Global Network Intelligence and Information Warfare:

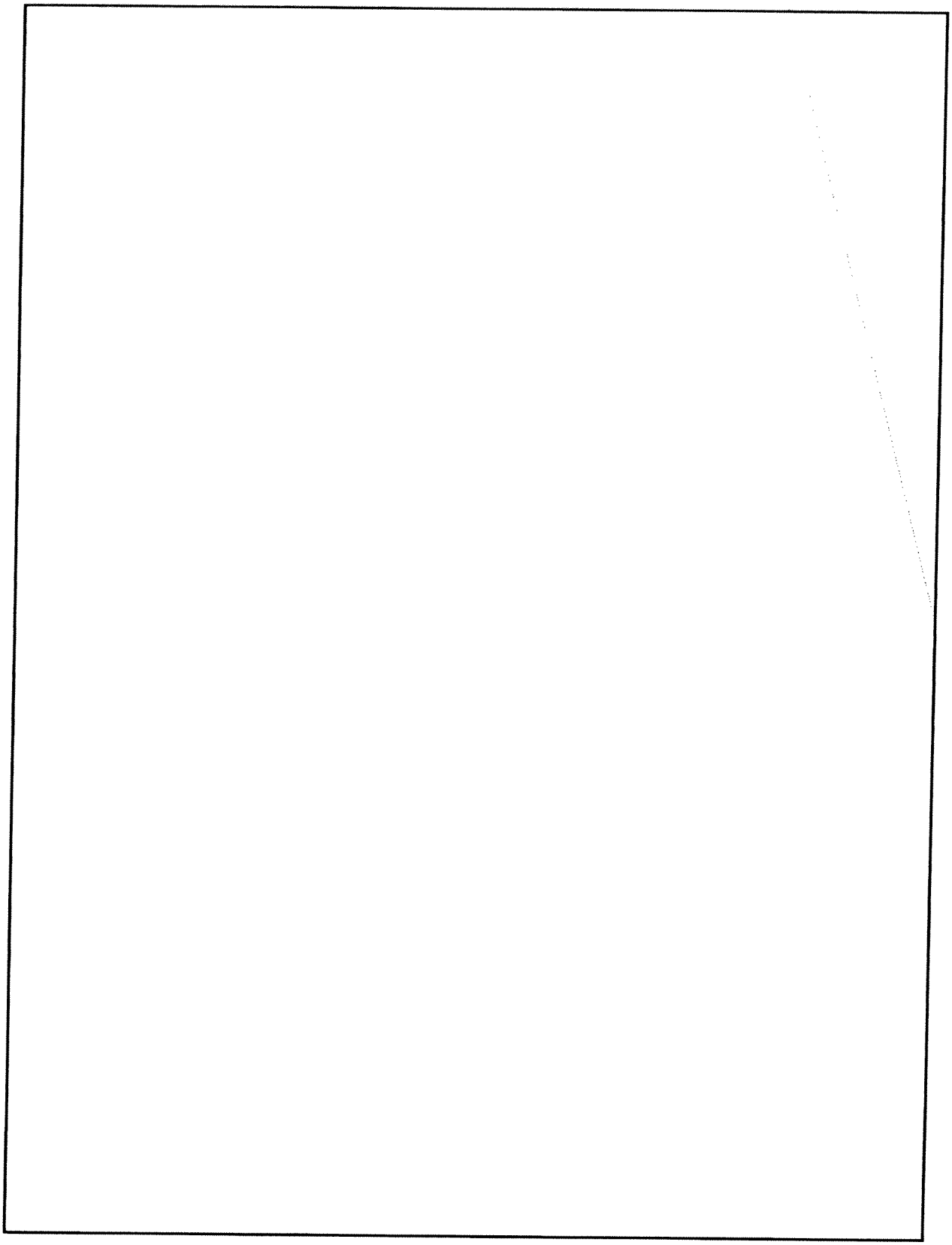
SIGINT and INFOSEC in Cyberspace

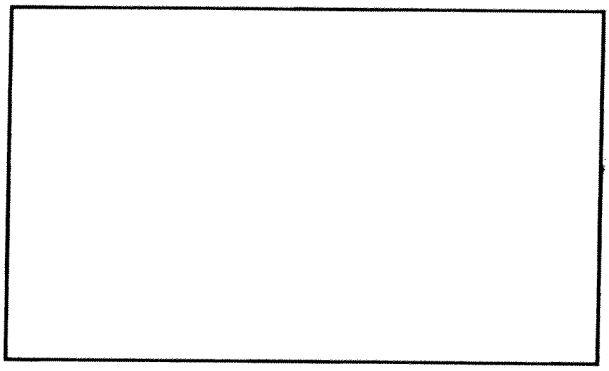
by [redacted] *Former chief, G4*

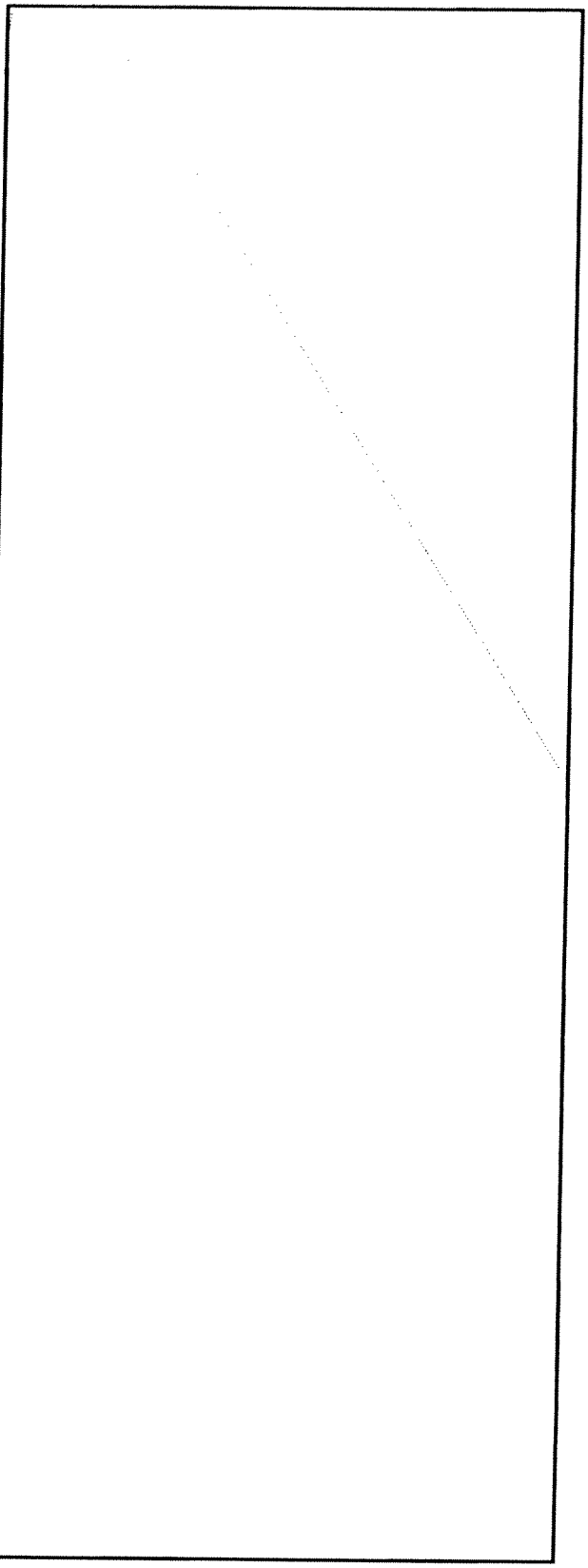
~~(S-CCO)~~ GNI (Global Network Intelligence) and IW (Information Warfare) are two acronyms that have become part of NSA's language over the past couple of years. Both convey new and comprehensive activities that are critical to NSA's future and both dramatically affect the Agency's offensive (SIGINT) and defensive (INFOSEC) missions. The purpose of this article is to provide a general overview of the background and ongoing activities in each area, to explain their interrelationships, and to discuss a few relevant challenges that are of general interest to the NSA workforce.

~~(TS-CCO)~~ GNI and IW are responses to the dramatic changes in global telecommunications that began with the transition from analog to digital communications in the 1980s. The rapid evolution of digital communications and concurrent advances in transmission media—especially fiber optics—and networking technologies have radically altered the complexion of the global telecommunications infrastructure. GNI and IW address these changes, but from different perspectives.

[redacted]





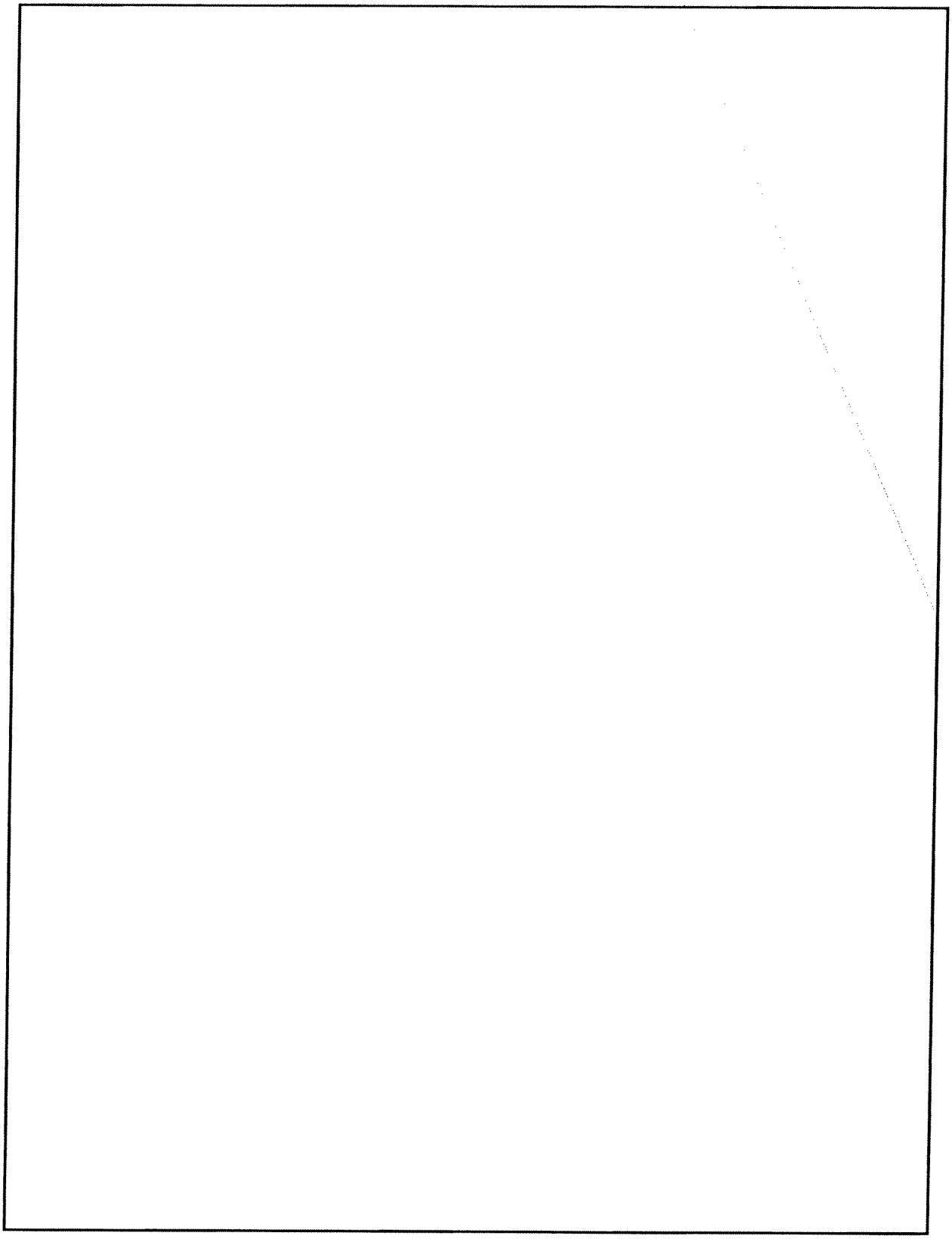


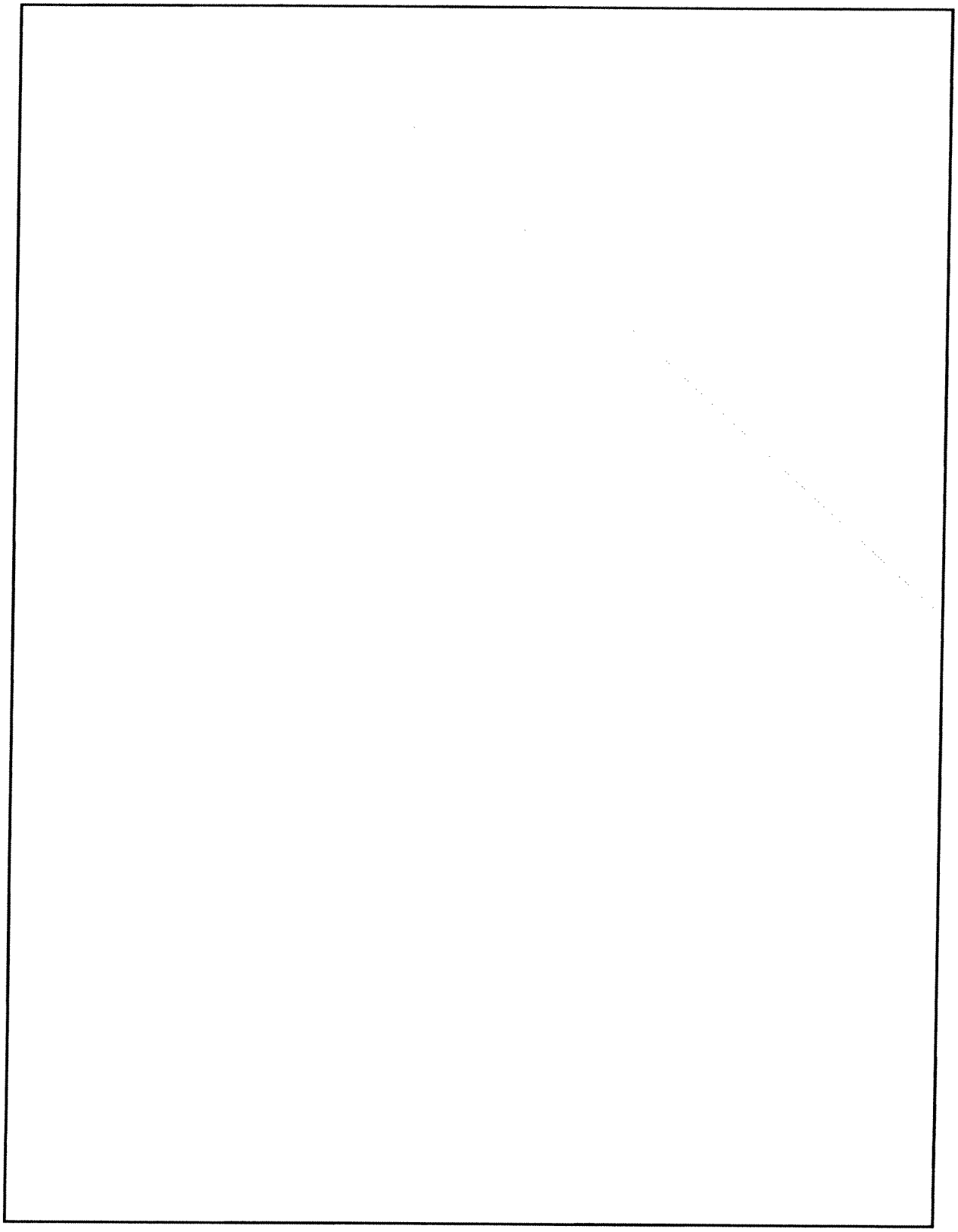
~~(FOUO)~~ Some examples may help to clarify the notion of a "global network" in terms of the telecommunications media involved and functions performed. When Mrs. Jones in Kansas City calls her sister in Tours, France, her telephone call is carried through the local and regional telephone network near her home, over the U.S. domestic fiber-optic network, through the undersea fiber-optic network between North America and Europe, then through the regional fiber-optic network in the U.K. and France, and finally into the local Tours telephone system. In another example, a cellular call from a Japanese businessman from his car in Tokyo to a branch office of his company in Los Angeles will traverse the Tokyo metropolitan cellular, microwave, and fiber-optic system, be routed through either the Pacific fiber-optic network or over a commercial satellite link to the U.S., then pass through the regional, metropolitan, and local fiber-optic network to the Los Angeles office. At the same time, the signalling information for this call—the 1's and 0's that provide key information to route the call and provide billing information for the telephone companies involved—may travel over a completely different path. The global network has the capacity and flexibility to provide many different pathways for connecting one user to another. As the network expands through connections of still more local, regional, and national networks, users will be able to contact other users anywhere on the globe without ever knowing exactly how their calls were completed. The same is true for data communications. This connectivity is already available for personal computer users through the Internet and for an increasing number of telephone and data services users. As technology improves, global connectivity will be faster, more diversified in terms of actual call routing, and encompass a wider variety of advanced services.

1. INFOSEC information in this and later paragraphs was derived primarily from the NSA/DI booklet, "Security Solutions for Today and Tomorrow," published in February 1994.

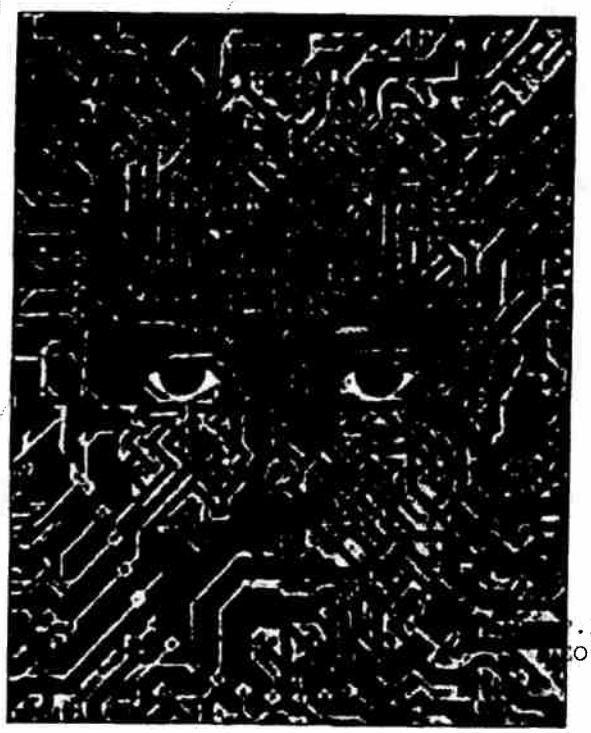
~~TOP SECRET~~

P.L. 86-36
EO 1.4.(c)





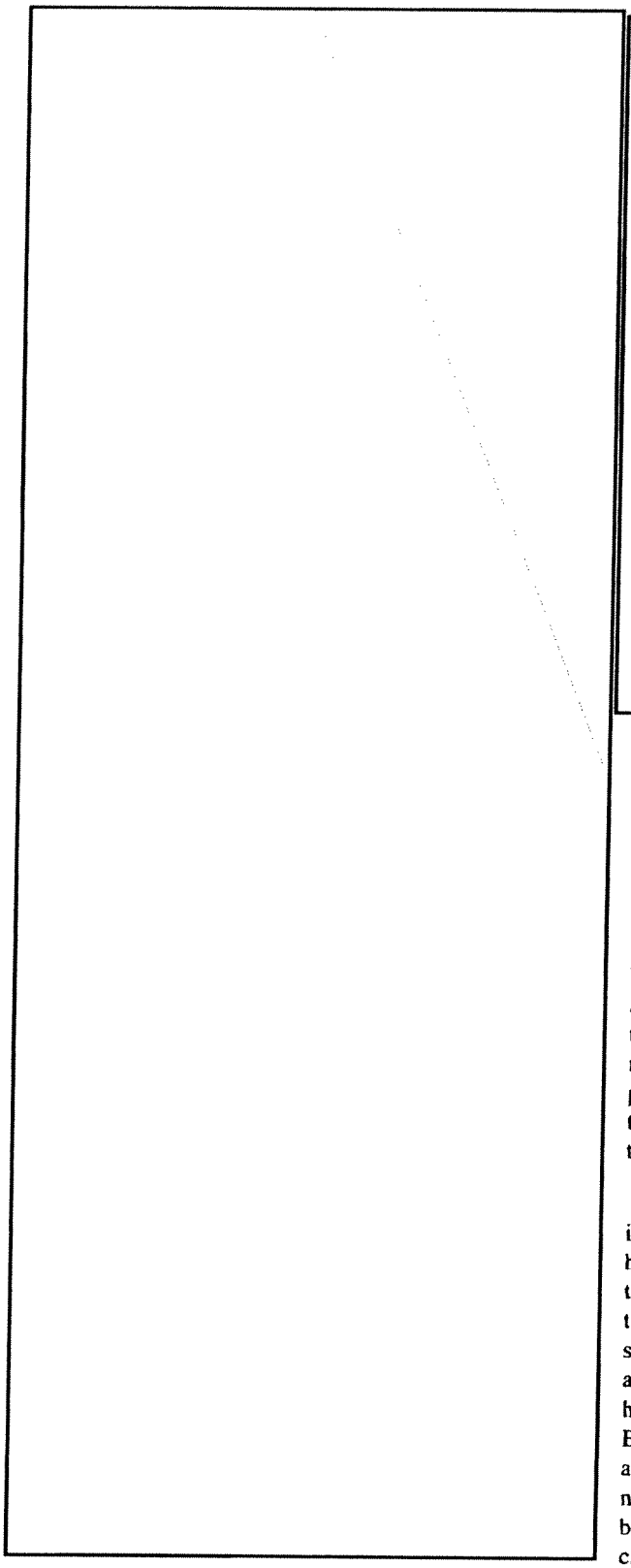
EO 1.4.(c)
P.L. 86-36

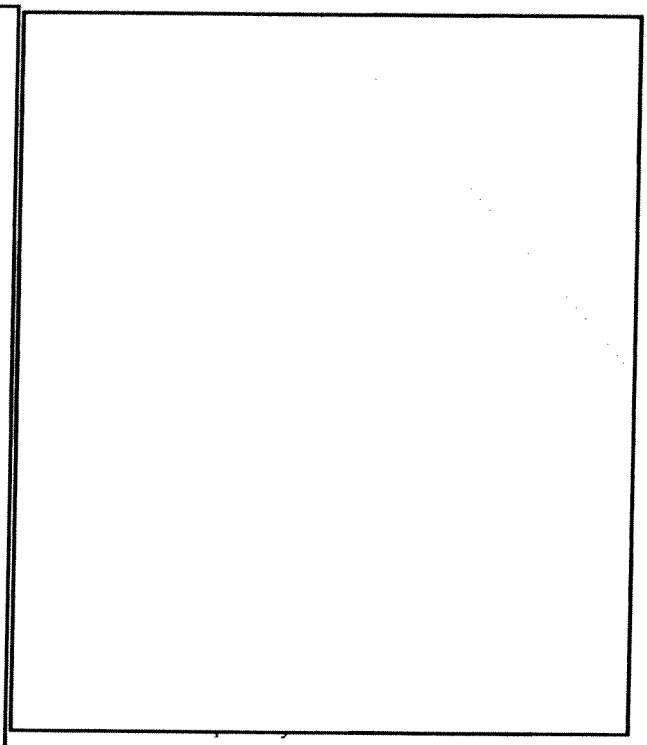


P.L. 86-36
EO 1.4.(c)

Information Warfare

~~(FOUO)~~ Information Warfare addresses the global network from a different perspective than GNI. IW recognizes that the rapid advances in telecommunications will directly affect the U.S. ability to wage war for U.S./ Allied forces as well as for potential adversaries. Future wars may well be fought and decided on the "information battlefield" without a shot being fired. The sophisticated telecommunications and data networks now being deployed worldwide make it possible to deny and degrade a potential adversary's command and control communications and sensitive commercial and diplomatic communications from great distances with little or no risk to life and limb. Conversely, the same network technologies make it possible for a potential adversary to damage or cause confusion in communications and information systems supporting U.S. military forces or the U.S. at large.

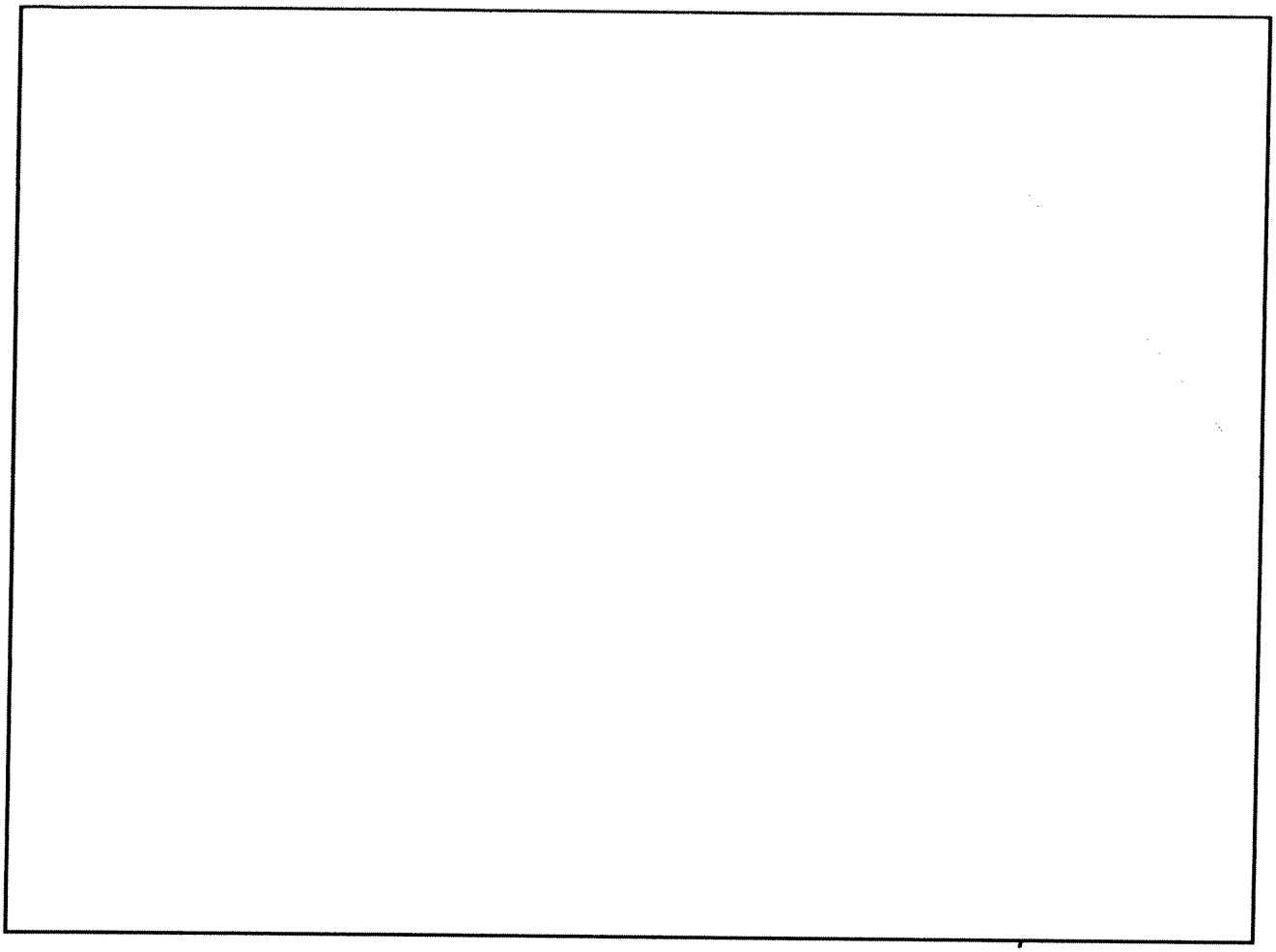




~~(FOUO)~~ Despite the many technical problems, in my judgment the more difficult challenges of the telecommunications revolution are in the organizational/cultural area. NSA has historically risen to technical challenges of SIGINT and INFOSEC by relying on the extraordinary talent and resourcefulness of the NSA workforce. Complex and creative solutions that would be considered science fiction by the general population are routine tools in NSA's approach to signals collection, processing, and forwarding, and information security. One should not take for granted that NSA professionals will be able to meet any and all future technology challenges, but we certainly have a good track record.

~~(FOUO)~~ More worrisome than the technology issues are the challenges posed to NSA as an institution, by which I mean the organizational culture and traditional ways of doing business. The Agency's organizational culture has changed dramatically over the past several years because of continuing budget reductions and the detailed examination of national priorities that has taken place since the demise of the Soviet Union. But as an institution we still tend to function too much as a collection of "stovepipes" in the development of new capabilities. Let me then conclude this essay with a brief description of the organizational/cultural challenges posed by GNI and IW.

EO 1.4.(c)
P.L. 86-36

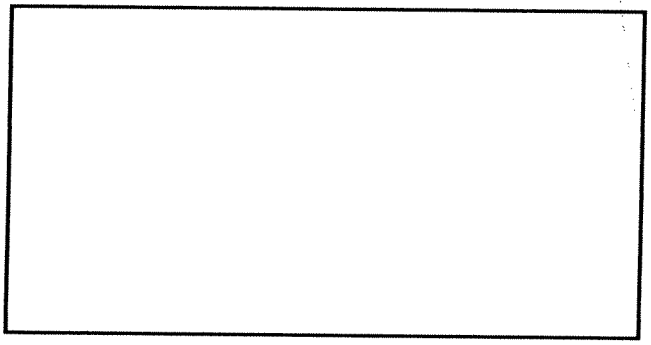


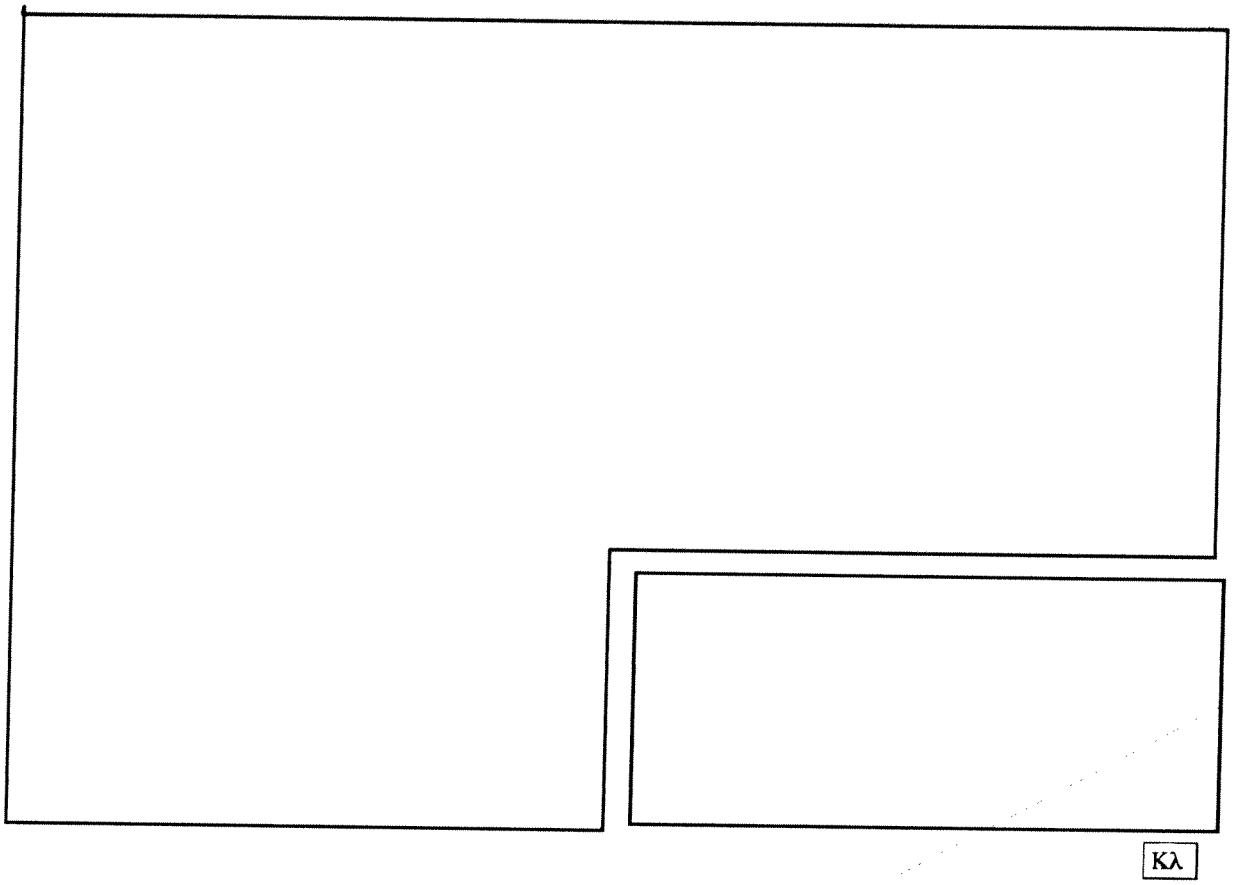
Cross-organizational Communications

(FOUO) Communications among and between NSA organizations is critical. To really achieve teamwork at NSA, individual developers, analysts, mathematicians, and other specialists have to maintain an awareness of what others are doing, and, conversely, must share knowledge of their work with others. This will allow greater cross-organizational communications about various aspects of a large problem and lead to faster, more complete solutions. We need to do a better job of communicating what is going on across the Agency so that those charged with developing new GNI or IW capabilities can keep abreast of all relevant activities. Communications with external partners is another essential ingredient for future success. Such communications are vastly improved now compared to the past, but GNI and IW impose new and slightly different demands.

(FOUO) There is an expanded need for cross-organizational communications internal to NSA, too. While there is some overlap between organizations working on GNI with those working on IW, this overlap is not total. There is a continuing need for managers and technical leaders to ensure they maintain awareness of what others are doing and communicate to other organizations the projects and activities underway in their own organization. This way, cross-fertilization of ideas can take place that will help both the GNI and IW efforts.

P.L. 86-36
EO 1.4.(c)





P.L. 86-36