Countersabotage--a Counterintelligence Function

~~SECRET~~

Eric W. Timm

Counterintelligence in its most elementary form creates channels through which enemy agents must pass. Port security control, censorship, and interrogation camps for prisoners of war are such channels. These control channels, however, can be made effective only when the enemy's potential and our own situation have been analyzed and the balance struck between hostile forces and friendly facilities.

Counterintelligence operations consist of obtaining and analyzing information on the adversary and then using it against him in accordance with the requirements of the situation and in the light of our knowledge of his practices and psychological outlook. An ideal counterintelligence system anticipates the enemy's move, notionally satisfies his needs, and indeed operates a notional intelligence service for him. This deception eliminates or at least minimizes the introduction of unknown enemy agents, lulling the enemy into a false sense of security. When properly carried out, counterintelligence operations will prevent the enemy from mounting intelligence operations.

A store of accessible information on the hostile intelligence system is necessary to realize this objective. We must know well the organizational

structure of the enemy's service, his personnel in key posts, his methods of recruitment, how he trains his agents and dispatches them on missions, and about many other of his activities and functions, both specialized and routine. Such a store is developed from a flow of accurate, detailed information maintained in properly indexed files.

Sabotage

The term sabotage is of ancient origin, deriving from the French *sabot*, or wooden shoe. In feudal times the peasants, with whom the sabot was traditional, used it to stamp down the landowner's crops. Later, during the industrial revolution, they took off their shoes and threw them into the machinery, thinking thereby to eliminate their unemployment by destroying its cause. Countersabotage is therefore counter-destruction in broad and varied senses. Almost every security measure we adopt has countersabotage implications.

Strategic sabotage is mounted against a specific critical target such as an essential production facility, though the importance of the target may sometimes not be generally recognized. A target of the German saboteurs sent to the United States in 1942 was a little-known plant in Philadelphia which, however, was the only source of supply for a necessary ingredient of aluminum; its destruction might have had serious results. The physical appearance of an industrial plant is not always an accurate indication of its importance.

Tactical sabotage operations are normally planned in conjunction with military operations and usually precede them. The destruction of railroad lines, bridges, and highways to hinder enemy movements are examples of tactical sabotage.

A countersabotage officer must put himself in the position of the saboteur. He must imagine what he would do if he had been given the enemy's training and partook of his psychological outlook. Ideally, every potential target should be protected in every possible way, but this ideal is obviously impractical. So we try to make the enemy sabotage agents come to us, compelling them to pass through the channels we have set

up before they can reach our vulnerable points.

The saboteur operates under physical and psychological handicaps. He must protect himself, and he can carry only so much weight. For these reasons he usually prefers self-destroying targets, such as ammunition dumps, gasoline stores, and other inflammable or explosive concentrations. The effects of a simple explosion can nevertheless not be disregarded: targets which perform functions entirely disproportionate to their size, like power plant generators, electric turbines, and mine shafts, are highly strategic. But we may assume that the saboteur will leave modern buildings, dams, concrete roads, and similar structures alone; these cannot be effectively sabotaged. All available targets must be thus analyzed before protective forces and equipment are assigned.

Analysis of Vulnerabilities

Since knowledge of sabotage possibilities is the first requisite in forestalling them, countersabotage officers must know how to make security surveys. If a modern factory building is most difficult to damage, it is still liable to what could be called nuisance sabotage, which would not destroy the plant but might curtail its operation for periods of time. A modern fireproof plant located on an island might be effectively attacked by blowing up the two bridges which provide access to it. Early in the war the security of the bridges to such a plant was completely overlooked while the most extreme precautions were taken to prevent unlawful entry into the plant itself.

Many factories are vulnerable in their electric power supply, and the destruction of power plants or lines can do grave damage. The intelligence officer cannot devote all his effort to protecting exclusively what he can see. He must determine what keeps the factory running, what facilities if damaged would cause it to close down. When these elements are identified, no matter how far they may be from the installation itself; they must be protected against sabotage.

Any plant that houses large machines falls into the category of a self-destroying target, and any complex system has vulnerable nodes. A small explosion in the turbine of a power station will throw the machine

off balance and cause it to tear itself apart. A train derailed on a bridge or in a tunnel will tie up a railroad line. The destruction of a single switchboard can be more effective in tying up a communications system than blowing up miles of telephone line. In planning countersabotage measures careful thought must be given to what targets would be most profitable to an enemy and fit into the complexion of his past activities.

The Counterintelligence Function

The countersabotage officer functions in almost the same way as an expert in counterespionage, and there is normally no difference in personnel qualifications for these assignments. Counterintelligence officers must be trained in both. Our best protection is to catch the saboteur before he begins to operate, because perfect physical protection is impossible.

We function most efficiently when we catch a saboteur, obtain through interrogation the information he has, fit his data into our mosaic of knowledge, and revise our operations to apprehend other saboteurs operating in the same manner. This is the first line of defense in countersabotage. Guards, gates, lights, and alarms are merely rear echelon defenses to back us up in case we fail.

In the counterintelligence officer's eyes espionage agents and saboteurs are virtually identical. Now and then the possession of a sabotage device may lead to the capture of a saboteur, but this is rare. Failure to find sabotage equipment on an individual crossing the frontier certainly does not mean that he is not a saboteur. Intelligence services have always trained their sabotage agents to make equipment on the spot and told them where the ingredients can be found. In some cases the sabotage materials may be cached for later use. Guards and security patrols should keep watch for suspicious items, but we cannot rely on this defense. In addition to the saboteur who comes in empty-handed and relies on cached devices or his own construction, there are those recruited from residents of the country who do not have to cross the frontier.

Thus the central mission of a countersabotage officer is the same as that of an expert in counterespionage--the utilization of knowledge to

guide executive action. In order to perform this function efficiently we must strive constantly to increase our store of information by interrogations and operational means. In addition, the countersabotage officer must supply to security and plant-protection officials the data they require to do their job; and in order to do this properly he must be well acquainted with their job. In all cases information concerning new sabotage devices and targets must of course be handed on as quickly as possible.

Plant Security

Behind our first line of defense, the operations officer, is erected the second line, consisting of obstacles placed around possible targets. These obstacles may be animate or inanimate, and their number and character varies with the importance and nature of the target. Highest-priority targets should be flood-lighted, patrolled, surrounded by fences, and guarded by armed sentries. But most targets cannot be given such elaborate protection, and many must rely on mere physical defense--walls, ditches, electrified or barbed-wire fences, locks and bars.

In theory, of course, these physical defenses can be breached, as indeed any guard system can. In actual fact, however, they are rather effective. The usual sabotage agent will approach with qualms the execution of his mission. When he was in training, failure to evade the obstacles put in his way did not mean death; but now he faces the real thing. He may rationalize his fears and substitute a less well protected and less important target, especially if he lacks strong ideological motivation.

Our saboteur may, instead of making a surreptitious breach of the defenses, try to gain legitimate access by some stratagem. He could then plant fused bombs or other devices for delayed-action sabotage and when the explosion or fire occurred be many miles away. Our second line of defense, therefore, includes measures to identify persons who are entitled to entrance and keep out the unauthorized. This defense rests with the plant guard system.

The guards may be either civilian or military, but in either case they should be thoroughly investigated. Once a guard force has been

established, some of the measures to be taken for its effective operation are the following:

> an identification or badge system; limited points of access; irregular patrols; controlled package delivery and check of lunch boxes; check of lockers and other private facilities inside the installation; escort for all unauthorized personnel inside the installation; inspection of unidentified or unordered deliveries before acceptance; control of railroads and harbor facilities near the installation.

Employees should be instructed to keep their eyes open for strange or unusual objects that may be lying about. They should be instructed in sabotage camouflage techniques. When practical, the installation may be compartmented and a different-colored badge used for each section to reduce access to sabotage targets and limit the number of possible suspects if sabotage should be attempted.

The countersabotage officer cannot know everything about all types of installations, and he should of course not pretend to knowledge he does not have. Officials of the installation who know it intimately should be consulted, and it is always well to ask them how *they* would go about sabotaging the plant.

Investigations

Although the investigation of sabotage incidents is not, strictly speaking, within the scope of the countersabotage officer's responsibility, he is interested in the results of investigation, because a physical attempt at sabotage means that our first line of defense has been breached. Someone failed. The results of the investigation must be studied to see what can be added to our store of knowledge. We must learn the identity of the saboteur, the techniques he used, how his operation was mounted, and by whom he was dispatched. He may know the identities of other sabotage agents and something about other operations.

The following are some of the initial points that must be examined in the

investigation of an apparent act of sabotage.

Was the incident in fact sabotage or merely an industrial accident?
Eye-witness and other first-hand accounts of the event must be obtained.
An expert description of the explosion or fire must be provided and every effort made to determine whether it was intentional or accidental.
The area must be examined carefully for remnants of sabotage equipment, incendiary elements, or explosives.
(The investigator would be well advised to get himself good and dirty in poking around the scene.)
If the damage was done by fire the color of the smoke must be determined; it may show the type of incendiary used.

As in all criminal investigation, sabotage incidents require a tedious and exhaustive checking of all pertinent details. An explanation must be sought for anything that varies even slightly from the normal.

~~SECRET~~

Posted: May 08, 2007 07:47 AM