Computer Security Discourse at RAND, SDC, and NSA (1958–1970)

Thomas J. Misa
Charles Babbage Institute

The 1967 Spring Joint Computer Conference session organized by Willis Ware and the 1970 Ware Report are widely held by computer security practitioners and historians to have defined the field's origin. This article documents, describes, and assesses new evidence about two early multilevel access, time-sharing systems, SDC's Q-32 and NSA's RYE, and outlines the security-related consequences for both the 1967 SJCC session and 1970 Ware report.

The Defense Science Board (DSB) report "Security Controls For Computer Systems," published in 1970 and known universally as the Ware Report, is widely cited by computer security practitioners as framing the computer security field. It is referred to in technical research articles on intrusion detection, high assurance, requirements engineering, and computer security education; in the US Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC), better known as the Orange Book (based on the color of its cover); and in papers by leading computer security figures such as Roger Schell, Stephen Walker, Marvin Schaefer, Carl Landwehr, Cynthia Irvine, and Deb Frincke. It was canonized in the secure software assurance "common body of knowledge."[1] The Ware Report is the "paper that started it all, first raising computer security as a problem," according to Matt Bishop.[2] Beginning in 1967, the RAND's Willis Ware and the DSB panel investigated computer security appropriate for multiuser (time-sharing) computer systems, especially those with varying security classifications. Different lessons have been drawn from the Ware Report.[3]

This article explores the emerging discourse about computer security at the think tank RAND, its spin-off System Development Corporation (SDC), and the National Security Agency (NSA) in the years leading up to the 1970 Ware report.[4] It draws on archival records at Charles Babbage Institute (CBI), including company records from SDC and the personal files of Ware himself as well as recently declassified NSA documents.[6] The 1970 Ware Report, the practitioners' recognized origin point for computer security, was substantially anticipated by Ware and others at the 1967 Spring Joint Computer Conference (widely accepted in historians' accounts).[6] This article points to new evidence that the 1967 Spring Joint Computer Conference (SJCC) papers (as well as the 1970 Ware Report itself) reported on—and indeed depended on—two early time-sharing systems: the SDC's Q-32 and NSA's RYE. These two computing systems vividly raised the problem of multilevel computer security. Owing significantly to the fog of classification, these two systems have remained in the shadow of Massachusetts Institute of Technology's better publicized CTSS (Compatible Time-Sharing System) and Multics. A technical genealogy can be fashioned that links SDC's Q-32 and NSA's RYE with the Ware Report of 1970 and the canonical question of multiaccess, resource-sharing computer systems.

The term "discourse" is sometimes limited to words, but this article follows Paul Edwards' wider sense of the term. In his book *The Closed World,* Edwards demonstrates the continual interplay of technical concepts, research programs, computing systems, and ways of thinking about politics, society, and the Cold War. For him, the term discourse emphasizes "the constructive and productive elements of the intersection of material conditions with knowledge, politics, and society."[7] This article shows that it is empirically productive to examine the origins of computer security as an intersection of material and conceptual elements. Conceptual problems at the core of computer security were raised by a certain type of computing—that is, time-sharing systems with multilevel access. The air-defense project SAGE, for which computers were manufactured by IBM and

Published by the IEEE Computer Society 1058-6180/16/$33.00 © 2016 IEEE

programmed by SDC, featured large-scale computing power, networked communications, distributed users, military-sensitive data, and real-time operations. SAGE did not, however, have multilevel access since its air-defense radar, airplane tracking, and missile telemetry data (and US Air Force users) did not involve multiple levels of security at the same moment of operation. The security challenges of multilevel time-sharing arrived with second-generation time-sharing—at SDC and NSA among others—that brought users at multiple levels of classification or clearance onto the same computing system at the same time. Other multilevel time-sharing systems, such as Multics, had parallel but distinct lines of influence.[8]

Because of their work on specific multiuser, multilevel computer systems, SDC and the NSA were each an early locus of computer security. As a successor of SAGE, SDC's Q-32 was the developmental context for an early high-level language (the Algol-inspired Jovial) widely used in command-and-control applications and led to the explicitly security-conscious ADEPT-50 time-sharing system that SDC developed for IBM System 360 computers.[9] Many aspects of NSA's massive efforts in computing are still obscure, but available documents make it abundantly clear that, beginning in the 1960s, the agency's RYE created a global networked communication system that handled some of the most sensitive classified materials in existence. More to the point, RYE was one paradigm for computer security presented in the 1967 SJCC session and the 1970 Ware Report. A review of computer security in 1972 explicitly identified NSA's RYE as one of two "examples of early attempts at achieving 'multi-level' security." It then elaborated: "Early intelligence oriented systems installed software safeguards to allow *concurrent processing* of *various categories* of Top Secret data" (emphasis added).[10]

Beginning in the 1960s, NSA's RYE created a global networked communication system that handled some of the most sensitive classified materials in existence.

RAND and Its Spin-Offs

RAND has long served as an archetype, sometimes even a caricature, of a Cold War–era think tank. In the 1960s RAND was targeted in popular culture by folk-singer Malvina Reynolds' biting "RAND Hymn" (1961) and filmmaker Stanley Kubrick's thinly disguised "Bland Corporation" in *Dr. Strangelove* (1964).[11] Herman Kahn's writings about nuclear holocaust inspired fellow RAND researcher Paul Baran's early conceptualization of packet switching. In recent work on RAND, historians have examined topics such as its secrecy practices, research policies, and wider social and political impact.[12]

RAND's spin-off SDC had its origins in Project SAGE, which transformed MIT's Whirlwind computer into a continent-spanning air-defense network. Facing the novel challenges and substantial risk of developing the SAGE software, RAND spun off the System Development Corporation (1955–1957). SDC grew rapidly in size and budget to be many times that of its parent RAND so that, famously, "at one point SDC employed about 90 percent of the nation's computer programmers."[13] In 1961 SDC's "in-house facilities [were] the largest computing complex in the world," according to one insider.[14] The MITRE Corporation, founded in 1959, was another SAGE-related spin-off from MIT's Lincoln Laboratory. MITRE also evolved into a prominent site for computer security research and evaluation.[15] Because of their common concern with multilevel time-sharing, RAND, SDC, MITRE, and other military and intelligence agencies (including the NSA) were key actors in developing early computer security artifacts, practices, and concepts.

Early computer security—an antecedent history to the Ware Report—comes into sharper focus by examining the careers and projects of key individuals. At SDC one such staffer was Clark Weissman, a 1956 graduate of MIT in aeronautical engineering who followed his early-career work at SDC on time-sharing and computer security with subsequent engineering and management positions with Unisys Defense Systems and Northrop Grumman and consulting for the NSA's network security working group.[16] The pivotal material context at SDC was his work on the Strategic Air Command Control System (SACCS), sometimes known as Super Sage. Lining up Weissman's publications and presentations beginning in the 1960s reveals a characteristic cluster of related problems and an impressive "who's who" of the pioneers in computer security. Weissman and his SDC colleague Jules Schwartz published seminal technical articles on SDC's Q-32 time-sharing system, and in 1969 Weissman published two articles on the security-conscious ADEPT-50 time-sharing system, commissioned to bring secure time-sharing to IBM 360 computers that, although spreading rapidly in industry, lacked effective and secure time-sharing for the government, military, and intelligence world. "Security aspects" were Weissman's special focus at a 1968 DARPA symposium on the ADEPT-50 system, and his presentation slides demonstrate an attention to physical, hardware, and time-sharing security as well as specific attention to different levels of classification and the challenges of multiple users, programs, and files. His discussion of security maintenance drew attention to such seemingly mundane but nonetheless critical elements as residue control, integrity monitoring, and security operation stations. "Demonstrations showing a nonprogrammer querying an on-line database on the status of Vietnam forces aroused wide interest in ADEPT's capabilities," noted a SDC staffer. In short order, ADEPT was installed in numerous military locations, including the Pentagon and the Strategic Air Command.[17]

Weissman's coauthors and copanelists in the early 1970s when he headed SDC's Security Systems Department are an impressive roster of computer security pioneers: James P. Anderson, Peter Denning, Roger Schell, Steve Lipner, William Wulf, and Peter Neumann. Weissman followed this with work on Blacker, a cryptographic gateway for the Defense Data Network, one of the first three computer systems successfully certified at the TCSEC topmost A1 category.[18] All these systems—Q-32, ADEPT-50, and Blacker—were networking or time-sharing systems with multiple levels of access that forcefully raised the problem of computer security.

A parallel genealogy comes from the career of Jules Schwartz, who joined RAND in 1954 after obtaining a master's in mathematics from Columbia University while working at Columbia's Watson Scientific Computing Laboratory. Whereas SAGE was programmed in machine language, Schwartz had experience developing several early high-level languages including the PACT (Project for Automatic Coding Techniques) compiler and a utility system for MIT's Lincoln Labs. Moving to SDC on its founding, Schwartz began work in 1958 on what became the Jovial programming language, which is eponymously "Jules' Own Version of the International Algebraic Language." Schwartz recalled that "JOVIAL really got its beginnings because of the launching by the Air Force … of the SACCS system. SACCS was to be developed from scratch. This means new computers, a new system, new programming techniques, and a new operating (executive) system."[19] In the 1960s, Schwarz concentrated on time-sharing and databases—indeed, he managed SDC's Q-32 system—and then in 1970 he moved to Computer Sciences Corporation. His publications also trace a lineage from the large military systems work through databases and interactive programming.[20] Like MITRE, Multics, Honeywell, and the NSA, SDC created the emerging computer security community. Additional SDC connections in this group include Richard Kemmerer, an established SDC consultant who worked with Secure Unix, formal methods, intrusion detection, and later the landmark TCSEC effort, and most notably, Marvin Schaefer, who did security work at SDC beginning in 1965 that led to his seminal work starting the TCSEC and setting up the National Computer Security Center.[21]

The Q-32 time-sharing system fell somewhat into SDC's lap. J.C.R. Licklider, as is well known, was a determined and resourceful advocate for interactive computing. The Air Force in the late 1950s planned a full-blown replacement for the vacuum-tube-based SAGE, so-called Super Sage, using transistorized computers and enhanced networking and communications. Questions about the feasibility of the follow-on project, and quite possibly frustrations with the original SAGE system, led to the cancellation of the main project in 1960. For SDC an ARPA contact also hung in the balance. "The only thing that was going to save it was the use of the Q32 computer," recalled Schwarz. "At that time Licklider was proposing his man-computer symbiosis ideas, and he had the idea that we should have a time sharing system on the Q32 computer which would service universities or researchers around the country."[22] IBM was gearing up to manufacture a dozen or more machines for SAGE's successor; in the event, two closely related Q-31s were sent to Strategic Air Command (SAC) facilities in Omaha, Nebraska, and one Q-32 was shipped to SDC in Santa Monica.

SDC's Q-32 was originally intended as a prototype for an all-embracing air-defense system, and to this end, Schwartz's Jovial programming language was used for 95 percent of its code—saving, by any estimation, thousands of programmer-hours over SAGE-era machine coding. With time-sharing realized by 1963, "about the same time as the better-known Compatible Time-Sharing System (CTSS) system"[23a] at MIT, Schwartz developed an interactive interpreter for Jovial. SDC's Q-32 supported a number of innovations in time-sharing and remote logins. Among the early remote users were Douglas Englebart's Augmentation Research Center at the Stanford Research Institute (SRI) and the SAC air-defense network. By 1963, there was a two-node network connecting a Control Data 160A minicomputer at SRI "400 miles distant from the Q-32."[23] A DEC PDP-1 minicomputer served as a communications gateway (similar to the Arpanet's interface-message processors, or IMPs) for all external network connections to the Q-32. This meant that local teletypes, local displays, remote teletypes, and remote computers like the CDC 160A (and soon MIT Lincoln Laboratory's TX-2 computer on the other side of the country) were connected to the PDP-1, which formed an interface to the Q-32 computer. Users of the teletype terminals also could avail themselves of an innovative messaging system, again substantially anticipating interactive text messaging. SDC's Q-32 was actively used by SAC, ARPA, the Air Force, and numerous other external users through 1970.[24]

The strong national security bent of computer security during these years is well known and well documented. "The ancestry of the Orange Book and derivative documents … was defense driven *ab initio,*" stated RAND's Willis Ware.[25] The DSB's computer security steering group, chaired by Ware, included representatives from SDC, Lockheed Missiles and Space, the DoD's Directorate for Security Policy, the Office of the Secretary of Defense's Director of Defense Research and Engineering (DDR&E), Central Intelligence Agency, NSA, and ARPA, as well as Edward Glaser from Case Western Reserve University. Its policy panel included additional representatives from these agencies as well as the Defense Communication Agency and Chemical Abstracts Service; the technical panel included representatives from MITRE, IBM, MIT, and the White House and consultant James P. Anderson, who authored a notable computer-security report. Three recent articles in *IEEE Annals* elaborate on the basic narrative following the 1970 Ware Report through the Orange Book, emerging in the mid-1980s.[26]

The single most important precursor to the 1970 Ware Report was the technical session that Ware organized for the 1967 SJCC.

The single most important precursor to the 1970 Ware Report was the technical session that Ware organized for the 1967 SJCC. In addition to Ware and two other RAND colleagues (Harold Petersen and Rein Turn), the conference session featured a notable paper by the NSA's Bernard Peters. In 2003 Ware recalled the growing importance of computing to the military services and his perception that the US government was becoming dependent of computing:

> We would talk amongst ourselves in the hallways at conferences and gradually there emerged a concern that we really ought to do something about finding out how to protect computer systems and all that information in them, because the country has become too dependent on them. That was the thread that began … computer or information security. We: myself, Paul Armer, probably Bob Patrick, maybe Pat Haverty, decided that we ought to put on a session … —four papers as I remember—offered it to this Spring Joint Computer Conference meeting in Atlantic City [in 1967]. So that was the first public discussion that I believe ever took place on what we now call computer security.[27]

The Context of Computer Security

Even here, with the military services' dependence on computing clearly in the foreground, there were other forces at work that loosened RAND's once-tight relationship with the Air Force and permitted discourse on computer security to move more readily between the classified and public realms. This was, after all, the 1960s. The political turmoil surrounding

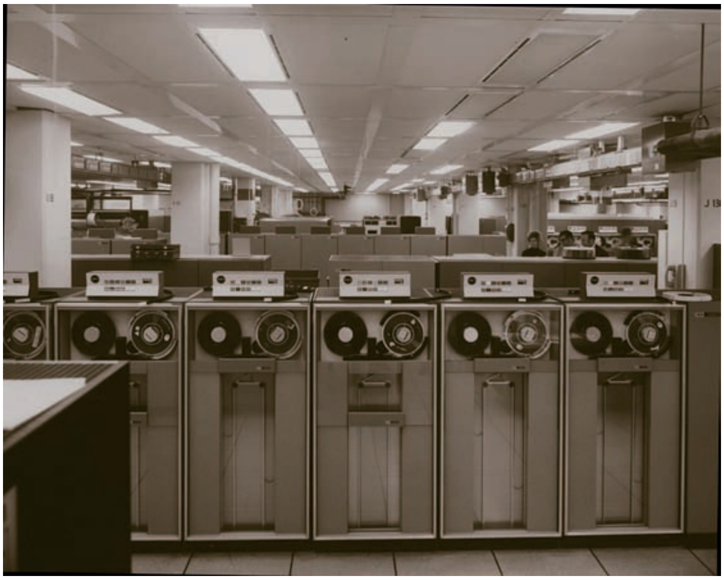


Figure 1. National Security Agency's Univac 494 and the time-sharing RYE computing system.[33] A color version dated 1972 appears online in an article by James Bamford.[34]

the Vietnam War, criticisms of the DoD's Federally Funded Research and Development Centers—so-called FFRDCs such as SDC and RAND—by private industry, and persistent congressional scrutiny of these relationships across the 1960s led to significant structural change. Since its founding, RAND had served the US Air Force as a prototypical think tank, but between 1963 and 1973 its level of funding from the US Air Force was cut in half. The decrease in funding across these 10 years resulted in a drop from roughly 900 Air Force-supported researchers down to 400.[28]

In his oral history, Ware recalled the 1967 retirement of RAND's long-serving president Frank Collbohm as a trigger for change. According to historian Roger Lotchin, Collbohm was "an ex-pilot with Douglas Aircraft and a close friend of General [Henry 'Hap'] Arnold" who had led RAND for nearly two decades since its founding as a spin-off from Douglas.[29] The political climate just described impinged on FFRDCs. SDC's management in May 1967 pointed to the worrisome "atmosphere prevailing in Washington" that meant "our sole-source contract acquisition methods [are] coming to a close."[30] SDC's parent RAND felt similar pressures. Ware recalled,

> The result of the [Daniel] Ellsberg flap and other things of the time was that Congress directed RAND to diversify, and so Harry Rowan [RAND's new president in 1967] was told to create a non-defense domestic program. That was really the start of change.[31]

RAND's subsequent activities in urban management and social-welfare policy have been documented by historians David Jardini, Jennifer Light, and others.[32] In this same vein, Ware's choice of the joint computer conference, sponsored by the American Federation of Information Processing Societies (AFIPS) (active 1961–1990) with support from the Institute of Radio Engineers (IRE), American Institute of Electrical Engineers (AIEE), and ACM, was a notable public venue for presenting computer security work previously done largely behind closed doors.

NSA's Bernard Peters took a public role, highly unusual for the time, in the 1967 SJCC session. "The enabling event," as Ware described it, was the NSA's development of a full-blown remote-access time-sharing system built around a Univac mainframe and installed at the agency's Fort Meade headquarters. This was RYE. It featured a "full set of security access controls" for terminals and users both at the NSA headquarters as well as worldwide (see Figure 1[33,34]). "Fortuitously, I knew details of the system," stated Ware.[35] Of course it wasn't by chance that he was unusually well informed about computing developments at the NSA. Ware's personal papers at CBI contain extensive folders on military agencies and national labs,[36] defense contractors,[37] and prominent computer manufacturers[38] from the early 1950s through the 1970s. He sat on numerous scientific advisory committees, including that of the NSA itself.[39]

As chair of RAND's Computer Science Department since 1964, Ware spent roughly equal thirds of his time supervising the RAND department, serving as a computing professional active in AFIPS and other organizations, and engaging in government advisory activities. Thus, his unique role in computing at the time helped bring NSA's RYE into the public eye. Secrecy at the NSA (for years it was dubbed "No Such Agency") formed one obvious barrier to the public's understanding of its key role in computer security.[40] In a semiofficial book on its supercomputer Stretch (an early one was delivered to the NSA), IBM disguised the existence of NSA's purpose-built code-breaking unit (codenamed Harvest) in a chapter on "A Nonarithmetical System Extension" with its contrived and misleading examples from the "soft sciences."[41] A less-recognized barrier was a common convention in the technical literature: conference papers describing a specific computer system (in a presented version) were frequently rewritten to emphasize its general "principles" in the published version.[42] The published paper by NSA's Bernard Peters did precisely that. Peters at the time gave almost no identifying details of RYE, despite his being the agency's director of the RYE system.[43] The agency has since declassified enough documentation to now permit a description of the RYE system and the immense NSA computing complex (see Figure 2[33]). NSA's RYE, like the other multilevel time-shared computer systems, shaped the emerging discourse of computer security.

The NSA's networked time-sharing system RYE was built during a period of dramatic expansion. Beginning in the early 1960s, the agency's computing capacity expanded at a sustained compound growth rate of 50 percent per year.[44] The NSA's computing resources, valued at $50 million in 1963, was according to an NSA history "by far the largest in the country and probably the world." Notable recent additions were the IBM 7030 Stretch computer with its Harvest code-breaking unit (see Figure 2). In 1963 the NSA bought its first DEC minicomputers and also initiated the RYE system. Around 1960, NSA had built an early computer-based communications network based on IBM 7010 computers that sped the delivery of traffic extracts or technical summaries from its far-flung field stations to its Fort Meade headquarters. In 1963 NSA purchased a Univac 490 mainframe computer (see Figure 1) and constructed a network initially consisting of 20 or 30 terminals located in the agency's Fort Meade headquarters and in field stations around the world. "The software, called RYE, was developed at NSA and was ideal for handling simultaneous inputs from the remote stations." The RYE complex, soon powered by two high-capacity Univac 494 models, became "the central nervous system" for the NSA's operations center (NSOC) that dealt with high-priority incoming traffic on the "Soviet problem."[45]

The era of intelligence officers pouring over piles of printed teletypes had ended. "Short highly formatted information fragments" came in on more than 100 "internetted" operational communication circuits, were processed by the Univac 494s, and then routed to CRT terminals being used by analysts on the "floor." Actually "any RYE terminal"—inside or outside NSA's headquarters (see Figure 3[33])—also had access through a file maintenance and retrieval system to "various end-product and technical files."[46] (In a few years RYE doubled again to four Univac 494s and 200 terminals.) As adjuncts to RYE, TIDE was the specialized time-dependent intelligence-processing software, while TIPS (Technical Information Processing System) was the "hardware devices, software executive routines, conventions, communication package, and data bases in support of the quick-turnaround, on-line, information storage and retrieval capability within RYE."[47] By 1965 RYE was integrated into the NSA computing complex, including the

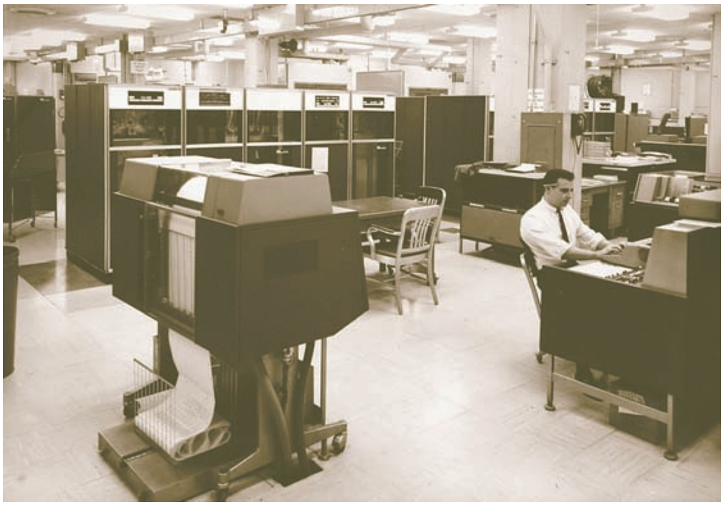


Figure 2. NSA in the 1960s relied on the IBM 7030 Stretch connected to the one-of-a-kind HARVEST unit, which was operational in 1962 (shown here in 1968).[33]

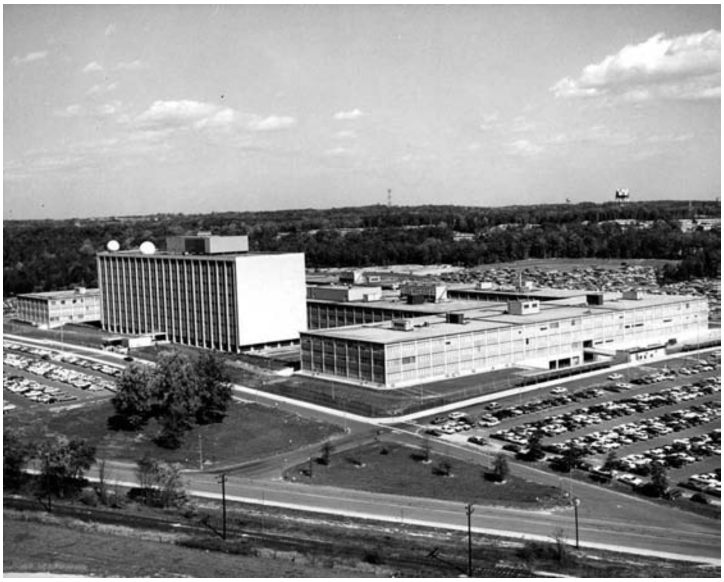


Figure 3. The NSA's newly constructed nine-story headquarters (circa 1964) was surrounded by the three-story Operations 1 buildings that housed "acres" of computing.[33]

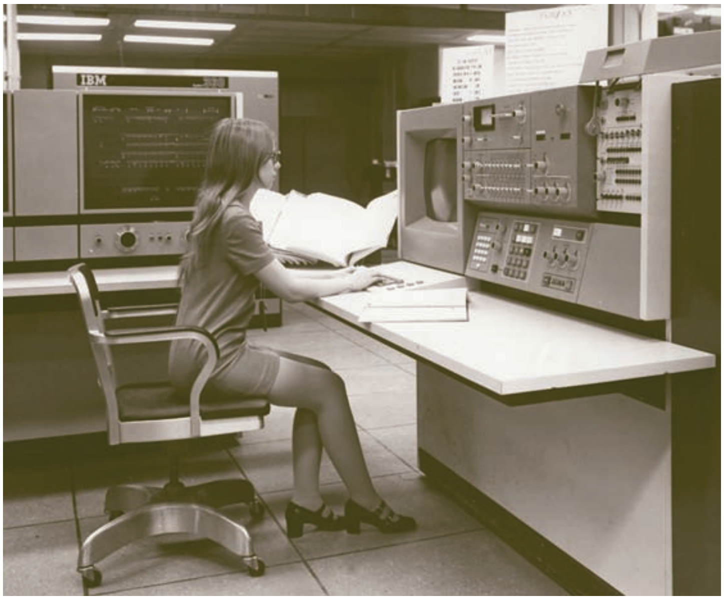


Figure 4. NSA's computing beyond exotic crypto. In the early 1970s, the NSA used four IBM 360 mainframes in its Central Data Processing Facility alone (soon replaced by IBM 370/165s).

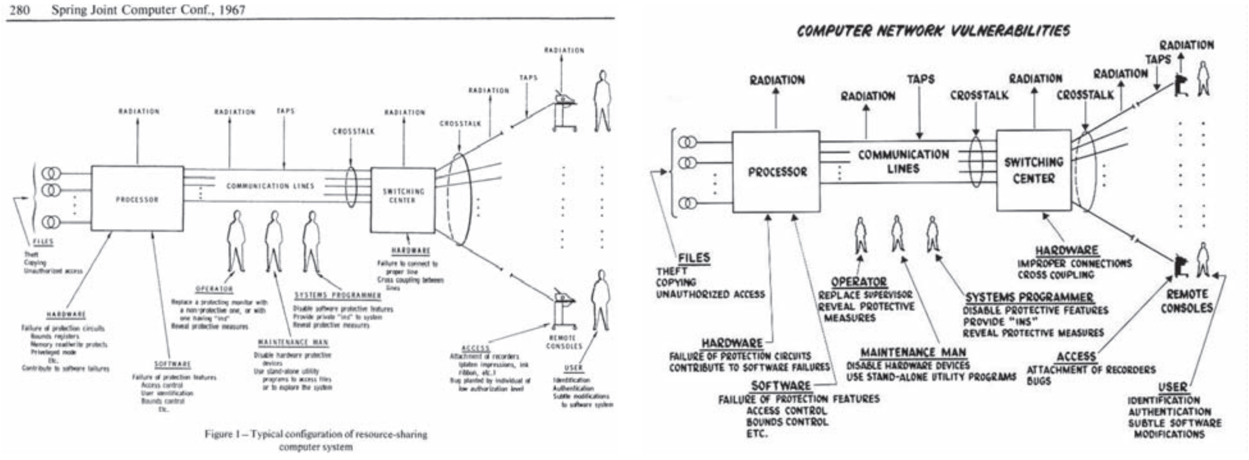
Stretch–Harvest system: "RYE has made it possible for the Agency to locate many more potentially exploitable cryptographic situations … Many messages that would have taken hours or days to read by hand methods … can now be 'set' and machine decrypted in a matter of minutes."[48] Intercepted communications in Vietnam could be sent to Fort Meade, decrypted there, and returned to US field commanders in four hours.[49] By 1968, with expansion of the RYE complex and installation of IBM mainframes and CDC supercomputers, "NSA had over 100 computers occupying almost 5 acres of floor space."[50]

It is worth reflecting on this detailed portrait of NSA's computing. Comprehending the scale and significance of computing in the intelligence and classified realms has been difficult for many years.[51] It is now possible to appreciate that NSA's computing was not merely immense in scale but also that it ranged far beyond specialized crypto (see Figure 4). In the early 1970s, NSA had seven defined accounting categories for its computing activities: missile and space telemetry (2 percent of total computing capacity), plain language processing (7 percent), electronic intelligence processing (10 percent), communication intelligence (10 percent), traffic analysis (13.5 percent), management and technical support (19 percent), and cryptanalysis (39.5 percent) as well as additional capacity in the RYE network (roughly 10 percent on top).[52] As additional documents are declassified, historians are likely to better document the intelligence agencies' impact on communications, networking, security, databases, high-capacity storage, text-mining software, and other computing areas.[53]

Here is one comparison from 1973. RYE then had 200 "internetted" terminals with a global network extending to Asia (there are clear reports of NSA's field officers in Vietnam preparing the structured technical summaries [TECSUMs] that were fed into RYE),[54] and the agency then had at least 30 mainframe computers (including seven CDC supercomputers and an untold additional number of minicomputers).[55] Thus, it seems inescapable that the NSA alone substantially exceeded the computing capability of the entire Arpanet (at the time roughly 20 TIP terminals and 20 full IMP nodes) providing network access to just 13 mainframes (mostly IBM 360s and 370s) and 30 minicomputers (mostly DEC PDPs). The agency's varied uses of computing, and ultimately its impact, is amply revealed when examining the entirety of computing—"hardware devices, software executive routines, conventions, communication package, and data bases."[47]

Ware himself explicitly connected the NSA's computing complex with computer security. "There will have to be a comprehensive solution to the matter of computer security," Ware stated in his 1973 NSA advisory committee assessment. He pointed to the agency's growing dependence on electronic computing and the pressing questions of reliability (which meant that feasible security measures could not impose undue computational burdens). There was also the delicate issue of the physical vulnerability of NSA's Fort Meade headquarters. The "centralization of business at Fort Meade" put the nation's signals intelligence "eggs into one basket," Ware stated. "The headquarters area would be a vulnerable target of immense and growing military significance."[56]

Bernard Peters was hardly the sole NSA staffer active in computer security. Long-time NSA researcher Daniel Edwards investigated and named "Trojan horse" attacks, and he later worked at NSA's National Computer Security Center on its development of the landmark TCSEC. Rebecca Bace helped develop the field of intrusion detection, writing an influential textbook on the topic and managing NSA's security research. Yet another


280 Spring Joint Computer Conf., 1967
RADIATION
RADIATION
TAPS
CROSSTALK
RADIATION
CROSSTALK
RADIATION
TAPS
RADIATION
PROCESSOR
COMMUNICATION LINES
SWITCHING CENTER
FILES
Theft
Copying
Unauthorized access
HARDWARE
Failure of protection circuits
Bounds registers
Memory read/write protects
Privileged mode
Etc.
Contribute to software failures
SOFTWARE
Failure of protection features
Access control
User identification
Bounds control
Etc.
OPERATOR
Replace a protecting monitor with a non-protective one, or with one having "ins"
Reveal protective measures
MAINTENANCE MAN
Disable hardware protective devices
Use stand-alone utility programs to access files or to explore the system
SYSTEMS PROGRAMMER
Disable software protective features
Provide private "ins" to system
Reveal protective measures
HARDWARE
Failure to connect to proper line
Cross coupling between lines
ACCESS
Attachment of recorders (platen impressions, ink ribbon, etc.)
Bug planted by individual of low authorization level
REMOTE CONSOLES
USER
Identification
Authentication
Subtle modifications to software system
Figure 1 – Typical configuration of resource-sharing computer system
COMPUTER NETWORK VULNERABILITIES
RADIATION
RADIATION
TAPS
CROSSTALK
RADIATION
CROSSTALK
RADIATION
TAPS
RADIATION
PROCESSOR
COMMUNICATION LINES
SWITCHING CENTER
FILES
THEFT
COPYING
UNAUTHORIZED ACCESS
OPERATOR
REPLACE SUPERVISOR
REVEAL PROTECTIVE MEASURES
SYSTEMS PROGRAMMER
DISABLE PROTECTIVE FEATURES
PROVIDE "INS"
REVEAL PROTECTIVE MEASURES
HARDWARE
IMPROPER CONNECTIONS
CROSS COUPLING
REMOTE CONSOLES
HARDWARE
FAILURE OF PROTECTION CIRCUITS
CONTRIBUTE TO SOFTWARE FAILURES
MAINTENANCE MAN
DISABLE HARDWARE DEVICES
USE STAND-ALONE UTILITY PROGRAMS
ACCESS
ATTACHMENT OF RECORDERS
BUGS
SOFTWARE
FAILURE OF PROTECTION FEATURES
ACCESS CONTROL
BOUNDS CONTROL
ETC.
USER
IDENTIFICATION
AUTHENTICATION
SUBTLE SOFTWARE MODIFICATIONS

(a) (b)

Figure 5. Comparison of (a) Figure 1 from the 1967 Spring Joint Computer Conference (SJCC) session and (b) Figure 3 from the 1970 Ware Report. The similarities suggest the significance of pre-1967 computer security work.

NSA staffer active in early computer security was Stephen Walker, who subsequently worked at ARPA's Information Processing Techniques Office (IPTO) and the Office of the Secretary of Defense. Then in the early 1980s, Walker founded Trusted Information Systems, a celebrated security start-up company that employed a stunning roster of security pioneers (including David Bell, Terry Benzel, Martha Branstad, Steve Lipner, and Marvin Schaefer as well as networking pioneer Steve Crocker). Among TIS's notable successes was Trusted Xenix and its groundwork that led to the modern security firewall industry.[57]

From SDC and NSA to 1967 SJCC

Ware's 1967 SJCC introduction as session chair was a broad overview of the problem of computer security. He pointed specifically to situations where multiple users with sensitive classified information used a single computing system, so "safeguards must be provided to guard against the leakage of information."[58] Anyone who has studied the 1970 Ware Report will experience a moment of disorientation, however, in seeing its often-repeated computer-security graphic[59] plainly printed in the 1967 session, labeled as "Typical configuration of resource-sharing computer system" (see Figure 5). One seeming result of the 1970 Ware Report was in actuality an input to that report, once again suggesting the significance of pre-1967 computer security work.

The labels in the 1970 Ware Report graphic were redrawn to be larger and more legible (see Figure 5b), but the two versions feature precisely the same computer-system components: "processor," "switching center," "communication lines," remote consoles/terminals, and several distinct types of people as well as virtually all the same text. The security concerns connected to distinct types of people are clearly identified: an operator might "replace a protecting monitor [roughly, operating system] with a non-protective one" or might "reveal protective measures," a maintenance man might "disable protective hardware devices" or use utility programs "to access files or to explore the system," and a systems programmer might "disable software" or "provide private 'ins' to system" or "reveal protective measures," and all the while a user might compromise security through identification, authentication, and "subtle modifications to software system." Left unidentified in both versions were who might attach "bugs" or recording devices to printers or terminals.

Of equal concern to Ware by 1967 was the physical hardware that emitted radiation at no less than five points (processor, communication lines, switching center, terminal connections, and terminals themselves) and so might be vulnerable to taps. Much energy in the security community has focused on the hardware, with the vulnerability or misuse of protective circuits, bounds registers, memory read/write protects, or privileged modes. Communication and terminal lines were vulnerable to "crosstalk." And finally, computer security researchers have focused immense attention on software (failure of protection features, access control, user identification, and bounds control). It would be impressive if the DSB's three-year effort had led to such an all-encompassing graphic; it's something else entirely to recognize the 1967 graphic more properly as an input to the Ware Report of 1970.

Early computer security work done by the RAND–SDC–NSA network beginning in the mid-1960s explicitly framed the 1967 SJCC session and 1970 Ware Report.

Harold Peterson and Rein Turn's 1967 SJCC paper, "System Implications of Information Privacy," focused on nonmilitary systems and highlighted that security and privacy are two sides of the same coin, as the notable IEEE Security and Privacy conference series has long expressed. NSA staffer Bernard Peters' SJCC contribution is a short but dense paper that, in its published version, developed nine specific principles in its discussion of "security considerations in a multi-programmed computer system." The paper's conclusion broadly hints at the NSA's specific real-world system that lay behind the published paper's abstractions: "The principles set forth in this paper have been generalized from the specific development of a specific system [that is, NSA's time-sharing Univac 494] which dealt with multi-levels of classified information [RYE]."[60] The nine principles were as follows:

- Computers must operate under a monitor approved by appropriate authority.
- Computers must have adequate memory to protect privileged instructions.
- Computers must have appropriate physical security to prevent local override of the monitor.
- Electrical separation of peripheral devices is not necessary provided the monitor has been approved by the appropriate authority.
- Computers may operate in multiprogrammed or multiprocessor modes provided the monitor has been approved for such modes.
- Operating personnel must be cleared to appropriate levels.
- A log of all significant events should be maintained.
- Every user should be subject to common discipline and authority.
- Individual remote terminals may need to change their security level upward.

The core of Peters' paper specifies the all-important "attributes of an acceptable monitor," the security-conscious elements of an operating system. For Peters the monitor was "the key defense, the key security element in the system."[61] The notion of a security-enforcing "reference monitor," typically credited to Roger Schell or James Anderson, was already emerging here. Peters optimistically estimated the security-conscious monitor might cost 10 percent more to develop than a typical multiprogramming monitor. It would strictly perform all input/output as well as manage the system clocks and main operating console. A specific concern was "critical coding" because when a programming interrupt occurred the computer was placed in a vulnerable situation in which the memory might not be protected or stable. Specifically, the "monitor must keep the user programs bounded by memory protect" while they are running.

If an unauthorized action or security violation occurs, the monitor must quickly suspend the offending process and bring about "a complete abort of all parts of that request" to prevent an insecure program from making multiple attempts to subvert the security system. Even debugging or testing must not escape control of the monitor, because the new program introduced "is the one most likely to violate security." Finally, in that era of unstable bits (and the common use of so-called parity bits), the data used for security levels (such as classified and unclassified) must never be single bits where a bit error could lead to a significant shift in security. Peters stated that he used a 60-bit flag in the (unnamed) machine that had a 30-bit word length so that four 15-bit "configurations" were "complementary" to specify and ensure the security classification.

Conclusion

Early computer security work done by the RAND–SDC–NSA network beginning in the mid-1960s explicitly framed the 1967 SJCC session and 1970 Ware Report. In December

1968, NSA's RYE is specifically named and credited: "Security Procedures for the RYE System" grounded the 1970 report's policy recommendations on management and administrative control. Also specifically cited was NSA's George Hicken, "representing the RYE and COINS systems." And the 1970 report acknowledges many staffers from RAND, SDC, and NSA: Robert Balzer and Wade Holland from RAND; Clark Weissman from SDC; and NSA's Hilda Faust and Thomas Chittenden, "who rewrote the entire document to produce the all-important second draft." Recall that Weissman led the SDC efforts in time-sharing and multilevel computer security.

This article suggests that computer security in these emerging years is aptly and accurately located at "the intersection of material conditions with knowledge, politics, and society." It has shown how material conditions at SDC and the NSA, especially the two multilevel time-sharing systems Q-32 and RYE, formed an immediate context for computer security research that informed and led to the pioneering 1967 SJCC papers and the landmark 1970 Ware Report. Expanding knowledge, experiences, and practices about how to operate complex multilevel time-sharing systems was the immediate backdrop. In this respect, SDC's Q-32 and NSA's RYE should be considered alongside the MIT and Honeywell Multics system as a generative locus for early computer security.

This article also highlights the importance of shifting funding patterns and political upheaval in the 1960s. Although we often remember that decade as a high tide in the Cold War, significant reductions in direct military support at RAND prompted Ware and RAND to engage the concerns and problems of the wider society more directly than ever before. Historians have so far emphasized RAND's noted efforts in social policy and urban modeling as expressions of this post-1967 vision, but it is appropriate to view RAND's computer security work (and attendant public activity) as responding to this same aim. Even as RAND's Air Force funding was on the wane, NSA's funding for computing was impressively rising, giving the agency ample experience with a global, time-sharing networked communication system. Thus, we can understand the antecedent events to the 1967–1970 origins of computer security as a product of material, political, knowledge, and social elements.

More broadly, the discourse surrounding computer security at RAND and elsewhere reminds us of three general reflections. First, computer security as a technical field interacts with institutional dynamics and the broader political and social environment. Second, this environment can shape the outlook and focus of participants in the technical field of computer security. And, finally, the real measure of computer security is, in addition to robust technical concepts, the wider dissemination and embedding of computer security practices in government, industry, finance, communication, and the entire range of computer-dependent institutions.

Close attention to this early computer security discourse suggests a lesson for computer historians who imagine distinct and meaningful differences between hardware and software. Instead, the 1967 and 1970 security graphics make plain that the power of computing as well as its vulnerabilities can be readily grasped when acknowledging the critical links among all elements in a computing system, ranging across hardware, software, communications, organizational routines, maintenance procedures, and the bonds of trust placed in programmers and computer operators. A history of computing attentive to this big picture is sorely needed to properly understand the security dilemmas that were recognized in the past and that we continue to face in the present and future.

References and Notes

1. S.T. Redwine, ed., *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software*, version 1.1, US Dept. of Homeland Security, Sept. 2006, notes 2–3.
2. See Matt Bishop's seminal papers at http://seclab.cs.ucdavis.edu/projects/history/seminal.html. Citations from Google Scholar, ACM Digital Library, and Web of Science include M. Bishop and D. Frincke, "Teaching Secure Programming," *IEEE Security and Privacy*, vol. 3, no. 5, 2005, pp. 54–56; M. Bishop and S. Engle, "The Software Assurance CBK and University Curricula," *Proc. 10th Colloquium for Information Systems Security Education*, 2006; C.E. Landwehr, "History of US Government Investments in Cybersecurity Research: A Personal Perspective," *Proc. IEEE Symp. Security and Privacy*, 2010, pp. 14–20; C.E. Irvine and J.R. Rao, "Engineering Secure Systems Introduction," *IEEE Security & Privacy*, vol. 9, no. 1, 2011, pp. 18–21; and C. Irvine,

"A Cyberoperations Program," *IEEE Security & Privacy*, vol. 11, no. 5, 2013, pp. 66–69.

3. W. Ware, "New Vistas on Info-system Security," *Information Security in Research and Business* (*IFIP* 1997), L. Yngström and J. Carlsen, eds., pp. 177–196; S.J. Murdoch, M. Bond, and R. Anderson, "How Certification Systems Fail: Lessons from the Ware Report," *IEEE Security & Privacy*, vol. 10, no. 6, 2012, pp. 40–44; and R. Bigman, "What Trusted Computing History Teaches Us About Today's Challenges," RSA conf. presentation, 2015; www.rsaconference.com/writable/presentations/file_upload/mash-f03-what-trusted-computing-history-teaches-us_about-todays-challenges_final.pdf.
4. This research was done with support from National Science Foundation CNS–TC 1116862 "Building an Infrastructure for Computer Security History" (2011–2015). An early version was presented at the 2015 Cryptologic History Symposium at the Center for Cryptologic History (CCH), where several participants generously suggested leads to follow. I acknowledge valuable assistance from my CBI colleague Jeffrey Yost.
5. Willis H. Ware Papers, CBI 40, http://purl.umn.edu/41431; see also W.H. Ware, *RAND and the Information Evolution: A History in Essays and Vignettes*, RAND, 2008; www.rand.org/pubs/corporate_pubs/CP537.html.
6. D. MacKenzie and G. Pottinger, "Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the U.S. Military," *IEEE Annals of the History of Computing*, vol. 19, no. 3, 1997, pp. 41–59; J.R. Yost, "The Origin and Early History of the Computer Security Software Products Industry," *IEEE Annals of the History of Computing*, vol. 37 no. 2, 2015, pp. 46–58.
7. P.N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America*, MIT Press, 1996, p. 31.
8. Jeffrey Yost is preparing an archive-based assessment of Multics.
9. P.R. Kennedy, "The ADEPT-50 System: A General Description of the Time-Sharing Executive and the Programmer's Package," 4 Apr. 1968, CBI 90 (Burroughs), series 98 (SDC), box 11, folder 1.
10. P.S. Browne, "Computer Security: A Survey," *ACM SIGMIS Database*, vol. 4, no. 3, 1972, pp. 1–12, DOI=http://dx.doi.org/10.1145/1017536.1017537; quotes appear on p. 4 (various categories) and p. 12 (early attempts). The second such system was identified cryptically as the DIS ANSRS System. Most computer security practitioners and existing historical accounts focus on US developments; research on the history of computer security outside the United States is sorely needed.
11. For a popular culture critique of RAND and game theory, see S. Belletto, "The Game Theory Narrative and the Myth of the National Security State," *Am. Quarterly*, vol. 61, no. 2, 2009, pp. 333–357.
12. Recent works include D. Hounshell, "The Cold War, RAND, and the Generation of Knowledge, 1946-1962," *Historical Studies in the Physical and Biological Sciences*, vol. 27, no. 2, 1997, pp. 237–267; M.J. Collins, *Cold War Laboratory: RAND, the Air Force, and the American State, 1945–1950*, Smithsonian Institution Press, 2002; S. Ghamari-Tabrizi, *The Worlds of Herman Kahn: The Intuitive Science of Thermonuclear War*, Harvard Univ. Press, 2005; H. Crowther-Heyck, "Patrons of the Revolution: Ideals and Institutions in Postwar Behavioral Science," *Isis*, vol. 97, no. 3, 2006, pp. 420–446; A. Abella, *Soldiers of Reason: The RAND Corporation and the Rise of the American Empire*, Harcourt, 2008; P. Erickson, "Mathematical Models, Rational Choice, and the Search for Cold War Culture," *Isis*, vol. 101, no. 2, 2010, pp. 386-392; J.F. Brodie, "Learning Secrecy in the Early Cold War: The RAND Corporation," *Diplomatic History*, 35, no. 4, 2011, pp. 643–670; P. Erickson, *The World the Game Theorists Made*, Univ. of Chicago Press, 2015.
13. Quoted in "A History of the Department of Defense Federally Funded Research and Development Centers," US Office of Technology Assessment, 1995, p. 24.
14. C. Baum, *The System Builders: The Story of SDC*, SDC, 1981, p. 92.
15. See K.C. Redmond and T.M. Smith, *Project Whirlwind: History of a Pioneer Computer*, Digital Press, 1980; K.C. Redmond and T.M. Smith, *From Whirlwind to MITRE: The R&D Story of The SAGE Air Defense Computer*, MIT Press, 2000. For MITRE's work in computer security, see CBI oral histories with David Elliott Bell, Steven B. Lipner, Teresa Lunt, and Terry Benzel at www.cbi.umn.edu/oh.
16. For a biographical sketch, see Clark Weissman's introduction as distinguished speaker for the 19th ACSAC Conference at www.acsac.org/2003/dist.html.
17. See Weissman's unpaginated slides in "ADEPT-50 Symposium," SDC papers, box 6, folder 2, 17 Apr. 1968; Baum, *The System Builders*, p. 118.
18. See papers authored or coauthored by Weissman: J.I. Schwartz, E.G. Coffman, and C. Weissman, "A General-Purpose Time-Sharing System," *Proc. AFIPS Spring Joint Computer Conf.*, 1964, pp. 397–411; J.I. Schwartz and C. Weissman, "The SDC Time-Sharing System Revisited," *Proc. 22nd ACM Nat'l Conf.*, 1967,

pp. 263–271; and C. Weissman, "Security Controls in the ADEPT-50 time-Sharing System," *Proc. AFIPS Fall Joint Computer Conf.*, 1969, pp. 119–133. Weissman further participated in a landmark 1972 session with Roger Schell, Peter Denning, and James P. Anderson on "Privacy and Protection in Operating Systems," *Proc. ACM Ann. Conf.*, vol. 2, 1972, pp. 665–666, as well as a 1974 session with Steven Lipner, William Wulf, Roger Schell, Peter Neumann, and others on "Security Kernels," *Proc. AFIPS Nat'l Computer Conf.*, 1974, pp. 973–980. See also his "BLACKER: Security for the DDN: Examples of A1 Security Engineering Trades," *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, 1992, pp. 286–292 (paper originally presented in 1986). Baum, *The System Builders*, p. 249.

19. J.I. Schwartz, "The Development of JOVIAL," *History of Programming Languages*, R.L. Wexelblat, ed., Academic Press, 1981, p. 370. For JOVIAL history and development, see CBI's SDC papers, box 11, folders 15–18.
20. In addition to the articles on Jovial and his publications with Weissman on SDC time-sharing, see these publications by Schwarz: J.I. Schwartz, "Observations on Time-Shared Systems," *Proc. 20th ACM Nat'l Conf.*, 1965, pp. 525–542; J.I. Schwartz, "Online Programming," *Comm. ACM*, vol. 9, no. 3, 1966, pp. 199–203; J.I. Schwartz, "Interactive Systems: Promises, Present and Future," *Proc. AFIPS Fall Joint Computer Conf.*, 1968, pp. 89–98.
21. R. Kemmerer, oral history conducted by J.R. Yost, Charles Babbage Inst. (CBI), Univ. of Minnesota (UMN), CBI OH 450, 30 Apr. 2014, http://hdl.handle.net/11299/168280; M. Schaefer, oral history conducted by J.R. Yost, CBI OH 435, 20 Nov. 2013, http://hdl.handle.net/11299/163870. Computer security pioneer Lance Hoffman interned at SDC.
22. J.I. Schwartz, oral history conducted by A.L. Norberg, CBI OH 161, 7 April 1989, p. 11, http://purl.umn.edu/107628; Baum, *The System Builders*, p. 91.

23a. D. Hemmendinger, "Messaging in the Early SDC Time-Sharing System," *IEEE Annals of the History of Computing*, vol. 36, no. 1, 2014, p. 52.

23. Hemmendinger, "Messaging in the Early SDC Time-Sharing System," p. 52; Schwartz, Coffman, and Weissman, "A General-Purpose Time-Sharing System," p. 397; Baum, *The System Builders*, p. 92. For more on early SDC networking, see D. Hemmendinger, "Two Early Interactive Computer Network Experiments," *IEEE Annals of the History of Computing*, vol. 38, no. 3, 2016, pp. 12–24.
24. "Q-32 Disposition," 11 July 1969, SDC papers, box 11, folder 24, p. 41.
25. W. Ware, "New Vistas on Info-system Security," *Information Security in Research and Business* (*IFIP* 1997), L. Yngström and J. Carlsen, eds., p. 180.
26. M. Warner, "Notes on the Evolution of Computer Security Policy in the US Government, 1965–2003," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 8–18; S. Lipner, "The Birth and Death of the Orange Book," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 19–31; J.R. Yost, "The Origin and Early History of the Computer Security Software Products Industry," *IEEE Annals of the History of Computing*, vol. 37, no. 2, 2015, pp. 4658; and J.R. Yost, "History of Computer Security Standards," *The History of Information Security: A Comprehensive Handbook*, K. de Leuuw and J. Bergstra, eds., Elsevier Science, 2007, pp. 595–621.
27. W.H. Ware, oral history conducted by J.R. Yost, CBI OH 356, 11 Aug. 2003, p. 13; http://purl.umn.edu/107703. Ware identified Robert L. Patrick and John P. Haverty in his foreword to C.P. Pfleeger and S. Lawrence Pfleeger, *Security in Computing*, 3rd ed., Prentice Hall, 2003.
28. "A History of the Department of Defense Federally Funded Research and Development Centers," US Office of Technology Assessment, 1995, pp. 27–32; "Chronology of Congressional Interest in Non-Profit Corporations," 1961, SDC papers, box 18, folder 10, p. 1.
29. R.W. Lotchin, *Fortress California, 1910–1961: From Warfare to Welfare*, Oxford Univ. Press, 1992, p. 180; "F. R. Collbohm, 83, Ex-Head of Rand, Dies," *New York Times*, 14 Feb. 1990, www.nytimes.com/1990/02/14/obituaries/f-r-collbohm-83-ex-head-of-rand-dies.html.
30. "On Some Fundamental Issues Confronting the System Development Corporation," SDC internal policy planning paper, SDC papers, box 18, folder 2, May 1967, pp. 3, 4; "Memorandum for Discussion," SDC papers, 7 June 1967, box 18, folder 27.
31. Ware, CBI OH 356, pp. 27–28. Ware slightly scrambled the chronology, since Ellsberg as a RAND researcher was working on the Pentagon's study of the Vietnam War, began copying its 7,000 pages in late 1969, and famously leaked the Pentagon Papers to the *New York Times* in March 1971. I interpret Ware's words as a reference to the upheaval of the Vietnam era and the criticism experienced by RAND and other FFRDCs.
32. D. Jardini, "Out of the Blue Yonder: The RAND Corporation's Diversification into Social Welfare Research, 1946–1968," PhD dissertation, Carnegie Mellon Univ., 1996; J.S. Light, *From*

Warfare to Welfare: Defense Intellectuals and Urban Problems in Cold War America, Johns Hopkins Univ. Press, 2003; A. Abella, *Soldiers of Reason: The Rand Corporation and the Rise of the American Empire*, Harcourt, 2008.

33. Figures 1, 2, and 3 are sourced from an NSA 60th anniversary timeline website that includes declassified documents and photos; see https://www.nsa.gov/news-features/declassified-documents/nsa-60th-timeline/1960s.shtml.
34. J. Bamford, "The NSA and Me," The Intercept, 2 Oct. 2014; http://theintercept.com/2014/10/02/the-nsa-and-me/.
35. See W. Ware, "Foreword," *Security in Computing*, 3rd. ed., C.P. Pfleeger and S. Lawrence Pfleeger, eds., Prentice Hall, 2003, p. xix.
36. Ware's personal papers contain folders on Argonne Nat'l Laboratory, AEC and Livermore Computers (1960–61), Lincoln Laboratory, Los Alamos Nat'l Laboratory, Naval Ordnance Research Computer (NORC), Oak Ridge Nat'l Laboratory, and US Air Force Project RAND (1954–1955).
37. Ware's personal papers contain folders on Ford Motor's defense division Aeroneutronic Systems, Ramo Wooldridge, Scientific Data Systems, and Thompson Ramo Woodridge (TRW).
38. Ware's personal papers contain folders on ALWAC, Bendix, Bull Machine, Burroughs, Computer Control Company, Control Data Corporation, Digital Equipment Corporation, Electrodata, Engineering Research Associates (ERA), Ferranti, General Electric, Honeywell, IBM, Librascope, National Cash Register, Packard Bell, Philco, Powers-Samos, and Univac.
39. M. Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security*, vol. 27, no. 5, 2012, p. 783; W. Ware, "Report of the Second Computer Study Group," NSA, May 1973. This report was approved for release by NSA on 26 Sept. 2012. See FOIA case 51546 at https://www.nsa.gov/news-features/declassified-documents/tech-journals/assets/files/report-of-the-second-computer.pdf.
40. One recent (post-Snowden) critical study of the NSA is L. Finley and L. Esposito, "'Digital Blackwater': The National Security Administration [sic], Telecommunications Companies and State-Corporate Crime," *State Crime J.*, vol. 3, no. 2, 2014, pp. 182–199.
41. T.J. Misa, *Digital State: The Story of Minnesota's Computing Industry*, Univ. of Minnesota Press, 2013, p. 128 (including the citation of NSA documentation on Harvest); W. Buchholz, ed., *Planning a Computer System: Project Stretch*, McGraw-Hill, 1962, pp. 254–271.
42. For example, see the transformation of two presented papers specifically on the Naval Tactical Data System into published articles on general principles and/or generic systems in Misa, *Digital State*, p. 256, note 44.
43. Warner, "Cybersecurity: A Pre-History," p. 783.
44. Ware, "Report of the Second Computer Study Group," pp. 21, 50–51; T.R. Johnson, *American Cryptology during the Cold War, 1945–1989*, Center for Cryptological History, NSA, 1995. I have supplemented the redacted version of Johnson's book on the NSA website with lighter or differently redacted FOIA-request versions at George Washington University's National Security Archive; see http://nsarchive.gwu.edu/NSAEBB/NSAEBB426/docs/2.American%20Cryptology%20During%20the%20Cold%20War%201945-1989%20Book%20IV%20Cryptologic%20Rebirth%201981-1989-1999.pdf. For instance, the following quotation (among many) was redacted from the NSA site's version but the GWU site has it complete (Johnson, vol. 3, p. 152): "The mammoth Soviet naval exercise Okean 1975 submerged [RYE's] Tide in 88,000 jobs per day, more than doubling the usual load. Two years later the overworked system crashed seven times in a single day."
45. Johnson, *American Cryptology during the Cold War*, vol. 2, pp. 362, 368.
46. Johnson, *American Cryptology during the Cold War*, vol. 2, p. 369, and vol. 3, p. 152; Ware, "Report of the Second Computer Study Group," p. 44. The phrase alluding to the Internet (from Johnson's NSA history published in 1995) reads: "Rye became the central nervous system for NSOC, and it internetted over 100 Opscomm circuits."
47. "Full Text of cryptolog_23-nsa," document ID 4019642, *Cryptolog*, Sept. 1976, p. 3; http://archive.org/stream/cryptolog_23-nsa/cryptolog_23_djvu.txt.
48. NSA, "Remote-Access Computer Systems," Cryptologic Milestones, Aug. 1965, pp. 1–4, quoted in J. Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, Doubleday, 2001, pp. 589, 699n.
49. M. Warner, *The Rise and Fall of Intelligence: An International Security History*, Georgetown Univ. Press, 2014, pp. 193–195.
50. Johnson, *American Cryptology during the Cold War*, vol. 2, p. 368. Johnson's source is a 1968 oral history by NSA director Marshall Carter; see Warner, "Cybersecurity: A Pre-History," p. 783.
51. J. Laprise, "The Purloined Mainframe: Hiding the History of Computing in Plain Sight," *IEEE Annals of the History of Computing*, vol. 31, no. 3, 2009, pp. 83–84; Paul E. Ceruzzi, "Let's Place Edward Snowden in the Context of History," *History News Network*, 25 May 2014, http://historynewsnetwork.org/article/155699; P.E. Ceruzzi, *Internet*

Alley: High Technology in Tysons Corner, 1945–2005, MIT Press, 2008, pp. 38–39, 77–78.

52. Ware, "Report of the Second Computer Study," pp. 41–52.
53. In a collaborative research effort between CBI and the High-Performance Computing Division at Los Alamos National Laboratory, Nicolas Lewis is investigating computing at Los Alamos, including networking, storage, security, and procurement. See N. Lewis, "Increasing the Yield: Nuclear Testing, Weapons Strategy, and Supercomputer Selection at Los Alamos in the 1960s," 2015 SIGCIS Workshop, www.sigcis.org/node/391#lewis.
54. See [redacted name] and E.A. O'Connor, "1972–1973: A Vietnam Odyssey," Dec. 1973, reprinted in *Cryptolog*, Oct. 1975, pp. 7–10, https://www.nsa.gov/news-features/declassified-documents/cryptologs/assets/files/cryptolog_13.pdf
55. Ware, "Report of the Second Computer Study," pp. 43–48, enumerated 2 Univac 1108s (plaintext scanning), 2 Univac 494s (TIDE), 2 Sigma 5s (internal data distribution), 1 IBM 7094 and 4 IBM 370/165s "plus many smaller 360/20s and 360/30s" (central data processing), 1 CDC 6400 and 3 CDC 6600s (ELINT), 2 CDC 6600s and 2 CDC 7600 (crypto), 4 Univac 494s (RYE), 4 Univac 1108s (data scanning), 2 Univac 494s (data communications beyond RYE), and on top of this, an unknown (redacted) number of computers used in the agency's R&D efforts. In sum NSA in 1973 annually consumed 800,000 hours of computer time, in its agency-standard IBM 7094(II) equivalents.
56. Ware, "Report of the Second Computer Study," p. 38.
57. D.J. Edwards, oral history conducted by J.R. Yost, CBI OH 427, 2 July 2013, http://hdl.handle.net/11299/162379; R.G. Bace, oral history conducted by J.R. Yost, CBI OH 410, 31 July 2012, http://hdl.handle.net/11299/144022; S. Walker, oral history conducted by J.R. Yost, CBI OH 409, 8 Nov. 2013, http://hdl.handle.net/11299/144021.
58. *Proc. 1967 Spring Joint Computer Conf.*, vol. 30, 1967, p. 279.
59. Most recently, the Ware 1970 graphic was reproduced as Figure 1.8 in C.P. Pfleeger, S. Lawrence Pfleeger, and J. Margulies, *Security in Computing*, 5th ed., Prentice Hall, 2015; http://ptgmedia.pearsoncmg.com/images/chap1_9780134085043/elementLinks/01fig08_alt.jpg. See also J. Healy, "The Sophisticated Threat – Yesterday, Today and Tomorrow," June 2014, www.slideshare.net/informaoz/jason-healy-atlantic-council; Healy notes that the Ware 1970 figure was reproduced verbatim elsewhere. For example, the file at http://cryptome.org/sccs03.jpg has the same file name as the one on the RAND website: www.rand.org/content/dam/rand/www/external/pubs/reports/R609-1/sccs03.jpg.
60. B. Peters, "Security Considerations in a Multiprogrammed Computer System," *Proc. AFIPS Spring Joint Computer Conf.*, 1967, p. 286; http://dx.doi.org/10.1145/1465482.1465524.
61. Peters, "Security Considerations in a Multiprogrammed Computer System," p. 285.

Thomas J. Misa directs the Charles Babbage Institute at the University of Minnesota, where he teaches in the Program for History of Science, Technology, and Medicine and holds the ERA Land Grant Chair in the History of Technology in the Department of Electrical and Computer Engineering. His most recent book, with CBI colleague Jeffrey Yost, is *FastLane: Managing Science in the Internet World* (Johns Hopkins University Press, 2015). Contact him at tmisa@umn.edu.