Studies in Intelligence

Journal of the American Intelligence Professional

Unclassified articles from Studies in Intelligence Volume 57, Number 3
(September 2013)

Center *for the* Study *of* Intelligence

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Studies in Intelligence. Volume 57, Number 3 (September 2013)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Central Intelligence Agency,Center for the Study of Intelligence,Washington,DC,20505**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**48**	

Studies in Intelligence is available on the Internet at: https:// www.cia.gov/library/center-for-the-study-of-intelligence/ index.html.

Requests for subscriptions should be sent to:

Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505

ISSN 1527-0874

The Mission

The mission of *Studies in Intelligence* is to stimulate within the Intelligence Community the constructive discussion of important issues of the day, to expand knowledge of lessons learned from past experiences, to increase understanding of the history of the profession, and to provide readers with considered reviews of public literature concerning intelligence.

The journal is administered by the Center for the Study of Intelligence, which includes the CIA's History Staff, CIA's Lessons Learned Program, the CIA Museum, and the Agency's Historical Intelligence Collection of Literature. The center also houses the Emerging Trends Program, which seeks to identify the impact of future trends on the work of US intelligence.

Contributions

Studies in Intelligence welcomes articles, book reviews, and other communications. Hardcopy material or data discs (preferably in .doc or .rtf formats) may be mailed to:

Editor
Studies in Intelligence
Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505

Awards

The Sherman Kent Award of $3,500 is offered annually for the most significant contribution to the literature of intelligence submitted for publication in *Studies*. The prize may be divided if two or more articles are judged to be of equal merit, or it may be withheld if no article is deemed sufficiently outstanding. An additional amount is available for other prizes.

Another monetary award is given in the name of Walter L. Pforzheimer to the graduate or undergraduate student who has written the best article on an intelligence-related subject.

Unless otherwise announced from year to year, articles on any subject within the range of *Studies*' purview, as defined in its masthead, will be considered for the awards. They will be judged primarily on substantive originality and soundness, secondarily on literary qualities. Members of the *Studies* Editorial Board are excluded from the competition.

The Editorial Board welcomes readers' nominations for awards.

CENTER *for the* STUDY *of* INTELLIGENCE
Washington, DC 20505

EDITORIAL POLICY

Articles for ***Studies in Intelligence*** may be written on any historical, operational, doctrinal, or theoretical aspect of intelligence.

The final responsibility for accepting or rejecting an article rests with the Editorial Board.

The criterion for publication is whether, in the opinion of the Board, the article makes a contribution to the literature of intelligence.

Studies in Intelligence

C O N T E N T S

Contributors

Kathleen M. Vogel, PhD is an associate professor in the Department of Science and Technology Studies and the Judith Reppy Institute for Peace and Conflict Studies at Cornell University. She is the author of *Phantom Menace or Looming Danger: A New Framework for Assessing Bioweapons Threats*, published this year.

Michael Aaron Dennis is an adjunct lecturer at Georgetown University. He has a PhD in the history of science from The Johns Hopkins University. His most recent work is *A Change of State: Political Culture, Technical Practice, and the Origins of Cold War America.*

Richard T. Willing is an officer of the Office of the Director of National Intelligence serving with the Center for the Study of Intelligence.

Mark Benbow is an assistant professor at Marymount University and former historian at the Woodrow Wilson House Museum in Washington, DC. His first book, *Leading Them to the Promised Land: Woodrow Wilson, Covenant Theology and the Mexican Revolution: 1913–1915*, was published in 2010. He has published articles in *Journalism History*, *Studies in Intelligence* (an award winning article), among others.

Hayden Peake is the curator of the CIA's Historical Intelligence Collection of literature. He has served in CIA's Directorates of Operations and Science and Technology.

❖ ❖ ❖

The Need for Greater Multidisciplinary, Sociotechnical Analysis: The Bioweapons Case

Kathleen M. Vogel, PhD

"Until fundamental issues are examined in depth, intelligence analysts will face blind spots in their bioweapons assessments, which may lead to future intelligence failures and poor national and international security policymaking."

> *The time when only a few states had access to the most dangerous technologies is past. Biological and chemical materials and technologies, almost always dual-use, move easily in our globalized economy, as do the personnel with scientific expertise to design and use them. The latest discoveries in the life sciences also diffuse globally and rapidly.*
>
> —James R. Clapper, Senate Committee on Armed Services, 18 April 2013[1]

Director of National Intelligence (DNI) Clapper's statement to the US Senate last spring reflects concerns that have arisen in recent years about advances in biotechnology and their implications as bioweapons threats. For example, observers in the policy and intelligence communities have asserted that once-difficult biological techniques are becoming automated, routinized, and done by people with minimal technical expertise.[2] These developments point to a "deskilling" of biotechnology, a term signifying that complex skill sets, know-how, and practices may no longer be required to produce novel agents or materials. According to some, such deskilling could lead to a Wikipedia-style radical democratization of biotechnology expertise by making it possible for anyone "to design and fabricate biological systems without being controlled by any kind of authority."[3]

Others have described how high school and college students as well as independent "do-it-yourself" biology groups can use new scientific tools and techniques to construct novel biological materials.[4] In 2009 the National Security Council released its *National Strategy for Countering Biological Threats*, which emphasized that "with advances in biotechnologies continuing to be globally available, barriers of technical expertise and monetary costs will continue to decline, making a potent bioweapons capability available to many US adversaries."[5] Other reports colorfully suggested that bioweapons capabilities are accessible to "garage bio-hackers," "mad scientists," and "bio-criminals."[6]

Such perspectives reflect the concern since 9/11 that new scientific developments and the globalization and diffusion of biotechnology have given terrorists or hostile states an expanded store of weapons to use against the United States and its allies. Such threats should raise concerns, but scholars who study the

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

Public treatment of potential bioweapons threats suggests that greater discussion of some fundamental analytic questions concerning these threats is needed.

development and diffusion of science and technology can't help but see in the public treatment of potential bioweapons threats the need for greater discussion of fundamental analytic issues concerning these threats. For example:

- How exactly do advances in the life sciences and biotechnology affect the nature of the bioweapons threat in coming years?
- What specific knowledge, skills, conditions, resources, and time scales enable the development of new biotechnologies and their weaponization?
- Moving from the global to the local, how can we better assess the ways in which a diverse set of actors may develop and use biotechnologies for harm?

To date, much is still not known about the fundamental drivers of emerging biotechnology and bioweapons threats, how they apply to specific actors and cases, and how these drivers are changing over time. Additional analytic challenges stem from the complexity of biological systems and the difficulty in predicting how innovations and discoveries in the life sciences and related technologies can be controlled and harnessed for misuse—and how, and to what extent, this is a different problem than that posed by older bioweapons threats. Until these fundamental issues are examined in depth, intelligence analysts will face blind spots in their bioweapons assessments, which may lead to future intelligence failures and poor national and international security policymaking.

These issues were discussed in a workshop composed of US and British scientists and social scientists held in London in September 2012. The workshop, which I helped arrange with the UK Economic and Social Research Council's Genomics Policy and Research Forum, addressed the issue of improving intelligence analysis of emerging biotechnology threats.[a] Also participating were current and former intelligence officers and policy officials. The workshop sought to:

- Examine new analytic approaches to take into account *both* social and technical factors in assessing emerging bioweapons and dual-use technological threats;
- Create a new, forward-looking dialogue and intellectual exchange between intelligence practitioners and academic experts on how both communities can think more holistically about bioweapons threats; and
- Challenge the conventional wisdom that substantive discussions of analytic methods for bioweapons threats can only occur in highly classified settings.

Competing Models of Analysis

A key panel at the workshop framed the challenge especially well. Entitled "Understanding the Emerging Life Science Landscape," the panel laid out two competing models for explaining innovations in biotechnology and the life sciences.[7] One, the "biotech revolution" model, was described by US Department of Homeland Security Deputy Assistant Secretary for Chemical, Biological, Radiological, and Nuclear Policy Gerald Epstein. This model emphasizes codified knowledge in biology and the material aspects of biotechnology and assumes that biotechnologies develop with a fixed linear or exponential technological trajectory.

Proponents of this model, such as those noted above, hold that biotechnologies will become more available due to the widespread geographical diffusion of biotechnology information, materials, infrastructure, and expertise across a wide range of commercial and academic settings. Biotechnology is seen as becoming more powerful, available, familiar, and decentralized. This model assumes that technology is the primary driver and that states, terrorists, or other nonstate actors will readily exploit modern biological materials and techniques to lower technical barriers, obviate existing controls, and create vulnerabilities for harm. Under this model,

[a] A brief description of this meeting can be found at http://www.genomicsnetwork.ac.uk/forum/events/pastevents/workshops/title,26429,en.html. Funding support for the workshop and its participants was provided by the UK ESRC Genomics Policy and Research Forum and the National Science Foundation. The Genomics Forum is based at the University of Edinburgh and is part of the ESRC Genomics Network (EGN), a major ESRC investment spanning five of the UK's leading universities examining the development and use of the science and technologies of genomics.

the bioweapons threat is expected to grow rapidly in the future.

An alternative model, which could be dubbed the "biotech evolution" model, was presented by University of Sheffield Professor of Sociology Paul Martin. This model focuses on the complex social, economic, scientific, and technical factors that shape biotech innovation and its applications, factors that can powerfully moderate potential bioweapons threats.[8]

This model, based on decades of in-depth qualitative academic social science research, some involving longitudinal (20–30 year) case studies covering a range of biotechnologies, reveals a slower, multifaceted, and nonlinear model for biotechnology development than the biotech revolution model. This is because biotechnological development occurs within social, natural, economic, and political contexts, and as a result, biotechnologies can develop in a number of different ways. This analytic approach studies local technical practices as well as the larger laboratory, institutional, industrial, and environmental settings in which technologies are developed and used.

These studies reveal that in the small number of cases where specific biotechnology products and innovations have emerged and been successful, it was the result of many decades of incremental collaborative research. Typically, it has taken 35 years for new biotechnology innovations to mature and be useful. While these case studies focused on commercial biotechnology rather than biological weapons development, they reveal patterns that may be common to all life science developments. These scholarly case studies demonstrate a different picture and understanding of biotechnology and its patterns of innovation, diffusion, translation, and uptake that are worthy of serious consideration for intelligence.

Following are my suggestions for addressing the need for better conceptual models in this aspect of proliferation analysis. As a proponent of the second model discussed at the workshop, I will argue that a combination of social and technical—what I call ***sociotechnical***—multidisciplinary analyses of biotechnology is needed for a fuller understanding of the problem. I will draw on academic literature from the social science field of science and technology studies (S&TS) to illustrate how sociotechnical factors underpin the diffusion of biotechnology and bioweapons threats. I will conclude by proposing how teams of intelligence analysts and different analytical practices could be established to apply sociotechnical methodology to this important challenge.

The Technical Model

As I have written elsewhere, existing intelligence and policy understandings of biotechnology and the life sciences have tended to be based on the first model discussed in the September 2012 workshop and focused on the material and technical aspects of the problem.[9] As a result, the dominant analytic framework has had as its primary focus the following elements:

- Codified biological knowledge, i.e., information found in journal articles, scientific textbooks, websites, databases (for example, genome sequences), and other written sources;
- The material end products of biotechnologies
- The accessibility of biological materials (pathogens, oligonucleotides), biological supplies (reagents, prep kits), infrastructure (DNA synthesizers, laboratory benches), and other tangible items (monetary resources)
- The economic drivers of biotechnology
- The globalized and diffused character of biotechnology

The upshot of this analysis is a rapidly climbing threat trajectory

Absent or marginalized in this framework are the important aspects of the biological sciences and biotechnology addressed in the second model. These include:

- The important role of tacit knowledge—more commonly referred to as know-how—in biology. This know-how involves important social dimensions related to hands-on laboratory work that can often not be reduced to written form
- The real challenges of producing these materials, including troubleshooting efforts, context, and the manpower required to produce a stable biotechnology end product
- The social and material conditions required for biotech equipment to work in different local contexts (for instance, in an outpost in Afghanistan versus in an academic laboratory)
- Recognition that even biotech and pharmaceutical industries, with ready access to resources, have struggled to harness new biotech-

...the intelligence and policy communities appear to have placed most attention on increasing within their ranks technical biological knowledge and expertise, and new programs and activities have focused on technical solutions.

nology developments for their specific applications[10]

- The role of specific social actors and how they can affect technology design, development, use, and transfer

Crucially, not only do the models consider different aspects of the problem, they will lead to different suggestions for intelligence and policy interventions.

Implications of the Technical Model

By framing the issue as a technical problem, the intelligence and policy communities appear to have placed the most attention on increasing within their ranks technical biological knowledge and expertise, and new programs and activities have focused on technical solutions.[11] In November 2006, the National Counterproliferation Center (NCPC) within the Office of the Director of National Intelligence (ODNI) established the Biological Sciences Experts Group (BSEG) to improve the Intelligence Community's access to biological expertise.[12] The BSEG grew out of high-profile public recommendations from the 2005 *Final Report* of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, the National Academy of Sciences, and the US House of Representatives Subcommittee on Prevention of Nuclear and Biological Attack of the Committee on Homeland Security.[13]

The BSEG maintains a cadre of external life science and bioweapons experts from universities, companies, and nongovernmental organizations.[14] These experts serve as independent consultants to the NCPC and are appointed through the National Intelligence Council Associates Program. The BSEG charter states that members may be assigned the following types of projects:

- Supporting intelligence customers in the design of scientific/technical experimental protocols, intelligence analyses, or collection methodologies against biological threat agents, biological warfare agents, and/or state and nonstate actors that do or may pose threats to the United States
- Advising on strategies to improve the execution or interpretation of results of experimental protocols, analysis, and collection
- Undertaking technical assessments and performance reviews of the Intelligence Community's scientific/technical programs, analytical products, and collection methodologies[15]

The establishment of the BSEG has made new, in-depth scientific expertise available to the US Intelligence Community and made it easier for intelligence analysts to identify and call on specific outside technical experts to help assess the security implications of new biological developments.[a]

This technical focus of BSEG is consistent with past efforts to improve assessments, which have tended to focus on the technical domain. For example, in the early 1990s, the CIA created the Nonproliferation Center, an analytic unit that focused on the technical aspects of proliferation. In 2001, that center was replaced by a new and larger center, the Weapons Intelligence, Nonproliferation, and Arms Control Center (WINPAC).

With its creation, WINPAC centralized CIA's technical weapons specialists in both nonproliferation and arms control issues. The creation of the NPC and WINPAC increased institutional consolidation, segregation, and prioritization of technical expertise on bioweapons issues within the CIA. This technical orientation was further reinforced by the decision in 2010 to create a new Counterproliferation Center,[16] in which National Clandestine Service elements (handling the collection of technical information) and WINPAC elements were united.

Other intelligence units have also relied mainly on technical knowledge and expertise to inform bioweapons assessments. In 1998, the

[a] Interestingly, BSEG members are hired through the National Intelligence Council (NIC) Associates Program, which was originally designed to bring multidisciplinary (typically social science) expertise to the CIA. But there is no indication that historians, social scientists, or relevant nontechnical experts have been incorporated into BSEG membership. Rather, the organizers of BSEG see the NIC Associates Program as a contracting mechanism to bring in technical experts, not as a source of valuable multidisciplinary expertise and different methodological approaches to study bioweapons threats. Anonymous US policy official, e-mail communication with author, 9 October 2010.

Defense Intelligence Agency created a science advisory group called BioChem 20/20. Its mission was to "lead and focus the defense intelligence community's assessments of emerging technologies that nation states or terrorists could use for biological or chemical warfare and to mitigate technological surprise from foreign biological warfare programs."[17]

The publicly available information concerning the above efforts suggests that left out of the organizational responses were relevant social science or other nontechnical experts who might have addressed the political, economic, and social dimensions underpinning technical work, including development of know-how, work disciplines, and interdisciplinary forms of weapons knowledge.[18]

Similarly, the dominant intellectual streams that have shaped understandings of weapons issues in the broader US security community come from science, engineering, and political science—the fields that have shaped strategic studies and terrorism studies.[19] Although they provide important tools and techniques for understanding weapons issues, these fields typically do not analyze the specific factors and mechanisms by which scientific and technological knowledge, work, and products can be shaped by social factors.

Examples of Shortcomings from Existing Assessments

Assessments of developments over the past decade in the new technical field of synthetic genomics offer examples of the problems of such narrow technical analysis. In 2002, virologists at the State University of New York, Stony Brook, created a synthetic polio virus using commercially available materials and equipment and without using any natural viral components.[20] The description of this experiment in the open scientific literature raised policy concerns about the ease of acquiring and using biological materials, information, and techniques for terrorism.[21]

Apparently left out of the organizational responses were relevant social science or other nontechnical experts who might have addressed the political, economic, and social dimensions underpinning technical work.

A closer analysis of the experiment, however, reveals how important particular kinds of know-how were in the preparation of the reagent necessary for a successful experiment. While acquisition of commercially available materials was relatively straightforward, creation of a particular reagent necessary for the experiment proved to be stumbling block.[22] The experiment only succeeded after the experimenters had developed the know-how—in this case a "sense" of the visual and sensory cues that allowed them to determine when the reagent had reached the stage that is was ready for use in the synthesis experiment.

Efforts to replicate the experiment by people without the sensory know-how have failed even with free access to materials and written protocols. Acquisition of these sets of know-how and related laboratory disciplines has proven difficult even for the small subset of national and international virologists who specialize in the polio virus. In sum, the polio virus synthesis experiment depended on the mastery of specialized and extremely difficult-to-achieve laboratory know-how and, contrary to popular assumptions, it could not be replicated by anyone who read the *Science* article about the experiment.

In January 2008, the J. Craig Venter Institute published a synthesis experiment that described the creation of a small parasitic bacteria, the *Mycoplasma genitalium* genome.[23] Although the experiment built on knowledge obtained in the Venter Institute's earlier laboratory work, the construction of the *Mycoplasma genitalium* genome was based on an entirely new approach.[24] Moreover, while this bacterial synthesis was a major advance because of the large size of the genome, the experiment took several years to come to fruition after a tedious, multistage process in which the Venter team—involving 10 researchers and help from three companies specializing in gene synthesis—had to build the genome one fragment at a time with many quality control steps along the way.

Thus, advances in synthetic genomics technologies and the commercial availability of biological materials have not eliminated the need for complex, specialized know-how and teamwork in advanced biotechnology work. If anything, experience is indicating that synthesis of larger genomes is actually getting more complicated, with a need for greater resources and additional manpower. A 2009 *Trends in Biotechnology* article has noted this complexity and the continued need for specialized skills for this emerg-

These examples also reveal how much is still not known about the fundamental drivers of the diffusion and standardization of biotechnologies.

ing science: "Most multi-gene-engineering projects involve ad hoc methods of DNA assembly…. [E]mploying custom cloning strategies … [and] are labor intensive and difficult to automate."[25]

Experts in gene synthesis note that the problems that remain in gene synthesis are not necessarily about resources or money. Rather, the challenges are intellectual and require hands-on work, time, teams of experts, and new (still unknown) techno-organizational processes involving important social dimensions of technical work. These examples from the field of synthetic genomics further illustrate the need to look at the sociotechnical complexities of biological work. These examples also reveal how much is still not known about the fundamental drivers of the diffusion and standardization of biotechnologies.

The Alternative: Creating New Sociotechnical Assessments

The social science field of S&TS has been developing the conceptual tools for studying how the science and technology behind emerging biotechnologies are shaped by social and environmental factors. This analytic approach involves detailed study of technical practices and related knowledge-generating activities in biotechnology and the life sciences, as well as the laboratory and institutional contexts in which this work is situated. This approach strives to understand how data construction, scientific work, and technologies are shaped by the skills, cultures, and routines of particular technical settings.

For example, S&TS scholars have studied the requirements and problems of moving scientific and technical knowledge to new settings.[26] Researchers have found that the transfer of technologies from one lab or technical setting to another often requires difficult adaptations. A successful translation often requires the presence of the original author or inventor of the technology to supervise or conduct the shift.[27] Although this transfer may also occur in the absence of its authors, under such conditions, the process becomes more challenging and time consuming.[28]

S&TS scholars have also focused on the importance of the "tacit" dimensions of scientific practice—or know-how. Probably one of the first academics to talk about this was Michael Polanyi, a chemistry professor who became a philosopher of science. He is the author of *Personal Knowledge* (1958) and *The Tacit Dimension* (1966), which argued that scientific knowledge was not reducible purely to material factors or pieces of explicit information but also required conceptual and sensory knowledge, which he called "tacit knowledge."[a]

S&TS scholars have since expanded the concept of tacit knowledge. Sociologist of science H.M. Collins wrote that tacit knowledge can consist of visual, sensory, and other unarticulated components and skills that are part and parcel of doing scientific work.[29] Thus, tacit knowledge refers to the unarticulated knowledge of researchers. Collins explains that tacit knowledge comes through practical, hands-on processes in two mechanisms, either through "learning by doing"—a painstaking trial-and-error process of individual discovery—or by "learning by example," as apprentices once learned from masters. Collins has also developed a useful set of categories of tacit knowledge that one can observe and document in scientific work, and he has shown how some of these types of know-how are more difficult than others to acquire and transfer.[30]

In looking at distinctions between codified (written forms of knowledge) and tacit knowledge, other sociologists of science have argued that the authors of step-by-step written scientific instructions in articles, textbooks, or manuals typically assume their readers will be competent practitioners who possess relevant know-how and the ability to troubleshoot and adapt the method to local circumstances.[31] Sociologist of science Michael Lynch, however, has found that even highly skilled practitioners are not able to competently carry out some scientific tasks without prior training in the specific lab in which a published technique was introduced, because of the particular local and personal dimen-

[a] See the following article in this issue by Michael A. Dennis, "Tacit Knowledge and the Proliferation of Nuclear WMD." Michael Polanyi, *Personal Knowledge: Towards a Post-Critical Philosophy* (University of Chicago Press, 1958) and *The Tacit Dimension* (Doubleday, 1966); both books have been reprinted several times.

sions of scientific practice in that specific lab.[32]

A few studies have looked at communal forms of tacit knowledge—tacit knowledge developed within teams or organizations—that are involved in creating complex technologies.[33] For example, some S&TS scholars have emphasized the importance of close working relationships among various interdisciplinary specialists to create a working technology.

In these studies, however, the type of communal knowledge varies. For example, some describe prolonged interaction between different types of scientists that leads to the production of a new type of communally synthesized tacit knowledge that cannot be separated into individual components, and is therefore more difficult to transfer. Other studies seem to allow for a simpler model in which communal tacit knowledge is the mere addition of the knowledge resident within individual scientists and engineers; such knowledge could be separated out and then more easily reassembled.

Benjamin Sims, an S&TS scholar, at Los Alamos National Laboratory has highlighted the importance of what he describes as "transactional knowledge," which Sims defines as the organizational and management skills (know-how) necessary to coordinate practices across multiple technical communities. This type of know-how allows each community to contribute to a larger technological goal. Sims argues that this is an important form of tacit knowledge related to technical work that is often overlooked.[34]

Other scholars working in the S&TS field point to how it is easy to overlook the presence and persistence of tacit knowledge in technical work. For example, science studies scholar David Gooding explains how scientists or other technical experts can overlook the importance of their own tacit scientific practices:

> *For experiments and instruments that work: they work in a particular world that has been ordered and prepared in ways that retrospective accounts hide from view.…As procedures and pathways are mastered, so the skills that enable them drop out of the account. They lose visibility as they are worked into the repertoire of the shared, taken-for-granted practices of a particular community.*[35]

Scholars of science and technology have emphasized the need to study the social dimensions of how technology travels, including its micro and macro-level features.

Because of such blind spots, it often takes the probing of outsiders to identify the know-how that underpins an experiment or technology.

In order to capture the tacit dimensions of technical work, S&TS scholars have used in-depth case studies. Typically, these studies consist of detailed historical or ethnographic data about scientific and technological cases that drive toward obtaining rich, in-depth understandings of the why and how of particular cases. The qualitative approach can make clear important contextual factors and understandings that quantitative and technical methods are unable to capture.

In applying this approach to analyzing emerging technologies and bioweapons, analysts would seek to study in detail:

- the specific factors, conditions, and time scales required to develop tacit knowledge in the biotechnology of concern
- the kinds of social engineering required (e.g., pedagogy, exchanges, management structures, etc.) for the development of tacit knowledge in the field
- the means by which tacit knowledge is transmitted locally and globally—or, conversely, the factors that prevent its transmission, including particular local conditions and unique practices
- the causes of failure, too often overlooked in studies[36]
- the conversion of tacit knowledge to codified knowledge

S&TS scholars have emphasized the need to study the social dimensions of how technology travels, including its micro- and macro-level features. For example, James Cortada, a historian of information technology, has discussed how computer technologies have been spread throughout the United States and the world.[37] He found that contrary to the popular assumption that the diffusion of IT knowledge is a special case, it actually resembles in many of its features the diffusion of other technologies across many countries and eras. He argues that conclusions about IT diffusion have been made prematurely, without adequate research into the contributions of social, economic, political, legal, technical, and infra-

With a more multidisciplinary approach to these challenges, intelligence analysts can develop more accurate and holistic understandings of how biotechnologies develop, spread, and are used.

structure factors. For example, he lists critical government interventions and the existence of important constituencies around the world (e.g., programmers, service providers, vendors, users, academics, and multinational corporations).[38]

Cortada's work illustrates the importance of multidisciplinary analysis of technologies. Because many developments in emerging biotechnologies have been described as paralleling IT, Cortada's work cautions on drawing early and simple conclusions about the patterns and implications of biotechnology diffusion and suggests doing in-depth, longitudinal case studies to look at both social and technical dimensions of biotechnology development and use.

Recommendations

How might the Intelligence Community better take into account both social and technical factors in assessing new technologies? Some mechanisms appear to exist and simply need to be applied. One is the Red Team approach, in which outsiders would specifically challenge dominant technical approaches and analytic practices. A Red Team might place particular importance on understanding in qualitative, micro-level fashion the social dimensions of a scientific and technological problem, including tacit knowledge; organizational and management styles; translation and adaptation of techniques and technologies to a local context; and relevant training and laboratory practices.

Such an effort would require a Red Team to focus on specific people, in specific places, with specific materials, in particular social contexts, and with localized practices, and the analysis of their interactions. I believe this approach would promote a creative, flexible, multidisciplinary knowledge environment if sufficient resources and authorities were granted to conduct in-depth analysis.

A February 2005 Intelligence Science Board study on collaboration in intelligence suggested the creation of interdependent work teams of analysts that would be

> *collectively responsible for a significant piece of analytic work—work that…can be larger in size and potential significance than usually is possible for a task performed by any single individual. Members of work teams bring their own special expertise to the work, of course, and over time evolve specialized team roles—but it is the team as a whole that produces and is accountable for the analytic product.*[39]

The report also proposed creating teams composed of members with different expertise and specialties in order to "foster the kinds of cross-functional exchanges that…result in unanticipated insights and syntheses."[40] This kind of work team would also be expected, encouraged, and enabled to draw on other internal and external experts for short- or long-term consultations and contractual work as needed.

Such a team, a sociotechnical work unit within the counterproliferation community, would inject greater multidisciplinary approaches to thinking about biotechnology or any technology of proliferation concern. This approach to knowledge-making would better account for the messy and contingent aspects that characterize the development of weapons technologies and would result in more holistic assessments of bioweapons threats.

Initiatives along these lines should be supported by government and non-government funds. Within the US intelligence community, the National Intelligence Council and the Department of State's Global Futures Forum—with track records of engaging with diverse experts in the academic community in unclassified settings—would be naturals in advancing this conversation on a larger scale. In addition, the ODNI's BSEG could be modified to include more disciplines for academic intelligence discussions

With new biotechnologies come new challenges for intelligence collection and analysis. With a more multidisciplinary approach to these challenges, intelligence analysts can develop more accurate and holistic understandings of how biotechnologies develop, spread, and are used. With greater insights, analysts will be better able to help policymakers identify better measures to address threats from emerging biotechnologies, and indeed from any emerging technology.

❖ ❖ ❖

Endnotes

1. James R. Clapper, Director of National Intelligence, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community," Senate Committee on Armed Services, (18 April 2013), accessible at: http://www.dni.gov/index.php/newsroom/testimonies/194-congressional-testimonies-2013/844-statement-for-the-record-worldwide-threat-assessment-of-the-u-s-intelligence-community,-sas

2. For some examples, see Dennis C. Blair, "Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee," 10 March 2009, accessible at: www.dni.gov/testimonies/20090310 testimony.pdf; Markus Schmidt, "Diffusion of Synthetic Biology: A Challenge to Biosafety" *Systems and Synthetic Biology* 2, nos. 1–2 (2008): 1– 6; Dana A. Shea, "Balancing Scientific Publication and National Security Concerns: Issues for Congress," *CRS Report for Congress*, 2006, accessible at: www.fas.org/sgp/crs/secrecy/RL31695.pdf; National Research Council, *Seeking Security: Pathogens, Open Access, and Genome Databases* (National Academies Press, 2004); James B. Petro, and David A. Relman, "Understanding Threats to Scientific Openness," *Science* 302, no. 5652 (12 December 2003): 1898; James B. Petro Theodore R. Plasse, and Jack A. McNulty, "Biotechnology: Impact on Biological Warfare and Biodefense," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* (1 September 2003): 161–68. National Research Council, *Seeking Security: Pathogens, Open Access, and Genome Databases (*National Academies Press, 2004).

3. Markus Schmidt, Helge Torgersen, Agomoni Ganguli-Mitra, Alexander Kelle, Anna Deplazes, Nikola Biller-Andorno, "SYNBIOSAFE e-Conference: Online Community Discussion on the Societal Aspects of Synthetic Biology," *Syst Synth Biol*, (August 2008), 12, accessible at: http://www.synbiosafe.eu/uploads///pdf/SSBJ-SYNBIOSAFE%20e-conference.pdf.

4. See DIYbio, http://diybio.org; Also, see: Kavita M. Berger, Carrie Wolinetz, Kari McCarron, Edward You, K. William So, *Bridging Science and Security for Biological Research: A Dialogue between Universities and the Federal Bureau of Investigation* (AAAS, 2012), accessible at: http://www.aaas.org/cstsp/publications/; Edward W. Lempinen, "FBI, AAAS Collaborate on Ambitious Outreach to Biotech Researchers and DIY Biologists," (1 April 2011), accessible at: http://www.aaas.org/news/releases/2011/0401fbi_biosecurity.shtml; Edward H. Yu, "Looking Ahead" (FBI Weapons of Mass Destruction Directorate: 11 March 2010), accessible at: www.synbioproject.org/process/assets/files/6409/_draft /you presentation.pdf.

5. National Security Council, *National Strategy for Countering Biological Threats* (November 2009), accessible at: www.whitehouse.gov/sites/default /fi les /National Strategy for Countering BioThreats.pdf.

6. US Central Intelligence Agency, "The Darker Bioweapons Future," (3 November 2003), accessed, www.fas.org/irp/cia/product/bw1103.pdf; Petro, Plasse, and McNulty, "Biotechnology: Impact on Biological Warfare and Biodefense":161–68; Petro and Relman, "Understanding Threats to Scientific Openness": 1898; Institute of Medicine and National Research Council, *Globalization, Biosecurity, and the Life Sciences* (National Academies Press, 2006).

7. For a more detailed discussion of the models presented at the workshop see Kathleen M. Vogel, "Intelligent assessment: putting emerging biotechnologies in context," *Bulletin of the Atomic Scientists* 69/1 (January 2012): 43–52; Also, see: Kathleen M. Vogel, "Framing Biosecurity: An Alternative to the Biotech Revolution Model?" *Science and Public Policy* 35/1 (February 2008): 45–54.

8. For a few examples, see: Paul Nightingale, "Technological capabilities, invisible infrastructure, and the un-social construction of predictability: The overlooked fixed costs of useful research," *Research Policy* 33/ 9 (November 2004): 1259–84; Paul Nightingale and Paul Martin, "The myth of the biotech revolution," *Trends in Biotechnology* 22/11 (November 2004): 564–69.

9. Kathleen M. Vogel, *Phantom Menace or Looming Danger?: A New Framework for Assessing Bioweapons Threats* (Baltimore: The Johns Hopkins University Press, 2013): 16–55; Vogel, "Framing Biosecurity: 45–54.

10. Paul Nightingale, "Technological capabilities, invisible infrastructure, and the unsocial construction of predictability: The overlooked fixed costs of useful research," *Research Policy* 33, no. 9 (2004): 1259-1284; Paul Nightingale and Paul Martin, "The myth of the biotech revolution," *Trends in Biotechnology* 22, no 11 (2004): 564–69.

11. Institute of Medicine and National Research Council. *Globalization, Biosecurity, and the Life Sciences*; James B. Petro, "Intelligence Support to the Life Science Community: Mitigating Threats from Bioterrorism," *Studies in Intelligence* 48, no. 3 (2004): 57–68, accessible at: www.cia.gov/library/center-for-the-study-of -intelligence/kent-csi/pdf/v48i3a06p.pdf; US Central Intelligence Agency, "The Darker Bioweapons Future"; Kenneth Brill, Melanie Elder, and Lawrence Kerr, "Intelligence Reform: Science and Technology and the Counterproliferation Challenge," Presentation at AAAS Center for Science, Technology, and Security Policy, Washington, D.C., (5 June 2007), accessible at: http://cstsp.aaas.org /content.html?contentid=927.

12. Biological Sciences Experts Group, "Charter, "Unclassified document, accessible at: www.fas.org/irp/eprint/bseg-concept.pdf.

13. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States* (31 March 2005): 510–16, accessible at: www.ise.gov/sites/default/files/wmd report 0.pdf.

14. Yudhijit Bhattacharjee, "Panel Provides Peer Review of Intelligence Research," *Science* 318, no. 5856 (7 December 2007): 1538 and Institute of Medicine and National Research Council, *Globalization, Biosecurity, and the Life Sciences*.

15. Biological Sciences Experts Group "Charter."

16. Central Intelligence Agency, "CIA Launches New Counterproliferation Center," (18 August 2010), accessible at: https://www.cia.gov/news-information/press-releases-statements/press-release-2010/cia-launches-new-counterproliferation-center.html

17. Institute of Medicine and National Research Council. *Globalization, Biosecurity, and the Life Sciences,* 237.

18. For an earlier proposal for more holistic assessments in the Intelligence Community, see: Richard Kerr, Thomas Wolfe, Rebecca Donegan, and Aris Pappas, "A Holistic Vision for the Analytic Unit," *Studies in Intelligence* 50, no. 2 (2006): 47–56.

19. Brian Rappert, Brian Balmer, and John Stone, "Science, Technology, and the Military: Priorities, Preoccupations, and Possibilities," In *The Handbook of Science and Technology Studies,* 3rd ed., edited by E. J. Hackett, O. Amsterdamska, M. Lynch, and J. Wajcman, (Cambridge: MIT Press, 2008): 719–39.

20. Jeronimo Cello, Aniko V. Paul, and Eckard Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297, no. 5583 (August 2002): 1016– 1018.

21. US Congress, "Expressing Serious Concern regarding the Publication of Instructions on How to Create a Synthetic Human Polio Virus, and for Other Purposes," 107th Congress, 2d session, H.R. 514, (26 July 2002), accessed at: http://Thomas.loc.gov/cgi - bin/query/z?c107:H.RES.514; National Research Council, "Scientific Openness and National Security Workshop," (9 January 2003), accessible at: http://csis.org/files/attachments/030109 agenda.pdf.

22. For a detailed discussion of this see: Vogel, *Phantom Menace*, 71–89.

23. For more information about this experiment, see Ibid, 89–101.

24. For a discussion of this past work see: Hamilton O. Smith, Clyde A. Hutchinson III, Cynthia Pfannkoch, and Craig J. Venter, "Generating a Synthetic Genome by Whole Genome Assembly: pX174 Bacteriophage from Synthetic Oligonucleotides," *Proceedings of the National Academy of Sciences* 100, no. 26 (3 November 2003): 15440–15445.

25. Michael J. Czar, Christopher Anderson, Joel S. Bader, and Jean Peccoud, "Gene Synthesis Demystified," *Trends in Biotechnology* 27, no. 2 (February 2009): 63–72.

26. Steven Shapin, "Placing the View from Nowhere: Historical and Sociological Problems in the Location of Science," *Transactions of the Institute of British Geographers* 23, no. 1 (April 1998): 5–12; Steven Shapin, "Here and Everywhere: Sociology of Scientific Knowledge," *Annual Review of Sociology* 21 (1995): 289–321.

27. Graham Spinardi, "Defence Technology Enterprises: A Case Study in Technology Transfer," *Science and Public Policy* 19, no. 4 (1992): 198–206.

28. Steven Flank, "Exploding the Black Box: The Historical Sociology of Nuclear Proliferation," *Security Studies* 3 (Winter 1993/94): 259–94.

29. H.M. Collins, "Tacit Knowledge, Trust, and the Q of Sapphire," *Social Studies of Science* vol. 31, no. 1 (2001): 71–85; Also, see: H.M. Collins, *Changing Order: Replication and Induction in Scientific Practice* (Chicago, IL: University of Chicago Press, 1st edn, London: Sage Publications, 1985).

30. H.M. Collins, "Tacit Knowledge," 72–73.

31. Michael Lynch, *Art and Artifact in Laboratory Science*: *A Study of Shop Work and Shop Talk in a Research Laboratory (*London: Routledge Kegan & Paul, 1985): 65.

32. Ibid., 154.

33. For examples, see: Donald MacKenzie and Graham Spinardi, "Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons," *American Journal of Sociology,* vol. 101, no 1 (1995): 44–99; Laura McNamara, PhD Dissertation, *Ways of Knowing about Weapons: The Cold War's End at the Los Alamos National Laboratory* (Albuquerque: University of New Mexico, 2001).

34. Benjamin Sims," The Uninvention of the Nuclear Weapons Complex? A Transactional View of Tacit Knowledge," paper presented at October 2007 Society for Social Studies of Science annual meeting: http:==www.4sonline.org=ProgramSynopsis 060907.pdf.

35. David Gooding, "Mapping Experiment as a Learning Process: How the First Electromagnetic Motor Was Invented," *Science, Technology, and Human Values* 15, no. 2 (Spring 1990): 168.

36. For one powerful example of the utility of studying technological failure, see: Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (University of Chicago, 1997).

37. James W. Cortada, "How New Technologies Spread: Lessons from Computing Technologies," *Technology and Culture*, 54, no. 2 (April 2013): 229–61.

38. Ibid, 238.

39. Richard J. Hackman, and Michael O'Connor. "What Makes for a Great Analytic Team? Individual versus Team Approaches to Intelligence Analysis," *Intelligence Science Board Task Force Report* (February 2005): 3-4, accessible at: www.fas.org/irp/dni/isb/analytic.pdf.

40. Ibid, 11.

❖ ❖ ❖

Tacit Knowledge as a Factor in the Proliferation of WMD: The Example of Nuclear Weapons

Michael Aaron Dennis

> ***"How important is tacit knowledge to the task, and how essential is such knowledge in the proliferation of such weapons?"***

What would it take, in addition to the will, for a nation to join the club of nations possessing nuclear weapons? An incomplete list of the prerequisites would include: enriched uranium or plutonium, physicists, chemists, computational power, processing plants, specialists in materials and electronics, money, institutions capable of building and managing a large scale construction project, and a site or sites to build and test a device.

Despite their destructive power, nuclear weapons are fragile objects. They require an elaborate sociotechnical support system that costs millions, if not billions of dollars each year simply to maintain their existence. One item not explicitly on the above list and seldom discussed in the analysis of this problem is "tacit knowledge," the knowledge acquired through the actual experience of building and developing an atomic bomb. How important is such knowledge to the task and how essential is such knowledge in the proliferation of such weapons?

The probable answer is that lack of tacit knowledge is not likely to a stop an illicit program in its tracks, but without it, a weapons program is likely to fail more often in its early stages, cost more through a period of trial and error, and take longer to reach fruition. Acquiring tacit knowledge requires time, providing analysts and policymakers with a much needed resource for thought and action. And because timing is a key element in intelligence analysis and policy responses, tacit knowledge is an important factor in the analytical equation. A clear understanding of the sources of tacit knowledge and how it is transmitted from one place to another is central in the consideration of policy responses to a technology development program with security implications.

In the following, I examine the nature and character of tacit knowledge, its origins, and its role specifically in the construction and spread of nuclear weapons since World War II.

An Introduction

Tacit knowledge first emerged as a concept for understanding the actual practice of research in the work of Michael Polanyi, an émigré chemist in mid-20th-century Great Britain. Polanyi's interest in tacit, or personal, knowledge, stemmed from his overarching fear that states, especially Nazi Germany and Stalinist Russia, had successfully attacked and endan-

Training and the time-consuming acquisition of skill, the essence of tacit knowledge, are among the vital prerequisites for successful knowledge transmission.

gered the very freedom of science. Even his new home had seemingly come under the sway of followers of J.D. Bernal, whose major work, *The Social Function of Science* (1939), called for the planning of scientific research by the state. These developments, as well as the mobilization of science for war, led Polanyi and others to form The Society for the Freedom of Science in 1940.

What made tacit knowledge central to Polanyi's conservative antistatist ideology was the idea that tacit knowledge was so personal that it would prove impossible for the state to possess. Given that such knowledge was essential to the growth and development of science, only those who had successfully practiced research might actually understand and manage the enterprise. That framework suggested that scientists need not be subject to the whims of politicians or government bureaucrats; instead, science had to remain an autonomous domain.[1]

Regardless of the political merits of Polanyi's beliefs, the concept of tacit knowledge has emerged as a powerful resource in understanding the growth and development of technical knowledge. Historians and sociologists of science have made use of the concept to understand how knowledge is made, used, and moved around.[2] Rather than assuming that technical knowledge refers to some simple correspondence among researchers, scientific knowledge, and the natural world, the idea of tacit knowledge recognizes the complex interactions at work in making science.

Experience matters. It cannot be acquired through the transmission of information or the act of reading a scientific paper. As Polanyi once explained, tacit knowledge was simply the observation that "we can know more than we can tell." Instead, as a vast literature demonstrates, moving scientific knowledge around requires a substantial amount of effort.[3] Even the seemingly trivial act of replicating a scientific experiment turns out to require a degree of skill that is difficult to acquire.

Training and the time-consuming acquisition of skill, the essence of tacit knowledge, are among the vital prerequisites for successful knowledge transmission. Even more important is the actual movement of people possessing these skills. Early builders of cyclotrons, the pioneering atom-smashing technology, often found themselves unable to build a device without access to one of the students of Berkeley professor E.O. Lawrence, the inventor and developer of the technology.

Despite the many papers the Berkeley group published on the cyclotron, including Lawrence's Nobel Prize lecture, only those who had actually built a cyclotron were able to rebuild one at a distance from the original location. For example, when Merle Tuve, one of the outstanding experimental nuclear physicists of the thirties, decided to build a cyclotron at the Department of Terrestrial Magnetism of the Carnegie Institution of Washington, DC, he imported a Berkeley graduate to guarantee success.[4] This personal component—the embodied character of tacit knowledge—is crucial to understanding tacit knowledge but it can also be misleading.

Understanding tacit knowledge demands a knowledge of history, because what counts as tacit knowledge changes over time. Take the case of PCR, the polymerase chain reaction, a key development in biotechnology and a critical component of much research including DNA fingerprinting. Initially, getting the PCR reaction to work in individual laboratories required a technician with "golden hands"—that is, in each laboratory there was one technician who, through training and experience, could make the technique work. Over time PCR became standardized and "black-boxed," so that it is now available as a technology that laboratories purchase and use, much as they use any sophisticated technology.

We can make a similar point about cyclotrons; today, one can purchase a sophisticated particle accelerator, a synchrotron, for use in a variety of industrial settings, such as X-ray lithography for computer chips. Over time, a fair amount of tacit knowledge is standardized and embedded in the actual hardware of research. In turn, what counts as tacit knowledge changes as one moves from mastering a set of skills to produce a result to using a standardized piece of apparatus to achieve the same end. You don't need to be a student of Kary Mullis, the inventor of PCR, to make PCR

work in a laboratory today; instead, you need training on the PCR machine used in your laboratory.[5]

Those new to the making of an atomic bomb may not possess the tacit knowledge of how to build one, but they will be required to possess explicit and tacit knowledge in a host of necessary precursor fields.

The Political Challenge of the First Nuclear Weapons

The designers and builders of the first atomic bomb did not possess tacit knowledge about building a weapon. Instead, they acquired that knowledge during the Manhattan Project while drawing upon vast repositories of tacit knowledge developed in the course of early-20th-century experimental physics and chemistry. We can use the Manhattan Project's history to make a more fundamental point: building nuclear weapons is a complicated, messy, and inherently political process.

Arranging the constellation of forces necessary to start a project, let alone keep it underway as it develops the inevitable problems accompanying technological innovation, is fraught with peril. For that very reason, the Army's choice of General Leslie R. Groves to run the Manhattan Project was an inspired one. The man who built the Pentagon, then the world's largest and most complicated structure, had the requisite managerial skills to assemble the staff and materials that would span the nation's geographical territory as well as coordinate with the British and Canadians as the project raced to a conclusion.

Before Groves was appointed, the atomic bomb had a difficult conception. When Niels Bohr brought word of fission to the United States in December 1938, Merle Tuve promptly demonstrated the effect at his Atomic Physics Observatory in Washington, DC. Nonetheless, researchers found it impossible to even interest the armed services in fission's possibilities. Although the Navy expressed an interest in fission as a potential power source for ships, there was little interest in a weapon. Even after President Franklin D. Roosevelt created a Uranium Committee under the director of the National Bureau of Standards, Lyman Briggs, little was accomplished.

Only with the arrival of Vannevar Bush and the National Defense Research Committee in June 1940 did real work begin. The nature and character of that work are worthy of comment. Bush funded research on fission and learned of British work on the topic (the MAUD Committee), but his major accomplishment was the creation of three separate National Academy of Science committees to study the problem of applying fission in a viable weapon.

Only after the third committee explicitly stated that a weapon might be built within a reasonable amount of time and with a limited amount of the isotope, U235, did Bush return to seek Roosevelt's approval to begin a full-scale effort to determine if a bomb was an actual possibility. In other words, Bush used the academy to cover his backside, but it was the academy's imprimatur that allowed the president to authorize early large-scale research. Only after Bush's research program answered the fundamental question of whether a chain reaction would even take place in uranium would FDR determine whether to proceed with full-scale production.

Fermi's group at Chicago did not achieve a chain reaction until December 1942. Ironically, Bush received FDR's initial approval in October 1941, before Pearl Harbor, and at roughly the same time that the Germans decided not to pursue their own Manhattan Project.[6]

There are two important points here. First, complex political choreography was required to orchestrate this kind of decision in a nation not yet at war and without an expanding and growing economy. Nuclear weapons are not for political neophytes. Second, our intelligence about other nations and their weapons programs has been limited since the beginning of the atomic age. The United States made one of its most important decisions based on the assumption that Nazi Germany would do the same, and our entire program operated under the equally false assumption that we were racing the Germans. Much as in the race to the moon, only one party was actually running.

Tacit Knowledge and the First Weapons

Those new to the making of an atomic bomb may not possess the tacit knowledge of how to build one, but they will be required to possess

explicit and tacit knowledge in a host of necessary precursor fields, ranging from metallurgy and detonation to theoretical and experimental physics. Physicists in 1930s America, especially experimentalists, also shared another common area of experience—ham radio. Amateur radio was the one hobby shared by virtually every male of a technical inclination in interwar America. With the hobby, which entailed building and modifying one's own radio, came a toolkit for then modern electronics, including skill at soldering; diagnosing the various afflictions that affected vacuum tubes; and the ability to read and write in the shared language of a circuit diagram.

Graduate education in a host of fields drew upon and improved the skills the ham radio operators had taught themselves. Equally important was the role of the Great Depression in selecting talent; graduate education was not a perfect meritocracy—there was substantial discrimination against Jews, as well as African Americans and women—but the selection pressures of the economic crisis allowed only those who were very good or independently wealthy to actually pursue advanced degrees. Even with this background, the United States had genuine difficulties in constructing its original weapons.

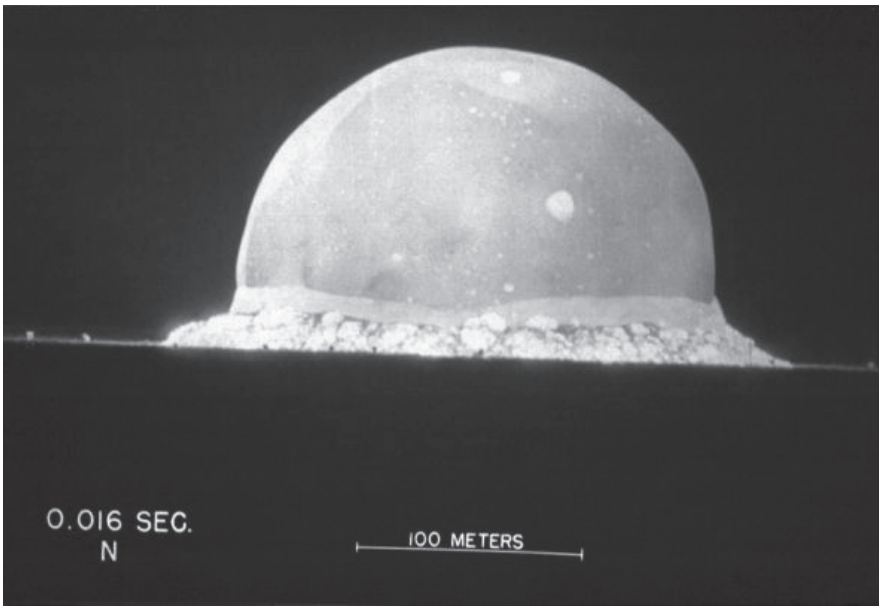
At the outset of the project it was assumed by the theoreticians that building a fission device would prove very simple. Some physicists even advised younger colleagues that the project would be solved once the raw materials were available in sufficient quantities. Chalk that up as another failed prediction.

Building the first weapons demanded the creation of new fields of research ranging from the study of the new element plutonium to the study of shock waves produced by explosives and focused through explosive lenses. As is now well known, the original plan for the weapon was that the bomb would employ a gun-type assembly in which one would fire one sub-critical mass of U235 into another; the same would hold true for Pu239.

Instead, the actual production of plutonium and the separation of the element into the required isotope and amounts required a whole new physical chemistry to understand the new substance. One can note that the much acclaimed Smyth Report, *Atomic Energy for Military Purposes* (1945), had much to say about the production and assembly of the U235 weapon but little about the Pu239 bomb. The physical chemistry and machining of plutonium, developed by Glenn Seaborg and his colleagues, were among the real secrets of the Manhattan Project.

Next, because of its chemistry and physics, Pu239 would not work in a gun-type assembly. When Pu239 was present in any quantity near that required for a bomb, the isotope underwent spontaneous fission. Rather than going "boom," the mass simply lay there, a pile of poison with no explosion. Making a plutonium bomb required a new method for the rapid assembly of the critical mass, implosion. Despite devoting the full resources of Los Alamos towards solving the problem of implosion, there remained genuine uncertainty about whether the method would actually work, even as researchers poured and molded the explosive charges that compress a hollow sphere of Pu239 into a critical mass.

One reason for the Trinity test in New Mexico in 1945 was to determine whether or not implosion would actually yield a working weapon. After all, the United States did not test a U235 gun-type weapon, but that was a decision driven by the inability to produce



The Trinity test on 16 July 1945. Photo © Getty Images.

enough U235 for another weapon before January 1946.[7]

Obviously, one important issue no longer confronts anyone struggling to build a weapon—they know it is possible. Among the other areas in which the United States produced individuals possessing tacit knowledge was in the purification and machining of plutonium, the enrichment of uranium, and the assembly of weapons.

As the Cold War progressed, the United States continued to acquire experience in the design and production of nuclear and later thermonuclear weapons. Central to the process was the development of computational simulations of what took place when a nuclear weapon detonated. This software, what designers called "codes," became essential to the ongoing development and improvement of the arsenal. As readers may recall, what made the charges in the Wen Ho Lee case so serious was the potential loss of such codes to a foreign power.

What we have learned from the work of scholars such as Hugh Gusterson, Donald MacKenzie, and Graham Spinardi is that 10 to 30 percent of all US nuclear tests were not done to test a particular weapon's configuration but to confirm the reliability of codes to accurately predict what took place during a detonation.[8] What counts as close enough is also up for debate and discussion, since designers are often happy if results are within 25 percent of their predictions.

What is striking in this research is the relatively small number of people who count as genuine, journeyman designers. It takes roughly 10 years for the US national labs to turn an excellent astrophysicist into a viable and creative weapons designer. Such people possess what they call judgment, the ineffable or tacit knowledge necessary to accurately evaluate the effects of seemingly minor design changes.

Such people possess what they call judgment, the ineffable or tacit knowledge necessary to accurately evaluate the effects of seemingly minor design changes.

Even at the height of the Cold War, the United States had only 50 people possessing this level of knowledge. It is important to keep in mind that these people were designers. Others, ranging from those who machined the raw materials to those who assembled the weapons, possessed their own tacit knowledge, all of which proved essential in manufacturing working devices. Tacit knowledge remains vital to US national security, given the importance of the Stockpile Stewardship Program and our national commitment to the Comprehensive Test Ban Treaty.

Proliferation: Or How Do You Move Tacit Knowledge Around?

Given the thickness and stickiness of tacit knowledge, it would seem nearly impossible to move it without moving the individuals in whom it is embodied. Clearly that isn't the case—other nations have developed nuclear weapons, but they have done so not entirely under conditions of their own choosing. As Steven Flank, a most interesting student of this problem put it:

> *Nuclear system builders face limits on all resources—money, political authority and consensus, laboratory quality reagents, access to imports, and so on. The process by which these scarce resources are recruited and fixed in a stable network capable of producing the comparatively simply artifacts of 'nuclear weapons' is the process of nuclear proliferation.*[9]

Take the cases of Britain and the former Soviet Union (USSR). Both started with the same source, Klaus Fuchs, although one, the UK, had access to him personally, whereas the USSR had access to him through the documents he provided through his espionage. Each nation attempted to build an implosion device and each nation ran into problems making a copy of the Trinity test weapon. In the USSR, the explicit knowledge of the plans still demanded the production of an entire nuclear industry, a task that took four years, slightly longer than the Manhattan Project itself.

The Soviet weaponeers found themselves having to reinvent the processes and practices that the Americans had already developed. In other words, they had to reinvent the tacit knowledge of the Americans.[10]

The British faced a slightly different set of problems. First, while the UK had participated in the Manhattan Project and had a group at Los Alamos, the Atomic Energy Act of

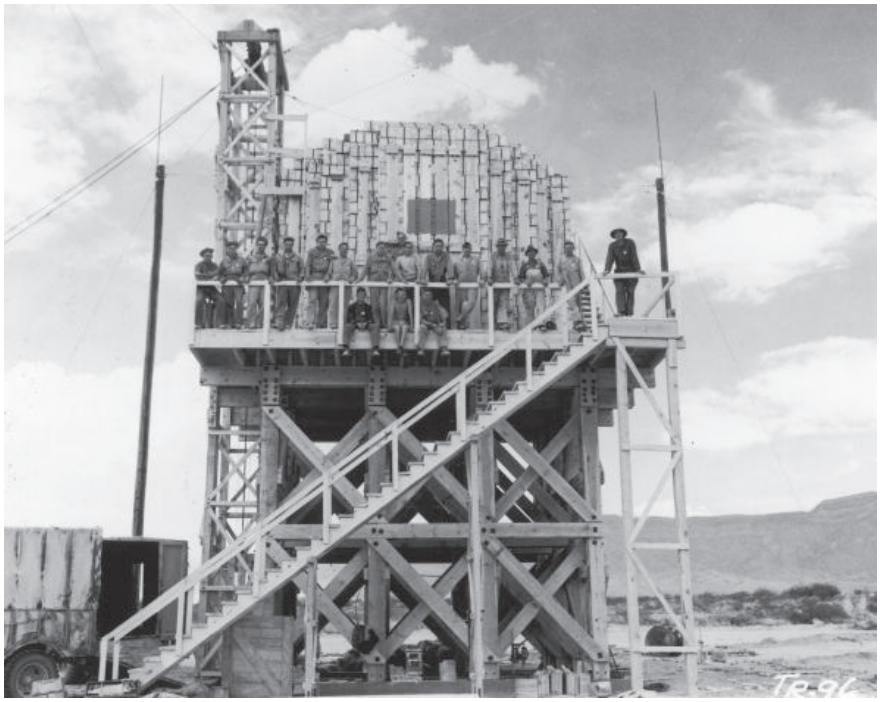
1946 cut off their American sources. Second, they seemed to have real problems with what was a wartime necessity in the United States—assembly of the weapon in-flight. Because of fears that their weapon might arm itself, the UK wound up developing a slightly different implosion device. In both cases, each nation found itself reconstructing a variant of the Manhattan Project's sociotechnical network. Tacit knowledge didn't so much move as it was invented anew.

Similar stories might be told of both France and China, and readers should examine the claims made by MacKenzie and Spinardi with respect to those national narratives. Still, an excellent example of the difficulties in building nuclear weapons took place in the United States. In the wake of the controversy over building a thermonuclear weapon, the United States decided in 1952 to build a second weapons laboratory—the Lawrence Livermore National Laboratory. What is striking is that while designers at the laboratory had access to all the explicit knowledge from Los Alamos, they were utterly unable to make a working weapon on their first two tests.

Part of their problem was that the designers at the new laboratory wanted to make weapons completely different from those made at Los Alamos and tried to use novel materials and techniques. They had never built a nuclear weapon and lacked the necessary tacit knowledge and skill. Livermore's first two tests were epic fizzles. One even failed to bring down the tower upon which the test device rested. Efforts of the Livermore group to pull down the test tower with a jeep were duly recorded by observers from Los Alamos. In other words, even in the same country and with equal access to classified information, it proved difficult for a group of well-trained and otherwise competent professionals and technicians to make a weapon.

Save for India and Israel, both of which seem to have taken some of the knowledge from their civilian nuclear programs and applied it to their weapons program, other proliferation cases appear slightly different. If news reports can be trusted, Pakistan appears to have acquired knowledge of enrichment through A.Q. Khan's now well-known work at URENCO. If news reports are trustworthy, Pakistan also received blueprints for a bomb as well as enough highly enriched uranium (HEU) for two bombs from China in 1982.[11]

This gift appears to have had minimal effect on the speed at which the Pakistanis developed their own bomb. They still had to learn how to build one, and that required a reinvention of the tacit knowledge that went into the Chinese device they apparently copied. More interesting is the Libyan case, where Khan apparently promised the Libyans a turn-key system for the production of nuclear weapons. Such a system included the ability to machine either enriched U235 or Pu239. It is entirely unclear who in Libya could make use of such a technology. Importing an entire nuclear weapons complex would have been an impressive achievement, but it doesn't appear to have taken place. And if it had, Libya would have been held hostage by its supplier for



Workers on the Manahattan Project in Alamagordo shown on a platform stacked with TNT interlaced with fission products. Explosion of the TNT was meant to make sure measuring and observation equipment functioned and was correctly calibrated before the first test. Such testing also provided experience and built tacit knowledge in capturing data from an atomic test. Photo © Time&Life Pictures/Getty Images.

all the skills necessary to assemble a weapon.

Kits for nuclear weapons sound frightening, and stories about them appear designed to scare Western governments. Where was the tacit knowledge and skill necessary to build a bomb going to come from? Was Khan going to set up an outpost of the Pakistani weapons complex in Libya? It is important to recall that Qadhafi purchased expensive, sophisticated weapons from the West that no one in his armed forces could actually use. One can easily imagine a program to effectively dismantle a Libyan nuclear program by sabotaging the equipment purchased from Khan. Given his scruples or lack thereof, he might even sell slightly defective equipment to unwitting buyers.[12]

Even the Iraqi program dismantled after the first Gulf War had serious problems, not the least of which was its use of calutrons—the same devices E.O. Lawrence built at Oak Ridge during WW II. What hampered our understanding of the Iraqi program appears to have been a lack of understanding by various intelligence agencies of the Iraqis' actual skill level. Apparently, we believed the Iraqis would not redo the Manhattan Project but take up where other states had started. After all, calutrons produced the raw, slightly enriched uranium that American weaponeers then poured into the massive gaseous diffusion complex, K-25.

Even after a year of operation, the United States had only enough raw U235 for the single device used at Hiroshima. Another uranium bomb would not be available until January 1946. Iraq may have been able to build a bomb, in time, but it was never going to be a major builder of nuclear weapons as long as it relied upon calutrons.[13]

Thinking about tacit knowledge suggests new or additional approaches to stemming the proliferation of illicit programs.

For me, a private citizen with no access to classified materials, the Iran case is an interesting test of these ideas about tacit knowledge. At the very least, it appears the Iranians want the capability to build a weapon that a missile might deliver to a target. The November 2011 IAEA report and subsequent commentary lends credence my assertions since it appears that the Iranians imported a former Soviet weapons scientist, Vyacheslav Danilenko, to instruct them in manufacturing the specialized electronics required for fast-acting detonators.[10]

Apparently, Iran has also tried to purchase tacit knowledge by enlisting the aid of those possessing the requisite skills, in this case the ability to design and build fast-acting detonators. As Sharon Weiner observed in the *Bulletin of the Atomic Scientists* in November 2011, the US enacted an array of programs to eliminate this possibility, but the individual in question appear to have fallen between the cracks.

Iran may have been able to develop fast acting detonators indigenously, without outside assistance, but without testing they would not know if they had a working device or a chunk of subcritical fissionable material. Perhaps, they believe that importing the knowledge makes an actual test unneeded, but testing seems necessary for nuclear states to establish their atomic bona fides.

So what?

Thinking about tacit knowledge suggests new or additional approaches to stemming the proliferation of illicit programs. To date, most of our efforts to halt proliferation rely upon attempts to interdict or destroy the sources of raw materials or the technologies necessary to make them. Examples of this are the Israeli raid on the Iraqi reactor and the widely reported deployment of the Stuxnet worm, the sophisticated piece of malware that targeted the specific Siemens industrial-grade controllers used in the Iranian enrichment program.[14] Similarly, reported efforts to target top Iranian nuclear scientists might be an ominous extension of efforts to slow Iranian weapons development.

However, understanding of such weapons programs as networks of activities, institutions, people, and resources may offer a greater variety of collection and intervention strategies, which are best left to those in a position to make such decisions.

One of Steven Flank's most interesting observations was about the Indian nuclear program, which he claimed attempted unsuccessfully to forge a connection with the nation's agricultural sector. Instead, the nuclear researchers found a home within the military's dense support network. More recent research by George Perkovitch and others disagree and hold that Indian research-

Interrupting the development and acquisition of tacit knowledge in regimes of proliferation concern might provide time and opportunity to allow diplomatic, economic, and other measures to take hold.

ers wanted to build a bomb from the very beginning of their program, but Flank's point is more basic and resonates with this paper's basic argument. Nuclear programs require time and sophisticated support and resource networks. Flank believed that offers of foreign aid tied to the agricultural sector might have linked the nuclear researchers to the agriculturalists and thus to peaceful purposes, but that is a counterfactual we don't have to accept.

True or not, the story helps to focus us on addressing tacit knowledge rather than the usual methods of stemming proliferation. It allows us to recognize that while the absence of tacit knowledge is not a show stopper, it is a "show slower," to coin an infelicitous phrase. If nations have the resources, the time, and a civilian nuclear power program, and elect to make the acquisition of nuclear weapons a priority, stopping them will be difficult, as the case of North Korea has shown. Still, interrupting the development and acquisition of tacit knowledge in regimes of proliferation concern might provide the international community time and opportunity to allow diplomatic, economic, and other measures to take hold.

❖ ❖ ❖

Source notes

1. The classic sources on tacit knowledge are Michael Polanyi, *Personal Knowledge: Towards a Post-Critical Philosophy* (Chicago: University of Chicago Press 1958); and *idem*, *The Tacit Dimension* (Garden City, N.Y.: Doubleday & Co., 1966). On understanding the origins of the concept, see John R. Baker, "Michael Polanyi's Contributions to the Cause of Freedom in Science." *Minerva* 16, no. 3 (1978): 382-96; and Mary Jo Nye, "Historical Sources of Science-as-Social-Practice: Michael Polanyi's Berlin." *Historical Studies in the Physical and Biological Sciences* 37, no. 2 (2007): 409-34.

2. To begin to understand how practitioners of science and technology studies have used tacit knowledge, see Harry Collins, *Changing Order: Replication and Induction in Scientific Practice* (Beverly Hills: Sage Publications, 1985); and *idem, Tacit and Explicit Knowledge* (Chicago: University of Chicago Press, 2010). A thought provoking article about tacit knowledge that also addresses its role in other fields is Tim Ray, "Rethinking Polanyi's Concept of Tacit Knowledge: From Personal Knowing to Imagined Institutions" *Minerva* 47 (2009): 75-92.

3. On the problem of moving scientific around, see Shapin, Steven. "Here and Everywhere: Sociology of Scientific Knowledge." Annual Review of Sociology 21 (1995): 289-321; and *idem,* "Placing the View from Nowhere: Historical and Sociological Problems in the Location of Science." *Transactions Institute of British Geography* 23 (1998): 5-12.

4. On the spread of the cyclotron, see Heilbron, J.L, and Robert W. Seidel. *Lawrence and his Laboratory: A History of the Lawrence Berkeley Laboratory.* Berkeley: University of California Press, 1989.

5. On PCR's development and dispersion, see Paul Rabinow, *Making PCR: A Story of Biotechnology.* (Chicago: University of Chicago Press, 1996); and Lynch, Michael, Simon A. Cole, Ruth Mcnally, and Kathleen Jordan, *Truth Machine: The Contentious History of DNA Fingerprinting* (Chicago: University of Chicago Press, 2008) 83-112.

6. On the decision to build a weapon, the definitive source is Stanley Goldberg, "Inventing a Climate of Opinion: Vannevar Bush and the Decision to Build the Atomic Bomb." *Isis* 83 (1992): 429–52.

7. There are many histories of the Manhattan Project. The best place to start remains Martin J. Sherwin, *A World Destroyed: Hiroshima and the Origins of the Arms Race*. New York: Vintage, 1975; 1987. Another excellent source to mine for information about tacit knowledge in the project is Hewlett, Richard G., and Oscar E. Anderson. *The New World, 1939-1946*. University Park: Pennsylvania University Press, 1962. On the centrality of ham radio in interwar technical culture, see Haring, Kristen. *Ham Radio's Technical Culture*. Cambridge: MIT Press, 2006. On the problems related to plutonium at Los Alamos see Hoddeson, Lillian. "Mission Change in the Large Laboratory: The Los Alamos Implosion Program, 1943-1945," in Peter Galison and Bruce Hevly (eds.), B*ig Science: The Growth of Large-Scale Research* (Stanford: Stanford University Press, 1992): 265-89; and Hoddeson, Lillian Hartmann, Paul W. Henriksen, Roger A. Meade, Catherine Westfall, and Gordon Baym. *Critical Assembly: A Technical History of Los Alamos During the Oppenheimer Years, 1943-1945*. Cambridge: Cambridge University Press, 1993.

8. See Gusterson, Hugh. *Nuclear Rites: A Weapons Laboratory at the End of the Cold War.* Berkeley: University of California Press, 1996; and Mackenzie, Donald, and Graham Spinardi. "Tacit Knowledge, Weapons Design, and the Uninvention of Nuclear Weapons." *American Journal of Sociology* 101, no. 1 (1995): 44-99.

9. See Flank, Steven. "Exploding the Black Box: The Historical Sociology of Nuclear Proliferation." *Security Studies* 3, no. 2 (1993/94): 259-294, quote 260-1. This is among the most astute and thoughtful essays written about nuclear proliferation.

10. The standard source on the Soviet program remains Holloway, David. *Stalin and the Bomb*. New Haven: Yale University Press, 1994. For this identification, see Sharon K. Weiner, "Who's a Weapons Scientist?" Bulletin of the Atomic Scientists (16 November 2011), http://www.thebulletin.org/web-edition/features/whos-weapons-scientist. [last accessed 27 November 2011]

11. R. Jeffrey Smith and Joby Warrick. "A Nuclear Power's Act of Proliferation: Accounts by Controversial Scientist Assert China Gave Pakistan Enough Enriched Uranium in '82 to Make 2 Bombs.," *The Washington Post*, 13 November 2009; and Feroz Hassan Khan, *Eating Grass: The Making of the Pakistani Bomb*, Stanford Security Studies (Stanford University Press, 2012).

12. John Prados, "How Qaddafi Came Clean," *Bulletin of the Atomic Scientists* 61, no. 6 (2005): 26–33.

13. On Iraq and calutrons as well as its entire program, see David Albright and Mark Hibbs. "Iraq's Bomb: Blueprints and Artifacts," *Bulletin of the Atomic Scientists* 48, no. 1 (1992): 30–40.

14. IAEA Report, November 2011, http://www.thebulletin.org/whos-weapons-scientist.

❖ ❖ ❖

The Way of the Knife: The CIA, a Secret Army, and a War at the Ends of the Earth

Mark Mazzetti (Penguin Press, 2013) 381 pp.

Reviewed by Richard T. Willing

Mark Mazzetti is one of a group of *New York Times* reporters who specialize in covering (and sometimes disclosing the secrets of) various elements of the US intelligence and national security apparatus. Mazzetti's particular specialty is CIA, and he has chosen the agency's efforts in the struggle against Islamist terrorism since 11 September 2001 as the focus of his first book.

The "Knife" in Mazzetti's title is drawn from a metaphor used by DCIA John O. Brennan while he served as President Obama's counterterrorism and domestic security advisor to describe America's approach to waging war against al Qa'ida. The nation, Brennan observed in a May 2010 speech, must "prudently" use force, relying at times on a "scalpel" rather than a "hammer."[1] It is Mazzetti's thesis that the scalpel approach, meaning the selective use of armed drones and small paramilitary forces, is far from the neat surgical incision that the word seems to imply. Instead, he argues, the scalpel approach has created enemies as well as destroyed them, has "short-circuited the normal mechanisms" for going to war, and has turned the CIA into a "killing machine" consumed with "man hunting."

From the first pages, the author's point of view is clear: he doesn't approve. The way of the knife, he argues, places the president in the unprecedented position of making individual targeting decisions in secret, which is bad for American democracy. It has caused the CIA, he continues, to become distracted from its singular role as producer of vital centralized intelligence. Inevitably, Mazzetti writes, the CIA and the Department of Defense have become tangled in a duplicative and often counterproductive rivalry, as intelligence gathering and paramilitary activities "bleed" into one another.

Mazzetti's conclusions won't come as a surprise to readers familiar with his coverage in the *New York Times.* His point of view seems to prevent him at times from seeing the larger picture or appreciating nuance as he seeks out anecdotes that seem to prove his case. For instance, he argues that the disaster in Benghazi in September 2012 is best described simply as a direct outgrowth of overreliance on the way of the knife. This is facile analysis.

The Way of the Knife is not a negative screed, but it does little to acknowledge the CIA's successes or to offer historical context. Readers won't learn, for instance, that the tension over whether and how to undertake covert operations, as well as rivalries between civilian intelligence and the military predate CIA's founding in 1947. Nor will they learn that what Mazzetti describes as the "shrunken and dispirited" CIA of early 2001 was already hard at work on its assignment to find, fix, and finish Usama Bin Ladin.

Notwithstanding its shortcomings, *The Way of the Knife* is a lively and worthwhile read. Which authorities and protections ought to be available to the CIA (instead of the military) in carrying out actions abroad is a question we are bound to continue to discuss. Our president and Brennan have signaled as much. Mazzetti's credentials ensure that his arguments will receive a wide airing. The intelligence professional, though, will also find that his thesis and the manner in

[1] www.whitehouse.gov/the-press-office/remarks-assistant-president-homeland-security-and-counterterrorism-john-brennan-csi

which he supports it require close and sometimes skeptical scrutiny.

Mazzetti's description of the drone program is a case in point.[2] He tracks its development from the post-9/11 stage to what he describes as parallel and competing military and CIA programs operating in the mountains of Pakistan, on the Arabian peninsula, and in Africa. (pp. 46–47, 267–68, 311)

Drones—precise, effective, unmanned, remotely piloted—prove, in the author's view, to be an irresistible weapon for administrations constrained by policy judgments and court rulings from taking prisoners or placing boots on the ground. Drones are also, in Mazzetti's telling, the perfect antidote for a CIA presumably demoralized by its "years in the detention-and-interrogation business." The CIA has seized on armed drones and "targeted killings" as its "new direction," Mazzetti argues. (26, 219)

The author describes in detail how collateral damage from drone strikes, including the deaths of innocents, has strengthened al Qa'ida's case and complicated America's relationship with its allies. Here Mazzetti relies on well-publicized but still unacknowledged details of operations and commentary from professionals with knowledge of the drone program and, usually, a viewpoint sympathetic to the author's. (162)

The CIA's relationship with the Department of Defense receives similar treatment. In Mazzetti's telling, a rivalry began in earnest after the 9/11 attacks, when CIA acted quickly to get operators on the ground in Afghanistan and became the lead agency in the global war on terror. The military, with a large array of Special Operations Forces available, lacked "actionable intelligence" (and possibly legal authorities) to get into the field quickly. Secretary of Defense Donald Rumsfeld complained, asking in a memo to the chairman of the Joint Chiefs of Staff, "Isn't it conceivable that the Department (of Defense) ought not to be in a position of near total dependence on CIA in situations like this?" (67–68)

Mazzetti then describes a period in which the military attempted to compensate by building up its intelligence collection capabilities, often relying on elite special units and private contractors. CIA, meanwhile, enlarged its paramilitary capabilities to meet the needs of its expanded mission. The result, the author concludes, often has been duplication, confusion, and an informal marketplace in which parallel or conflicting programs are created and providers can shop their services to the highest bidder.

"Everything is backwards," former CIA lawyer W. George Jameson is quoted as saying. "You've got an intelligence agency fighting a war and a military organization trying to gather on-the-ground intelligence." (314) Perhaps this is so, especially for those overly concerned by organizational charts. But the fact remains that the CIA did continue to collect and analyze, and the military did its share of fighting (recall that a Navy SEAL team, not a CIA unit, carried out the raid on Bin Ladin's compound). Organizational "bleed" or not, the combined efforts of the Intelligence Community, with the CIA in the lead, and the American military largely have been getting the job done over the past 10 years. Mazzetti gives this little consideration, leaving the reader to wonder what other inconvenient truths were cast aside as he assembled his book?

❖ ❖ ❖

[2] The Predator's pre-9/11 roots are described in Frank Strickland's "The Early Evolution of the Predator Drone," *Studies in Intelligence* 57, no. 1 (March 2013).

Hiding in Plain Sight: Felix A. Sommerfeld, Spymaster in Mexico, 1908 to 1914

Heribert von Feilitzsch (Henselstone Verlag, 2012) 468 pp., index.

Reviewed by Mark Benbow

This decade marks the centennial of both the Mexican Revolution (1910–1920) and the First World War (1914–1918). They overlapped in more ways than simple chronology. During the prerevolutionary regime of Porfirio Díaz (1876–80, 1884–1911), American, British, and German businesses competed for opportunities in Mexico, especially in mining, oil, and railroads. After WW I began, Washington, London, and Berlin's interest in Mexico intensified in large part because a new Mexican-American war could distract the United States and divert arms then going to the Allies. In short, Mexico became an important front in the WW I intelligence effort.

Numerous studies related to this subject have been released over the past few years, most notably books by Charles Harris III, Louis Sadler, and Thomas Boghardt.[1] Independent scholar Heribert von Feilitzsch has added a new volume with *In Plain Sight*, which discusses the career of Felix Sommerfeld, sometime miner and soldier of fortune, who became an adviser to Mexico's President Francisco I. Madero during his short-lived presidency (November 1911–February 1913). While acting as Madero's adviser and gatekeeper, Sommerfeld worked as an agent for the German government, reporting not just on Mexican affairs, but also on US policies in Mexico.

Sommerfeld was born in 1879 into a middle-class family in Germany. He studied to be a mining engineer before emigrating to the US to join a brother. He enlisted in the US Army for the Spanish-American War, deserted—perhaps out of boredom—and returned to Germany. Sommerfeld served in the Kaiser's army in China during the Boxer Rebellion. He returned to the United States, avoided arrest for desertion, and passed through Arizona and northern Mexico working as an engineer.

Sommerfeld's actions during 1906–1908 are hazy, but Feilitzsch suggests that he returned to Germany to train for intelligence work. Sommerfeld reappeared in Mexico as a German agent and in 1910, while officially a reporter for the Associated Press (AP), worked his way into Madero's inner circle. After Madero's assassination, Sommerfeld began working for various revolutionary factions, often collaborating with the US Bureau of Investigation while secretly sending reports to Berlin.

By 1915 Sommerfeld was "Pancho" Villa's major arms broker in the United States. At the same time he worked for German Naval Attaché Karl Boy-Ed, who was then running a large espionage and sabotage organization in the United States aimed at interfering with US arms deliveries to the Allies. Sommerfeld suggested using Villa to create an incident to drag the United States into war with Mexico. In March 1916, Villa's raid on Columbus, New Mexico, came very close to doing just that. Interned as an enemy alien once Washington entered WW I, Sommerfeld was interviewed by the US Army in 1918. Much of this book is based on those interviews. Sommerfeld disappeared from the historical record in the 1930s.

---

[1] Harris and Sadler, *The Secret War in El Paso: Mexican Revolutionary Intrigue, 1906–1920* (University of New Mexico Press, 2009) and Boghardt, *The Zimmermann Telegram: Intelligence Diplomacy, and America's Entry into World War I* (Naval Institute Press, 2012). The latter was reviewed in *Studies in Intelligence* 57, No. 2 (June 2013).

Sommerfeld successfully juggled his multiplicity of roles, at least initially. But even in a preelectronic era, he left traces which Feilitzsch successfully follows to pierce Sommerfeld's slightly amateurish denial and deception campaign. For example, Sommerfeld often travelled under his real name and left immigration records. Sometimes the lack of a record proved useful. Feilitzsch found no evidence to substantiate Sommerfeld's claim that he was the manager of several Mexican mines just before the revolution. (36) Still, some parts of Sommerfeld's activities remain clouded, such as any role he might have played in sparking Villa's Columbus raid.

In Plain Sight is well researched and well argued. The bibliography is fine; Feilitzsch used libraries and archives in the United States, Mexico, and Germany as well as the major scholarly works on international involvement in the Mexican Revolution. He is, however, sometimes prone to overstatement. When discussing Sommerfeld's activities, he often says "the only explanation is…." His conclusions are logical, but while they are the most reasonable explanations for Sommerfeld's activities, they are not the only explanations. For example, Feilitzsch describes Sommerfeld's relationship with the German vice-consul in Chihuahua before the revolution. Sommerfeld's reports praised the vice-consul's work and the man received a promotion. The consul then put Sommerfeld on his payroll. "There is only one interpretation of what Sommerfeld was paid to do" von Feilitzsch writes, "Espionage." (75) While that's a likely explanation given Sommerfeld's role in Mexico at the time, it is not the only possible reason for the consul's actions. It might also have reflected gratitude for aid in winning promotion. Often replacing "only" with "likely" would have improved the author's arguments.

In Plain Sight was published by Henselstone Verlag, the author's own company. Self-published books are usually ignored by academics, often for good reason. However, they seem to be increasingly popular. For example, The History Press has found a niche releasing local histories by talented, if sometimes irregularly trained historians. Self-published authors often have little or no training as historians, but Feilitzsch earned an MA in Latin American history at the University of Arizona.

Nonetheless, the book would have benefitted from the services of a professional editor at a scholarly press. There are a few too many awkward phrasings, and the author often slides into passive voice. The rather spare index is merely adequate. Despite these issues, Feilitzsch has done an exemplary job of tracing the activities of a shadowy character in a chaotic time and place. *In Plain Sight* is a welcome addition to the growing literature of the intelligence war of the 1910s and is well worth the read.

❖ ❖ ❖

Intelligence Officer's Bookshelf

Compiled and reviewed by Hayden Peake

Current

Terrorist Financing, Money Laundering, and Tax Evasion: Examining the Performance of Financial Intelligence Units, by Jayesh D'Souza.

Trading Secrets: Spies and Intelligence in an Age of Terror*, by Mark Huband.*

General

Decoding Organization: Bletchley Park, Codebreaking and Organization Studies, by Christopher Grey.

Talk at the Brink: Deliberation and Decision during the Cuban Missile Crisis, by David R. Gibson.

Work Like a Spy: Business Tips from a Former CIA Officer*, by J. C. Carleson.*

Historical–US and Worldwide

A Brief History of the Spy: Modern Spying from the Cold War to the War on Terror, Paul Simpson.

The Houseguests: A Memoir of Canadian Courage and CIA Sorcery, by Mark Lijek.

Intelligence in the Cold War: What Difference Did It Make? edited by Michael Herman and Gwilym Hughes.

The Rice Paddy Navy: U. S. Sailors Undercover in China—Espionage and Sabotage Behind Enemy Lines in China During World War II, by Linda Kush.

Saul Steinberg: A Biography, by Deirdre Bair.

Stalin's Secret Agents: The Subversion of Roosevelt's Government, by M. Stanton Evans and Herbert Romerstein.

Historical—non-US

Empire of Secrets: British Intelligence, the Cold War and the Twilight of Empire, by Calder Walton.

The Imperial Security State: British Colonial Knowledge and Empire-Building in Asia, by James Hevia.

The Man Who Was George Smiley: The Life of John Bingham, by Michael Jago.

Spying for the People: Mao's Secret Agents, 1949–1967, by Michael Schoenhals.

Under Every Leaf: How Britain Played the Greater Game from Afghanistan to Africa, by William Beaver.

Women of Intelligence: Winning the Second World War with Air Photos, by Christine Halsall.

Intelligence Abroad

India's Spy Agencies: Shaken Not Stirred*, by Lt. Col. Sunil S. Parihar.*

Current Topics

Terrorist Financing, Money Laundering, and Tax Evasion: Examining the Performance of Financial Intelligence Units, by Jayesh D'Souza (CRC Press, 2012), 212 pp., end-of-chapter references, index.

How do terrorists pay for travel, weapons, training, and all the day-to-day costs of communication, web monitoring, computers, food, and more that allow them to function? In *Terrorist Financing*, Canadian author and financial management specialist Jayesh D'Souza identifies potential sources of funds and various money laundering techniques employed by terrorists and their sympathizers. D'Souza's primary focus is on interrupting the flow of money to terrorists. The key organizations working toward that goal, he suggests, are national financial intelligence units (FIUs).

After a review of changes made to intelligence organizations in order to track money after 9/11, D'Souza uses case studies to describe the nature and types of terrorist financial dealings and how they are done. (65ff.) The case studies are really illustrations with few specifics, and the "how" is hard to see, although he does describe the kinds of things that are done.

D'Souza then turns to risk management, performance measures, various administrative impediments, and the functions of the FIUs in nations where they exist. His scope is worldwide, and he discusses the principal countries one by one, highlighting key organizations and their functions. The US merits three pages and Canada one, for example.

The two final chapters deal with what FIUs need to do in order to improve performance, the role of the private sector, and the gains possible with better cooperation. As a guide to the problem, *Terrorist Financing, Money Laundering, and Tax Evasion* is a valuable source.

Trading Secrets: Spies and Intelligence in an Age of Terror, by Mark Huband (I. B. Tauris, 2013), 260 pp., endnotes, bibliography, index.

Mark Huband became an "expert" on spies and intelligence agencies while serving as the *Financial Times s*ecurity correspondent between 2001 and 2003. In a statement that will astound those who remember the Church Committee era in the United States and the Peter Wright kerfuffle in the United Kingdom, he writes that, thanks to 9/11, "never before had the CIA, SIS, MI5 and other intelligence services been under such scrutiny." (2) He then observes that "part of the trauma to the Americans and the wider world has lain in the realization that the ability to *surprise* has been lost to the other side." (3) Thus it follows from his line of thinking that gaining an intelligence advantage over al-Qaeda "necessitated an understanding of just how redundant the established practices of intelligence gathering had become."(9) Redundant is used here in the sense of "no longer needed." He argues, but never really demonstrates, that "trading secrets" is an obsolete objective.

To make his point historically, he invokes a comparison with Irish nationalism since 1798. From then until 9/11, he argues, espionage had been based on "the 'trade' in secrets." (6, 9) "As all intelligence agencies failed to learn of al-Qaeda's most devastating attack until it was too late, so the British in Ireland failed to detect just how strong were the nationalist sentiments that in 1922 brought an end to centuries of occupation in all but six counties of what became Northern Ireland." (40–41)

Huband devotes several chapters to the Irish precedent. Then he examines the Cold War practices of the CIA, with emphasis on Africa and to a lesser extent the Middle East, in order to show how the West failed for so long to see the "emerging trends…as threatening Western interests." (95) This is followed by a summary of how Bin Laden operated and a review of CIA pre-9/11 attempts to deal with what some saw as a genuine threat. But, he adds, "even the best secret intelligence on al-Qaeda's intentions might not have averted 9/11…because it was al-Qaeda's destiny." (118) Then, after a digression discussing the intelligence failures he claims preceded the most recent Iraq war, Huband assesses the post-9/11 rendition and prisoner interrogation issues. In each case he draws parallels with the Irish experience to show how traditional espionage—or "spying" as he calls it—was inadequate.

Trading Secrets doesn't supply an unambiguous alternative to the "redundant" trading of secrets. He acknowledges that the "trade in secrets" is still practiced, but he argues, without evidence, that the secrets needed today are in the hands of those "who have no interest in selling what they know." (226) He concludes that "eavesdropping has taken the lead" and hints that private security firms staffed by former intelligence officers seeking personal gain have major roles to play. (227) Huband's suggestions point to the conclusion that he has not acquired sufficient understanding of the intelligence profession to be regarded as an expert.

General

Decoding Organization: Bletchley Park, Codebreaking and Organization Studies, by Christopher Grey (Cambridge University Press, 2012), 322 pp., end-of-chapter notes, bibliography, appendix, glossary, index.

Professor Christopher Grey chairs the Organizational Studies Department of Royal Holloway University of London. His man objective in writing *Decoding Organization* was "to develop a way of conducting organizational studies" (5) and only secondarily to discovering why Bletchley Park (BP), with its unique operating circumstances, was able to function successfully. He recognizes that, given the complexity of many organizations, there is doubt that "what works within one organization can ever be replicated within another." (21) Thus his title has a double meaning: decoding or understanding BP's structure in order to decode the underlying organizational theory.

What, then, is the potential takeaway for the intelligence officer? Grey's discussion of BP's structure and how it evolved in an ad hoc fashion while accomplishing its mission under great stress is of interest historically and to managers who may have to consider similar situations. Toward this end, Grey evaluates cultural aspects, personnel conflicts, and managerial disputes. But, as he admits, with its emphasis on organizational theory, the "book contains some extremely detailed empirical material" that "may be a confusing swirl of acronym, special terms, events and people." (39)

For those not schooled in organizational theory, it may be useful to read the conclusions first. Here, Grey explains in greater detail the "decoding BP" metaphor. Also valuable are the appendices, which provide a timeline of major BP events, a list of interviewees, a summary of the roles of key players, and organizational charts that show structural development.

Decoding Organization considers many factors—human trust, leadership, culture, and management styles, as well as organization—that affect intelligence officers in their careers. It is an unusual perspective into the intelligence profession and that itself can be of value.

Talk at the Brink: Deliberation and Decision during the Cuban Missile Crisis, by David R. Gibson (Princeton University Press, 2012), 218 pp., endnotes, bibliography, index.

David Gibson is an assistant professor of sociology at the University of Pennsylvania specializing in the meaning of conversation, or talk. He characterizes the main argument of *Talk At The Brink* as follows:

> *Insofar as a decision arises out of talk, and there is no "right" answer simply waiting to be discovered or decreed, that decision emerges from an intersection of individuals' perspectives and interests; conversational rules, procedures, and vicissitude; and external events that may impinge on the decision making process before it has run its course.* (159)

Gibson's analysis is based on the now-public recordings of conversations of President John F. Kennedy's Executive Committee (ExComm)—the core group of NSC members and White House advisors that met throughout the crisis. Although Gibson acknowledges that "Kennedy was the person who would ultimately make the crucial decisions and who would principally be held accountable for them," (72) the concept that the

president's decisions resulted from a spirited exchange of ideas is too simplistic, from his point of view. Those who have accepted that interpretation are judged incorrect for reasons Gibson enumerates.

To make his point, Gibson provides an extensive review of the ExComm and how it functioned, quoting many exchanges. There follow several chapters of detailed analysis of the conversations, many portions of which are reproduced. He notes that Kennedy himself described "the decision making process as impenetrable…mysterious even to those most intimately involved." He goes on to suggest that Kennedy would have been surprised if he thought that decisionmaking involved "a cerebral exercise in which the decision maker was entirely in charge and at the mercy of his… cognitive limitations [and] the information available." (165) No one knows what Kennedy thought on the subject, but Gibson does not make clear why he would have been surprised.

Gibson relies heavily for his views on the disorganized and repetitive nature of the ExComm's discussions. Here he employs often esoteric social science concepts. Nevertheless, for nonsociologists, the interpretations found in *Talk At The Brink* do not discount the simpler explanation that Kennedy considered all the evidence, as disorderly as it was, and simply made the decision that he thought would avoid a nuclear exchange with the Soviet Union.

Work Like a Spy: Business Tips from a Former CIA Officer, by J. C. Carleson (Penguin, 2013), 198 pp., index.

After returning to private life, former CIA case officer J. C. Carleson realized that many of the skills acquired during 10 years in the clandestine service could be used to enhance performance in the corporate world. *Work Like a* Spy identifies those skills and illustrates their application. But Carleson is quick to emphasize that her book is not about, nor does it advocate, industrial espionage. And it is not a traditional memoir, though the examples she uses to draw parallels with business practices are based on firsthand experience.

The book has three parts. The first is a review of the basics of human intelligence, the practices involved, and how they relate to business. Of particular interest is a chapter on business counterintelligence, or security, in which corporate and personal vulnerabilities are discussed.

In part two Carleson reviews personnel recruiting and screening techniques for forming good teams. The work ethic is important here, and the 12 principles she introduces were drawn from lessons she learned in dealing with agents and intelligence officers. The final chapter in this part considers crisis management strategies and how leaders and corporate managers can implement them successfully.

Part three deals with getting people—targets as she calls them—to make a sale. Carleson describes a number of techniques, then considers various methods of control or supervision likely to enhance success while underlining the merits of "the unorthodox approach" she recommends. She reviews techniques for handling suppliers and competitors and in each case draws on her CIA experience to illustrate her ideas.

In conclusion, Carleson points out that good case-officer tradecraft produces results in the business world, as demonstrated by her own experience since leaving the CIA. Dirty tricks are not the answer, she writes: "Today's rival can be tomorrow's ally." (192) The key to acquiring information in the business world is finding the right people and adhering to "firm ethical parameters…while maintaining your integrity." (192) *Work Like A* Spy is interesting and provides a valuable, if unfamiliar way of thinking about the intelligence and corporate worlds.

Historical–US and Worldwide

A Brief History of the Spy: Modern Spying from the Cold War to the War on Terror, Paul Simpson (Constable and Robinson, Ltd, 2013), 288 pp., bibliography, glossary, index.

Most books on intelligence history discuss a single agency, a war, or a geographic area. This one is different. It is a chronological narrative, beginning—the title notwithstanding—with a brief account of the events that led to the creation before WW I of Britain's principal agencies, MI5 and MI6. It then turns to the interwar period and reviews the operations of MI5 and MI6 and the successful recruitment of British agents by the Soviet services. This is followed by a summary of WW II activities, bringing in Bletchley Park and the roles played by the Allied and Axis agencies.

The next 11 chapters, with an occasional digression into espionage and popular culture, are devoted to the Cold War and its major cases, which are well summarized. In his coverage, Simpson discusses principal officers, agents, defectors, and organizations from both sides of the war. The final two chapters cover intelligence and the "war on terror" up to 2013.

Despite the absence of source notes, there are relatively few errors, and most are minor. For example, Admiral Canaris, head of the German Abwehr, was hanged, not shot. (9) Guy Burgess was not "the prime mover" who "set out to create his own 'light blue ring of five.'" Kim Philby was the first, and he had Burgess on his list. And Philby was not recruited by Teodor Maly in Vienna; that task was handled by Arnold Deutsch in London, after Philby had returned from Vienna. (11) Finally, James Angleton's tenure as chief of the Counterintelligence Staff ended in 1974, not 1975.

For a single book, Simpson has provided a very good introduction to modern intelligence.

The Houseguests: A Memoir of Canadian Courage and CIA Sorcery, by Mark Lijek (Booknook.biz), 305 pp., photos, no index.

After Antonio Mendez was named one of 50 *Trailblazers* during the CIA's 50th anniversary ceremonies in 1997, he revealed the reason for the award in a *Studies in Intelligence* article, "A Classic Case of Deception," which mentioned the word "Argo"—the name of the operation he led—for the first time.[1] In 2012, it became a household word when Mendez published his book, *Argo*, and the motion picture based on it won three Academy Awards, including one for best picture.[2] Before 2012, Robert Wright published a book describing the crucial Canadian role in the Argo operation.[3] Each of these accounts told the story—from a slightly different perspective—of the six American foreign services officers who escaped capture by the Iranians when the US Embassy in Tehran was overrun in 1989. *Houseguests* author Mark Lijek, one of the six, adds further details from a first hand point of view.

The first two of the five parts of *Houseguests* are something of a memoir about college, joining the US Foreign Service, training, and "volunteering" for a first assignment—in Lijek's case, Tehran. After Mark had spent two months there, Cora Lijek joined her husband. Two months later, on 4 November, Iranian "students" seized the embassy, and the hostage ordeal began. Lijek describes how each of the six houseguests ended up in the home of Canadian diplomat John Sheardown and their fears as they thought about what might happen if they were caught by the Iranians. Lijek's concern was heightened since he learned that the previous attack on the embassy, in February 1989, was not the relatively peaceful event the State Department spinners had claimed—people had died. (110)

[1] Antonio J. Mendez, "CIA Goes Hollywood: A Classic Case of Deception," *Studies in Intelligence* 42 No. 2 (June 1998), 1–16; reprinted in *Studies in Intelligence*, Winter 1999–2000, 1–16. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter99-00/art1.html.

[2] See CIA Chief Historian David Robarge's review of both the book and the movie in *Studies in Intelligence* 57, No. 1 (Unclassified Extracts, March 2013).

[3] Robert Wright, *Our Man In Tehran: The True Story Behind the Secret Mission to Save Six Americans During the Iran Hostage Crisis and the Foreign Ambassador Who Worked with the CIA to Bring them Home* (Other Press, 2011).

Thanks to the Sheardowns, day-to-day life was reasonably comfortable for the six. Lijek tells how they occupied their time while wondering what to do next. Anxiety increased when they learned that word of their presence had leaked and the Iranians were looking for them. (178) They then began considering options for escape presented by the Canadians, but none seem likely to succeed. The situation changed when two men from the CIA showed up with a new option, and they realized they had not been abandoned. The actual escape went more smoothly than depicted in the film *Argo*.

Lijek concludes his story with the events that occurred after they returned home. These included a visit with President Carter, TV appearances, and after-action debriefings. And Lijek explains why many of the escape details remained secret for years. When it was decided to make *Argo* the film, the couple observed production on the set. Lijek makes it clear he was upset that the film did not give appropriate recognition to the Canadian efforts. This was one of the reasons he decided to write the book. An epilogue discusses what happened to each of the six in the years that followed.[4]

Houseguests is exciting reading and fills an important gap in a history-making story.

Intelligence in the Cold War: What Difference Did It Make? edited by Michael Herman and Gwilym Hughes (Routledge, 2013), 150 pp., footnotes, index.

The Norwegian Institute for Defence Studies in Oslo has sponsored two conferences since 2000 on a crucial question for historians and intelligence officers alike: did intelligence matter in the Cold War?[5] In 2009, it was the subject of the annual workshop of the Oxford Intelligence Group at Nuffield College. *Intelligence in the Cold War* presents the papers delivered at that conference by seven scholars, some with direct experience in the field.[6] Beyond the central question, three subtopics were addressed: Did intelligence speak truth to power? Did governments listen? Did intelligence make the Cold War hotter or colder?

Aberystwyth University Professor Len Scott considers the questions as applied to the Able-Archer '83 exercise. Analyst John Prados examines them based on studies of the military balance. British intelligence analyst Peter Davies reports on estimating Soviet power by the Defence Intelligence Staff. Cambridge University Research Associate Julie Fedor surveys conspiracy theories in Soviet literature, with emphasis on "the mythical so-called Dulles Plan," (89ff.) which is seldom mentioned in Western literature. Bar-Ilan University Professor Shlomo Shpiro looks at KGB operations in Israel since 1948 and how they affected security issues. Oxford University professor and former GCHQ analyst Michael Herman sums up the topic.

Not all the papers examine the subtopics directly. Most, however, agree that despite estimating errors, the technical accomplishments of the intelligence agencies made a difference when it came to monitoring nuclear arms agreements and in some other areas. When it came to the adversary's intentions, however, the authors' judgments were expressed with fortune-cookie ambiguity, a result that may be the best that can be expected.

This is a very valuable collection of views that should remind intelligence officers that "What Difference Does It Make?' is a question worth serious consideration.

---

[4] John Sheardown died on 30 December 2012. His role was widely recognized in obituaries published throughout the United States, Canada, and the United Kingdom. See, for example, Douglas Martin, "John Sheardown, Canadian Who Sheltered Americans in Tehran, Dies at 88," *New York Times,* 4 January 2013.

[5] Michael Herman, J. Kenneth McDonald, and Vojtech Mastny, *Did Intelligence Matter in the Cold War?* (Norwegian Institute for Defence Studies, 2006).

[6] The papers presented in this volume first appeared in the journal *Intelligence and National Security* 26, No. 6 (2011).

The Rice Paddy Navy: U. S. Sailors Undercover in China—Espionage and Sabotage Behind Enemy Lines During World War II, by Linda Kush (Osprey Publishing, 2012), 294 pp., endnotes, bibliography, photos, index.

The Rice Paddy Navy tells the story of an unusual US Navy intelligence unit, the Sino-American Cooperative Organization (SACO), and its operations in China during much of WW II. Two other books have been written about SACO, both by former members of the unit.[7] The first, *SACO—The Rice Paddy Navy,* appeared in 1950. The second was by SACO's commander, Captain (later Admiral) Milton 'Mary' Miles, who was always known by the nickname given him by his Naval Academy classmates in honor of the silent movie star Mary Miles Minter. Author Linda Kush provides a more substantial view.

By the end of the war, SACO had a complement of 2,500 US servicemen—Navy, Marines, Army—as well as 97,000 Chinese guerrillas and 20,000 pirates. Kush explains SACO's origins and mission, interservice rivalries, tension with OSS, its relationship with the not always cooperative Chinese, and what its members tried to do.

SACO's nominal mission was to provide weather data for the Pacific Fleet, to monitor Japanese ship movements along the China coast, and to assess potential landing sites for an eventual Japanese invasion. On his own initiative, Miles also conducted some sabotage and "secret operations." (253) The Army objected that since SACO's mission involved land operations, it should have been assigned to the Army. But General Joseph Stilwell, the commander of the China-Burma theater, liked Miles. Furthermore, Miles had served in China, spoke the language, and had established a working relationship with the ruthless head of nationalist Chinese intelligence, Tai Li.[8] The OSS had been denied the right to operate in the Pacific Theater under MacArthur's command. OSS head William Donovan decided to establish a presence in China and persuaded US Chief of Staff General Marshall to also make Miles head of OSS China, which Kush sometimes calls the Office of Special Services in China.

Kush describes how poorly these arrangements worked in practice. Miles continually fought with the OSS, and those ties were soon severed. The OSS, a source of money and supplies for the Chinese, nevertheless expanded operations in the China-Burma theater, though Donovan had his own confrontations with Tai Li. SACO remained to work with the Chinese and accomplished its mission to a degree. In the end though, Miles was viewed by many "as a hostile renegade gone native." (254) Despised by the new theater Army commander, General Albert Wedemeyer, his authority eroded until SACO was disbanded when the war ended.

The Rice Paddy Navy is an interesting and balanced view of SACO, one of the most controversial military units in WW II.

Saul Steinberg: A Biography, by Deirdre Bair (Doubleday, 2012), 732 pp., endnotes, bibliography, photos, index.

In its early years, the *New Yorker* magazine did not have a table of contents, and loyal readers paged through each issue to see what was offered. Its unique cartoons soon became a popular feature. In 1942, Romanian artist Saul Steinberg joined the *New Yorker.* Except for a period of service during the war, he never left, and he went on to draw many of the journal's cartoons and 90 covers.

Steinberg was born in 1914. He studied philosophy at the University of Bucharest before going to Italy, where he earned a degree in architecture in 1940. When Italy passed anti-Semitic laws, he began a circuitous journey to the United States. With the help of Cornelius Vanderbilt and the *New Yorker*, Steinberg was granted resident alien status in the United States in 1942. While waiting to be drafted, Steinberg came to the attention of a friend of *New Yorker* editor Harold Ross, Colonel William

[7] Vice Admiral Milton E. Miles, USN, *A Different kind of War: The little known story of the Combined Guerrilla Forces Created in China by the U.S. Navy and the Chinese during World War II* (Doubleday & Company, Inc., 1967); Roy Olin Stratton, *SACO—The Rice Paddy Navy* (C. S. Palmer Publishing Co, 1950).

[8] See the extraordinary biography of Tai Li by Frederic Wakeman, *Spymaster: Dai Li and the Chinese Secret Service* (University of California Press, 2003) and Bob Bergin's review of the book in *Studies in Intelligence* 53, No. 1 (March 2009).

Donovan, who was searching for artists to serve in the Morale Operations Branch of the OSS.

Donovan sent a naval officer to interview Steinberg in New York. The officer's report lists Steinberg's principal strengths: he was fluent in Romanian and Italian, with good German and French; he had traveled widely; and he could draw. His weaknesses were equally dramatic. Steinberg's English was poor, and the doctors diagnosed a mild "psychoneurosis," a heart murmur, and heart disease. Plus, he was an alien, and his qualifications for a commission in the Navy were nil. Donovan was nonetheless interested, and had Steinberg "reexamined." On 19 February 1943, he became a citizen and an ensign in the US Navy.

In her engaging biography, author Deirdre Bair devotes two chapters to Steinberg's OSS service. He served first with the Sino-American Cooperative Organization in the Pacific under Admiral Milton Miles, who wrote him a glowing fitness report. (128) His job was to prepare drawings to convey allied propaganda to those who could not read English. Later he was assigned to an Army unit in Italy and served as an interpreter in the Psychological Warfare Branch. During his exit interview before returning to the states, Steinberg noted that "he found very little tangible value in the work he did as a morale officer…there is no way of measuring effectiveness." (127) But he added, he enjoyed his OSS experience.

Bair has provided a glimpse into the life of an OSS officer whose contribution, while not well known, is characteristic of OSS service.

Stalin's Secret Agents: The Subversion of Roosevelt's Government, by M. Stanton Evans and Herbert Romerstein (Simon & Schuster, Inc., 2012), 294 pp., endnotes, photos, index.

With the publication of *Spies*: *The Rise and Fall of the KGB in America*,[9] the claims of many authors that Soviet spies hadn't really existed, or, if they had it didn't really matter, were debunked with irrefutable evidence. What more was left to say? M. Stanton Evans and Herbert Romerstein hint at the answer, quoting Whittaker Chambers: "The power to influence policy has always been the purpose of Communist Party's infiltration. It was much more dangerous…and more difficult to prove than espionage." (8) While Chambers did not have access to material that supported his judgment, Evans and Romerstein have found documents in the heretofore unexamined papers of former secretary of state Edward Stettinius that, they argue, do just that. *Stalin's Secret Agents* states their case.

A principal focus of *Stalin's Secret Agents* is on the extraordinary influence exerted by Alger Hiss at the Yalta Conference in February 1945. Roosevelt's foreign policy advisor, Stettinius, had been secretary of state for only two months and often allowed Hiss to speak for him in the presence of the principals. The authors provide examples. One instance involved China policy, a topic Hiss later claimed he didn't address. Stettinius' diary—the page is reproduced in the book—shows that Hiss had indeed raised the question, encouraging "support for an agreement between the Comintern" and the anticommunist Chiang Kai-shek government. The official State Department record omitted the exchange. (43–44)

The authors discuss many other examples of known communist agents, for example Harry Dexter White and Lauchlin Currie, working to influence US policies. In one case, they describe a report written by OSS officer, Linn Farish—named as an Soviet agent in the Venona decrypts—that praised Tito and compared the Chinese communist movement to the "American revolution." Somehow the document found its way from OSS files to the White House and was shown to Stalin. (163–64)

Evans and Romerstein do not neglect espionage performed by Americans serving as Soviet agents. One example involved Duncan Lee, the OSS officer who supplied a list of suspected communists to the Soviets through Soviet agent Elizabeth Bentley. The list, heavily redacted in the Venona decrypts, is reproduced in full for the first time in this book.

---

[9] John Earl Haynes, Harvey Klehr, and Alexander Vassiliev, (Yale University Press, 2009).

Will *Stalin's Secret Agents* put to rest the view that Hiss and the other agents mentioned really acted in the best interests of the United States? Probably not. The actions of "agents of influence" will likely be interpreted by some as simply aiding an ally in the war. Evans and Romerstein have made that judgment much more difficult to support.

Historical–non-US

Empire of Secrets: British Intelligence, the Cold War and the Twilight of Empire, by Calder Walton (HarperCollins, 2013), 411 pp., endnotes, bibliography, photos, index.

After two world wars, imperial Britain no longer had the capacity to deal simultaneously with economic crisis at home, a growing Soviet threat, and rising independence movements in its colonies and protectorates. As the world watched, one former colony after another achieved nationhood in what appeared at the time to be a relatively orderly process. In *Empire of Secrets*, British historian Calder Walton reveals these events were anything but orderly, despite attempts by the UK's intelligence services to achieve that goal.

Walton's account focuses on the British Security Service (MI5), the agency responsible for imperial security and intelligence at home and in the colonies, but he includes the contributions of the Secret Intelligence Service (MI6), the SIGINT agency (GCHQ), military intelligence, and local Special Branch sections with arrest authority. He begins with the story of a bomb placed in a London Colonial Office restroom by an agent of the Stern Gang, an Israeli paramilitary organization fighting to get the British out of Palestine. The bomb was detected by chance and failed to go off because of a faulty timer. The contemporary echoes are obvious, and more will be found in later episodes in which insurgent elements competed for power throughout the empire.

Britain's period of decolonization involved counterinsurgency and counterterrorist operations in the Middle East, Africa, South Asia, and Latin America, and Walton deals with each in considerable detail. MI5 had personnel—some declared, some undercover—in nearly every country involved. In the immediate postwar era, combatting terrorism was its priority. MI5 failed in Palestine, where terrorism was a major contributor to the British withdrawal. (111) Later in Malaya, where dollar earnings exceeded the entire industrial output of Britain in 1948, the MI5 branch struggled against the communist-inspired insurgency. Years of jungle warfare followed and sometimes "interrogators tortured detainees" while recruiting double agents, a topic that Walton discusses at length. (188–97) Ultimately, he notes, the Malaya operations stabilized the local economy and was considered a qualified success.

Elsewhere, the results were mixed at best. MI5 stations in the African colonies trained indigenous security elements while monitoring sources of local political unrest and supporting American attempts to neutralize Soviet penetration operations. Here, too, the record shows occasional "shocking levels of violence" before the British withdrew. (286) In several cases, MI5 elements remained after independence to continue training, deal with security matters, and provide cryptographic equipment—thus allowing GCHQ to monitor local communications.

Most of the details Walton presents are based on recently released archival documents. When he turns his attention to Cold War counterintelligence, however, he is on less firm ground. For example, Roger Hollis was not "a wartime entrant to MI5" (68); he joined in 1938. Kim Philby was not the first head of Section IX; he succeeded John Curry. And Walton's claim that Anthony Blunt was named as a Soviet agent by Andrew Boyle in his book *The Climate of Treason: Five Who Spied for Russia* (1979) is inaccurate. For legal reasons, Boyle used the pseudonym Maurice for Blunt.[10] Finally, the

[10] Boyle did identify Blunt in the 1982 edition of *The Climate of Treason*, and Walton cites that edition in his bibliography, but he names the wrong publisher; it was Coronet-Hodder & Stoughton, not Hutchinson, which published the 19779 edition.

Soviet bug in the US Great Seal was discovered in the ambassador's residence, not the embassy—and in Moscow, not in London. (144).[11]

Empire of Secrets is an impressive work and reveals the role of Britain's intelligence services in decolonization. It offers many parallels for any country struggling to help new nations establish representative government where none existed before.

The Imperial Security State: British Colonial Knowledge and Empire-Building in Asia, by James Hevia. (Cambridge University Press, 2012), 304 pp., footnotes, bibliography, photos, maps, index.

If asked about the components of modern day intelligence, most people would be likely to think of recruiting and handling agents, SIGINT, satellites, cybersecurity, and analysts briefing policymakers. In *The Imperial Security State*, James Hevia, professor of international history at the University of Chicago, examines an earlier era, when intelligence informed the imperial state on different topics and in different ways. His focus is on the origins and evolution of British and Indian Army intelligence organizations in the so-called "Great Game" era in South Asia. His objective is to convey how both contributed to shaping contemporary Asia and modern intelligence practices.

Hevia begins by demolishing a familiar, if not cherished, metaphor: the term "Great Game." The "Anglo-Russian rivalry," he points out, was not the romantic adventure characterized by Kipling. During the 19th century, the British fought two bloody wars with Afghanistan, in addition to "repeated clashes on the Northwest Frontier of India." (9) He also makes a strong case that the term was not coined, as Peter Hopkirk and others have suggested, by Arthur Conolly shortly before his execution.[12] (10–11) It evolved as a metaphor as historians wrote about the era.

Early in the 19th century, intelligence needs concerned terrain, security of supply lines, and statistics about the enemy. Initially, the requirements were met by officers leading small groups to map terrain and collect data about people and conditions in regions they visited. Sometimes they were charged with negotiating agreements with local chieftains. By the late 1870s, the British army was responsible for providing intelligence for India's defense.

Hevia discusses the gradual reforms in intelligence organization, training, collection, and reporting that occurred and gives examples of their application in Afghanistan, India, and China. Espionage is not forgotten, and the need to weigh carefully information from spies is stressed. At the same time, he shows how local culture gradually became an important factor in collection and assessment.

In the chapter on the "uses of intelligence," Hevia describes a well-organized intelligence system whose products—route books, maps, intelligence reports, and area handbooks—were considered by leaders in India and London during planning and war games. Sometimes the conclusions drawn by different staff elements were not the same, and disputes arose. In one example, strength figures and other statistics were challenged, as was the failure to adequately address military capabilities. (155–56) In other instances, there were political disagreements and challenges from the press. Hevia deals at length with the impact both had on public opinion and military intelligence.

Many of the intelligence and geopolitical issues dealt with in *The Imperial Security State* have a contemporary resonance, and Hevia concludes with a discussion of the parallels for Britain and the United States. He also recognizes the new aspects of modern insurgency, including "social network analysis," which is an extension of the need for cultural awareness. (263) On this point, the book ends with an Afghan poem that shows another side of the culture. This book is thoroughly documented and will be of value to military historians, analysts, and contemporary critics alike.

[11] This incident has been widely discussed. For a summary and numerous sources of more information see http://en.wikipedia.org/wiki/Thing_(listening_device).

[12] Peter Hopkirk, *The Great Game: The Struggle for Empire in Central Asia* (Kodansha, 1992).

The Man Who Was George Smiley: The Life of John Bingham, by Michael Jago (Biteback Publishing, 2013), 308 pp., photos, index.

"There are currently two schools of thought about our Intelligence Services. One school is convinced that they are staffed by murderous, powerful, double-crossing cynics, the other that the taxpayer is supporting a collection of bumbling, broken-down lay-abouts."[13] And so began John Bingham's most famous book, *The Double Agent*, published in 1966. Bingham's comments, suggests author Michael Jago, were directed at his one-time protégé, John Le Carré for Le Carré's "brutally inhuman" characterization of MI5 and MI6 in *The Spy Who Came In From The Cold* (1963) and *The Looking Glass War* (1965). Accurate or not, Bingham continued, "They could do no good to either service…and only encourage the enemies of democracy." (191) Despite the harsh critique, Bingham's friendship with Le Carré "was not irreparably damaged." (193) *The Man Who Was George Smiley* explains how Bingham became Smiley.

When David Cornwell—Le Carré—joined MI5 in 1958, he found John Bingham leading a double life as a respected agent handler and a successful author writing under his true name. These unusual circumstances, Jago explains, were the one constant in Bingham's life. Born in 1908 into an aristocratic family—he would later become Lord Clanmorris—he watched his parents squander much of the family fortune. His public school education didn't lead to university, so he traveled to Europe to learn French and German, necessary qualifications for the Colonial Service. While there, he acquired both languages, a mistress, and a wife who was not in favor of service in the colonies. Through connections, he tried his hand at journalism, eventually becoming a successful but low-paid humor columnist. To add income, he joined the Royal Engineers. As war approached, Bingham decided to apply to MI5, though as Jago writes, he never told how he did it. He did reveal that he was interviewed by a legendary agent recruiter, Maxwell Knight, known as "M," who became a valued friend.

Guided by Knight during the war, Bingham did well. But he was only a reserve officer, and when the war ended, MI5 had no full-time positions. Thus he spent two years interrogating ex-Nazis and POWs in Europe before returning to London and journalism. But he wasn't happy, and in 1950, as the Cold War intensified and MI5 expanded, he contacted Knight. The extraordinary arrangement they worked out allowed Bingham to pursue a writing career and serve as a full-time agent handler. He had found his calling. Jago tells of one agent that Bingham ran successfully for 20 years. This was the John Bingham that Le Carré later acknowledged served as a model for George Smiley. Others argued that Smiley was based on MI6 officer Maurice Oldfield, an allegation Le Carré vehemently denied and, for reasons not explained, Jago does not mention.[14]

Bingham's wife, Madeleine—she also worked for MI5 and was herself a writer—knew Le Carré well and always insisted her husband was the sole model. But, as Jago notes, Smiley possessed qualities that Bingham did not. The added qualities were supplied, he suggests, by the Rev. Vivian Green, whom Le Carré had known at Oxford.[15] (251)

The Man Who Was George Smiley reveals that Bingham performed occasional tasks for MI5 after he retired in 1979, while still pursuing a writing career that turned out to be less successful than it was in his early years. After a slow decline into dementia, Bingham died in 1988.

This is a very interesting account of an unusual man, and it provides a link between espionage fiction and reality.

[13] John Bingham, *The Double Agent* (Victor Gollancz, 1966), 5.
[14] Tod Hoffman, *Le Carré's Landscape* (McGill-Queen's University Press, 2001), 46–47. David Stafford suggests that David Cornwell himself was a convincing model for Smiley; see *The Silent Game: The Real World of Imaginary Spies* (Lester& Orpen Dennys Ltd., 1988), 198.
[15] Hoffman cites an article by George Plimpton in the *Paris Review* 39 (1997), which quotes Le Carré as agreeing that Green also served as a model for Smiley.

Spying for the People: Mao's Secret Agents, 1949–1967, by Michael Schoenhals (Cambridge University Press, 2013), 266 pp., footnotes, index.

Michael Schoenhals is a professor of Chinese studies at Lund University, Sweden. As he was conducting research on Chinese society, it became obvious to him that the "Maoist surveillance state" was a part of everyday life in China. Moreover, he concluded, it was a topic long "underexploited" by historians.

Schoenhals eventually solved the daunting problem of finding sources in ways only possible in post-Mao China. He found materials from "the official CCP's declassification regime" and "primary data…once intended exclusively for in-house consumption" in various university libraries throughout the world. Then there were the "chance discoveries in flea markets and backrooms of antiquarian bookshops in urban China of archival material." One example was a "tattered copy of a 1957 book, *Lectures on the Subject of Agent Work*." (vii, 12) The outcome of this research is *Spying for the People*, a work that adds domestic security intelligence collection by citizen-agent informers to the existing history of China's Cultural Revolution.

The period of agent activity Schoenhals treats ends in December 1967 (only a little more than a year into the Cultural Revolution) because in that month, Mao ordered the Ministry of Public Security (MPS) to institute an "indefinite suspension of all operational use of agents…as well as the decommissioning of safehouses nationwide…[and persons] who [in the trite-sounding translation of the minister's words] had 'done any bad stuff.'"(1) This extraordinary move applied only to the government's own domestic agents, who monitored mainly urban Chinese civilians and foreigners in the country. *Spying for the People* focuses on the purpose of domestic agents—as provocateurs and collectors—as well as the system's command structure, duties, technical capabilities, and historical context.

Readers will find echoes of Stalin-era methods in the performance of officers of the MPS, whose training included and dealt with ethical issues—"no sex please" (101)—in addition to agent handling, and political circumstances. Schoenhals identifies three types or categories of agents used by the MPS during 1949–67. One typed served as spotters or "informers." The second, called "enablers," or case agents, might investigate or penetrate targets. The third, "guardians" performed CI functions primarily, at important institutions. The assignment of agent targets was done by dividing areas into geographic or functional sectors. An example of the latter was the national railroad grid, said to have required "10,000 agents," though records are not precise. Operations of this magnitude posed significant administrative problems for the MPS and its supervising officers in terms of control—including corruption, payments to sources, debriefings, and "orderly termination" of sources or cases. (231)

In a postscript to *Spying for the People*, Schoenhals questions the meaning of it all. Beyond dealing with foreign spies, what did the PRC accomplish with its blanket domestic espionage? Even Mao, before the agent program was shut down, expressed a wish to see the public and legal sectors "beaten to a pulp." (234) In the end, Schoenhals concludes only that he has documented that the system existed legally, and the lessons yet to be learned will be part of Mao's legacy. This is an extraordinarily fine work of historical scholarship on a topic about which little had been known.

Under Every Leaf: How Britain Played the Greater Game from Afghanistan to Africa, by William Beaver (Biteback Publishing, 2012), 341 pp., endnotes, bibliography, photos, index.

It February 1855, the British Secretary for War created the Topographical and Statistical Department, subsequently renamed the Intelligence Department (ID). It was staffed by specially selected military officers and made answerable, over the outraged objections of army generals, to War Department civilians. Its mission was to furnish analyzed intelligence directly to the department, bypassing senior generals, if necessary. The secretary could do this because he controlled the military's purse strings. The ID had a very impressive record and became a part of the newly created General Staff before WW I. The ID's story, based mainly on memoirs and letters, has been summarized in several intelligence histories.[16] Working with new material found in the British

National Archives, Oxford historian William Beaver provides the first complete account in *Under Every Leaf*.

The title of the book is taken from a Farsi expression that reflects the pervasiveness of Victorian empire: "Anywhere in the world that a leaf moves, underneath you will find an Englishman." (7) Managing the empire fell to the War Office, and that required intelligence. The ID was created to provide it in finished form, unprejudiced by military biases. One example of how the ID worked in practice concerned the "Great Game" in the mid-1880s. The generals in India foresaw a major threat from Russia on the northern frontier and proposed moves to thwart it. The ID was tasked to assess the situation and concluded a "Russian attack on India would be so difficult as to be unlikely…[and] well nigh impossible." (56) The Army turned its attention to Afghanistan and was supported by the ID with maps and other essential data.

The ID did more than make assessments. It established its own agent networks, a library, and a print plant. The presses were a source of real power, allowing the ID to produce its own reports and maps. But the ID's reports were not heeded. When war loomed in South Africa, ID warnings of upcoming trouble with the Boers were ignored. (278)

The ID's capabilities were not acquired quickly or without difficulty, and much of the book is devoted to the incessant bureaucratic battles with the Horse Guards and key figures on both sides. The principal lesson from the ID experience is that intelligence without organizational parochialism is critical to sound government policy. This view may sound commonplace today, but *Under Every Leaf* shows it was not always so.

Women of Intelligence: Winning the Second World War with Air Photos, by Christine Halsall (The History Press, 2012), 192 pp., endnotes, bibliography, photos, index.

There were no photo interpreters (PIs) in the US Navy in early 1941. When the US naval attaché in London learned of the extensive British capabilities in this area, he arranged for LCDR (later admiral) Robert Quackenbush to come over and observe the British PI program. He returned three months later and established the Naval School of Photographic Interpretation in the Anacostia neighborhood of Washington, DC. His model was the British program at RAF Medmenham. *Women of Intelligence* tells the story of Medmenham and the allied personnel—men and women—that made the British effort a success.

Author Christine Halsall, BBC consultant and curator of today's Medmenham collection of photographs, used archival records and interviews to document her story. She chose the book's title to emphasize the precedent-setting role that women played during WW II as PIs, target plotters and analysts. She quotes one former female PI as recalling, "I do not remember any tinge of the 'old boy network' at Wembley [the first location for PI work] or Medmenham...man or woman it didn't matter." (20) Sometimes this was hard for the Americans eventually assigned there to accept, but they adjusted.

But it wasn't that way in the beginning, when women were hired as clerks and secretaries, regardless of their qualifications. The story of their rapid transition to equal-status PIs and managers is a major theme of the book. Ability was the key. Prior experience was not a major consideration. There were actresses—and one male actor Dirk Bogarde—university graduates, draftees, former MI5 officers, journalists, photographers, balloonists and pilots. At least one, Sarah Churchill, had political connections. Getting through introductory training was all that mattered.

Women PIs did the preparatory terrain analysis for Operation TORCH, the amphibious landing in North Africa; Operation HUSKY, the invasion of Sicily; and OVERLORD, the D-Day invasion. Perhaps the best known PI was Flight Officer Constance Babington-Smith, who headed the team that found the V2—quickly labeled *Doodlebug*—launching sites. PIs were also

---

[16] Sir George Aston, *Secret Service* (Faber & Faber, 1930); B.A.H. Parritt, *The Intelligencers: The Story of British Military Intelligence up to 1914* (Intelligence Corps Assoc., 1983); Thomas G. Fergusson, *British Military Intelligence 1870–1914: The Development of a Modern Intelligence Organization* (University Publications of America, 1984).

crucial to bomb damage assessment, the results of which caused controversy when PI results contradicted initial pilot reports.

Halsall also provides background and insights into the personal lives of many of the PIs. Some married while at Medmenham. Nearly all disliked the government-issue stockings. And from time to time there was interservice rivalry and a struggle to get preferred assignments—women PIs eventually served in all war zones.

Women Of Intelligence tells an inspiring story of accomplishment, where the job came first and doing it well was everyone's objective.

Intelligence Abroad

India's Spy Agencies: Shaken Not Stirred, by Lt. Col. Sunil S. Parihar (Manas Publications, 2012), 235 pp., endnotes, index.

After graduating from the Indian Military Academy, Sunil Parihar served in the infantry and in a number of intelligence assignments. *India's Spy Agencies* expresses his concerns about the performance of India's intelligence services and how they compare to similar agencies in other nations.

Pakistan's 1999 surprise invasion of Kargil—India's Pearl Harbor—in the Kashmir region, is the focus of Parihar's concerns. A postinvasion study of the operation listed numerous failures by the Indian army and the intelligence agencies. (60) Parihar reviews the organization and track record of each of India's services with regard to Kargil and other operations in which they have been involved. He includes a discussion of the CIA and Pakistan's ISI and some of their failures in order to demonstrate that India is not the only service to experience such difficulties. This is followed by a discussion of "what ails India's spy machine," (83ff.) with separate chapters on "dirty tricks," the role of analysis, and suggestions for reform.

A chapter lists the "top ten spy agencies" (149ff.) in the world, in reverse order—Pakistan's ISI comes out on top, the CIA is fourth—followed by a listing, by title, of the "world's major intelligence agencies" (161ff.). The final chapter is a timeline for 2011 that summarizes significant intelligence events in India for that year.

India's Spy Agencies is a somewhat disjointed account of an important topic by a firsthand participant.

❖ ❖ ❖


CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA


UNITED STATES INTELLIGENCE COMMUNITY
VIRTUS
COLLABORATION
FIDES