Information

Another unique aspect of an image is the fact that it also contains technical information about the imaging system. Analysis of an image will provide insight into the operation and capabilities of the imaging system. This does not always require a sophisticated analysis. Simply viewing a picture usually will reveal the position of the camera in relation to the imaged scene. It becomes clear whether the particular scene was imaged from a horizontal, ground-level perspective, or imaged from an overhead, vertical perspective. In addition, a simple geometric analysis of an overhead image will reveal whether the imaging system was on an airborne or spaceborne platform. Before 1972, when the "fact of" space reconnaissance was maintained under SCI control, all satellite imagery—because it inherently revealed this "fact of"—also had to be maintained under SCI control. And it is only since 1978, with declassification of the "fact of," that proposals to declassify satellite images can be considered.

Further analysis of an image will disclose other parameters, such as acquisition information (altitude, position over Earth); camera description (focal length, resolution, conventional optical or electro-optical nature)(b)(1) (b)(3)(n) the same time, any individual part of the PIR (a "cropped" image or film "chip") often comes close to being the equivalent of the whole in terms of what can be disclosed about the imaging system through analysis of that film chip.

(b)(1)
(b)(3)(n)

Information Record

The shapes and patterns of a particular feature depicted in an image only begin to take on meaning when they are perceived in relation to the background and the neighboring features shown on the image. Factors such as brightness, tone, contrast, scale, resolution, and resolving power all contribute to ambiguity and complicate analysis.

The subjective process of interpreting or analyzing photographic images can often result in multiple interpretations of the same information. The animal drawings clearly illustrate this perceptual problem. Figure 1A is a line drawing of nine ducks with only the head of the center "duck" showing. Figure 1B is a similar drawing of nine rabbits. Only the head of the center "rabbit" is showing. When the two center drawings are compared, it becomes obvious that they are identical images. What

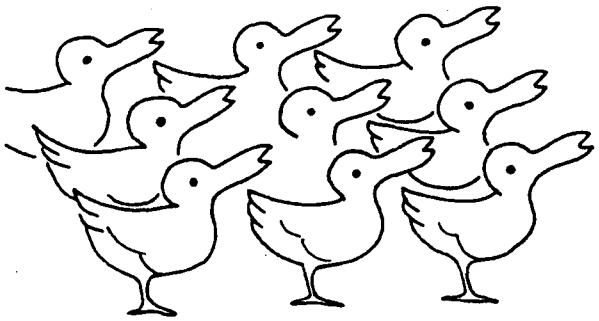

Figure 1A
Drawings from BIOPOLITICS by Thomas L. Thorson, copyright 1970 by Holt, Rinehart and Winston, Inc., Reproduced by permission of the publisher.

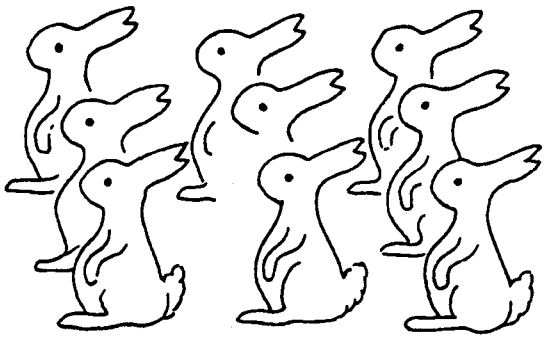

Figure 1B

initially was perceived as a duck, can also be seen as a rabbit. It is either a duck or rabbit or neither, depending on the context of the analysis.

The imagery analyst has to interact with outside information, as well as the representations of reality recorded in the image. As new collateral information becomes available, analysts often may need to return to the image; frequently repeated analyses are required before the critical information becomes apparent. This is the nature of human perception and a characteristic of imagery. The real intelligence value—and the true sensitivity of the information content—may not become known until long after acquisition and repeated analyses. While an image on first inspection may not reflect anything unusual, subsequent detailed analysis may reveal unique information not previously observed in the scene.

The information record is both ambiguous and complex. The content and technical information in the image often are commingled. Reporting one kind of information can inadvertently reveal the other. For example, though a consumer might have little interest in embedded technical information—with the exception of how it might be an indicator of source credibility—this does not simplify separating content and technical information. The fact that the information is commingled will preclude "sanitizing out" the technical information from the content information, whether or not it is sensitive.

The ambiguity and complexity of the information content of an image have contributed to the difficulty in deciding how to protect only what is sensitive and give wide dissemination to what is not sensitive. It may not always be clear at first inspection what the full information content of an image is, or what the meaning of the information is. At the same time, the complex commingling of the embedded information has made it difficult to separate sensitive from nonsensitive information. Because of this ambiguity and complexity, the community has been reluctant to disseminate broadly the PIR and tended to err on the conservative side. Over the past 30 years the decision to keep the entire PIR under compartmented SCI control has been an effort to protect future, unknown, sensitive intelligence discoveries and served as a hedge against uncertainty.

(b)(1)
(b)(3)(n)

Predicting Information Sensitivity

It is difficult, if not impossible, to predict with complete confidence the sensitivity of an image before its collection and subsequent analysis. To some extent it may be possible to anticipate the general information content and sensitivity of a photograph. The best that one can hope to do, however, is to develop a general expectation that a particular image will likely contain sensitive information.

For content sensitivity, an analyst might be able to develop a general prediction about how likely it would be for an image to include coverage of a sensitive activity.

(b)(1)
(b)(3)(n)

(b)(1)
(b)(3)(n)

It is the reality of being uncertain about the national security sensitivity of imagery that has reinforced the argument to protect the entire PIR in SCI channels. Only after frame-by-frame analysis could broader dissemination be given to those portions of the PIR that were identified as nonsensitive. The basic principle for 30 years has been "all imagery is presumed sensitive until analyzed and proven otherwise."

The Vulnerability of Imaging Satellites

The imaging satellite reconnaissance program has a limited number of assets fixed in space and time. The satellites are few in number and highly predictable—cost and technology limit their number, and the laws of physics determine their orbits and schedule. Their orbital deployment, at any particular time, represent the total US Government investment in imaging satellite reconnaissance.

(b)(1)
(b)(3)(n)

Information Denial

During the Cold War, the USSR was a primary target for US imaging reconnaissance satellites, and US policymakers closely watched for Soviet responses. The Soviet Government was sensitive to foreign governments collecting any information, especially space reconnaissance information.

(b)(1)
(b)(3)(n)

The Soviets had instituted a program that was nationwide in scope and consistent with *maskirovka*—a general doctrine designed to deceive, confuse, and deny information to enemy intelligence in peacetime and in wartime.

(b)(1)
(b)(3)(n)

Concealment

Soviet concealment activities constituted a broad effort to conceal from overhead view items or activities of potential military value, many of which previously had not been afforded such protection.

(b)(1)
(b)(3)(n)

Deception

(b)(1)
(b)(3)(n)

Evidence of extensive Soviet countermeasures raised serious concerns for the Intelligence Community. First, the community saw Soviet denial of information to US reconnaissance satellites as limiting the capability of the satellites.

(b)(1)
(b)(3)(n)

Intelligence analysis would be based on incomplete information. Second, the community saw Soviet deception directed at US reconnaissance satellites as resulting in flawed intelligence analysis.

(b)(1)
(b)(3)(n)

Intelligence Community's fear of either being denied information or being deceived by false information resulted in strong incentives to maintain strict classification and SCI control over satellite reconnaissance products.

(b)(1)
(b)(3)(n)

Countermeasures as Response to Knowledge

During the 1980s, there appeared to be an increase in the number of espionage cases and leaks related to imaging satellite reconnaissance. There also was increased speculation about US reconnaissance capabilities in the press and in scholarly literature.

With this increased public awareness of US success with imaging satellite reconnaissance, the USSR and other targeted governments appeared to put greater emphasis on information denial countermeasures.

(b)(1)
(b)(3)(n)

This line of reasoning reinforced the argument for maximum protection of the satellite IMINT product. The pressure for continued TK control was even greater when imaging satellite reconnaissance was viewed as a high-cost, high-value program.

Developmental Cost

The US Government had invested billions of dollars to acquire an imaging satellite reconnaissance capability. The level of technology necessary to develop the current constellation, which can produce a large volume of high-quality images on a near-real-time basis, is costly in terms of both time and money. R&D efforts have to be programmed years in advance to develop a system. At the same time, the dollar cost can run into the billions. For example, the total cost during the life cycle of one of the deactivated, film return systems was some

(b)(1)
(b)(3)(n)

Unique Value

The true value of acquired imagery is difficult to quantify. What figure can be assigned to an accurate and up-to-date target folder that is used during a combat strike mission? What value equates to evidence of an arms control violation? What is the value of intelligence that otherwise would not have been known had it not been acquired by imaging satellites? And what is the value of a capability that takes 4 years to develop when you need it today?

Imaging reconnaissance satellites have demonstrated their value by responding to a wide range of difficult and critical intelligence questions. In the case of historically denied areas, such as the former Soviet Union, they have been one of very few intelligence sources able to collect information. They also have supported a broad spectrum of other requirements: monitoring arms control agreements, developing targeting materials, maintaining order of battle data bases, deriving intelligence from foreign scientific and technical activities, assessing economic strength, providing indications of impending hostilities, and searching for unknown targets.

Changing Attitudes

Until the 1990s the Intelligence Community was convinced, although not universally, that the threat of countermeasures justified the implementation of stringent SCI controls. Recently, the mood has been changing. The new mood, as reflected in recent DCI decisions, sees a decline in the risk of countermeasures and an increased need for wider dissemination of imagery. The trend to relax the tight SCI security controls is consistent with the changing US political and policy environment.

- With the end of the Cold War, there is a growing perception that the international community is becoming more open. Reconnaissance satellites are not the only source of overhead imagery. As a result, there is less of a need to protect the overhead intelligence source. The mere "fact of" acquiring such information is no longer sensitive.

- Regional conflicts and coalition peacekeeping are beginning to dominate the international scene. Experiences, such as those in Desert Storm, have underscored the value of satellite reconnaissance imagery in supporting these military operations, as well as the need to share IMINT with coalition partners. Strict SCI control is inconsistent with this. Policymakers are concluding that the value in disseminating and using IMINT outside of TK channels outweighs the traditional security risks.

- There is new emphasis on environmental problems, and national security tools are being called on to address them. This has created pressure to decompartment, and even declassify, much of the imaging satellite reconnaissance product to support this effort.

- The US no longer has a monopoly on sophisticated remote sensing from space. What was a unique technological breakthrough on 18 August 1960—imaging 1,650,000 square miles of Soviet territory with a capability to see ground objects of some 35 feet—is no longer state of the art. Today's best commercial system, SPOT, has a resolution of 33 feet, and the planned French Helios intelligence system has an anticipated resolution in the 3.3 foot to 9.9 foot range. The proliferation of reconnaissance technology is no longer considered sensitive.

- US policymakers are becoming more concerned with economic competition than military competition. There is pressure to declassify reconnaissance technology so that US industry can use this technology to compete in the open market. What is the point in denying US businesses the opportunity to market a technology that foreign competitors will be marketing? Foreign sources will not comply with US Government attempts to protect the technology as national security secrets.

- There are pressures across the government for more openness as evidenced in the findings of the National Performance Review. The Intelligence Community Implementation Plan calls for reviewing current classification policies, using the lowest practical levels of classification. There also are recommendations to develop programs to educate the public on intelligence. This philosophy will make it increasingly difficult to maintain strict SCI controls for all aspects of satellite IMINT.

Despite pressures to use satellite reconnaissance for non-national security applications, there will continue to be intelligence challenges that need a viable imaging satellite reconnaissance capability. These challenges include the proliferation of nuclear and other weapons of mass destruction; the threat of terrorism; worldwide environmental assaults on the Earth's ecosystem; and support to regional military conflicts. The dilemma will be to respond to these new pressures for expanded use, yet continue to provide adequate security so that satellites can effectively continue to support the traditional national security requirements—the future Desert Storms, the future Iraqi violations of international agreements, and the future North Korean nuclear proliferations. Policymakers will look to the Intelligence Community to find novel ways to increase the utility of IMINT products while still protecting critical capabilities and successes in observing the Earth's surface from above.

With the approval and implementation of CIO recommendations to decompartment almost all the satellite IMINT products, the issue of whether imaging satellite reconnaissance material should remain classified or be declassified for public use now will be debated.

As this new issue is addressed, the Intelligence Community will have to consider whether the move to declassification will set precedents that require new legislation—legislation to raise the community's confidence level that the DCI will have the necessary authority to ensure protection of any remaining sensitive reconnaissance material. At the same time, the community will have to address the resource implications of conducting classification reviews and responding to an increasing number of Freedom of Information Act requests.

The fundamental policy question today is what degree of protection and what kind of security framework are necessary and appropriate for the current environment, especially with its new complexity and demands for wider dissemination of imagery? We do not want to expose our satellite reconnaissance capability and its successes so completely that we encourage and facilitate the development of fatal countermeasures. At the same time, we do not want to "pile on the armor until the reconnaissance capability is absolutely safe and absolutely useless." The challenge as we move toward the year 2000 will be to develop a security framework that will protect two categories of imaging satellite reconnaissance information:

(b)(1)
(b)(3)(n)

The new criteria for classifying reconnaissance data should focus less on identifying sensitive technology and more on identifying the kinds of information that reveal US successes in intelligence collection and analyses. The publicizing of these successes may represent the greatest potential damage to intelligence sources and methods. It is one thing to know intellectually that a technical capability is possible; it is another to have

hard evidence of that success. It is being confronted with the success that will provide the knowledge, as well as motivation, for countermeasures.

In addition to balancing the need to protect intelligence sources and methods versus the requirement for wider dissemination and increased utility, policymakers will need to consider economic impacts. What is the cost to national security of replacing a reconnaissance investment that might be lost as a result of compromised critical information? Funding for new national security projects is now more difficult than it was in the 1980s.

If security rules require classifying most space reconnaissance technology, US industry will be prohibited from using this technology to compete in the international market, and this could erode our industrial base, which is looking for new non-national security markets. What is the cost to US industry if the Intelligence Community declassifies and publicly disseminates high-quality imagery—the same kind of imagery US industry hopes to market? This could erode the economic opportunity to market high-resolution imagery.

Despite these new economic questions, the core national security questions will remain: are we moving toward decompartmenting and declassifying information that could be used by foreign powers to collect intelligence more effectively against the US, and are we moving toward decompartmenting and declassifying information that potential targets could use to counter our reconnaissance operations and neutralize this national security asset? In answering both sets of questions, DCI Woolsey has warned against disclosing any information that could jeopardize the nation's security: "Our intelligence assets and capabilities are precious commodities—we invest heavily to develop and maintain them—and there are those who would benefit from the information to the detriment of our security."

~~*This article is* SECRET~~