U.S. Department of Justice
National Institute of Justice

International Summaries

A Series of Selected Translations in Law Enforcement and Criminal Justice

National Institute of Justice/NCJRS
NCJ 107152

From West Germany

Bank Robbery and Technology: Does Technology Affect Security?

The behavior of employees is of greater significance than the mere presence of physical security.

By Heinz Buechler
and Heinz Leineweber

Introduction

The increase in bank robberies in the Federal Republic of Germany (FRG) calls into question the effectiveness of technological security systems. This study is the first to examine the security technology used for the past 20 years in the German banking industry. The increasing calls for removal of security systems due to their cost and questioned value in preventing robberies are the reasons for this study.

The report looks at attempted and completed bank robberies as portrayed in the Federal Bureau of Criminal Investigation files; it also includes robberies where hostage-taking occurred. The term "bank robbery" is used in its broad criminological sense and the strict penal distinction between robbery and extortion is ignored.

This is a summary of *Bankraub und technische Pravention*, Federal Bureau of Criminal Investigation Research Series, Vol. 18, Wiesbaden, West Germany. 1986. 213 pp. NCJ 106495. The original document contains a bibliography and appendixes. Summary published Spring 1988.

Purpose and methodology

The authors compiled data on the place, time, and duration of the robberies, as well as on the robbers' personal characteristics. They examined the effectiveness of alarm systems, optical surveillance (electronic eye monitoring devices and cameras), and physical security (primarily bulletproof structures, but also special-access doors, etc.) in preventing or stopping a robbery in progress. Comparisons with earlier studies show whether technological security has changed the nature of bank robbery. Also explored are the robbers' reactions to the situations they are confronted with during robberies (such as activation of surveillance equipment), and the interaction among robbers, employees, and/or customers in the presence of security technology.

Police and criminal prosecution files and banking association statistical reports covering the period from January 1, 1981, to June 30, 1983, provided the data. A high degree of reliability exists since one source was used to check the other. It was felt that a 2½-year period was sufficient to reflect developing tendencies. The 1,828 cases occurring in this period were arranged chronologically, but for this study approximately every other case was examined, for a total of 963. The methodology used is a form of content analysis that seeks to understand the objective quality of the robbery and the subjective experience of those involved.

The development of bank robbery in the FRG

According to police statistics, bank robbery increased 169 percent from 1971 to 1984, and the rate of successfully solved cases remained constant. However, in comparison with other forms of robbery, which increased during those years at a steady rate, bank robbery decreased in 1974, 1980, and 1983. Physical and technological security devices were installed during these three years. The 1983 drop is attributed to optical surveillance equipment.

Case-related research results

Place

While the highest percentage of cases (25.9 percent) occurred in communities of less than 5,000 population, these areas experienced a drop in the overall rate of

bank robbery (down from 62 percent of all cases between 1962 and 1964). City centers also experienced a drop (from 23.1 percent in the mid-1970's to 12.1 percent at the end of the study period). An increase (from 19.8 percent in the mid-1970's to 31 percent) in the outlying districts and suburbs of large cities was also found.

Time of robbery

Most robberies occurred in the winter months (December through February). This is consistent with earlier studies. The choice of winter is explained by the earlier onset of darkness during normal business hours, which provides favorable getaway conditions. When the time of year is related to the time of day, it was found that in the winter the typical time of a robbery was between 4:00 p.m. and 6:00 p.m. Statistics show that the number of unsolved cases occurring at this time is strikingly higher than the yearly average. When cases were examined regardless of the time of year, it was found that most robberies occurred during opening and closing times. The number of robberies between 5:00 p.m. and 6:00 p.m. (the end of extended hours) is extremely high. Further, the critical importance of completing the robbery within the first 15 minutes after opening or in the last 15 minutes before closing is seen by the fact that the robbery success rate during these times is 79 percent.

Thursdays and Fridays (respectively) are the days most often chosen for robbery, with earlier studies showing a greater preference for Fridays. This shift is most likely due to the change in extended banking hours from Fridays to Thursdays. In earlier studies, the preference for Fridays was explained by the increased amount of money on hand. However, when the amount stolen was compared with the days of the week no significant monetary differences were found among the days.

Duration of the robbery

Speed is essential to success. The robber knows that he or she must finish as quickly as possible since the presence of advanced security technology will bring about an earlier arrival of the police. The rate of robberies accomplished in 3 minutes or less (87.3 percent) has doubled since earlier studies.

So-called "direct" robberies (where no hostages are taken) usually last 2 minutes. A comparison of robberies and their duration showed that a single robber took 1 minute while multiple robbers took 3 minutes or more (when hostages are taken, this relationship shifts—lone robbers most often take 3 minutes). Robberies occurring during business hours usually last 2 minutes, while those after hours take longer.

The role of technological security in bank robbery prevention

In the field of law enforcement, prevention has focused more on the crime itself than on the criminal. Using the concept of secondary prevention, those in the criminal justice field seek to change the opportunity for crime to the disadvantage of the potential criminal. From the robber's perspective, environmental factors combine to form an incentive or disincentive to commit the crime. Such factors may be the availability of a suitable object, the criminal energy necessary to execute the crime, and the risk of the crime being solved and the offender punished. Secondary prevention may increase the disincentive and thereby increase the surge of criminal energy necessary to commit the crime.

The following secondary prevention model is an ideal type—it should lead to an increase in the required surge in criminal energy for robbers and have an effect on their estimation of the risk involved and the usefulness of criminal behavior:

- Cash should not be readily available (as little ready cash as possible should be kept on hand).
- Optical surveillance of entrance areas to safes should be conducted and personnel should be trained to resist a robbery.
- "User-friendly" alarm systems should be installed, with personnel trained in their operation, and the presence of security guards should be visible.

Physical security devices

Since 1967, protective measures have been required of all banks and their branches. Bulletproof division of the work areas (teller windows from the areas where money is counted), and between areas used by or adjoining those accessible to customers, is required.

Bulletproof protection of employees

The presence of bulletproof structures is a necessary, though not a sufficient, condition for employee security. Employees must also be familiar with the operation of security devices, and use them.

While 85.1 percent of the victimized banks were outfitted with bulletproof protection, in 40.3 percent of the cases no employees were in a bulletproofed area. Employees were not in otherwise secured areas for 25.8 percent of the robberies.

A connection between the presence of physical security structures and the success of a bank robbery can be assumed. Of 128 attempts on banks not physically secured, 106 were successful; of 820 attempts on physically secured banks, 644 were successful. The absence of customers is next in importance to physical security in thwarting a robbery. A highly significant dependence exists between stopping a robbery and the lack of customers in the teller window area.

Has the use of physical security led to a higher proportion of unsuccessful robberies? This often-made positive relationship between the presence of security devices and attempted robberies is simplistic. Security devices *and* behavior of employees should be compared with success rates. It is false to conclude that an increase in security measures will hinder the robbers' success; the behavior of employees is of greater significance than the mere presence of physical security. Physical security structures are only of help when they are appropriately used—doors must be kept closed and keys taken from locks. And tellers must not open bulletproof glass to better hear a customer.

Alarm systems

Next to physical security structures, alarm systems are the most important security devices. They are defined as devices which emit an optical or acoustical signal to alert the public, or responsible people and institutions such as police or security agencies. The primary goal is to report a robbery and call for help as soon as possible.

Activation of the alarm

In 42.9 percent of robberies, the alarm was activated after the robbery; in 54.9 percent it was activated during the robbery—before and after money was handed over. The latter figure is a large increase over earlier studies.

In robberies lasting 2 minutes, the alarm was more often activated during the robbery; in those robberies lasting longer, the alarm was more often activated afterwards. This confirms the assumption that robbers planning a robbery of 2 minutes' duration seek to skirt the effect of the alarm system through speed in execution. Those planning robberies of longer duration attempt to hinder activation of the alarm system. Optical/acoustical alarms were found to be less effective than silent alarms since employees were aware of the increased risk and therefore activated these alarms hesitantly.

The capability of activating the alarm from outside the tellers' area is necessary if activation is to be attained during the robbery. In 45.5 percent of the cases studied another employee activated the alarm during the robbery. Since the robber's attention is most often focused on the teller (who is assumed to be at greater risk), other employees must be sensitized to the various ways they can react.

Optical surveillance systems

Optical surveillance systems include mechanical and electronic equipment which supply, store, and sometimes evaluate an image of a certain area for the purpose of surveillance. High quality photographs assist the police in reconstructing the crime and also provide courtroom evidence. The visibility of equipment may have a secondary preventative effect.

In 718 cases, optical surveillance equipment had been installed in the banks. In 217 of those cases it was not in use; in 28 cases its presence was unknown to employees. The authors suggest that the quality of the camera might figure in an employee's likelihood to activate it. If the noise created by the camera is loud, the employee may fear the robber's reaction.

Quality of photos

The quality of photographs taken by optical surveillance equipment varied greatly. Of the 473 cases in which the camera was in operation (out of the 963 total robberies), 306 produced excellent photos. Technical problems arose that caused pictures to be unusable in 86 other cases. This means that in only 31.8 percent of all 963 robberies were acceptable pictures available. This rate is considered unsatisfactory. Use of the camera at the teller window and in adjoining areas should be increased, and training of employees is also necessary.

Employee behavior

Specific behavior can have a direct effect on the course of a robbery. In half the cases the employees did exactly as the robber instructed, resulting in almost all of these robberies being successful. In the remaining cases, when employees tried to influence the course of events, the robbers were less successful. The rate of attempted robberies was clearly higher when employee behavior was a contributing factor in thwarting the robbery.

The authors isolated four types of employee behavior: (1) passive resistance (hesitation or refusal to hand over the money); (2) other resistance (lying, delaying tactics); (3) resistance by activating the alarm system; and (4) aggressive resistance (aimed directly—and partly aggressively—at the robber). In those cases where more than one type of behavior could be observed, success at foiling the robberies doubled. Categories (1) to (3) above are risk-minimizing behaviors, but rash or aggressive behavior often led to escalation of the situation. In those cases where injuries occurred, more than half were cases of aggressive resistance by an employee.

Reasons for failure of attempted robbery

Many different factors interact in a bank robbery, any one of which alone or in combination with others can foil the robbery. Passive resistance is a necessary, though not a sufficient, contributor to failure of a robbery. Of the 202 attempted robberies, the failure of 190 was due, in part, to employee behavior. This relatively high number of robberies foiled before the money was handed over points to the relevance of hesitant behavior combined with technological security.

Steps taken by the robber

The following analysis will focus on steps against security systems, customers, and employees to examine how technological security has affected bank robberies.

Measures against security technology

Behavior directed against the security systems/devices was found 233 times. In 10 instances, physical security structures (bulletproof glass) were attacked; in 27 cases, telephone lines were the target.

Steps taken against employees and customers

In the 1960's, hostage taking was an exception. Today it is common, and increased bulletproofing of the teller area is considered the reason. In 114 of the 152 cases involving hostage-taking, the robber took the hostage at the outset, prior to approaching the teller area.

In 34 cases, hostages were taken during the robbery due to escalation of the situation. When a hostage was taken as a measure against the technological security, no other action against this technology was taken by the robbers.

Use of a weapon. In 91.1 percent of all cases, a weapon was used solely to threaten employees or customers.

Injured/Killed. The contention that bank robbery is accompanied by an increase in death and injuries, supported by earlier statistics, is contradicted by the authors' data. The authors feel that because in the 963 cases only 53 people were injured or killed, the thesis of the increasing brutality of bank robberies is disproven.

Amount stolen. In comparison with earlier studies, the percentage of cases with a high amount stolen (more than DM 100,000) has increased. However, amounts between DM 5,000 and 10,000, and DM 15,000 and 20,000 are stolen most of the time.

Arrival of police. Of the 500 cases in which the arrival of the police was documented, the police arrived during the robbery only 5.1 percent of the time.

Solving the crime. The success rate for solving the crime was 59.5 percent. The percentage of crimes solved on the day of the robbery is approximately 50 percent of all crimes solved. Timely activation of the alarm was the major reason the robbery was solved the same day.

Technological prevention. The "neutralizing" effects of technological prevention were isolated during the research in robbers' attempts to direct their criminal energy at other unsecured objects, or to change their approach. For example, a robber demanded that the money be brought to him out of secured areas, often while he threatened bodily harm. This behavior should not call the validity of preventive security into question, however, since neither increases in brutality, use of guns, nor injuries/deaths were found. Escalation in the robbers' behaviors to circumvent the "neutralizing" effects or obstacles of technological prevention appears to be the only negative consequence of the changes in bank robbery brought on by technological security. The research results show that the possible dangers can be ignored in light of the advantages.

Research results—the robber

The study also examined the social characteristics of robbers and their reactions to security technology. The possibilities of researching the social characteristics are limited due to the methodology used. Psychological factors, for example, could not be taken into consideration.

The number of robbers

The number of robbers participating in the 963 cases was 1,395. Lone robbers made up the greatest proportion of the cases (66.6 percent); 2 robbers followed with 25 percent; and three robbers with 6.1 percent. Only 2.3 percent of the robberies were carried out by 4 to 6 robbers. The authors found the assumption that a robbery was more often successful if carried out by multiple robbers to be true. However, the rate of crimes solved is also higher for robberies committed by multiple robbers.

Personal characteristics

The age group of 21 to 25 was most often represented (31.6 percent), followed by the age group of 18 to 20 (19.9 percent). As the age range increases (from 25 to 30), a significant decrease in representation occurs. While 63.5 percent of the robbers were single, 20.9 percent were married; others were divorced or separated. Those with a low level of schooling were heavily represented.

Previous offenses

Whereas 45.3 percent of all robbers were previous offenders, 33.4 percent were first offenders. This is an increase in first-time offenders and also in the number of first-time offenders under 18. The crime is increasingly seen as an opportunity for quick money.

Use of a mask

Of the 1,395 robbers, 1,000 wore masks (704 full masks, 165 partial, and 131 "light" masks). The most commonly used materials were helmets or ski masks, which were removed by 256 while leaving the building, 100 while on the street immediately afterwards, and 27 during the robbery. These figures point to the need for camera surveillance to cover the exits. Use of better masks has not led to an increase in the number of unsolved cases, as was assumed.

Reaction to the activation of the alarm and optical surveillance systems

Of those robbers remaining in the area after the crime, 568 either did not or could not notice activation of the alarm because it occurred after the robbery. In cases where activation occurred during the robbery, the reactions of those remaining at the scene differed. Most abandoned the attempt, some took a hostage, others acted aggressively toward the alarm, or increased their threats and became noticeably nervous. Of those confronted with activation of optical surveillance, 92.3 percent did not notice it.

Reaction to employee resistance

Reactions of the robbers to employee resistance varied from shooting at the employee or firing warning shots to taking hostages. Training of employees to meet the challenges of any situation is necessary. Calls for help by others at the scene elicited a similar response from robbers, who reacted just as aggressively to this as to aggressive resistance of employees.

Conclusions

Despite the increase in bank robberies, the rate of successfully solved cases has remained constant. The authors conclude that an effective technological security system—and especially use of optical surveillance—has contributed to the continued success in solving cases.

Technological security has not caused basic changes in the nature of bank robbery. Too much emphasis should not be placed on escalation of the crime to include other criminal behavior because this has not occurred on a wide scale and consists primarily of the temporary taking of a hostage.

This study shows that principally positive effects have been brought about by the application of the concept of technological prevention. Its advantages outweigh its disadvantages, but caution should be taken in freely experimenting with the concept.

The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program Offices and Bureaus: National Institute of Justice, Bureau of Justice Statistics, Bureau of Justice Assistance, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.