(London, 1977), pp. 8-13, 49-79, 110-18.

12. Nicholas Bethell, *The Palestine Triangle: The Struggle Between the British, the Jews and the Arabs, 1935-1948* (London, 1979), *passim*; Hurewitz, pp. 295-329.

13. Curtis et al, pp. 52-62, 70, 131.

14. Nadav Safran, *Israel: the Embattled Ally* (Cambridge, Mass., 1978), pp. 67-82, 385.

15. *ibid.*, pp. 258-61, 266-71; Bard E. O'Neill, *Armed Struggle in Palestine: a Political-Military Analysis* (Boulder, Colo., 1978), pp. 43-50, 107-23; Curtis et al, pp. 114-16, 139.

16. The war stirred considerable controversy within Israel, especially in the Israeli Defence Forces. For a useful account and analysis see Chaim Herzog, *The War of Atonement: October 1973* (Boston, 1975).

17. George Lenczowski, *The Middle East in World Affairs*, 4th ed. (Ithaca, N.Y., 1980), pp. 568-71.

18. O'Neill, PP. 215-17.

19. Lenczowski, pp. 606-10; Safran, p. 567.

20. Colin Legum, ed., *Middle East Contemporary Survey, Vol. 2, 1977-78* (New York, 1979), pp. 213-15, 227-30, 232-33.

21. See "A Sudden Vision of Peace", *Time*, 25 Sept. 1978, and "A Glimpse of Peace", *Newsweek*, 26 Mar. 1979; *New York Times*, 5 June 1980; *Economist*, 23 Aug. 1980; *Washington Post*, 5 Mar. 1981.

22. Adeed Dawisha, "Saudi Arabia's Search for Security", *Adelphi Papers*, no. 158 (1980); *Washington Post, 6 Feb. 1980; Newsweek*, 3 Mar., 4 Aug. 1980; *Time*, 16 Mar. 1981.

23. Interviews with Yasser Arafat, *Time*, 9 Apr. 1979, *International Herald Tribune*, 31 July, 6 Aug. 1980; see also, *Time*, 14 Apr. 1980; *Newsweek*, 8 Sept. 1980; *Guardian Weekly*, 16 Mar. 1980; *Economist*, 21 June, 9 Aug. 1980.

24. *New York Times*, 1 June 1980, 5 Feb. 1981; *Newsweek*, 11 Aug. 1980, 23 Mar. 1981; *Economist*, 28 Feb. 1981; *Time*, 16 Mar. 1981.

SECURITY OR CENSORSHIP? THE CRYPTOGRAPHY CONTROVERSY

by

Rodney H. Cooper

Cryptography, the study of secret codes and cyphers,[1] has long been the preserve of governments. In 1952 the United States Government created and designated the National Security Agency (NSA) to be the sole agency responsible for developing and employing cryptographic techniques on the government's behalf. It was also richly endowed with funds to encourage research in this field which was carried out, often with joint sponsorship of the National Science Foundation (NSF), at a limited number of universities.[2] Until recently the knowledge gained from this research was distributed on a highly restricted "need to know" basis — the only keyword on research papers was MOST

SECRET. But in the 1970s cryptography began to emerge from the shadows. Books such as *The Ultra Secret*[3] were published, universities with computer science faculties began to offer courses in cryptography and a scholarly journal was established.[4] By the end of the decade issues of national security and academic freedom were once again on collision course. At the heart of the dispute is disagreement over the extent to which cryptographic research should remain classified.[5] This article will discuss some of the issues involved.

It is not generally recognized, even by the informed public, that cryptography represents a large, expensive and important part of the global equation of security between nations. Secure communications are essential for diplomacy, policy-making and military planning and operations. Governments need to be able to transmit and store vital information without leakage and encryption systems make such security possible. At the same time governments recognize implicitly the importance of having a capability to "break" the cyphers of their opponents, for this too enhances the security of the more skilful government. The tension between these apparently contradictory principles is accepted. Consequently, cryptography is a study of cyclic efforts. As each technique or code system is invented, a penetration effort is mounted to by-pass or break it and governments must evaluate the cost of penetration (and preventing it) in terms not only of dollars, time and people, but also in relation to the value of the information being stored or transmitted. If the cost of penetration exceeds the value of the information gained then the encryption system may be said to be effective. Nonetheless, cryptographic research and operations are very expensive — the NSA's annual budget exceeds one billion dollars.[6]

One fear, however, haunts security planners — the fear that the variables of the global equation may slip and destabilize the balance of security. With the growth of public and published research in cryptography, slippage in one vital part of the equation is already taking place. Such is the extent of non-government research in the field that in 1979 Admiral Bobby Ray Inman, then Director of NSA (and now Deputy Director of the CIA) broke with established precedent to warn publically that: "There is a very real and critical danger that unrestricted public discussion of cryptologic matters will seriously damage the ability of this government to carry out its mission of protecting *national security information* from hostile exploitation."[7] Until Admiral Inman spoke out it was virtually unheard of for the NSA Director to make a public statement of any kind. Given the Admiral's reputation as an honest efficient bureaucrat who "thrived in the spotlight of Congressional oversight" of intelligence operations,[8] his concern should not be dismissed lightly. Where in the spectrum of low intensity conflict could the expansion of cryptographic research make a difference?

Terrorism is one form of conflict which could benefit from the extension of cryptographic knowledge, since the effectiveness of terrorism depends very largely on accurate information about intended targets.[9] Since information on the plans and activities of security forces and the leaders or other persons they are supposed to protect is usually stored or transmitted in code or cypher, a penetration capability would be useful to terrorists. In most western countries files, magnetic tapes, and computer storage facilities can be kept secure only to an extent. Those authorized to have access are often unprotected, vulnerable to deception, coercion or compromise. Moreover, the universities are accessible and the journals are available. Mathematicians as good or better than those employed by government are leaving analysis, statistics and algebra (the areas essential as background for research in cryptography), taking their knowledge with them, studying coding systems, inventing and breaking them, meeting with their colleagues, exchanging ideas, and publishing. In addition there is profit motivated capital infusion from large computing and telecommunication corporations interested in the lucrative markets of data storage, transmission, and retrieval for industry, government, and the individual. Research into privacy technology is being seen as a definite commercial edge with a public currently obsessed with a fear of too much "Big Brother" government, indiscriminate dissemination of public information, and the loss of the human right to privacy.

Not all governments have access to giants like the NSA to guarantee the safety of the secrets they wish to store or send. These governments, unable to maintain a concerted effort of their own in cryptography and denied the knowledge of the large powers, have to service their security requirements with published algorithms, small groups of mathematicians without adequate training in the area, and a new industry that can claim expertise without adequate justification. In these smaller countries a terrorist group armed with this sudden surfeit of previously inaccessible information may probe and break the security codes, thereby gaining intelligence and hence, a degree of effectiveness they did not have previously. They may also employ these techniques within their own organization making it more difficult for the security forces to disrupt their activities. This is scarcely a fanciful threat. Both the Provisional IRA and the Italian Red Brigades have demonstrated considerable expertise in the field of communications intelligence and in France a group known as Direct Action has carried out concerted attacks on government computer centres.[10]

Terrorism is merely one form of conflict which can be affected by the spread of cryptographic knowledge. Espionage is another, but it is beyond the scope of this essay. Clearly there are implications for civil liberties that lie well beyond the field of conflict studies.[11] But the clock cannot be turned back on cryptographic research and it is to be hoped that western nations can devise a formula which balances the needs of national security, academic freedom and the individual right to privacy.

Footnotes

[1] A code uses an agreed text as a dictionary to translate a word or message to and from its hidden meaning. A cypher employs a mathematical transformation to achieve the same object. For definitive account of the history, theory and practice of cryptography see David Kahn, *The Codebreakers: The Story of Secret Writing* (New York, 1967).

[2] See Kahn, pp. 672-733; and Tyrus G. Fain et al, ed., *The Intelligence Community: History, Organization, Issues* (New York, 1977), pp. 347-75.

[3] F.W. Winterbotham, *The Ultra Secret* (London, 1974).

[4] *Cryptologia*, published by Albion College, Michigan.

5. In January 1981 an NSF-funded committee of the American Council on Education recommended that editors of science journals review scientific papers on cryptography to identify those that may be candidates for censorship. Opposition to any restriction on such publications continues. See for example articles in the *Washington Post*, 8 Jan. 1981; *Los Angeles Times*, 1 Feb. 1981; *New York Times*, 10 Feb. 1981; *Chicago Tribune*, 21 Feb. 1981.

6. A 1978 estimate placed the NSA's budget at $1.2 billion. It employs 24,000 people. *Time*, 6 Feb. 1978.

7. *Signal* (March 1979). *Signal* is the official journal of the US Armed Services Communications and Electronic Association.

8. *Newsweek*, 16 Feb. 1981.

9. Paul Wilkinson, *Terrorism and the Liberal State* (London, 1977), p. 114.

10. Peter Janke, "Ulster: a Decade of Violence", *Conflict Studies*, no. 108 (1979), p. 17; Vittorfranco S. Pisano, "The Red Brigades' a Challenge to Italian Democracy", *Conflict Studies*, no. 120 (1980), p. 10; *Newsweek*, 28 Apr. 1980.

11. Computer crime — such as unauthorized access to bank accounts — being a case in point. See Donn B. Parker, "How People Get Computers to Steal Money", in *Leaders*, vol. 4, no. 2 (1981).

INFRASTRUCTURES OF TERRORIST ORGANIZATIONS[1]

by

J.K. Zawodny

The purpose of this article is to answer three questions: first, what is the main characteristic of terrorist organizations that affects their infrastructure? Second, what does the infrastructure look like? Third, how does this infrastructure affect the behavior of terrorists? The analytical level of concern here is that of group dynamics.[2] "Infrastructure," for the purpose of the article, means an *internal organization structure, including formal and informal networks within that structure.* It is this writer's thesis that this structure affects the behaviour and activities of terrorists.

The data comes from nonclassified, open sources (in five languages), dealing with active terrorist movements in the USA and abroad. Since it is quite impossible, for security reasons, to acquire reliable information from first hand interviews with terrorists, this article by necessity relies on scattered data that in many instances defies verification. Nonetheless, in the view of this writer, who had five years of combat service as an urban guerrilla during World War II, the data provides sufficient basis for conclusions to be drawn from uniformly present characteristics across several cultures.

Main Organizational Characteristics Affecting Infrastructure

The principal characteristic is the relatively small size of the organizations. It might be useful for comparative purposes to realize that the European under-