

**NAVAL POSTGRADUATE SCHOOL**  
**Monterey, California**



**THESIS**

**CLANDESTINE COMMUNICATION  
SYSTEMS**

by

John T. Corley

December 2001

Thesis Advisor:  
Second Reader:

Gordon McCormick  
George Lober

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE December 2001	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Clandestine Communication Systems			5. FUNDING NUMBERS
6. AUTHOR(S) John T Corley			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE
13. ABSTRACT (maximum 200 words)  Subversive elements, whether insurgent, terrorist, or criminal, all require a communication system to coordinate and control operations. The development of a clandestine communication system requires special considerations in the development of the nodes and links that are responsible for the transmission of information. A closure analysis of these processes, professionally referred to tradecraft, assists in the planning and development of a communication system to support or counter subversive operations. This thesis analyzes tradecraft as a communication system to identify the constraints and opportunities to which different technologies have proven useful and the strengths and weaknesses of the same.			
14. SUBJECT TERMS Communication, clandestine communication, subversive, organizational communication, insurgent, terrorist			15. NUMBER OF PAGES 61
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**CLANDESTINE COMMUNICATION SYSTEMS**

John T. Corley  
Major, United States Army  
B.S., Virginia Military Institute, 1989

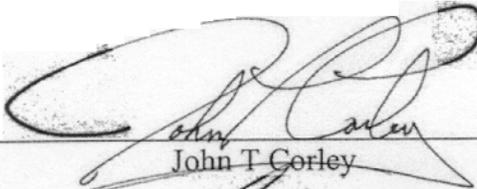
Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS**

from the

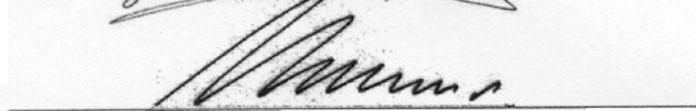
**NAVAL POSTGRADUATE SCHOOL  
December 2001**

Author:

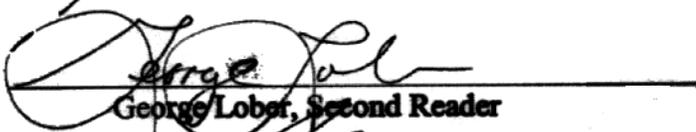


John T. Corley

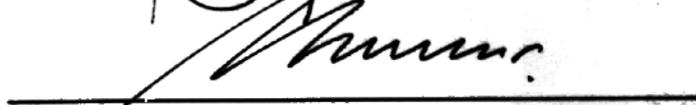
Approved by:



Gordon McCormick, Thesis Advisor



George Lober, Second Reader



Gordon McCormick, Chairman  
Special Operations and Low Intensity Conflict

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Subversive elements, whether insurgent, terrorist, or criminal, all require a communication system to coordinate and control operations. The development of a clandestine communication system requires special considerations in the development of the nodes and links that are responsible for the transmission of information. A closure analysis of these processes, professionally referred to tradecraft, assists in the planning and development of a communication system to support or counter subversive operations. This thesis analyzes tradecraft as a communication system to identify the constraints and opportunities to which different technologies have proven useful and the strengths and weaknesses of the same.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

I.	INTRODUCTION.....	1
II.	COMMUNICATION SYSTEM .....	3
III.	NODES.....	7
A.	COURIERS .....	7
1.	Bridges .....	8
B.	CUT-OUT .....	11
1.	Liaisons .....	11
a.	<i>Line Switch</i> .....	13
b.	<i>Message Switching</i> .....	16
c.	<i>Queuing Switch</i> .....	18
d.	<i>Automated Switches</i> .....	20
IV.	LINKS .....	23
A.	WRITTEN .....	23
1.	Invisible Inks .....	24
2.	Disguised Letter .....	25
3.	Encryption .....	25
a.	<i>Playfair Cipher</i> .....	26
b.	<i>One-Time Pad</i> .....	27
c.	<i>Computer Generation</i> .....	27
4.	Reduction .....	27
B.	TELEPHONE.....	30
1.	Mobile Telephone.....	33
C.	RADIO .....	35
V.	CONCLUSION .....	39
	LIST OF REFERENCES .....	41
	INITIAL DISTRIBUTION LIST .....	47

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

Figure 1.	Network Bridge.....	9
Figure 2.	Liaisons.....	12
Figure 3.	Queuing Switch.....	19
Figure 4.	Hiep Hoa Village .....	29
Figure 5.	Clandestine Switch.....	32
Figure 6.	Telecommunication Access .....	33
Figure 7.	Cellular Networks .....	34

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	Playfair Cipher.....	26
----------	----------------------	----

THIS PAGE INTENTIONALLY LEFT BLANK

## I. INTRODUCTION

The purpose of this paper is to analyze the technology employed by subversive elements to construct an efficient and secure organizational communication system. As in data communication, the efficiency of the system depends on the nodes that route messages and the links that connect them. To understand “the effects of the communication systems on messages ... the characteristics of the system must be known” (Thomas, 1988, p.2). When possible, the terminology familiar to data networks will be incorporated to assist in the clarification of a function and graphical renditions for visual comparisons. Several terms associated with data communication are applicable and descriptive in explaining the techniques and tradecraft of clandestine communication and can be useful in the planning of a local, national, or international communication system.

THIS PAGE INTENTIONALLY LEFT BLANK

## II. COMMUNICATION SYSTEM

Formal communication systems control and direct the flow of information throughout an organization. These processes are needed to “disseminate and enforce organizational goals, rules, and regulations; coordinate the activities of organizational members in the accomplishment of organizational tasks; provide formal leaders with feedback about... the state of organizational activities; and socialize organization members into the culture of the organization” (Kreps, 1981, p.271). Organizations that exist in a dynamic and complex environment cannot easily sustain operations with static rules or policies and must continually adapt to changes in the environment. Within the subversive organization’s dynamic and complex environment the members’ motivation and commitment to organizational goals is in constant flux and the maintenance of which requires the leadership to continually influence the decisions and activities of the members. “The more an organization is people- and idea- oriented, the more important communication becomes” (Hall, 1972, p.271). This process of directing, influencing, controlling, and motivating is expedited with a communication channel that links the leadership to the subordinates by the most direct and shortest means possible. The building of this system is of importance to the leadership of all organizations and essential to subversive elements. “The importance of communication to secret activities cannot be over emphasized. It is the efficiency of the communication system which makes possible the rapid [information] procurement and dissemination” (Brown, 1976, p.66).

The conditions imposed by a hostile environment and the necessity of the subversive organization to counteract these conditions requires that the channels used to alert elements, disseminate orders, and control operation be transmitted in a timely and reliable manner. “Direct supervision is the fastest and tightest means of coordination” (Mintzberg, 1993, p.141) between nodes and allows for the exchange of clear, accurate, timely, usable information. However, in large organizations direct exchange is not always practical and requires a modification of the communication process. The inclusion of additional nodes and links in the system increases the distance between elements and can

easily impede communication. Intuitively, responsiveness is the duration between the transmission of a directive and the initiation of action by the receiver. When defining the responsiveness of a communication system it is a factor of where the message is routed and the time necessary to complete the transmission. Mechanically, the responsiveness of the system depends on the reliability of the nodes to route messages to the appropriate recipient and the timeliness of a particular link to transmits the correct information.

Though most subversive elements are not considered large by corporate standards, the desire to maintain security also requires the inclusion of additional nodes and links in the communication process. “Communication is, by definition, a relational one” (Hall, 1972, p.272) and direct communications between nodes establishes an association. Security is maintained by regulating direct communication between members. This methodology commonly referred to as compartmentalization, limits the connectivity of the organization’s members and eliminates the redundancy in the communication network. Redundancy in communication is two fold: 1) it provides a “multiplicity of paths” (JP 6-0, 1995, p. II-6) linking any two network members, thus increasing the probability a message will reach the intended receiver, and 2) it is the “repeating of a message over different channels, in different forms, or over time” (Rogers, 1976, p.92). Redundancy increases the accuracy of information and the reachability of any individual member by either direct or indirect connections. The number of routes between two nodes determines the connectivity of a network. The minimum number of nodes whose removal “results in a graph with two components” (Cravis, 1981, p.5) is the minimum cut-set of the networks. The subversive network is “organized so that if one element fails, the consequences on the total organization will be minimized” (Molnar, 1963, p.54). This minimization is possible by maintaining a minimum cut-set of one between nodes. As the security environment relaxes, the organization can broaden the connectivity to facilitate coordination and planning but in a high threat environment, the fewer links connecting organizational members, the fewer members that can be identified by any particular member during interrogation.

The development of an efficient clandestine communication network requires the continuing evaluation of the constraints, opportunities, contingencies, and problems (Khandwalla, 1977, p.328) created by the competitive environment to identify the best

node or link to utilize in the appropriate situation. The efficient system requires the appropriate combination of nodes, the couriers, cut-outs, etc. responsible for the distribution of messages, and links, the means (written, radio, telephonic, etc.) by which this information is transferred. A thorough understanding of these components can assist in devising an efficient system.

THIS PAGE INTENTIONALLY LEFT BLANK

### III. NODES

Nodes are components in the system responsible for the routing and distribution of information. Not only does the communication system responsiveness depend on node reliability, the appropriate node utilized to complete a connection must conform to the constraints and opportunities of the environment. When selecting nodes for the system, the safety and dependability must both be evaluated. Safety is the ability of the node to perform its function without compromising the organization. Dependability encompasses the trustworthiness of the node to complete the function with an acceptable level of assurance for the organization. Nodes are the couriers and cut-outs responsible for the distribution of messages to the appropriate recipient node in the network.

#### A. COURIERS

Courier are proven nodes in secret communication networks. The “use of couriers is probably the safest means of communication and transmission of information between various agents” (Molnar, 1966, p.103). The courier receives a message and delivers it to a specified individual or location. The detainment and the possible interception of the message can jeopardize the entire organization. The courier’s ability to safely transport a message through hostile terrain is a function of the quantity and quality of security forces and adversarial elements in route. Will the couriers remain undetected, do they have the proper documentation, and are there checkpoints at every street corner? Despite varying levels of threats in the area, the courier is a most dependable means of communication. Couriers return and provide the sender with the assurance that the message has been delivered in tact and may provide feedback from the recipient. Despite advances in communication technology the courier remains effective even in strictly policed societies.

Simha Rotem (*Kazik*) joined the Zionist youth movement in 1942 and would later become the aid-de-camp for Yitzak Zuckerman (*Antek*), the leader of ZOB the Jewish Fighting Organization in Poland. Kazik participated in several subversive activities, one of which was courier for Antek. The ZOB courier duties were critical to bridging the gap between the organization and other resistance elements and the constituency in Poland.

Couriers were responsible for “maintaining contact with [Jewish] people in the camps and ghettos... delivering money... forged documents... underground publications...[and] supplying weapons to places where uprisings were planned and prepared” (Kazik, 1994, p.67). The courier minimizes the personal contact between the leadership and the subordinates by inserting an additional node into the communication channel. The courier eliminates the need for the leaders to expose themselves to hostile elements in the environment. Kazik’s position not only increased the security for “the commander of the ZOB throughout Poland” (Rotem, 1994, p.66) but also made him a competent lieutenant for the organization.

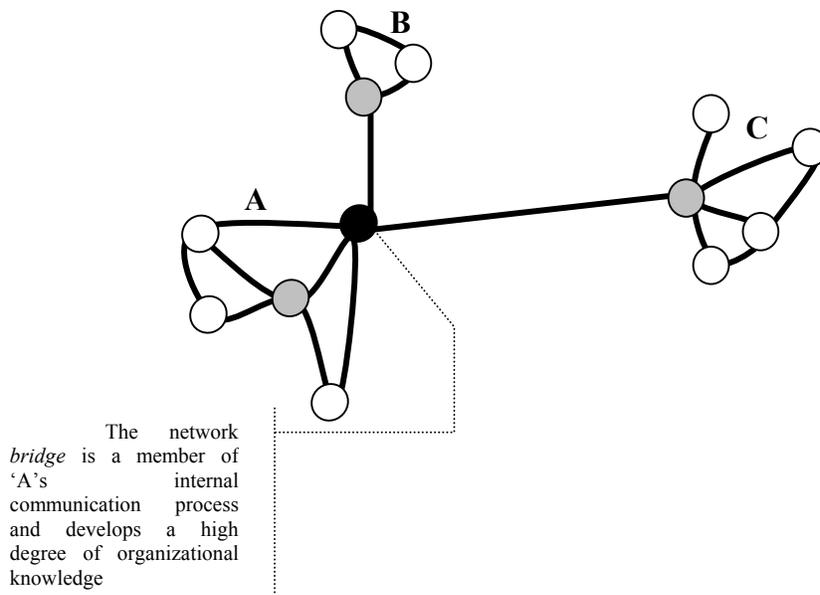
Kazik’s functional capacity exceeded the normal duties of the courier, as he became a trusted member of ZOB. Kazik “was Antek’s deputy, and in that role [he] had to make decisions required by the circumstances at any given moment” (Rotem, 1994, p.67). Kazik was present for organizational meetings between Antek and the other branches of the Jewish Resistance, the Armia Krajowa (AK), the Polish Home Army, and the Armia Ludowa (AL), the People’s Guard. Kazik’s position in the organization permitted him access to the individuals and information to make him a more influential representative of Antek. Kazik’s contact with Antek maintained a short and direct line of communication between the leadership and the other branches, which assisted in the dissemination of directives. Kazik’s familiarity allowed messages to be verbally transmitted, which avoided the complications of composing and concealing written information or the memorization necessary by less informed couriers. When messages are passed through a series of nodes, the message is continually degraded. This degree of familiarity with organizational activities, members, and contacts can place significant risk for the organization.

### **1. Bridges**

Kazik established the communication bridge that linked Antek to the ZOB members and other resistance elements. A bridge “shares information ... and facilitates coordination” (Kreps, 1986, p.220) between networks. Underground leadership is typically isolated from the environment to limit exposure to hostile forces and delegates the supervision of operations to intermediaries, lieutenants and deputies. Structurally, a bridge is a “an organizational member who connects a [network] to which they belong

with members of another [network]” (Kreps, 1986, p.220) and therefore included within the organizational boundaries that are created by the communication process. The bridge converses with other members, is involved in deliberations, and develops a high degree of organizational knowledge. The information acquired by the bridge increases his capacity to coordinate activities and influence subordinates. The Polish Resistance used the couriers extensively. The courier who is a member of the internal channels creates considerable security risks for the organization as they are constantly exposed to hostile forces and adversaries. The knowledge the courier has acquired can easily compromise the organization. The courier’s routine exposure must be continuously analyzed and equilibrium between communication and security maintained.

Figure 1. Network Bridge



Occupied Warsaw was a special environment that posed significant threats to the ZOB courier. Jews were not only pursued by Gestapo agents but were the targets of non-sympathetic Poles as well. The “German’s internal security system was extensive ... and assisted by local residents” (Rotem, 1994, p.96). Blackmailers would attempt to extort goods from Jews in return for their safe passage in the Warsaw streets (Rotem, 1994, p.68). These threats impacted the safety of completing a mission and were a consideration in assigning missions. “When a specific mission was assigned, we always

weighed carefully who had the best chance of performing it” (Kazik, 1994, p.67). The courier is constantly exposed to opposition forces and vulnerable to intercept and, therefore, must maintain the appearance of legitimacy to remain successful. Kazik’s successfully exploited opportunities that were created by the occupation environment within Warsaw.

Proper documentation was a necessity to maneuver through the city and the countryside. The use of forged documents was common but still created a degree of risk. Kazik was native to Warsaw and presented himself not as a Jew from the surrounding countryside. Kazik’s obtained the official documentation required to reside outside the ghetto through associates in the Polish underground (Rotem, 1994, p.60-61). Kazik assumed the identity of a deceased Polish Aristocrat with the assistance of the department of records. Kazik was also familiar with Warsaw and the ghetto, unlike the individuals that were relocated from outside the city. These traits and the proper preparation increased the dependability of Kazik as a courier and deputy. The courier like other members of the organization must operate a conventional lifestyle to avoid conspicuous behavior. Therefore the use of individuals who can perform the duties of the courier in the conduct of normal activities assists in the disguise of clandestine activity. Kazik exploited the opportunities created by the environment. The access to official documentation, the Aryan appearance, and familiarity with the city allowed him to move with assurance through the city. When the constraints of the environment are such that one’s ability to move safely are minimized, other methods of employment should be adopted.

The Armia Krajowa used women almost exclusively as couriers. These women “ensured the constant and accurate communications of the AK. They distributed the Underground press and publications” (Polish, 1999, p.1). The courier was closely regulated to maintain safety because the ability for them to be compromised was significant in Poland. Molnar comments in reference to the Polish Home Army that “the problem of avoiding police suspicion was immense, and these couriers were usually uncovered after they had served a few months. In view of this, these women were not allowed to assume other duties in the underground, so as to limit the information they could be forced to disclose under interrogation” (Molnar, 1963, p.80). For the

communication network, this structural modification is referred to as a liaison; in the subversive world it is frequently called the cut-out.

## **B. CUT-OUT**

The cut out is a fundamental structural feature of clandestine networks implemented to minimize association between cells and members by inserting an “intermediary who meets each agent separately and conveys messages back and forth” (Molnar, 1966, p.103). Kazik was a cut-out for Antek but the security afforded the leadership was not replicated in the organizational structure. A more secure methodology retains not only the protection of essential leaders but also the counsel within which he confides. The development of a liaison structure increases the security of the organization. The Viet Cong utilized cut-outs to limit exposure between the district and hamlet organizational members (Lanning, 1992, p.112). A VC communication-liaison officer captured in the fall of 1966 explained:

The VC secretary received orders from the district secretary, who in turn sent messages to the cadre who were staying in the hamlet. In each hamlet there was a fixed place where I would come with my message. At that place there was a man who would know me. He was in touch with the cadres of that hamlet and he would deliver the orders to the cadre. I gave the message to this man, not to the cadre. I knew therefore, the fixed place and I knew this man, but I did not know the cadres. The cadres in turn, at some other time, went to another place to pick up the messages (Lanning, 1992, p.112).

This method is straightforward, but inefficient. The district secretary dispatched a courier with a message. The courier would contact an intermediary in the hamlet who may have been a cadre member but was more likely an individual recruited to represent the cadre. For the organization, both the courier and the representative are neither members of the district or the hamlet communication network. Structurally speaking the roles of the courier and the representative can be considered liaison.

### **1. Liaisons**

The hamlet representative was the liaison between the cadre and the district personnel. Liaisons are “organization members who connect two [elements] without themselves belonging to either one” (Kreps, 1986, p.220). The organization prevents

membership disclosure by relying on the liaison to represent the cadre. The liaison is only a node in the group's external communication channels and not privy to internal deliberation and planning. The cadre members control what information the liaison can access by message content and use of encryption. "Because the representative's vulnerable position as a contact...he is limited to this one duty and knows little about other aspects of the underground" (Molnar, 1963, p.81). The security of the organization is further increased with the replacement of the liaison with other switching mechanisms designed to route messages to the appropriate receiver without compromising organizational knowledge.

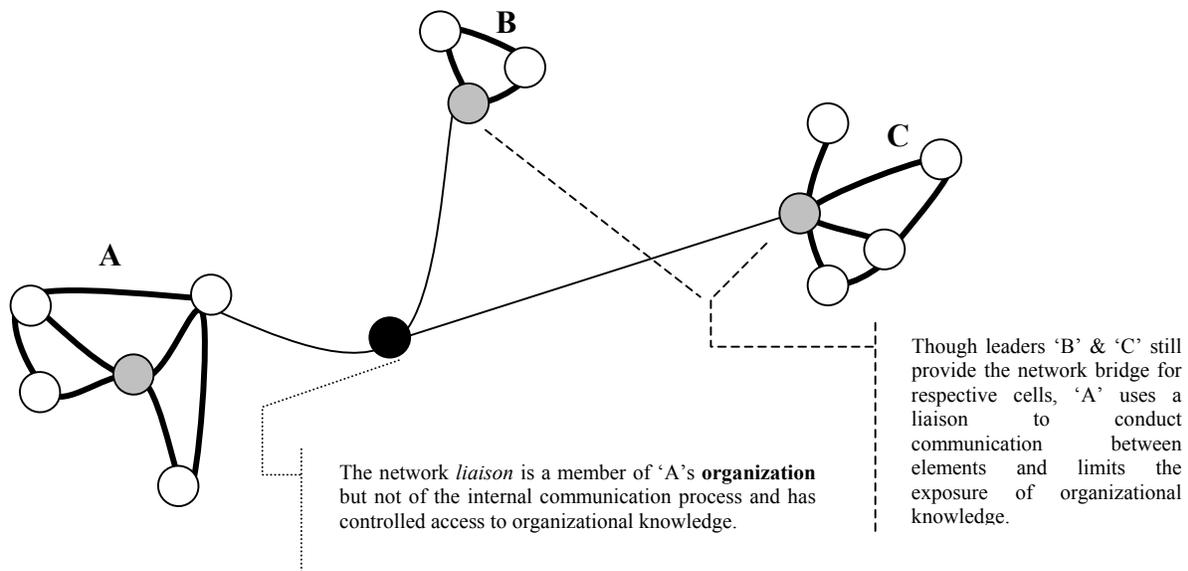


Figure 2. Liaisons

Messages are transmitted through the system by a series of nodes and the links that connect them. How these nodes route the message to the appropriate receiver is a primary consideration of the system and the subject of this section. How the separate nodes are linked is a paramount importance and is the key to creating a functional system that transmits information in a timely and reliable manner. The assurance that a message has departed and arrived at a particular node requires feedback from the system and is most readily attained through a direct linkage. Indirect linkage limits the responsiveness of the system but increases the security by limiting association between nodes. The process by which this is possible in a communication network is through the reliance on switching mechanism that route messages to appropriate recipients. Communication

through a cut-out is either by establishing a temporary link between two nodes long enough to complete the transmission or the storage of the message until the next node becomes available to receive the message. When two nodes establish a link that completes the circuit between otherwise separate entities the message is transferred and the process is affirmed. The line switch is the most secure method in ensuring the message arrives to the correct location, but creates the danger of compromising two nodes at one time.

*a. Line Switch*

The *line switch* establishes a non-permanent connection between two nodes for a brief period of time to allow a message to be transferred. “A news dealer or a tobacconist might be used to receive and pass messages” (Brown, 1976, p.123) that would otherwise require contact between organization members that would arouse suspicion or disclose one’s identity. During the contact, a message, coded in an expression or concealed in an item, is transferred to the individual that presents the proper bona fides (a phrase, garb, or motion used to confirm one’s identity). This transfer requires some harmonization but is dependable and reasonably safe to execute frequently as the switching nodes actions are disguised in legitimate activities. Sometimes referred to as a live drop, the switch is designed to reduce the conspicuousness of the message transfer.

The British DF circuits during the Second World War used line switches to assist in the transfer of escaping prisoners of war, downed airmen, and agents between safe houses located along the European escape lines. DF operatives would hide newly acquired passengers in designated safe houses and notify a switch that was responsible only for the receiving an arrival message and transferring that information to the next node. The DF operative would escort the passengers to a pre-arranged contact location to be picked up by the next escort. The transfer of the message and the passenger were dependent upon the contact initiated by the receiving node and therefore the passenger may conduct the contact procedure several times before an actual transfer. A former DF circuit operative provided an example of an exchange process in M. R. D Foot’s, The SOE in France:

One agent passes a message in simple code to the cut-out; it might be a book seller, saying, "I have two volumes of Anatole France that need binding; can you arrange it for me?" The cut-out holds the message till approached by the next agent down the line, who rings up and asks, 'Have you any Anatole France in stock?', and will infer from the answer, 'Yes, two volumes have just come in', that there are two escaper to be collected from the circuit safe house in the Boulevard Anatole France (Foot,1966, p.94).

When the receiver was certain that the situation was safe to transfer personnel along the lines, the escort would contact the switch and request whether or not personnel were in need of transport. After receiving an affirmative answer from the clerk, the escort would contact the passenger in waiting at the appropriate rendezvous location and complete the transfer. Other switches did not rely on the verbal transfer of information but used written and visual signals to alert personnel. In Lyons, a safe house owner would send a personal letter with the necessary information hidden in the contents to a fictitious resident in town. The postmaster recognizing the name would route the message to the local cobbler. "The cobbler put a particular shoe ... in one corner of the shop window" (Foot, 1966, p.95). A courier would pass the window daily and receive the signal and subsequently move the passenger to the next safe house. Though the transmission of information can experience a considerable delay between nodes, the process is reasonably safe and dependable. Had the bookstore been under surveillance the clerk could redirect either node with an answer that avoided suspicion. Though the Lyons postmaster could deliver messages either as a daily duty or through covert means, written communication can be transmitted more surreptitiously.

Pass. When the ability to camouflage a message transfer in a legitimate exchange does not avail itself, the opportunity to conceal the transmission must be seized. Unlike an exchange with the tobacconist, there may be no justification for an encounter between two nodes and any apparent contact can be incriminating; therefore, crowds and confusion are incorporated to mask the *pass*. Occasionally referred to as the 'brush pass' the technique offers "a brief encounter where something is passed between [operatives]" (Mendez, 1999, p.344). Antonio Mendez, the former Chief of Disguises for the Central Intelligence Agency, described his first surveillance training exercise when he and his partners lost their surveillance targets that "'brushed' by one another and exchanged

packages or dropped a message in each other's pocket or shopping bag, undetected by surveillance" (Mendez, 1999, p. 66). The pass establishes a momentary link between two nodes that allows the abrupt exchange of information. Structurally, this technique is no different than the previous telephonic or letter exchanges but does create the opportunity to transfer an item or a larger quantity of information directly to another node and avoids the caching of a message for recovery at a later time by the recipient. Such an exchange can prove very difficult to detect in large crowds with small items and can be a safe method of communication if coordinated and practiced. The pass is quite dependable as it "keeps any sensitive message in the hands of the operatives only – it is not left anywhere or with anyone" (Myers, 1991, p.41). To attain a higher degree of communication effectiveness, the organization must establish interpersonal contacts in a secure and concealed location.

Safe House. The safe house is not a communication node per se but has been incorporated in systems analysis as a cover for such activities. "A 'safe house' (one where the people were friendly and willing to take the risk of harboring an agent or subagent) might be necessary to assist in concealment" (Brown, 1976, p.123) of escapees, conferences, or training of members. In the selection of a safe house, the organization should "try to avoid neighborhoods where persons noted for anti-regime activities reside, for they are likely to be under government surveillance and ... might arouse suspicion ... and also, places near the homes of block wardens" (Molnar, p.1963, p.75). ZOB used the safe house extensively to conceal resistance activities and hide Jewish residents. The couriers would visit the houses regularly but not excessively as "every house in Warsaw had a concierge who gave information to the police on everything that went on in the house ... [and] investigated strangers to find out which of the tenants the stranger was visiting" (Rotem, 1994, p.97). The safe house is more than a place to house pursued people; for urban organizations, the safe house is the only location through which the leadership can influence the members directly.

The communication opportunity provided by the safe house is decisive to the organization. Whether an apartment in the ghetto or a camp in the mountains, these sanctuaries are the only headquarters for local groups where the leadership can establish and maintain the organization's direction, which, in turn, is only effective with member

cooperation. Leaders “depend on the development of effective interpersonal relationships with other organization members to help gather information and elicit cooperation” (Kreps, 1986, p.168). The courier lines of Tito’s resistance forces allowed “Partisan leaders [to] safely visit the regional political and military headquarters, coordinate their political and military activities, evaluate on site the competence and loyalty of regional leaders, replace those who didn’t measure up, and ensure that directives from Tito and the Central Committee were faithfully followed” (Lindsay, 1993, p.65). The use of a meeting area like a safe house cannot be relied on continually and must be rotated to avoid the attention of hostile forces. “Resistance movements must maintain several safe houses in the same city or district in order to hold conferences, or to go underground temporarily or permanently” (von Dach Bern, 1965, p.109). When the constraints of the environment do not afford the opportunity to exchange information directly, the message switch can transfer information between nodes.

***b. Message Switching***

*Message switches* receive and hold a message until retrieved by the correct agent. Frequently called a drop, dead drop, letterbox, etc. the switch may require a special container to conceal the contents and blend with the environment. The switch replaces the liaison with a temporary storage facility to retain the message until picked up. Stanislav Lunev, former GRU Colonel and Soviet defector, used a container that replicated a Coca Cola can that he retrieved from the roadside. “It was like one of those cans with a screw lid that people buy in specialty stores to stash their jewelry and thwart burglars, except this one was designed by the GRU to destroy its contents should it be opened by someone other than the GRU” (Lunev, 1998, p.144). The device was dropped at the specified site at which Lunev visited in accordance with a designated time schedule. The message switch institutes a compromise between the dependability and safety of the mechanism. The switch is vulnerable not only to adversaries but damage in general. The device may be unknowing removed by passers-by or garbage collections and must be placed to avoid these dilemmas. The OSS used what was referred to as “inanimate letter drops for the actual transmission of intelligence reports over great distances... An agent might place intelligence material at a designated spot on a railroad car or locomotive...[to be] removed by a confederate in another city and forwarded”

(Brown, 1976, p.123). The emplacements of these switches are “places such as telephone booths or washrooms where an individual commonly goes alone without suspicion” (Molnar, 1963, p.103). However, message switches do not have to be concealed in the thoroughfares of everyday activity and can be at locations away from a society’s natural lines of travel.

When the Dong Loa Dong moved to regain control of South Vietnamese villages in the late 50’s, the first objective was to establish a clandestine cell within the targeted village to further develop the movement. Before entering a village, the Party would conduct a survey to determine the village’s overall disposition and level of government control. Based upon these findings the cadre would attempt to recruit a few new members to the Party who would form the Civil Affairs Committee. The survival of the Committee required a communication system that would maintain security for both the personnel and the higher headquarters. When the cell needed to contact higher headquarters, the message was delivered to a message switch that was usually a “clay jar buried in the ground and carefully camouflaged. A courier from the district committee would later empty the ‘mailbox,’ carry the message to yet another clay jar near the district Party Committee headquarters, deposit them, and then leave” (Andrews, 1973, p.49-50). Directives from the District were transmitted using the same methodology. Not all switches have relied on proper camouflage in the urban or rural terrain to remain concealed.

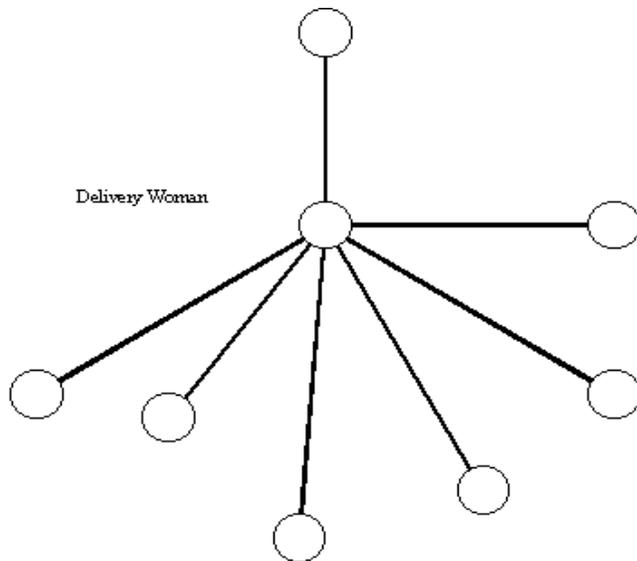
Francois Suttill parachuted into France early in October of 1942 to “re-create an active circuit in and around Paris” (Foot, 1966, p.198) for the Special Operations Executive (SOE). The SOE began infiltrating agents into France in the Spring of Forty-one to organize resistance networks in preparation for the invasion of Europe. Suttill was provided contacts by the CARTE circuit to begin setting up operations to recruit and organize the new PROSPER circuit. The networks would collect intelligence, distribute firearms and equipment, train resistance personnel, and conduct sabotage of German lines of communication. Suttill’s made his first CARTE contact with Germaine Tambour in October. Suttill had been impressed with Tambour and arranged to “used her house as a letter-box and rendezvous” (Foot, 1966, p.309) for PROSPER members. The switch located at the Tambour’s residence was now accessed by Suttill, his two radio

operator Amps and Norman, his courier, Andre' Borrel, and Peter Churchill, another contact (Foot, 1966, p.309) presumably for correspondence. Additionally, these individuals, minus Churchill, were also using another apartment in the building as a switch along with six other SOE operatives (Foot, 1966, p.309). The Tambour residence and the building as a whole were now servicing ten SOE personnel, some of whom were members of another circuit. Unbeknownst to PROSPER, the courier for the CARTE network had fallen asleep on the Marseilles to Paris train carrying the names, addresses, telephone numbers, and appearances of over two hundred CARTE personnel which were subsequently taken by an Abwehr agent (Foot, 1966, p.205). The probable disclosure of the Tambour residence would have easily compromised the individuals accessing the residence to retrieve messages or attend meetings. Tambour was arrested the following April and virtually all of the PROSPER network was rolled up in the following months.

The residence concealed the switch from observation of the delivery or retrieval of messages but placed at risk several organizational members by allowing multiple members to access the identical switch. Foot points out that as a guide, “a cut-out ought to be able to give away only, at worst, the people on either side of him or her in the system” (Foot, 1977, p.41). The overall safety of the switch and its dependability cannot override the fundamental practices of regulated association. The opportunities provided by the apartment did not consider the constraints imposed by the Paris security forces' capabilities. To utilize a single node to route messages to multiple nodes the process must be thoroughly analyzed and planned to integrate the proper resources.

### *c. Queuing Switch*

The efficiency of a communication system increases with the ability of a single node to maintain and route numerous messages in waiting correctly. This *queuing switch* can have significant security concerns as well as repercussions and demand special consideration in a network. Clandestine switches are regulated by the activity within which they are disguised and can be difficult to detect.



The 'queuing switch' increases the efficiency of the system by using a single node to route several messages. As possible with the delivery woman, the individual conducting the transfer process may be ignorant of the message contents or even the message its self, significantly increasing security but lowering the dependability of the delivery system.

Figure 3. Queuing Switch

During the early 1950's Col. Ed Lansdale was working in the Philippines as an advisor to Ramon Magsaysay, Secretary to the National Defense, when a member of the Communist Politburo operating clandestinely in Manila "let slip a clue as to [the method] ... communications between Politburo members were convey[ed]" (Lansdale, 1991, p.63). The Politburo incorporated a woman courier as a switching mechanism to transfer messages around Manila. The woman "delivered baskets of food; hidden in the baskets were secret messages for distribution to the members" (Lansdale, 1991, p.63). Details as to the frequency of delivery or scheduled verses on call were not available, but either of these techniques utilizes a system with a self-imposed "user-to-user delay ... that depends largely on the queuing" (Cravis, 1981, p.85) method or simply the delivery sequences. This store-and-forward switch regulates the flow of information throughout the Politburo. Surveillance of the delivery service established an "identifiable link between the top members of a clandestine group" (Lansdale, 1991, p. 63) and resulted in the arrest of several members and the confiscation of documents concerning activities, meetings, and future plans. The communication channel should appear as "conventional and as open as possible" (Molnar, 1966, p.73) so as not to attract the authority's attention but incorporate written messages to maintain accuracy or limit the exposure of operational concern to third parties; the delivery woman.

The switch routed messages throughout Manila under the guise of a legitimate delivery service. However, the centralization of the mechanism aided in the identification of several Politburo members. The maintenance of a dedicated system with a low failure rate, standardized procedures, and the capability to prevent interception can ensure the delivery of information to proper receivers but “is not suitable for immediate exchange of messages and replies” (Cravis, 1981, p. 85). The ability to transmit information in a timely manner is the corner stone of the automated switch.

*d. Automated Switches*

*Automated switches*, made possible through data communication and the Internet, are some of the “easiest and most secure” (Wettering, 2001, p.346) ways to transfer messages between agents covertly in a reliable and timely manner. Worldwide information systems facilitate clandestine communication with ease of encryption or concealment (which is fundamentally a means to link nodes and will be discussed further under written mediums), multiple access storage and retrieval nodes, and virtual anonymity. Frederick L. Wettering, a retired Central Intelligence Operations Officer, points out that the Internet has “made easier the method and techniques of espionage” (Wettering, 2001, p.348). Internet services have created the ability of an organization to establish switches that can be accessed remotely and in anonymity. An Internet Bulletin Board System (BBS) can be established with over the counter software and open to access from one’s home, business, library or Internet café with any personal computer. “Computer bulletin boards could be used to post messages, [send automatic notifications, or conduct electronic file transfers of encrypted data] between agents” (Wettering, 2001, p.348) while maintaining password protection. Web pages, more frequently used for the dissemination of propaganda, can allow controlled or secret access to additional sites that provide organizational information to be utilized in the execution of operation. However, just as these switches are electronically accessible from remote locations, they are easily monitored when targeted.

A centralized server that controls access to all files maintains the automated switch, whether a BBS or a web page. User attempting to access the switch can be scanned by systems (Carnivore, Omnivore, etc.) integrated into the server and a record of the exchange. “Security agencies monitor messages through the service

provider” (Wettering, 2001, p.348). These devices scan exchanges looking for specific features, works, encryption, etc. and isolated the identified messages for analysis later. The identification of the nodes either sending and posting information or the retriever can be readily attained. Despite the vulnerabilities, the sites offer the organization an efficiency of communication that is difficult to replicate outside of the Internet. An efficient communication node or link is almost by definition one that can allow two-way exchange between multiple nodes simultaneously. No line, message, or queued switching process can transfer the quantity of information to various nodes as timely, reliably, or securely as these sites. Wettering also identified the increased uses of peer-to-peer file sharing applications like Napster as devices that can easily support clandestine communication. These peer-to-peer programs support “communication between computers (mainly trading files...) without going through a server (service provider) and with perfect anonymity” (Wettering, 2001, p.348). Whether an organization can establish the centralized inventory control system that’s allows one to search for and access a particular file or whether particular files can be made available and transferable but cloaked in a coded name of otherwise incomprehensible letters or with an embedded data is beyond the scope of this paper but Wettering points out probably the most significant advantage of the Internet which is anonymity.

Internet services abound with the ability to create a temporary or permanent mailbox with no requirement for one to verify his identification. One can use several identities to send and receive information continually or once. The use of ‘anonymous re-mailers’ can allow one access to the Internet sites from one’s residence protecting the identity of the node. The re-mailer is similar to the Joessing switchboard manipulation.

THIS PAGE INTENTIONALLY LEFT BLANK

## IV. LINKS

The particular means by which to link nodes is generally viewed as a question of practicality in open communication but for the subversive it is the complexity of the contents and the consequences of the means utilized that are the deciding factors in a medium's selection. Complex messages are employed for detailed instructions and operational concepts that cannot be translated through a series of cut-outs and brief, coded statements. Complex messages may require lengthy documentation, prolonged phone conversations, or interactive Internet web pages. The consequences of selecting a means is not limited to the ramification of message compromise, but also the resources that must be committed to the preparation and transmission process. Urgency may demand a radio transmission lasting ten minutes, the consequences of which are the hasty departure and relocation of the equipment to a new concealment location to avoid the raid made possible by direction finders. All mediums are vulnerable to interception and require messages be prepared to counter this weakness. A courier may be interdicted but the concealed message is not intercepted unless discovered. The discovered message should be incomprehensible due to encryption and/or the courier's ignorance. In an effort to make the message concealable or reduce the encryption process, information can be omitted and distorted. **Distortion**, "the transformation of the meaning of a message by changing its content, [and] **Omission**, the deletion of all or part of a message" (Roger and Agarwala-Rogers, 1976, p. 93) is the consequence and the guiding principles in the selection of many clandestine links. The telephone, radio, mail, messages, computers, etc. are common methods of linking the nodes and are typically the target of counter-intelligence efforts because of their ease of accessibility. The composition of these messages to prevent the revelation of information to ones adversary is the subject of this section.

### A. WRITTEN

Written communication provides leaders with the opportunity to transmit complex information. For the courier, written communication demands first and foremost either the concealment of the message to prevent disclosure, or the disguise to prevent scrutiny. The recognition that there is a difference between concealment and disguise is not to

assign another classification to techniques but to identify that each has a separate purpose that should be considered in the preparation of the message. Though the differences can be ambiguous, as some techniques could easily be classified in either, both are markedly different from encryption, which is necessary to maintain confidentiality and the second line of defense. “One obvious way to conceal messages is to memorize them. Messages that must be written can be concealed by the messenger on his person or they can be either coded or integrated into innocuous documents like letters. Disguised messages are less liable to discovery than concealed ones” (Molnar, p. 1963, p.77). Memorization has its purpose but as discussed previously, the consequences of the procedure must be weighed in so far as its capacity to deliver clear and accurate information is limited and thus procedures such as invisible inks, disguised messages, field encryptions and reduction techniques are of such importance.

### **1. Invisible Inks**

Invisible inks have been used for centuries and were likely superceded by the development of the microdot and photographic reduction techniques (Mendez, 1999, p.223). A written message in an ink that requires the development by a receiver with the appropriate solution allows members to use ordinary appearing documents to conceal the message. The message could be included on personal letters, receipts or bills, etc. The Special Operation Executive taught several techniques that required only over the counter medication that could be procured without arising suspicion. “Most trained agents knew about secret inks; so did most good security officers. At a careful control, a patrolman would sit at a table with a couple of pots of secret-ink-developer and a brush ... [or] a magnifying class [that] would probably reveal the supposedly invisible pen strokes” (Foot, 1977, p.99). These inks could prove useful but were time consuming and limited in their ability to transmit complex information. The concoction of lemon juice or goats milk has been replaced with sympathetic inks readily available from specialty shops in pen and liquid form. These inks are primarily designed for the quick identification of equipment, test answer keys, or an impediment to criminal activities and are easily readable under ultraviolet light. The more frequently used mechanism was the disguised letter.

## **2. Disguised Letter**

The insertion of operational information into a seemingly innocent personal letter was a difficult task but attainable given the proper time. The concept required a pre-arranged process that identified particular positions in the letter from which the words were extracted and re-consolidated into a comprehensible message. The Barn Code was used by SOE agents to conceal internal network communication in Europe and required no elaborate devices or compromised any official encryption methods. Lorraine gives a detailed description of the technique but will only receive a cursory overview here.

The Barn Code conceals the message in an ordinary appearing letter that contains a key located at a specific position in the first paragraph. The key was used to construct a numerical decipher chart into which the second paragraph was transcribed. The message was reconstructed by extracting the words from each column in numerical order and the corresponding row. Particular bits of information that would be obvious even in the letter would be replaced with the letter 'A' and encrypted using the Playfair Cipher in the postscript. Encrypted messages would require additional pre-designated word positions from which the first letter of each word would be extracted and decrypted. "Although this system is long and it required a lot of effort to draw up a plausible letter, it is practically impervious to analysis" (Lorraine, 1972, p.78). The Bar Code and similar methods reduced the demand for the ever-incriminating encryption but doesn't eliminate it from clandestine communication.

## **3. Encryption**

Encryption and coding are frequently mixed and must be clarified for further discussion. The encryption of information is the mixing of letters and symbols to make the message incomprehensible. Codes are used to represent particular bits of information. Line switches use codes to affect an exchange; 'two books' was synonymous for 'two passengers' and didn't attract unwarranted attention. Links require encryption to limit the information that can be extracted from intercepted messages. Historically the development of encryption devices has been paramount to the successful transmission of secret military and diplomatic messages but has been inapplicable to clandestine communication as the necessity to conceal the equipment and the security risks that arise from a system's compromise have deemed the items inappropriate for use by subversives.

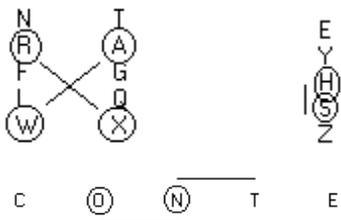
However, the inaccessibility of encryption devices did not eliminate the requirement and promoted the use of other methods to maintain confidentiality of information.

*a. Playfair Cipher*

The Playfair was developed before the turn of the century and used during World War I. The Playfair was based on a memorized line that was converted into a 5X5 square from which the encrypted letters were drawn. The cipher was easy to use and required no special equipment beyond pencil and paper. However, the shortness of the encryption key allowed the identification of patterns in the encrypted text and made the encrypted message readily decipherable. Later developments introduced transposition and double transposition, which amounted to shuffling the plain text around in accordance with a specific numerical key. Transposition security was further enhanced with the distribution of a fixed key imprinted on a silk handkerchief to communication personnel. The essential concept behind ciphers development was the pursuit of a system that allowed for encryption in a timely and efficient manner while realizing a higher degree of security. Eventually the one-time pad was developed which significantly improved both the security and efficiency of encryption.

The Key is placed in the first boxes of the square and completed with the remaining alphabets (J omitted). Two-letter groups are encrypted using the following method.

- Two letters in the same column are encrypted with the letter directly below.
- Two letters in the same row are encrypted with the letters directly to the right.
- Letters not in the same col. or row are encrypted with the letter directly opposite in the diagonal created by the two letters.



**KEY:**  
**CONTEMPORARY**

*Plain Text:*  
Wa sh in gt on

*Encryption:*  
XR ZS LC QA NT

The cipher provided organizations an encryption system for internal communication but the use of a repeating key made the cipher readily breakable. Security of use would require frequent changing of the key and the acknowledgement that security was only a factor of the time it took to break the cipher when messages were intercepted.

C	O	N	T	E
M	P	R	A	Y
B	D	F	G	H
I/J	K	L	Q	S
U	V	W	X	Z

Table 1. Playfair Cipher.

**b. One-Time Pad**

The one-time pad entered operations in September 1943 and remains in use today. The one-time pad used a table containing twenty-six lettered columns for each key letter and in each column, the twenty-six letters of the alphabet and the corresponding encryption. The users were provided a key that was used to encrypt plain text in accordance with the table and subsequently destroyed after each use. The one-time pad is “extremely quick and easy system, [that] does not require constant attention, and does not generate many errors ... [and] is mathematically unbreakable” (Lorraine, 1972, p.74). Much of the reliance on field expedient encryption techniques has been replaced by computer-generated methods.

**c. Computer Generation**

The computer has increased the ability to intercept and decipher encrypted messages but it has also assisted in the development of encryption methods by legitimate and subversive elements. Most individuals are familiar with Phil Zimmerman’s *Pretty Good Privacy (PGP)*, an encryption program that was available to most Internet subscribers in the past, but there are also other techniques that can be developed with the computers random number generator. Most personal computer random generators utilize the internal clock to create a series of characters that can be used to develop an encryption key for the one-time pad if needed. Though the PC methods have their weakness, the accessibility of an individual/computer capable of decrypting the message is ultimate target of all encryption processes. <sup>1</sup>

**4. Reduction**

The reduction of a message’s size can aid in the concealment and decrease the probability of detection during a search. The development of films and microdots has been utilized in the espionage business frequently, but is not necessarily a viable option for subversive elements. Though the methods can be improvised and replicated using certain equipment, the possession of such devices requires concealment and sufficient facilities. The limitations of an individual’s ability to reduce messages without access to

---

<sup>1</sup> Meyers discusses some techniques to develop an encryption key for a one use which are credible. He includes a program written by Ken Balch which manipulates the internal clock time and uses the new number to generate a random number.

special equipment has traditionally been a factor of the amount of additional information that can be omitted from the message while still retaining legibility. The result is the marginalizing of a means selected for capacity to transmit complex and detailed information. However, the process can allow the messenger to remain ignorant of contents minimizing the consequences of the operation. “The well worn trick of inscribing the message on a thin, tight roll of paper, inserted into a cigarette with a needle, usually worked well” (Foot, 1977, p.112) and would attract little attention if discarded or delivered to designated ash tray for removal by the net node. Photo-static reduction equipment and the accessibility of these devices have significantly improved the opportunity for concealment, as do computer-generated messages that can be produced in virtually any legible size. Technological improvements in data storage and the proliferation of concealment devices have made message transport easier but the consequences of interception still remain detrimental to the organization.

In the Hiep Hoa village, the Vietcong maintained a “clear chain of command, carefully compartmented so that one member’s knowledge of the hierarchy was often limited to one contact man” (Herrington, 1997, p.35). However, when the security environment subsided or the organization’s control of the region expanded, the ability for members to coordinate overtly increased. When ‘Hai Chua’ defected from the Vietcong, as the village secretary and highest-ranking Vietcong in the Hiep Hoa, he brought knowledge of the infrastructure established in the village of about 4000 residents. Stuart A. Herrington, working with Operation Phoenix, initiated a series of interviews with Hai Chua to identify members and activities. However, Chua was concerned with his personal safety and was not interested in providing an abundance of information to the program. Chua would frequently explain, “that he had been expelled from his post as a village secretary several months earlier, and for this reason, he didn’t know much about his former comrades’ situation” (Herrington, 1997, p.19). Herrington was also able to contact one of Hai Chua subordinates who had rallied several months earlier but neither of the two former Viet Cong would contribute accurate reliable information.

One night a patrol ambushed a courier who dropped his message pouch while escaping. The enclosed documentation provided Herrington with the information he needed to accurately question Chua and the other Viet Cong. The documents “clearly

belonged to the village's Vietcong security chief ... [and identified] names of the village guerrilla unit ... government informants ... and key members of the village revolutionary committee" (Herrington, 1997, p.19-20). The information Herrington needed to reconstruct the village infrastructure was now replicated in multiple locations within the communication network.

Accurate information requires redundancy in communication to provide alternate sources, confirmation, and reiteration. "Redundancy is the repeating of a message over different channels, in different forms, or over time" (Rogers, 1976, p.92). Indifferent to one's relationship to the networks, an insider like Chua or an outsider like Herrington, an accurate picture of the village infrastructure must be attained from multiple sources. A single channel can only handle a limited amount of information and is therefore subject to distortion and omission. The multiplicity of connections allow for the crosscheck of the informant reports and the confirmation of memberships. When information "is replicated at several locations in the network [it] can be [readily] recovered" (JP 6-0, 1995, II-6), and poses significant risk to the organization. Though not all individuals serve as centralized nodes, the knowledge that any particular non-isolated node maintains can provide an entry point into the communication network.

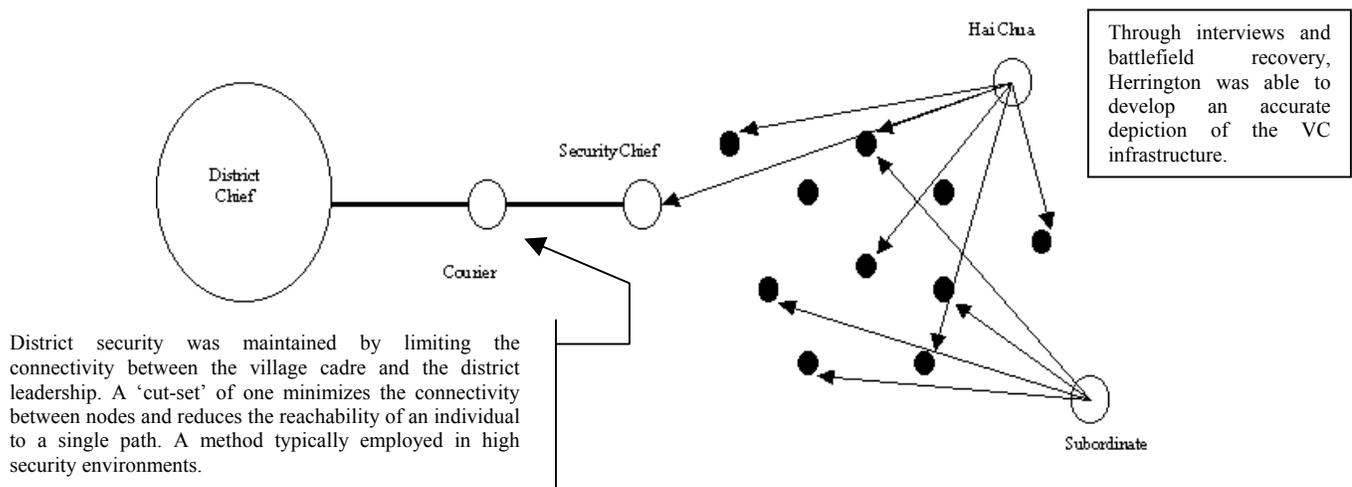


Figure 4. Hiep Hoa Village

Though the Hiep Hoa network was compromised through a redundancy of links and information, the district command was easily isolated from further damage by utilizing a single communication link between nodes. In the absence of multiple links between the district and the village, commanders must rely on one particular path to

transmit and confirm information reports. The transfer of detailed and complex information through multiple links and nodes requires a written communication to ensure accuracy. As in the Hiep Hoa example, the reliance on written documentation can significantly endanger clandestine operations. To reduce the probability of compromise, networks net reliable switching mechanisms to route information to the proper receiver.

## **B. TELEPHONE**

The reliability and accessibility of the telecommunication networks allowed leaders to retain an influential link to organizational members from a distance that has traditionally required face-to-face interpersonal conversation. Whether a pay booth or a video conference call, the phone offers the individual a channel that can readily transmit messages with the proper informational and emotive overtones. However, the communication infrastructure essential to integrating local and international channels has increased the opportunities for surveillance and emplaced its own constraints on the operational personnel. The vulnerability to surveillance and the accessibility of the system has required the implementation of operational techniques to incorporate the efficiency of the telephone system. “Telephones are used in an emergency, the individual goes to a pay station and uses a pre-arranged code” (Molnar, 1966, p.103).

There have been times when the phone can be utilized with a higher degree of safety. The manipulation of the network can provide the deception necessary to prevent the direct identification of participants.

Helen Astrup had lived in Oslo for seven years before the Nazis occupied it in April of 1940. Astrup joined the Joessing Resistance the following year through social contacts. The group she worked with, Frognerveien, was contacted by the telephone and a pre-arranged code.

Our telephone number was in fact no number at all. It was what was called a ‘spare’ at the automatic exchange, and the operator there could pick up the call and answer it. Contacts we wanted could be passed on to the ordinary telephone at Frognerveien, while those it seemed best to avoid could be stopped. The number could never be traced to anyone, anywhere (Astrup & Jacot, 1954, p.203).

The exact mechanics of this procedure may not be discernible but the inclusion of an unassigned jack at the central switch inserted an intermediary node into the channel.

The switchboard operator conducted the initial caller screening and forwarded appropriate callers. The cell could have simply been assigned a spare jack at the exchange that only certain operators were familiar with or the call could have been routed through a spare jack before connecting to the Frognerveien location. Regardless of the systems details, the opportunities created by the resistance personnel's unfettered access to the telephone exchange significantly improved the groups contact security procedures. The recruitment of post and phone personnel to gain access to legitimate communication networks was not uncommon during World War II, but is not the only way to manipulate the telephone system.

Europe has frequently provided sanctuary for Middle Eastern subversives in hiding. The international calls from Europe to the Middle East are frequently intercepted in search of information. In an attempt to bypass interception efforts, Nabil Maksumi, a member of the Ahmed Jibril's Popular Front for the Liberation of Palestine-General Command, set up a telephone relay on Cyprus "that allowed European agents to talk directly to Jibril through the link" (Bell, 1999, p.160). Maksumi's Cyprus switch was an intermediary node that concealed the Germany - Syria connection. Unfortunately for Maksumi, Cyprus has frequently been utilized as a staging area for terrorist activities and all international phone calls in and out of Cyprus were monitored. The connection between the Germany - Cyprus and Cyprus - Syria was identified and intercepted (Bell, p.160). Other elements have been more fortunate in the communication realm as they have had a better understanding of the situation than Maksumi.

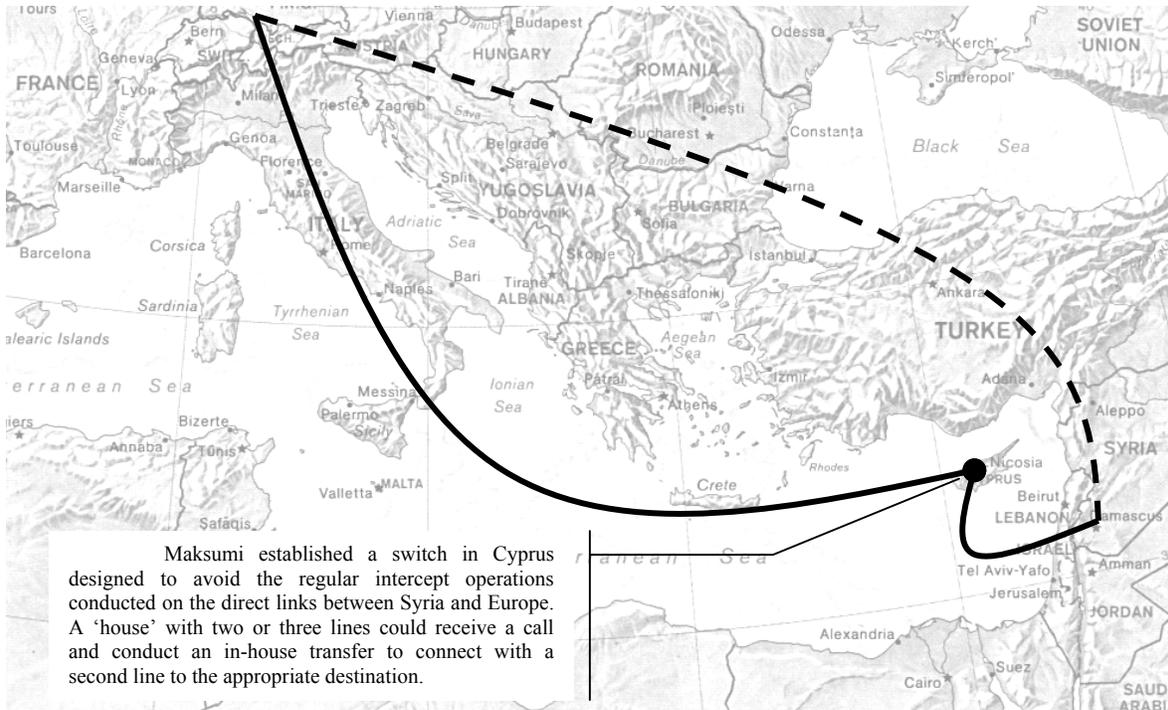


Figure 5. Clandestine Switch

The reliability of the telephone system has promoted its use in maintaining communication with members. However, Italy's Red Brigade lacked competence in the local system and opted to use international lines to talk locally and bypassed the local security constraints imposed to control subversive activity. "The Brigade Rosse ... avoided the local Italian telephone system by recourse to the international system: when in Rome to talk to the Roman Brigade rosse one needed to call Toronto in Canada and so be connected back to Rome through a link that, being international, tended to work, unlike the local Italian system, and which was not monitored by the Italian security forces who were seeking terrorist in Rome not Toronto" (Bell, 1999, p.159-160). The circumvention of interception strategies is not always necessary and can be minimized by rotating phones regularly.

Though expansive, utilization of the telecommunication system to transmit confidential information requires the structuring of activities around the existing access nodes. For example: The use of one's residential or business telephone can easily establish the relationship between two actors; to avoid this dilemma, the members may conduct calls between exterior phones only. A thoroughly designed communication plan would include a rotation of nodes so as to avoid establishing suspicious patterns. One's

daily activities must coincide with pre-arranged phones to maintain contacts. However, even rotations and switching, the lack of assurance that a conversation is not intercepted compels the use of codes and argot that can only be vaguely understood by an adversary and tend to distort or omit information. Such a process is not always feasible and limits the usability of the phone to sending and receiving concise messages that only serve to alert the receiver of a situation and omit practical details. Once again the concept of disguising one's activities as normal behavior reduces the individual's probability of attracting unnecessary attention: for example, the calling of a hotel may inquire about a specific room's availability, or a restaurant's menu items. As in the DF circuit's routing process "competent agents ... took care always to use café call-box telephones ... and to get away from the instrument promptly after making the call" (Foot, 1966, p.95).

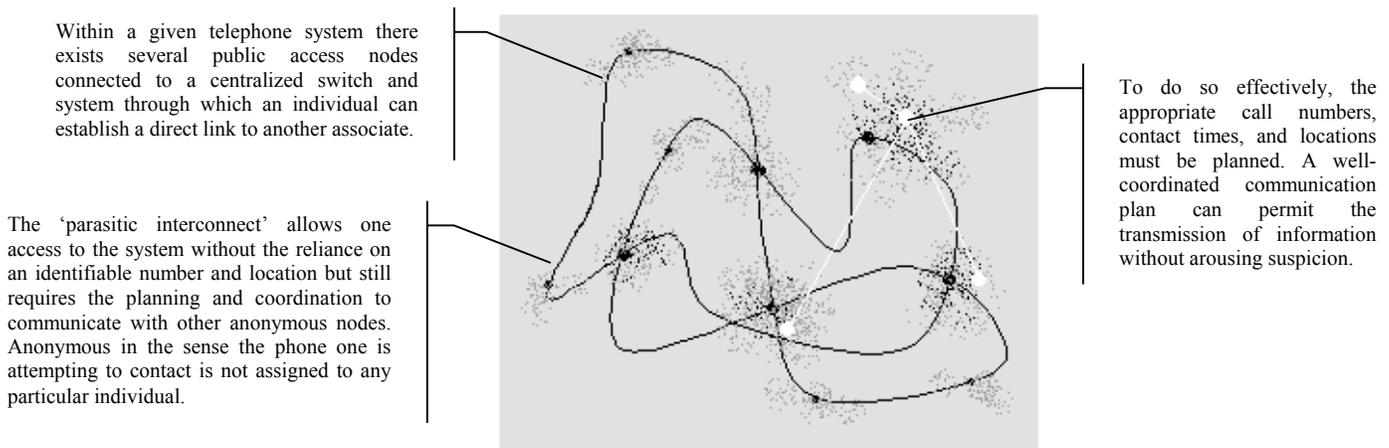


Figure 6. Telecommunication Access

In his book SPYCOMM, Lawrence Myers offers some methods to attain "a parasitic interconnect" to existing phone lines where the individual "installs a secondary extension into the system from an access point that is selected on the basis of security and function" (1991, p.151). With the proper equipment, one can enter the phone network without obtaining an official phone service.

### 1. Mobile Telephone

The mobile telephone eliminates the reliance on stationary terminals and allows reasonably unfettered access from anywhere within a cellular network. The increased mobility and the sustained connectivity with personnel are decisive to personnel related organizations, but create new vulnerabilities. Like other systems that rely on radio waves,

the cell phone is easily intercepted and readily pin pointed by direction finding equipment. Regardless of the exposure of one's conversation on a mobile phone, some subversives have been able to capitalize on the opportunities provided by the cellular technology.

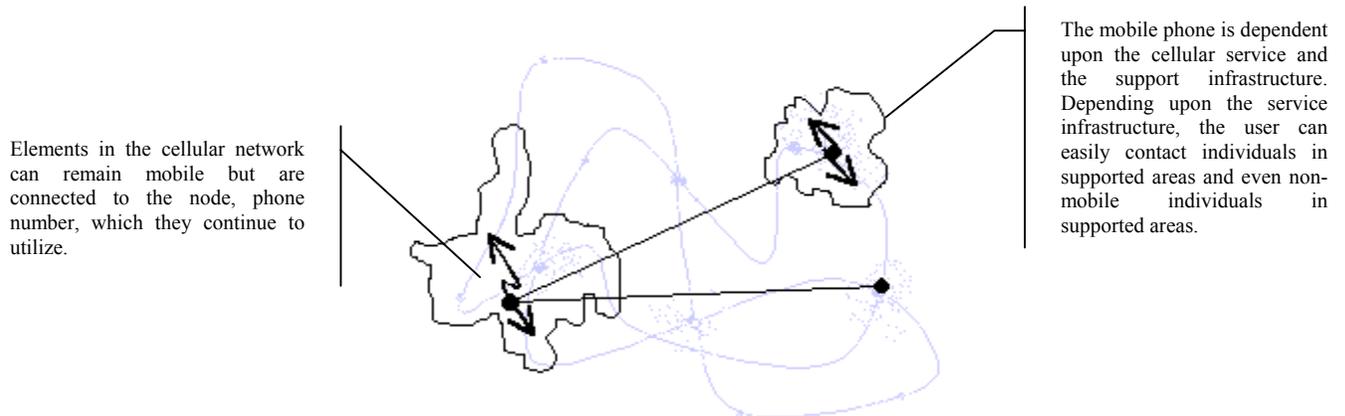


Figure 7. Cellular Networks

Pablo Escobar created a cocaine empire by establishing unchallenged control of the Colombian production and the Medellin drug cartel. Escobar and his lieutenants relied extensively on coercion, retribution, and the cellular telephone. Escobar who relied on “normal hands-on management of the cartel” (Bowden, 2001, p. 117-118) used the cell phone extensively to sustain contact with his lieutenants and other personnel.

Even after his imprisonment, to which his reliance on cell phone usage contributed significantly, Escobar continued to run the world's premier cocaine distributorship through a network of cellular and standard phone connections. Though continually monitored, Escobar was able to manage the Cartel through his lieutenant and other communication techniques that he prioritized according to the needs of security. “Pablo was careful about his communications, using the [carrier] pigeons for his most important messages” (Bowden, 2001, p.115)<sup>2</sup>.

Upon Escobar's return to the fugitive life, the Colombian authorities initiated a massive effort to apprehend and return Escobar to prison. Airborne and ground mobile intercept equipment capable of monitoring and triangulating any radio transmission were

<sup>2</sup> Escobar was not the first subversive to use the pigeon. SOE included pigeons on covert supply drops to resistance elements. The drop Zone party would complete the enclosed message and return the carrier to Britain to confirm receipt of the cargo.

employed around the clock while assault forces stood ready to launch and raid his safe houses. One of the airborne devices provided by the United States, Centra Spike, could intercept and convert multiple vectors into a pinpoint location in a matter of seconds. The ground intercept equipment could establish a vector to the source, but required additional nodes to attain a pinpoint. Regardless of the resources committed to the pursuit, Escobar remained at large and in command of his Cartel. While in prison, Escobar learned to adapt his operational procedures to the constraints imposed by the surveillance methods. A practice he continued after his escape. Carlos Lehder, a former accomplice turned informant provided authorities some insight into Escobar's habit to increase the effectiveness of the pursuit. "Escobar always tries to keep within distance range for his cellular phone to reach Medellin's phone base. That's approximately 100 miles, so he can call any time... occupies the main house with some of his hitmen, radio operator (Big High Frequency radio receiver), cooks, whores, and messenger" (Bowden, 2001, p.183). Escobar would use multiple phones in an attempt to evade detection and even employed a "digital cell phone with scrambling devices, [which took] Centra Spike just fifteen days to adapt" (Bowden, 2001, p.171) and intercept. When "conversing on open lines with his family or friends, he employed elaborate impromptu codes that required remembering specific dates, places, and events" (Bowden, 2001, p.175). When the authorities discontinued the cell phone coverage of Medellin, hoping to make Escobar's communication with personnel, friends and family more difficult, "the drug boss just switched over to radio or communicated by messenger through a series of couriers so that recipient would have no idea where they originated. To ensure that there would be no question about the message's author, Pablo signed with his thumb print" (Bowden, 2001, p.175). Even though the cellular networks provide a means of convenience by which to conduct business, the system relies on the support of an infrastructure that can be turned off in some location if targeted. A link that relies only on the self-contained capacity to broadcast a message a great distance directly is the radio.

### **C. RADIO**

Despite the radio's ability to sustain communications independently of other infrastructures it is still highly vulnerable to interception and direction finders, as well as atmospheric or technical interference. In view of these constraints, transmissions are

generally brief and encrypted. Appropriate operating procedures like frequency changes, relocation of transmitters, or remote antennas, may reduce the vulnerability of the system but can also interfere in the communication process. For many organizations the radio is frequently reserved for priority communication between headquarters and its subordinates, though it has more universally been used as one-way transmission into contested and hostile areas to disseminate information to subordinate elements. As discussed previously, the encryption of messages is a requirement to maintain security, but has been significantly impeded by the inaccessibility of equipment in hostile areas. Radios have seldom been used for an organization's internal communication when couriers were dependable because "monitoring radio transmissions and the use of direction finders are easier for the enemy than the interception of couriers who disappear among the ... citizens." (van Dach Bern, 1965, p.118). Despite advances in both the radio and radio intercept capabilities, secure use of the radio still requires a dynamic process that limits the ability of an adversary to track and locate one's resources.

As authorities began to close in on Pablo Escobar, and adversarial gangs continued to eliminate his lieutenants and associates Escobar was forced to rely exclusively on the radiotelephone for direct communication. The radiotelephone is frequently used in maritime operations between ships and shore assets but is a line sight instrument that is subject to static and other interference. Despite the vulnerabilities to intercept, the radiophone is easy to use and requires little training. The radiophone provides the mobility necessary to maintain freedom and the range to communicate throughout the region Escobar operated. The radiophone's characteristics that make the system particularly susceptible to intercept high power and line-of-sight also make it ideal for avoiding pursuers. Escobar would contact his family and organization "from the back seat of a moving taxi, using a high-powered radio-phone that was linked to a larger transmitter that his men constantly moved from place to place" (Bowden, 2001, p.237). The highly mobile low profile system could be transported virtually anywhere in Medellin with a van, taxi, car or boat. Escobar further complicated the electronic pursuit by frequently changing frequencies, which he initiated with coded communications. Escobar would tell his son Juan Pablo, "Let's go up to the next floor,' or 'the evening has ended,' it was a signal to shift to a specific frequency" (Bowden, 2000, p.2).

The availability of equipment has enhanced the capabilities of the individuals to develop a communication system that can adapt to threats. The commonality of radio devices in the society has made the items less noticeable. Meyers suggest the use of a hand held citizen band radio to receive one-way broadcasts to be retrieved later by the element. The radio equipped with the AC adapter uses a plug in timer to activate the system during the appropriate window. The message is recorded through a voice-activated recorder with a direct link through the tape's external microphone and the CB's earpiece jack.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. CONCLUSION

The preceding discussion was intended to provide an exposition of the techniques, practices, and principles of the clandestine communication system that are necessary for the leaders to control, and maintain the organization's operations as well as the personal contributions of the membership. The system's analysis is not to identify and select an optimum route for traffic but to demonstrate that clandestine communication is a process composed of various actions, which can easily impede the organization's communication. A subversive relies on a single critical path linking elements because the organization is structured in manner that limits the exposure of organizational personnel and the damage that can be inflicted in the event of compromise. "Communication with another underground member is the most dangerous activity in clandestine and covert operations" (Molnar, 1966, p.103). Establishing boundaries between nodes and relying on a switching process to sustain communication throughout the organization control this danger. The switches metaphor for clandestine tradecraft is not to suggest that every communication transfer relies on a combined series of nodes to connect two individuals at the opposite end of the organization, though that is sometimes the case, but to demonstrate the relative difficulty of balancing communication and security. The ability to sustain a *throughput* substantial enough to disseminate orders, ideology, and rewards is a factor of the systems that can readily constrain the organization's ability to adapt to the environment.

The subversive survives in an environment with constantly changing political, economic, social, and personal situations. The dynamics and complexity of the environment increase the demand for accurate, timely, and useable information. The constraints imposed by the security environment significantly limit the development of a responsive communication system and increase the uncertainty within which decisions must be made. To better cope with this uncertainty the organization is structured to reduce the demand for information and incorporate slack resources into the decision and planning process. This slack resource is time.

The connectivity and relations that support timely reliable information flow are a detriment to the subversive. The greater the density of communication channels in a subversive element, the greater the reachability of any member either directly or indirectly. The organization is forced to rely on single channels and multiple switches to route correct information to the appropriate individual. These switches not only deliver information but also establish boundaries that separate important nodes, i.e. the individuals that are necessary to sustain the movement. The organization accepts that information is slow and the necessity to adapt great. To prevent the failure of a single node from compromising the entire organization, that node remains afar from the leadership and easily cut off. The Hollywood depiction of every individual rushing to save the lives of a compromised cell is correct in depicting one's empathy for the compromised individual, but for the well-constructed organization, the penetration is insignificant to the organization's survival. The fate of the movement does not hinge on the ability of one to sustain him/herself through hours of interrogation but on the belief that no individual outside of an isolated cell can be reached in a timely manner. The organization survives by the fact that those individuals know only what is within their boundaries, only the individuals with whom they have trained and depended upon.

## LIST OF REFERENCES

- Adler, R. B., & Rodman, G. (1994). Understanding Human Communication (5<sup>th</sup> ed.). Fort Worth, TX: Harcourt Brace College Publishers.
- Anderson, D., Sweeney, D. & Williams, T. (1976). An Introduction to Management Science Quantitative Approaches to Decision Making. New York, NY: Westing Publishing Co.
- Andrews, W. R. (1973). The Village War. Columbia, MO: University of Missouri Press.
- Astrup, H., & Jacot, B.L. (1954). Oslo Intrigue A Woman's Memoir of the Norwegian Resistance. New York, NY: McGraw-Hill Book Company, Inc.
- Aubrac, R. (1997). The French Resistance 1940-1944. (L. Guiney, Trans.) Paris, FR: Hazan Pocket Archives.
- Bell, J. B. (1998). The Dynamics of the Armed Struggle. Portland, OR: Frank Cass Publisher.
- Bernard, C. I. (1956). The Functions of the Executive. Cambridge, MA: Harvard University Press.
- Bowden, M. (2001). Killing Pablo The Hunt for the Worlds Greatest Outlaw. New York, NY: Atlantic Monthly Press.
- Bowden, M. (2000). Columbia: Killing Pablo – Trackers Get A Line On Elusive Escobar {Electronic version}. Media Awareness Project, 27, 1-4. Retrieved 5 October 2001 from the World Wide Web: <http://www.mapinc.org/drugnews/v00/n1843/a05.html>
- Brown, A. C. (Eds.). (1976). The Secret War Report of the OSS. New York, NY: Berkley Publishing Company.
- Certo, S. (2000). Modern Management (8<sup>th</sup> ed.). Upper Saddle River, NJ: Prentice Hall, Inc.

- Choo, C. W. (1998). The Knowing Organization How Organizations Use Information to Construct Meaning, Create Knowledge, and Make Decisions. New York, NY: Oxford University Press, Inc.
- Conwell, C. (1937). The Professional Thief By a Professional Thief. Chicago, IL: The University of Chicago Press.
- Cravis, H. (1981). Communication Network Analysis. Lexington, MA: Lexington Books.
- DA Pamphlet. (1966). U.S. Army Handbook of Counterinsurgency Guidelines for Area Commanders An Analysis of Criteria. Washington, DC: Special Operations Research Office.
- Foot, M. R. D. (1977). Resistance European Resistance to Nazism 1940-1945. New York, NY: McGraw-Hill Book Company.
- Foot, M. R. D. (1966). SOE in France. An Account of the Work of the British Special Operations Executive in France 1940-1944. Rochester, Kent, ENG: The Stanhope Press.
- Galbraith, J. R. (1973). Designing Complex Organizations. Reading, MA: Addison-Wesley Publishing Company.
- Galbraith, J. R. (1995). Designing Organizations. San Francisco, CA: Jossey-Bass Inc., Publisher.
- Hall, R. H. (1972). Organizations Structure and Process. Englewood Cliffs, NJ: Prentice-Hall, Inc.
- Harris, T. (1993). Applied Organizational Communication Perspectives, Principles, and Pragmatics. Hillsdale, NJ: Lawrence Erlbaum Associates, Publishers.
- Heath, R. L. (1994). Management of Corporate Communication From Interpersonal Contacts to External Affairs. Hillsdale, NJ: Lawrence Erlbaum Associates, Inc., Publishers.

- Herrington, S. A. (1997). Stalking the Vietcong Inside Operation Phoenix A Personal Account. Novato, CA: Presidio Press.
- Horne, A. (1977). A Savage War of Peace Algeria 1954-1962. Harmondsworth, Middlesex, ENG: Penguin Books, Ltd.
- Jablin, F. M., & Putnam, L. L. (Eds.). (2001). The New Handbook of Organizational Communication Advances in Theory, Research, and Methods. Thousand Oaks, CA: Sage Publications, Inc.
- Joint Pub 6-0. (1995). Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Washington, DC: Department of the Army.
- Khandwalla, P. N. (1977). The Design of Organizations. New York, NY: Harcourt Brace Jovanovich, Inc.
- Knoke, D. & Kuklinski, J. H. (1982). Network Analysis. London, ENG: Sage Publications.
- Kreps, G.L. (1986). Organizational Communication Theory and Practice. White Plains, NY: Longman Inc.
- Lansdale, E. G. (1991). In the Mist of War An American's Mission to Southeast Asia. New York, NY: Fordham University Press.
- Lanning, M. L. (1992). Inside the VC and the NVA: the real story of North Vietnam's armed forces. New York, NY: Ballantine Books.
- Leites, N., & Wolf, C. (1970). Rebellion and Authority: An Analytic Essay on Insurgent Conflicts. Chicago, IL: Markham Publishing Company.
- Lindsay, F. (1993). Beacons in the Night With the OSS and Tito's Partisans in Wartime Yugoslavia. Stanford, CA: Stanford University Press.

- Lorain, P. (1972), Kahn, D. (1983). Clandestine Operations The Arms and Techniques of the Resistance, 1941-1944. New York, NY: MacMillan Publishing Company.
- Lunev, S. (1998). Through the Eyes of the Enemy. Washington, DC: Regnery Publishing Inc.
- Marighella, C. (1969). Mini-Manual of the Urban Guerrilla. Ft. Bragg, NC: USAJFK Special Warfare Center.
- McPhee, R. D. (1985). Formal Structure and Organizational Communication. Organizational Communication: Traditional Themes and New Directions, 13, 149-177.
- Mendez, A.J. (1999). The Master of Disguise My Secret Life in the CIA. New York, NY: William Morrow and Company, Inc.
- Mintzberg, A. R. (1993). Structure in Five Designing Effective Organizations. Englewood Cliffs, NJ: Prentice Hall.
- Molnar, H. (1966). Human Factors Considerations of Undergrounds in Insurgencies. Washington, DC: Headquarters, Dept. of the Army.
- Molnar, H. (1963). Undergrounds in Insurgent, Revolutionary, and Resistance Warfare. Washington, DC: Special Operations Research Office.
- Myers, L. W. (1991). SPYCOMM Covert Communication Techniques of the Underground. Boulder, CO: Paladin Press.
- O'Brien, J. A. (1996). Management Information Systems Managing Information Technology in the Networked Enterprise (3<sup>rd</sup> ed.). Chicago, IL: Irwin.
- Polish Home Army Ex-Servicemen Association. (1999). *The Polish Home Army During the Second World War*. Montreal, Canada: Retrieved December 2, 2001 from the World Wide Web:[http://www.citinet.net/ak/polska\\_41.html](http://www.citinet.net/ak/polska_41.html)

- Race, J. (1972). War Comes to Long An Revolutionary Conflict in a Vietnamese Province. Berkeley, CA: University of California Press.
- Rogers, E. M., & Agarwala-Rogers, R. (1976). Communications in Organizations. New York, NY: The Free Press.
- Rotem, S. (1994). Memoirs of a Warsaw Ghetto Fighter. (B. Harshav, Trans.) New Haven, CT: Yale University Press.
- Schultheis, R., & Sumner, M. (1998). Management Information Systems The Manager's View (4<sup>th</sup> ed.). Boston, MA: Irwin/McGraw-Hill.
- Scott, W. R. (1981). Organizations Rational, Natural, and Open Systems. Englewood Cliffs, NJ: Prentice-Hall, Inc.
- Szilagyi, A. D., Jr. & Wallace, M. J., Jr. (1980). Organizational Behavior and Performance (2<sup>nd</sup> ed.). Dallas, TX: Scott, Foresman and Company.
- Thomas, J. B., (1988). An Introduction to Communication Theory and Systems. New York, NY: Springer-Verlag.
- Tompkins, P. K. & Cheney, G. (1985). Communication and Unobtrusive Control in Contemporary Organizations. Organizational Communication: Traditional Themes and New Directions, 13, 179-210.
- von Dach Bern, H. (1965). Total Resistance. Boulder, CO: Paladin Press.
- Wettering, F. L. (2001). The Internet and the Spy Business. International Journal of Intelligence and Counterintelligence, 14, 342-365.
- Wilson, R. J., & Watkins, J. J. (1990). Graphs An Introductory Approach. New York, NY: John Wiley & Sons, Inc.

THIS PAGE INTENTIONALLY LEFT BLANK

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Superintendent  
ATTN: Professor Gordon H. McCormick  
(SO/LIC)  
Naval Postgraduate School  
Monterey, CA 93943-5000
4. Jennifer Duncan  
(SO/LIC)  
Naval Postgraduate School  
Monterey, CA 93943-5000