Communications Security and the Problem of Hamlet: To Be or Not to Be

DANIEL J. KNAUF

Editor's Note: Mr. Knauf presented this paper at the convention of the Armed Forces Communications Electronics Association (AFCEA) in Anaheim, California, on 29 January 1985. We believe that Mr.Knauf's comments on communications security from the perspective of a Shakespearean tragedy will be of interest to many of our readers.

1. INTRODUCTION

At risk of offending the many serious students of Shakespeare, all English majors, and assorted other literati, I should like to examine the communications security of the United States against a slightly unusual backdrop: the tragic story of *Hamlet, Prince of Denmark*.

William Shakespeare, after all, begins this psychological drama with two words of special interest to those of us in the telecommunications business: "Who's there?" asked by a soldier named Bernardo. The guard to whom he addresses this question, Francisco, has obviously been briefed on proper challenge-and-reply authentication procedures (i.e., that the called party must always initiate the challenge), and stoutly replies:

> Nay, answer me: stand, and unfold yourself.

Fortunately for Bernardo, they are using an easy-to-remember if not-very- secure password ("Long Live the King"), and so we are allowed to enter into one of the greatest plays ever written – one which adds to its greatness by clearly showing the consequences of poor communications security (Comsec). We may admire, for example, Hamlet's use of Comsec as a "force multiplier" in his neat disposal of that treacherous duo, Rosencrantz and Guildenstern, as he tells his friend, Horatio, in Act V: Scene 2. Hamlet relates how he forged a letter for them to carry from the Danish King to the English King:

> That, on the view and knowing of these contents,
> Without debatement further, more or less,
> He should the bearers put to sudden death,
> Not shriving-time allow'd.

As further evidence of the excellent Comsec briefing program in Hamlet's Denmark, Horatio inquiries:

> How was this seal'd?

To which the resourceful Hamlet replies:

> Why, even in that was heaven ordinant.
> I had my father's signet in my purse,
> Which was the model of that Danish seal:
> Folded the writ up in the form of the other;
> Subscribed it; gave't the impression; placed it safely,
> The changeling never known.

Amusing as such echoes of Comsec's beginnings may be, we will do better to look more deeply into the fundamental nature of *Hamlet* in search of an overarching perspective from which we may view the telecommunications security challenges facing our nation into the next century. This is a tall order, of course, but then William Shakespeare was not your average, garden-variety Comsec analyst.

Shakespeare focuses his version of the Hamlet tale on the apparent inability of the Prince to carry out a clear-cut, if formidable, task. In a nutshell, Hamlet's Uncle Claudius has killed Hamlet's father (Claudius' brother), the King; has placed himself on the throne; and even worse, has married Hamlet's mother. The ghost of Hamlet's father appears at the beginning of the play to deliver Hamlet's marching orders for the rest of the play: "Revenge his foul and most unnatural murder." Hamlet is, understandably, a bit upset by all this ("O cursed spite / That ever I was born to set it right"), but he recognizes the validity of his "charter" ("... it is an honest ghost") and resolves to carry out the deed.

He takes his time about it, however. So much time, in fact, that his hesitancy has become one of the Great Unsolved Mysteries, appropriately called the "Sphinx of Modern Literature," and universally recognized as the "The Problem of Hamlet." The debate has raged for centuries now, with every conceivable explanation and excuse offered for Hamlet by writers from Goethe to Coleridge to Santayana. The question echoes and reechoes through the celestial corridors of Literature: why did he wait so long to act? Why couldn't this educated, intelligent, capable person bring himself to carry out his morally correct and clearly necessary task?

As a communications security analyst, I have sometimes asked myself a basic professional question with striking parallels to the debate over Hamlet's bias towards inaction. Why has the United States done so much to advance its total telecommunications capability, yet done so little to secure and protect those communications? Why have we been so slow in recognizing and responding to the vulnerability inherent in telecommunications? In a more positive vein, where are we today, what are our basic problems, and how can we solve them?

Just as the debate over Hamlet starts with such fundamental questions as whether or not there really *was* any delay or hesitancy on his part, and whether or

As further evidence of the excellent Comsec briefing program in Hamlet's Denmark, Horatio inquiries:

> How was this seal'd?

To which the resourceful Hamlet replies:

> Why, even in that was heaven ordinant.
> I had my father's signet in my purse,
> Which was the model of that Danish seal:
> Folded the writ up in the form of the other;
> Subscribed it; gave't the impression; placed it safely,
> The changeling never known.

Amusing as such echoes of Comsec's beginnings may be, we will do better to look more deeply into the fundamental nature of *Hamlet* in search of an overarching perspective from which we may view the telecommunications security challenges facing our nation into the next century. This is a tall order, of course, but then William Shakespeare was not your average, garden-variety Comsec analyst.

Shakespeare focuses his version of the Hamlet tale on the apparent inability of the Prince to carry out a clear-cut, if formidable, task. In a nutshell, Hamlet's Uncle Claudius has killed Hamlet's father (Claudius' brother), the King; has placed himself on the throne; and even worse, has married Hamlet's mother. The ghost of Hamlet's father appears at the beginning of the play to deliver Hamlet's marching orders for the rest of the play: "Revenge his foul and most unnatural murder." Hamlet is, understandably, a bit upset by all this ("O cursed spite / That ever I was born to set it right"), but he recognizes the validity of his "charter" ("... it is an honest ghost") and resolves to carry out the deed.

He takes his time about it, however. So much time, in fact, that his hesitancy has become one of the Great Unsolved Mysteries, appropriately called the "Sphinx of Modern Literature," and universally recognized as the "The Problem of Hamlet." The debate has raged for centuries now, with every conceivable explanation and excuse offered for Hamlet by writers from Goethe to Coleridge to Santayana. The question echoes and reechoes through the celestial corridors of Literature: why did he wait so long to act? Why couldn't this educated, intelligent, capable person bring himself to carry out his morally correct and clearly necessary task?

As a communications security analyst, I have sometimes asked myself a basic professional question with striking parallels to the debate over Hamlet's bias towards inaction. Why has the United States done so much to advance its total telecommunications capability, yet done so little to secure and protect those communications? Why have we been so slow in recognizing and responding to the vulnerability inherent in telecommunications? In a more positive vein, where are we today, what are our basic problems, and how can we solve them?

Just as the debate over Hamlet starts with such fundamental questions as whether or not there really *was* any delay or hesitancy on his part, and whether or

not he believed the ghost, understood the task, or agreed that it was the *right* task, so too, we must begin with similar questions for Comsec.

2. THE TASK/THE PROBLEM

One of the more obvious – and significant – events taking place today is the incredible growth in the availability and use of modern telecommunications systems. This phenomenon has justly been termed the "Communications Explosion"; it is directly affecting virtually every individual American, as well as much of the world's population. It has had an increasingly profound effect on every aspect of the government and private sector in the United States. Without elaborating on the obvious, we would do well to consider the following items:

- Robert W. Kleinert, president of AT&T Communications, recently noted that the demands for services such as videotext, electronic mail, videoconferencing, and high-speed data transmission is growing by more than 20 percent a year.

- James B. Graham, president and chief operating officer of Cellular Radio Corporation, has predicted that the number of cities with cellular phone markets will double to 60 by next year.

- *Business Week* recently projected an annual expenditure on voice and data communications increase to $150 billion by 1990.

- Federal Express is expanding its "ZapMail" system, using an improved version of facsimile technology (improving quality and transmission time) and its fleet of vans. Two months after ZapMail was started by Federal Express in July 1984, it carried documents at a rate of 33,500 per month.

- Both Western Union's Easylink and MCI Communications Corporation's MCI Mail now offer high-speed data transmission services, and Federal Express has applied for permission to launch two satellites in 1988, which would position it to enter the high-speed data transmission field.

- Airfone, Inc., continues its efforts to market commercial air-to-ground telephone services.

- Mr. Peter Waal, Vice President of Marketing and Plans for the Network Services Group of GTE Telenet, noted during testimony at a Congressional hearing that "Market Projections indicate that there will be over seven million personal computers in use within three years. . .of these, nearly two million will have the ability to communicate with remote computers."

- The convergence of telecommunications and data processing is adding a tremendous new force to the Communications Explosion. The recent IBM acquisition of Rolm Corporation is expected to produce a new office workstation

blending the IBM PC and a telephone into a desktop package. Other companies such as Compaq Computer Corporation and the Zaison, Inc., of Houston, are exploring the integrated telephone/computer workstation.

- Eric Kobren, marketing director of Fidelity Investments Group, estimates that by 1990, fully 75 percent of the securities trading orders placed by personal computer will be fully automated, and that 25 percent of the company's total volume will be handled without human intervention.

These particular changes in the marketing of telecommunications – all noted in the public press – are neither comprehensive nor balanced across all types of communications media. They do provide, however, an accurate picture of the awesome dimensions of our Communications Explosion and the impact it is having. The news is essentially good, and as the technological leader of the telecommunications revolution, our nation may expect to reap many tangible benefits. There is, however, a darker side to such progress, i.e., the problem of how to protect the information being communicated from interception and exploitation by hostile parties, be they foreign governments, business competitors, terrorists, or criminals. As Hamlet himself might say, were he here to witness all this:

Communications Security, Ay, there's the rub...

The problem stems from the simple fact that information transmitted over any communications media may be intercepted and recorded by anyone having access to those media. The magnitude of the challenge facing us may be better appreciated when one realizes that the primary transmission media for today's communications are satellite links and terrestrial microwave. AT&T, for example, currently estimates that it uses satellites or microwave towers for 70 percent of its domestic traffic and 60 percent of its foreign traffic. As much as 90 percent of all U.S. telephone calls are carried, at least in part, over the nearly 200,000 miles of easily interceptable microwave circuitry. Communications satellite downlink "footprints" typically cover immense areas and are extremely susceptible to interception by unauthorized parties. Virtually every type of traffic is carried on these vulnerable links, including voice, computer data, facsimile, TWX/Telex, teleconferencing, and communicating word processors.

The importance of the telecommunications security issue has grown to the extent that it is now a major public issue, receiving increasing public attention. A tiny sample of recent public notice of the security issues associated with telecommunications includes the following:

- The 29 October 1984 issue of *Time* Magazine addressed some of the basic issues in an article, "Is It Safe to Use the Phone?" Using terms appropriate to and reminiscent of the *Hamlet* literature, the article noted that "...the U.S. has been bewilderingly slow in dealing with another potentially enormous security problem: most Government and business officials daily discuss sensitive matters over ordinary, unsecured equipment."

- *People* Magazine of 3 December 1984 carried an article and interview under the title "Spy Expert David Kahn Says We Need Scrambled Phones to Avoid Serving Up Info to the Soviets." Mr. Kahn stated that "the best-known 'listening post' is in the attic of the Soviet weekend retreat in Glen Cove, Long Island." He felt that their obvious targets of interest were "calls from defense contractors in Connecticut, financial centers in New York and the high-tech regions around Boston to government offices in Washington."

- New York Senator Daniel Patrick Moynihan, Vice Chairman of the Senate's Select Committee on Intelligence, recently noted that "the targets of Soviet interception of telephone communications now include our businesses, our banks, our brokerage houses, as frequently as our Government Agencies...private communications of all sorts have been violated, and on a scale that dwarfs any previous surveillance effort by friend or foe."

- A recent report by Fremont, California, police chief Robert Wasserman recognized that the Soviets' San Francisco consulate is "in a strategic location for the interception of microwave signals from radio and telephone communications" of "Silicon Valley" high-tech firms. Reporter Peter Grier of the *Christian Science Monitor* noted in a 17 April 1984 article that the new Soviet Embassy in Washington, D.C., has two readily apparent characteristics:

1. The Soviets will have a great view.
2. Their antennas will pick up more than HBO and "This Week with David Brinkley."

Mr. Grier went on to describe the fundamental problem: "Whiz-bang technology makes the United States system the best in the world. . .but that same technology makes it relatively easy to intercept messages."

- Mr. Walter G. Deeley, the senior government official responsible for communications security, and as such, the person closest to the fundamental issues on a daily basis, summarized the situation accurately and bluntly: "They're having us for breakfast. We're hemorrhaging. . ." (*New York Times*, 6 October 1984).

- The *value* of much unclassified commercial data has been emphasized by several business leaders. Mr. Julius Cohen, technical director of the information resource department of Grumman Aerospace, testified at hearings of the 98th Congress that much of Grumman's unclassified data was of value, including both private data (e.g., medical records, payroll information, employee information) and proprietary data (dealing with business plans, manufacturing capabilities, and financial information).

Even with such attention being drawn to the telecommunications security issue by responsible journalists, business leaders, and government officials, we as a nation have done little in this area beyond securing our most sensitive, classified, government communications. In particular, the protection of sensitive

private sector communications has been proceeding at a very slow pace relative to the expansion of telecommunications. This may appear puzzling in view of the high commercial stakes. Generally speaking, information being communicated is worth far more than the equipment used to transmit, receive, and protect it. Major U.S. banks, for example, conduct daily electronic funds transfers of around $50 billion through a worldwide network of 15,000 terminals (after a few days, this adds up to real money!). Some securities brokers are concerned about their potential liability for unauthorized tampering in an automated trading process. One such broker was recently quoted as saying: "If a customer puts in an order for 100,000 shares and then heads for the Bahamas, or if he tries to take control of GM while drunk and then claims the morning after it was the broker's error, the broker is on the hook with a trade that goes through automatically." Yet the fact remains: We continue to be extremely vulnerable throughout the private sector and much of the government.

- Mr. J. Michael Nye of Marketing Consultants International, Inc., recently reported that American Satellite has offered encryption services to their customers at an additional cost of about 10 percent, with "few takers." Individuals at other companies have suggested similar views, i.e., that few of their customers have shown any interest in security. Victor Walling of SRI International, Menlo Park, California, was recently quoted by Peter Grier as saying that, on the whole, there may not be a big private demand for cryptography, at least for the near future. He emphasized the point by suggesting that "somebody will have to do a D. B. Cooper with data, before people will really pay attention." (Cooper disappeared after he jumped from the tail of a Boeing 727 with $200,000 cash.)

The situation we have identified above is one of massively expanding telecommunications – of high value to users and, more generally, to the nation – which are extremely vulnerable to interception and exploitation because they are largely unprotected. We are then, at this point, in a position not unlike Hamlet's when, about midway through the play, the ghost of his father returns to remind him of his fundamental task. Hamlet admits that he has been less than assiduous in carrying out his business, although he is not himself certain of the reasons why:

> Do you not come your tardy son to chide,
> That, lasped in time and passion, lets go by
> The important acting of your dread command?
> O, say!

Like *Hamlet*, there are many plausible explanations for why we as a nation have not fared better in our communications security. Among them:

Lack of User Awareness

The need for Comsec is not inherently obvious. On the contrary, those who exploit our communications go to considerable lengths to do so very discreetly. The government shares some of the responsibility for the general lack of Comsec

awareness on the part of U.S. industry and many government personnel because our Comsec educational programs have, until now, not reached out to many of those who could benefit from them. Another culprit, in the author's view, has been the generalized tendency for many in and out of government to wait for, and rely on, the so-called "smoking gun" threat information which "proves" that such-and-such communications are being actively exploited by so-and-so. Any information of this type invariably suffers from being scarce, sketchy, and classified. It is also unnecessary. By this I mean that telecommunications security measures, such as encryption, should be dictated by and tailored to the *value* of the information, the *vulnerability* of the communications media, and, least important, the demonstrated *threat* to those communications. If commercial communications users make the effort, they can very easily – and very accurately – determine the most important basis for protecting their communications: its *value*. With slightly more effort, users can develop an accurate estimate of how *vulnerable* their communications are to unauthorized intercept and exploitation. Given these two pieces of information, they can develop a more accurate picture of their true Comsec requirements than a thousand pieces of "threat" information could provide. As Mr. Walter G. Deeley said in his 6 October 1984 interview with the *New York Times*: "If it is going via satellite, you can *presume* the other guy is listening to it" (emphasis mine). It is excellent advice.

Cumbersome Government Comsec Procurement Process

The development and production of cryptographic equipment has largely been accomplished through the National Security Agency (NSA) as the Government's central procurement point. Although this process works well for certain equipment applications, it does not have the flexibility to meet the challenges of fast-paced technology rollovers, expanding, highly diversified markets, and the "designing in" or integration/embedding of cryptography into telecommunications systems during "up front" development. This lack of flexibility has contributed to the occasional production of over-engineered cryptographic devices, on a 10- to 12-year requirement-to-fielding cycle, which could cost more than the rest of the telecommunications system equipment they serve (typically $5,000 to $35,000 per Comsec device). It has also led to delays in fielding equipment incorporating the very latest technology.

Lack of a Small Standard Comsec Product Line

An additional problem which has helped to retard the spread of telecommunications security devices has been the proliferation of a specialized Comsec product line in which much of the engineering effort is spent, not on the cryptography per se, but on the surrounding interfaces. This has, in turn, contributed to smaller contract quantities and higher prices.

Lack of an Overall National Assessment Capability

Until mid-1984, there was no organized approach to assess the *national* status of telecommunications security, with the result that it was extremely difficult to

allocate scarce national Comsec resources to those areas with the most pressing needs, in a prioritized manner.

Restrictive Comsec Doctrinal Controls

Until recently, the users of Comsec devices were a fairly homogeneous group: primarily civil and military government, using the equipment to protect classified information. The overall approach the government took towards doctrinal controls on cryptographic devices reflected this, and contributed towards defining those who could purchase and use government Comsec equipment. In particular, the classification of many Comsec devices automatically put severe limitations on the distribution, and markets, for those devices. As with some of the other problem areas, this, too, contributed to smaller quantities and higher costs.

The problems I have briefly outlined above have, in part, led to our "bewilderingly slow" progress in addressing the nation's *total* telecommunications security needs. Taken together, they amount to a *fundamental* challenge to this nation, and it is the fundamental nature of the Comsec challenge which once again leads one back to *Hamlet*. Although Hamlet had a definite problem in spurring himself into effective action, his personal soul-searching is, if nothing else, profoundly fundamental. Hamlet, in his mental analyses of the great issues of life and death does not deign to mess around, but gets right down to basics in a manner which commends itself to all who contemplate the fundamental issues of U.S. telecommunications security:

> To be, or not to be: that is the question.
> Whether 'tis nobler in the mind to suffer
> The slings and arrows of outrageous fortune,
> Or to take arms against a sea of troubles,
> And by opposing end them?

3. CHANGES NEEDED

Unlike some of Shakespeare's other plays, notably *King Lear*, *Hamlet* is not devoid of all hope and optimism. Although he does take a while to get around to it, Hamlet in the end does indeed carry out the "dread command." In fact, once he finally decides to get down to business, he is rather efficient and ruthless in pursuing his goals. Some writers have suggested that Hamlet was unable to carry out his duty until certain basic changes had occurred which allowed him to proceed. Ernest Jones, for example, proposes one of the more interesting theories for Hamlet's behavior in his book, *Hamlet and Oedipus* (W. W. Norton & Company, 1949). In that work, Jones suggests that Hamlet was blocked from carrying out his task not because of something lacking in his own personality, but because of something in the nature of that specific task for Hamlet. He goes on to suggest that Hamlet's problem was that, on a deep psychological level, he could not bring himself to kill Claudius simply because he, Hamlet, *identified* with the villain; that Claudius had in reality fulfilled Hamlet's childhood "Oedipal" desires to remove and replace his father in his mother's affections. In this somewhat far-fetched but entertaining view, Hamlet was only free to act after a few basic

conflicts had been resolved, i.e., his mothers' imminent death after drinking the wine poisoned by Claudius (but intended for Hamlet). The "bottom line" of the Jones school of thought on the "Problem of Hamlet" is that certain fundamental operating principles had to be changed before significant progress could be made.

The Communications Security Organization of the National Security Agency, while not particularly concerned with either Hamlet or Oedipus, has recognized the need for fundamental changes if we are to get on with the important task of protecting this nation's telecommunications. To that end, we have reviewed our basic way of thinking about, and our approach to, Comsec, and have made some significant changes in both our thinking and our approach. Organizationally, the fundamental convergence of computers and telecommunications has been recognized in the recent issuance of National Security Decision Directive Number 145, signed by the President on 17 September 1984. The NSDD assigns the NSA a larger role in protecting the security of government and industrial communications.

Internally, the NSA Comsec Organization has restructured itself to focus personal authority and responsibility in our Program Managers – those individuals primarily responsible for the development and production of cryptographic equipments, subassemblies, components, and software.

Commensurate with these changes, NSA's managerial emphasis has been concentrated upon the following major goals:

Fielding of Large Numbers of Devices

The "Communications Explosion" requires that our Comsec efforts dramatically increase to a scale appropriate to the challenge. One of the most important security actions America can take, therefore, is the fielding of large quantities of security devices in step with the expansion of telecomputing and telecommunications technology. To this end, the National Security Agency has begun an initiative to develop a new family of narrowband secure telephone equipment for widespread use throughout the United States. This family of equipment has been designated the Secure Telephone Unit-III/Low Cost Terminal (STU-III/LCT). The STU-III/LCT will be available in versions compatible with conventional office requirements and standard telephone systems/PBXs, as well as cellular mobile radio-telephone systems, and portable/briefcase applications. In a significant departure from past practices, the STU-III/LCT will be made available to the U.S. business and industrial community, as well as to U.S. Government agencies and Defense contractors. NSA is currently working with five leading telecommunications manufacturers – AT&T, ITT, GTE, Motorola, and RCA – who are participating in a competitive concept definition for the new system. The award of development contracts will be made in early 1985, with an initial target of 100,000 secure telephone units in the first two years of production. NSA has identified some ambitious features for this new family of equipment:

- Unit price goal of $2,000
- Availability in early 1987

- Devices unclassified when unkeyed
- Easy installation with standard TELCO interface; easy to operate
- Small size, approximating that of a conventional multiline deskset
- High quality, full duplex communications over a single telephone line
- Multilevel security with positive authentication
- Direct support from the manufacturers for installation, keying, and maintenance
- Optional secure data capabilities
- Availability of direct purchase from a minimum of two vendors.

The STU-III/LCT features, listed above, add up to an aggressive program to protect the voice communications of the United States. From our Hamletian perspective, however, the salient feature is the very scale of the program – in quantities ultimately expected to exceed one million devices. For the first time, the response to the telecommunications security challenge is being sized to the magnitude of the problem. This basic change in the scale of Comsec development and production will be carried over into other areas of the telecommunications "explosion" such as Local Area Networks (LANs) and Personal Computer Networks.

Expanding Comsec Education

The goal here is to dramatically increase "Comsec Literacy" in the United States. Over the next several years, the National Security Agency will be expanding its Comsec education programs, working with the government departments and agencies, and with industry, to increase awareness of the "Comsec Trivium":

- The VALUE of communicated information
- The VULNERABILITY of telecommunications systems
- The THREAT to those communications

Because Comsec education is a constant process, it will only succeed with a cooperative government-industry approach, and this will form the basis for the new NSA effort in this area.

Integrating/Embedding Cryptography

In the past, the vast majority of Comsec devices were of the "stand-alone" variety, developed independently of the telecommunications systems they were to serve. Such an approach fosters gross inefficiencies, and in fact, has become impossible for many new telecommunications systems. Technology is simply moving too fast for NSA to follow the traditional 10- to 12-year requirements definition, R&D, production, and fielding cycle. We can no longer efficiently design and produce general-purpose cryptographic devices geared to the highest bidder with the most stringent requirements.

Instead, Comsec in most cases must be truly "designed-in," integrated and embedded during the up-front development of the telecommunications system. This has many serious implications for the way America produces its Comsec equipment. It implies that telecommunications systems designers are adequately knowledgeable of cryptographic techniques to do the job. It implies that Comsec can be marketed as a standard telecommunications system option. It implies changes in the way we currently nomenclate, control, maintain, and account for Comsec devices. And it, of course, implies major changes to the way Comsec requirements are identified, contracted, and funded. Assuming once again our Hamletian concern with fundamentals, and given the convergence of computers and communications technology, there is simply no other way to go – cryptography will increasingly find integrated/embedded applications, and for all the right reasons: technological necessity, cost, implementation timeliness, and Comsec system transparency.

Limiting the Standard Cryptographic Product Line

One major goal of the NSA for the next decade and on into the next century is to develop a limited number of standardized cryptographic chip sets which can be effectively used in the "designing-in" process referred to previously. NSA intends, therefore, to work with industry to develop standardized chip sets and Comsec modules (with standard I/Os) as well as to develop a limited number of basic Comsec I/O standards. This aspect of fundamental change is viewed as critical to the success of our other goals, specifically the fielding of large quantities of security devices and the successful integration/embedding of cryptography into telecommunications systems.

Establishing a National Comsec Assessment Capability

In mid-1984, the National Security Agency established a new organizational element specifically to provide a National Comsec Assessment program. This element has now grown into the National Communications Security Assessment Center (NCAC) and is currently working with government departments and agencies, as well as the private sector, to establish a cooperative program which can be used for the direction of Comsec resources and activities to those areas which need it most critically. The NCAC is organized along the lines of the "Comsec Trivium" noted above – Value, Vulnerability, and Threat – and has taken, as its first order of business, the establishment of a telecommunications

data base. Once developed to an adequate level, this data base will be available for use by other government departments and agencies, and it will provide the point of departure for periodic assessments of the true status of telecommunications security in the United States.

Modifying Comsec Doctrinal Controls

As evidenced by the STU-III/LCT goal to produce a telephone terminal which is unclassified when unkeyed, NSA recognizes that certain traditional controls on Comsec devices must be more closely tailored to the environment in which the devices operate, and to the application for which they are intended. It is equally clear that the trend toward integration/embedding of cryptography into telecommunications systems, and the need to field Comsec devices in very large quantities, both require a careful consideration of appropriate philosophies of control. The fundamental changes of direction for cryptographic doctrine, however, ultimately derive from the projected nonhomogeneous nature of the user communities. Particular cryptographic embodiments in the near-future (e.g., standardized Comsec modules and chip sets) will have to serve widely diversified user communities – from those with the most to those with the least sensitive communications. It is with respect to this diversification that NSA has established the development of a graded system of controls as a major goal and on-going activity.

Aside from the general objectives and activities described above, the National Security Agency is aggressively pursuing an increase in both the demand for, and the supply of, cryptographic equipment.

Demand

The government demand-side efforts include many of the initiatives described earlier, i.e., increased Comsec education awareness, lower costs, system transparency through integrated and embedded Comsec, graded doctrinal controls, etc.

In addition to those activities, there are two other efforts which merit comment here.

On 4 June 1984, the Director, NSA, signed into effect *National Comsec Instruction 6002*: "Protection of Government Contractor Telecommunications." This document, at root, is designed to increase the demand for the application of cryptography in a very critical area – that of government contractor communications. It does several things:

- It requires government departments and agencies to identify contractor Comsec needs early on in the contracting process and to specify implementation provisions.

- It offers an alternative to the traditional provision of Government Furnished Equipment (GFE) by allowing contractors' Comsec charges to be placed into the contract just as any other security charges.

In a desire to foster the rapid expansion of cryptography into the private/commercial sector, the standardization of cryptographic formats, and the integration/embedding of Comsec into telecommunications systems, consideration is being given to the development of federal tax incentives for the purchase and use of NSA-approved Comsec devices.

Supply

On the other side of the equation, the National Security Agency is taking – and has already taken – major steps to implement what could very reasonably be termed "Supply-Side Comsec." The hallmark of this effort is to dramatically increase the supply of cryptographic equipment – as evidenced by the STU-III/LCT program – with the knowledge that the limited *supply* of Comsec equipment in the past has artificially depressed the latent *demand* for protection. The primary thrust of this effort has been to develop newer and more flexible options for government-industry business relationships in the development and production of Comsec hardware. To this end, NSA has identified five basic approaches to the production of Comsec devices, and all five are currently available and being implemented. They are

Traditional. This relationship reflects the traditional approach with NSA acting as the central procurement authority for the development and production of Comsec hardware. Although this approach will find more limited applications in the future, it remains available for use where appropriate. It will probably be used for the NSA development and production of Comsec modules/LSI chip sets for integration into telecommunications systems developed by commercial and government organizations independent of NSA.

Delegation. This is another existing, traditional type of government relationship generally used in those cases where there is single-user applicability, lower overall national priority, limited NSA resources, or sound technical/fiscal reasons for delegation. In these cases, NSA continues to provide analytic/technical assistance to the developing agency on an as-requested basis.

User Partnership. This is a variation on the "delegation" theme above. The essentials of this approach are for NSA to become a full-time partner member in a government user's development team for the production of a new Comsec product or a system which includes a Comsec product. Here NSA funds for the cryptographic development, and the user funds and controls the rest of the program. NSA expects the user partnership relationship to become one of the primary mechanisms for integrating/embedding cryptography into government-developed telecommunications systems.

Authorized Comsec Vendor. The essentials of this important new approach are for NSA to "license" a contractor or contractors to build-to-print an existing/mature Comsec device, and then directly market the device and continuing support services to an expanded, authorized Comsec market.

Arrangements will be made for NSA to endorse contractor-generated product improvements and to encourage such improvements, in order to bring the benefits of commercial competition to bear on Comsec markets.

Commercial Comsec Endorsement Program (CCEP). As the newest and most flexible of the government-industry business relationships for the development and production of Comsec hardware, this program deserves special attention. The CCEP offers a very promising approach in which NSA provides a vendor with the essential elements of a cryptographic design and a set of up-front standards. A variation on this approach is for NSA to provide Comsec modules/LSI chip sets together with the technical standards for their integration. The vendor then designs his own product to the standards (with NSA technical assistance) and finally obtains NSA *endorsement* of the finished product, after which the vendor pursues his own direct marketing, sales, and support to the expanded Comsec market – to government, commercial, and private entities. This approach recognizes and takes advantage of the leadership and expertise of American industry in the design, development, and production of telecommunications systems. NSA currently has several programs involved with the CCEP and views this particular approach as the key to protecting such large and growing areas of telecommunications as LANs, personal computers, and similar emerging technologies.

4. SUMMARY

I have attempted to describe some of the major elements of the challenges and opportunities facing the United States in the protection of its telecommunications today and on into the next century. In viewing the "Problem of Comsec" from the Shakespearean heights, two topographical features stand out:

- The nation will only succeed in protecting its vital resources, technologies, secrets, and sensitive information through a cooperative and large-scale government-industry effort.

- Such an effort will require *fundamental* philosophical departures from the way we have done things in the past, if we are to be successful.

In pursuing a Shakespearean theme for an analysis of telecommunications security, several plays, either by their content or their titles suggested themselves – *The Comedy of Errors, Much Ado About Nothing, As You Like It, The Taming of the Shrew, The Tempest,* and perhaps optimistically, *All's Well That Ends Well!* Because the subject of telecommunications security has such serious implications for the well-being of our country, and because the issue ultimately comes down to a question of "To be, or not to be" – for us as a nation – there was no question but that *Hamlet* would provide the analogy, if I might provide the analysis. And as

with *Hamlet*, it is, in the final analysis, as with all things, an issue of fundamental responsibility, to act, or not to act:

> What's Hecuba to him, or he to Hecuba,
> That he should weep for her? What would he do,
> Had he the motive and the cue for passion
> That I have? . . .

(b)(6)

~~(FOUO)~~ **Mr. Knauf, a communications security analyst in S072, began his career as a Naval Officer, commissioned in October 1968 at Naval Officer Candidate School, Newport, Rhode Island. He attended Advanced Elint Course at NCTC, Pensacola, Florida, and was graduated from the Defense Language Institute in 1969. He served as a Naval Security Group officer in a variety of positions at Naval Communications Station, Rota, Spain, 1970-74, and at present is a Commander in the U.S. Naval Reserve. Mr. Knauf joined the Agency in 1975 and was graduated from the Comsec Intern Program in 1977. In 1984 he completed an assignment at the Command and Control Communications Systems Directorate USCINCEUR HQ, Vaihingen, West Germany. Mr. Knauf**