Non - Responsive

[redacted]

NATIONAL SECURITY AGENCY

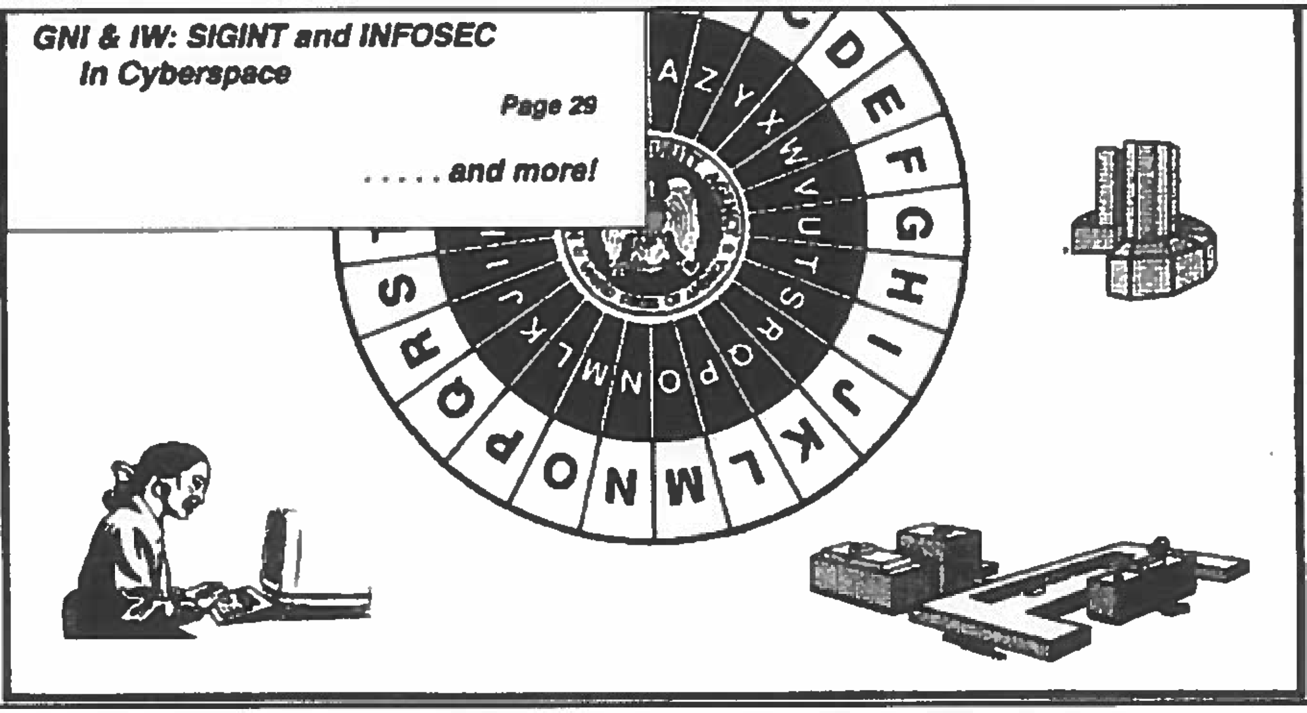
# CRYPTOLOG

## The Journal of Technical Health
## 1995

Non - Responsive

VOL. XXI NO. 1

[redacted]



**GNI & IW: SIGINT and INFOSEC In Cyberspace**

*Page 29*

*. . . . . and more!*

[redacted]

# Global Network Intelligence and Information Warfare:

# SIGINT and INFOSEC in Cyberspace

PL 86-36/50 USC 3605

*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. GNI is focused on access to information while IW encompasses the concepts of denying potential adversaries access to their information and simultaneously protecting U.S. communications from adversary attacks. Both concepts have origins in NSA and DoD activities begun in the mid-1980s; the new names reflect the expansion of these activities that has occurred during the past several years.

~~(S-CCO)~~ GNI is the sum total of the Agency's efforts to retain access to target communications in response to the global telecommunications revolution. Dramatic and rapid changes in telecommunications technology—including the transition from analog to digital, the proliferation of fiber-optic cable, and the expansion of networking—are affecting virtually all of NSA's SIGINT targets. Many of the techniques that worked so well in the past to collect signals from military, commercial, and diplomatic targets cannot be used against telecommunications systems being deployed in the 1990s. New techniques must be developed to ensure NSA continues to produce SIGINT that counts for an expanding and diverse set of customers. By the same token, new techniques and capabilities must be developed for INFOSEC to ensure NSA and other U.S. Government agencies and departments can take advantage of current and emerging telecommunications technologies without jeopardizing security. While the SIGINT crowd worries about fiber optics and network access, network security is the primary headache-inducer for the INFOSEC organization.

~~(S)~~ IW is a concept that grew out of Pentagon discussions about the impact of the telecommunications revolution on warfare. These discussions focused on the same technologies that are key to GNI, but considered them from the perspective of the warfighter. The basic question from an offensive perspective was how U.S. military forces could achieve a military advantage by disabling all or part of a potential adversary's telecommunications and information infrastructure, thus effectively denying the adversary the ability to command, control, and communicate with his deployed forces. From the defensive point of view, the issue was how to protect the communications of U.S. forces to ensure no adversary could deny U.S. command, control, and communications. While Information Warfare includes other components (e.g. Operations Security, Psychological Warfare), telecommunications is the area of most direct interest to NSA and the area in which NSA is most involved.

~~(TS-CCO)~~ GNI and IW have several things in common. First, they are both "culture-modifying" in the sense that they challenge the traditional ways NSA has done business. GNI is causing us to rethink the SIGINT target. IW is bringing new focus on NSA relations with the services. Both have a major impact on INFOSEC. Second, each places new demands on NSA as a corporation and on the workforce in general. Both topics are thus the subject of Agency-wide strategic planning; the GNI and IW strategic plans are reviewed by the BoD annually and updated as necessary. In addition, Agency Steering Groups have been established for both subjects to provide routine guidance and to report to the BoD as appropriate. Training has been an important part of this activity, particularly for GNI. A GNI familiarization seminar was taught for all NSA employees in grades GG-13 and above; a Learning Center course is offered for junior employees. Military personnel assigned to NSA were included in all this training. Third, both call for extensive teaming among NSA organizations and between NSA and, where appropriate, external organizations. Attempts to address all the challenges posed by GNI or IW by a single organization or within the boundaries of a single project are doomed to failure. The technologies, activities, operational aspects, program and budget dimensions, and many other facets of GNI and IW are too complex for "stove-pipe," single-point solutions. Fourth, both GNI and IW have compartmented aspects. IW is generally more compartmented, and this compartmentation is derived largely from military service Special Access Programs. GNI activities also have compartmented aspects, most of which protect new and evolving access techniques. Finally, many of the same people are involved in GNI as well as IW, and both activities are the subjects of continuing interest in the Intelligence Community, the Department of Defense, and the Congress.

## Global Network Intelligence

[redacted] Global Network Intelligence describes NSA's overall efforts against modern telecommunications. It includes the things we're now doing—in many cases very successfully—as well as the things we need to do in the future to produce SIGINT that is valuable and relevant to policymakers. As the telecommunications revolution continues to connect local and regional networks into the long-haul communications networks linking countries and continents, SIGINT targets of interest will increasingly be available through access to the global network. In this context the singular use of the word "network" is misleading. The global network is not a single entity, but rather a conglomeration of many different networks covering geographical areas of many sizes, from countries to continents, from metropolitan areas to hemispheres. The component networks comprise satellite communications, fiber optics networks, cellular, microwave, and wireless radio-frequency (RF) networks as well as local and regional telephone systems. Any communications system or network can be part of the global network as long as it is connected to the other networks that provide global connectivity. More generally stated, then, GNI is the "network problem" for SIGINT.

([redacted]) For INFOSEC, global networks present a different set of challenges. As U.S. government and industry users transition their communications systems over to networks or take advantage of the exploding array of networked services being offered commercially, they need certain assurances. They need to be sure that the data they receive is authentic, that it has been originated and received by valid parties, and that it is protected from unauthorized users. Another aspect of the INFOSEC problem is the need to provide multi-level security so that users can send information at various levels of classification over common networks. And, with continuing budget declines, it is important to migrate data-assurance techniques to the commercial market so that U.S. Government and industrial users can take advantage of lower prices introduced through economies of scale. Ensuring data integrity, authenticity, availability, and privacy of information are difficult challenges in any communications scenario; they are especially daunting in a world increasingly characterized by networks.[1]

~~(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.

~~(S-CCO)~~ These dramatic changes in the world's telecommunications are having a direct impact on the ways NSA thinks about its SIGINT and INFOSEC missions. To facilitate GNI activities, a GNI Strategic Plan developed in 1993 defines approximately 25 objectives with responsibilities assigned to many organizations throughout NSA. The purpose of this plan is to stimulate consciousness-raising in the Agency's workforce regarding new trends in target telecommunications and to describe the types of end-to-end processes needed to ensure corporate success. The GNI plan takes account of the many activities underway to gain/retain access to global telecommunications critical to SIGINT, and underscores the need for teaming among Agency key components to ensure success. In January 1994, a Transition Management Team comprising 15 SIGINT and INFOSEC professionals from the DO, DT, DI, and DS organizations was established in G Group to monitor the actions spelled out in the GNI Strategic Plan and to facilitate their implementation. This effort has been very effective in getting people together to work on common problems, to learn (or "relearn") the SIGINT business from a more corporate perspective, and to provide a cadre of people (the TMT) that will return to their respective organizations with a solid foundation for future activities. In addition, K06, DT's focal point for GNI, is conducting a comprehensive analysis of technical SIGINT activities in the DT to identify potential gaps where additional technology development is needed.

~~(S-CCO)~~ In fact, much exceptional work has already been done to ensure NSA retains access to key target communications as they move from traditional, point-to-point circuits to the global network or as the technology is upgraded in the existing components of the network. [redacted] changes in collection require commensurate changes in SIGINT communications and processing architectures, and many upgrades and new technologies are being introduced in these areas, too. New analytic tools are in development to help filter out communications with little or no intelligence potential and to select those communications that do have potential to meet reporting thresholds. In addition, new techniques are being developed that take advantage of the technical features of net-

[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.

EO 1.4.(c)
PL 86-36/50 USC 3605

worked communications building on the capabilities [redacted]

[redacted] Future SIGINT targets will become increasingly more complex. We need continuing ingenulty and creativity to ensure we can collect and process data, relate the various communications media, and reconstruct communications transactions to present to analysts in usable and meaningful form. This is not a trivial set of tasks. We also need an overall SIGINT architecture that addresses these needs in a comprehensive way.

~~(S-CCO)~~ Analysis of networked communications is critical to our ability to continue to exploit global communications. The Signals Research and Target Development (SRTD) effort has had a tremendous impact in clarifying how new telecommunications technologies are being introduced into current and potential target countries. SRTD activities are ongoing in virtually every office in the DO, and a senior-level Steering Group provides overall guidance to SRTD activities and addresses common concerns in training, policy, and other areas. At the working level, an SRTD working group meets regularly to facilitate the exchange of information among analysts. Two conferences have been held—one in 1992 [redacted] and one in 1993 [redacted] to foster interaction between SRTD activities at NSA HQ and field elements. In addition, many ad-hoc activities are underway, such [redacted] exchange of information among analysts at NSA and elsewhere. Finally, analysts in several organizations and the SRTD Steering Group and Working Group are working on a variety of tools to automate many aspects of network analysis.[2]

[redacted]

[redacted]

[2] Information in this paragraph was derived from a draft paper written by [redacted]

EO 1.4.(c)
PL 86-36/50 USC 3605

[redacted]

~~(FOUO)~~ In the area of INFOSEC, the DI is pursuing the Multilevel Information Systems Security Initiative (MISSI). By incorporating user-provided requirements to continually upgrade its capabilities, MISSI holds great promise for providing cost-effective and operationally efficient security solutions. This will have a major, positive impact on the ability of U.S. governmental users and other customers to communicate with confidence in the integrity, authenticity, and privacy of their data when transmitted over the public switched network. A key feature of MISSI is its built-in flexibility to tailor specific products to the needs of different customers. Integral to MISSI is the capability to evolve along with new technology to respond rapidly and effectively to user requirements.

[redacted]

[redacted]

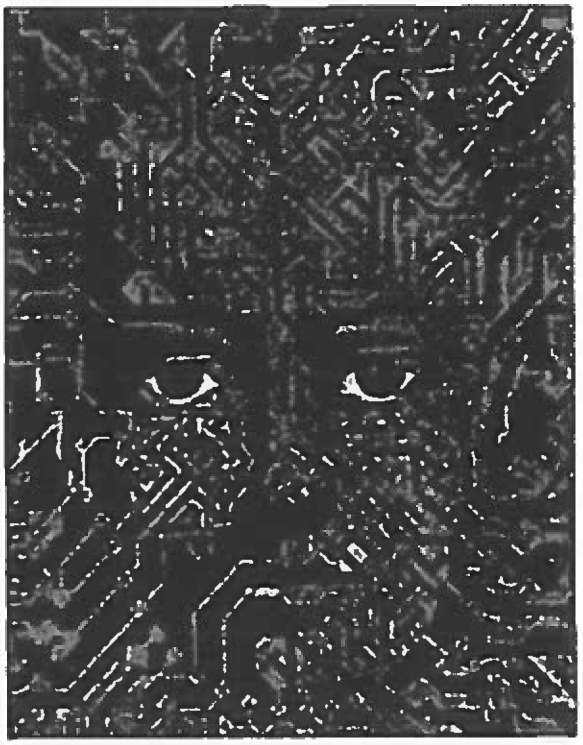
~~(S-CCO)~~ NSA's activities to enhance collection of networked communications has stimulated important thinking about what else needs to be done. [redacted] Manager of Special Programs and one of NSA's leading thinkers about the future, has described NSA's SIGINT mission in terms of "information space" instead of "signals space." In this paradigm, traditional thinking about signals, modulation, RF, cryptologic monopolies is replaced with notions of various information domains associated with SIGINT targets that are much more dynamic. Some of these domains will occur in communications networks, while others will be found in organizational and home environments. The job of accessing target communications will thus have a necessary first step of determining which of these domains has the highest potential of producing intelligence.

~~(TS-CCO)~~ [redacted]

PL 86-36/50 USC 3605

EO 1.4.(c)
PL 86-36/50 USC 3605

[redacted]



## 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.

~~(S-CCO)~~ Because of our focus on telecommunications and networks, it is clear that NSA has key roles to play in Information Warfare. First, as a combat support agency, NSA has responsibilities to provide intelligence support to the services who in turn are responsible for developing information warfare capabilities. NSA's long-standing partnerships with the services are thus being strengthened and redefined to encompass this new mission. Second, because of its expertise in SIGINT and information systems, NSA is being asked to support military service R&D efforts in developing techniques that would be useful in information warfare. Third, the DI organization is working with other defense and government agencies and with the services to enhance the information security of U.S. military communications as well as "unclassified but sensitive" data crucial to the nation's infrastructure.

~~(TS-CCO)~~ Like GNI, a strategic plan has been developed for information warfare. This plan has four key elements: the refinement of national, DoD, and NSA policy to specify objectives and define roles; enhancement of existing technical capabilities; redefinition of relationships with the services and other governmental and Defense agencies; and the need to adapt NSA to the IW mission in terms of organizational culture, budget and program, and other dimensions. Implementation of this plan will require close coordination across and among key components and with the GNI and other Agency strategic plans.

~~(FOUO)~~ One of the most important areas of NSA IW activity is in the engineering of multilevel security solutions to ensure the security, integrity, and reliability of U.S. government and defense information systems. Several well-publicized intrusions into the Internet have occurred, heightening awareness of Defense policymakers to the need to provide enhanced security solutions to U.S. communications. NSA's Information Systems Security Organization and the Defense Information Systems Agency (DISA) are working together on the Multilevel Information Systems Security Initiative (MISSI)—mentioned above—that will provide such security for networked information systems. MISSI will ensure that users can only access the information to which they are authorized, that information is protected from unauthorized modification, and that users are identified and authenticated. As a first increment of MISSI, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence recently directed that all workstations and personal computers acquired by DoD in the future be equipped with two PCMCIA slots to accommodate NSA-developed FORTEZZA cards. These cards will provide encryption/decryption capabilities for e-mail and computer-generated faxes, and will implement the digital signature standard for authentication. Ultimately, NSA and DISA hope to provide comprehensive security solutions for U.S. communications on the Defense Information Infrastructure (DII) as well as the evolving National Information Infrastructure (NII).

## Challenges and Opportunities

~~(TS CCO)~~ GNI and IW present many formidable technical and organizational challenges to NSA. Many of the technical challenges have been discussed above. To summarize, the major technical issues fall into the following categories:

- ○ *Access:* Gaining access to networked communications, whether for purposes of producing SIGINT or conducting some of the more sophisticated IW techniques is not trivial. [redacted]

- ○ *Processing and Communications:* Once access to a network has been attained, problems of data filtering and selection come into play as do concerns about forwarding the data back to a processing and analysis center at NSA or elsewhere. Emerging requirements for increased technical data to support IW will also pose processing and reporting challenges.

- ○ *Search:* How do we ensure we are accessing the right networks. [redacted] Much work will remain for SIGINT search organizations, too.

- ○ *Product Development:* [redacted] For INFOSEC, the challenge of producing network security products is especially critical.

~~(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.

## Teaming

~~(S-CCO)~~ The teaming of NSA organizations and people is the single most important key to success in GNI and Information Warfare. As target technologies become more sophisticated and more complex, it will no longer be possible for individual organizations to work solely on "their target" or "their technology" and be successful. Dynamic, task-oriented teaming of collection, processing, and communications professionals will be essential for the successful development and deployment of collection systems and technologies. Teaming of analysts of various types will also become more important; linguists will need insights into cryptography and signals analysts will have to become more familiar with computer systems. This is not easy. Creating horizontal teams poses a cultural challenge to an organization like NSA, which historically has been structured along vertical lines of authority. Teaming is already occurring today in many parts of the Agency, and with great positive impact. (For example, the Cryptologic Mathematics Program depends on teaming between the DI and DO organizations, and DI-DO-DT teaming is growing in the area of networks generally.) Such teaming tends to happen more readily when NSA has to respond to a crisis, when all the bureaucratic walls collapse and people from many organizations work together as one. The key to the future will be to institutionalize the concept of teaming for the routine as well as the crisis situations.

## 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.

~~(S-CCO)~~ GNI requires extensive interaction with external partners and customers. DoD, the Congressional intelligence committees, the Service Cryptologic Elements (SCEs), Second and Third Parties, and the [redacted] can be considered "partners" in GNI, while the military services, Commerce, State, and other U.S. governmental organizations can be considered "customers." Comprehensive and ongoing dialogue with partners is necessary for GNI to ensure NSA gains and retains the ability to access the global network. New and creative solutions to the access problem must be found (and are being found); many of these techniques cost more money than NSA has programmed in its budget. Or the funds have been programmed for another purpose and Congress must approve a different use. While Congress is a key source of authorizations and resources, other partners are critical to GNI because they provide information that leads to the access we need.

~~(TS-CCO)~~ Information Warfare also brings new demands for external communications. The military services all have IW programs that extend in scope well beyond the technologies of SIGINT and INFOSEC. For the past two years, NSA has been working together with the SCEs to foster communications with the SCEs' parent services who manage the respective service IW programs. In addition, non-intelligence agencies and departments of the U.S. Government are involved with the broader policy aspects of IW and must also be consulted.

~~(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.

## Compartmentation

~~(S-CCO)~~ While the mutually beneficial needs for greater teaming and better communications are clear, it is also true that much of the detailed work being done in GNI and IW is and will remain compartmented. Some NSA professionals complain about this and use it as an excuse; others may deny the need for compartmentation at all. Like many other facts of life, however, the need for compartmentation of GNI access methods and IW techniques must be accepted. Many of these methods and techniques are among the most fragile activities in the U.S. Government and must be protected. This need for compartmentation is unlikely to change.

[redacted] However, much can still be done to improve NSA's overall capabilities despite necessary compartmentation. For example, software and engineering specialists working on a technology for GNI SIGINT collection purposes may discover a technique that could be used to disable a target communications system and, therefore, be a useful tool for Information Warfare. Similarly, analysts may identify a potential weakness in a U.S. communications system; this knowledge may then be used by the DI to develop additional security measures. In the past, managers may have discouraged any further pursuit of the non-SIGINT or INFOSEC aspects of their employees' activities. Now, though, these managers have a responsibility to find out (by contacting the NSA Information Warfare policy staff in DP or the Information Warfare Center in G Group or the DI Information Warfare Special Program Office in V) whether the techniques identified by their workforce is of potential value to NSA's IW effort. In this way, work that begins as non-compartmented, or compartmented for a different reason, can be applied to more than one set of activities. It is this "dual-use" approach that defines the essence of NSA's Information Warfare effort.

[redacted] NSA's future is heavily dependent on how we as an Agency respond to the challenges of GNI and IW. So far, our efforts have been productive and on track. More work needs to be done, however, especially in the cross-over areas of technology development that will serve both GNI and IW, in SIGINT as well as in INFOSEC. Teaming and communications are the critical success factors. The high caliber of NSA's technical workforce will allow the Agency to meet these challenges. But it will take all our technical creativity and perseverance as well as unprecedented collaboration to ensure NSA performs with the same credibility and levels of excellence in these new areas as we have in the past.

(U) *This article has benefitted from comments by* [redacted] *Responsibility for the opinions and judgments expressed, however, rests with the author, based on his experience as Chairman of the NSA GNI Executive Steering Committee and as Executive Secretary of the NSA Information Warfare Steering Group.*

KA

PL 86-36/50 USC 3605

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~