Chapter Eleven

ASSESSING MILITARY INFORMATION SYSTEMS

Stuart H. Starr

The assessment of military information systems is an art form that has evolved substantially since the mid-1970s.[1] Until then, national security assessments generally neglected information system issues. Such systems were either assumed to be "perfect" (i.e., providing perfect information with no time delays), capable of no more than second- or third-order effects, or totally irrelevant. When they were considered, they were often treated as a "patch"—something introduced into force-on-force calculations to reflect imperfect information systems.

This chapter begins with a historical perspective on how military information systems assessment evolved. It describes the change that took place 25 years ago, which entailed a basic reengineering of the assessment process, one that involved integrating leadership, institutions, people, processes, resources, tools, research and development (R&D), and products. An initial period of innovative assessments of military information systems was followed by a hiatus in the 1980s as Department of Defense (DoD) leadership lost interest in analyzing information systems. "Paralysis through analysis" was an oft-heard criticism in the Pentagon. Budgets for military systems, including military information systems, were at historically high levels, and the Pentagon's emphasis was on acquiring military information systems, not assessing them.

[1] Stated more precisely, this would read "information systems in support of military operations, including systems owned and operated by nonmilitary organizations." These include command and control centers, communications, sensors, and ancillary systems (e.g., navigation).

The chapter then addresses how this attitude shifted in the early 1990s, thanks in large part to profound changes in the international scene. The Soviet Union dissolved and the Persian Gulf War provided an insight into how innovative military information systems could support contemporary warfare. Thus emerged new challenges in assessing military information systems, and hence a new information assessment process. The chapter then moves to the key principles and insights related to the assessment of information systems in the context of conventional conflict. These insights are encapsulated in the 1999 *NATO Code of Best Practice for Command and Control Assessment*,[2] a product of six years of deliberations by nine NATO nations.

The chapter concludes by summarizing the advances made in the art of assessing military information systems since the mid-1970s, and then turning to the challenges that remain, such as the development and implementation of novel assessment tools and the treatment of emerging "new world disorder" missions (i.e., coercive operations using a mix of diplomatic, informational, economic, and military resources to convince an adversary to withdraw military forces from a neighbor), and peacekeeping, homeland defense, counterterrorism, counter-weapons of mass destruction (WMD), and information operations.

HISTORICAL PERSPECTIVE

Figure 11.1 summarizes the factors that fundamentally changed how military information systems were assessed from 1975 to 1985. Key civilian and military leaders in the defense community—Robert Hermann (then assistant secretary of the Air Force for Research, Development, and Acquisition), Harry Van Trees (then principal deputy assistant secretary of defense for Command, Control, Communications, and Intelligence), Charles Zraket (then executive vice president, MITRE), and MG Jasper Welch (then director, Air Force Studies and Analyses), and others—launched a search for the "Holy Grail,"

---

[2] *NATO Code of Best Practice (COBP) on the Assessment of C2,* Research & Technology Organisation (RTO) Technical Report 9, AC/323(SAS)TP/4, Communication Group, Inc., Hull, Quebec, March 1999. (Text also available at http://www.dodccrp.org/nato_supp/nato.htm.)

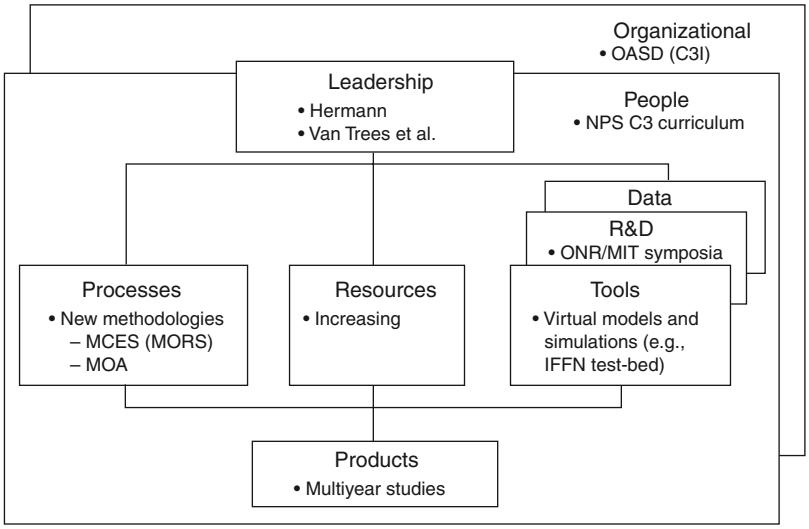

Figure 11.1—A Business Process Reengineering Perspective of Information Assessment (1975–1985)

i.e., for the ability to assess the impact of C2 systems on force effectiveness.[3] They acted out of intellectual curiosity, but also because of their emerging awareness of the importance of military information systems in modern warfare and their need to justify budgets for military information systems to a skeptical Congress.

This initiative was helped by the creation of the office of the assistant secretary of defense (OASD) for command, control, communications, and intelligence (C3I), an action that brought together the disparate DoD organizations responsible for C2, communications, intelligence, and defense support systems (e.g., electronic warfare, navigation). The contemporary establishment of a C3 curriculum by the Naval

[3]Major General Jasper A. Welch, Jr., "Command and Control Simulation—A Common Thread," keynote address, *AGARD Conference Proceedings*, No. 268 ("Modeling and Simulation of Avionics Systems and Command, Control and Communications Systems"), Paris, France, October 15–19, 1979; and OSD, with the cooperation of MITRE Corporation, C3 Division, *Proceedings for Quantitative Assessment of Utility of Command and Control Systems*, National Defense University, Washington, DC, January 1980.

Postgraduate School (NPS) helped create the human capital needed to assess military information systems. Finally, the Office of Naval Research (ONR) established a multiyear program with the Massachusetts Institute of Technology (MIT) to pursue R&D on information system assessment; the principals were innovators in the field of optimal control systems. Although the optimal control paradigm proved to have only limited applicability to the major issues associated with information systems, it helped address a key subset of them (e.g., the multisensor, multitarget fusion problem). The program built a vibrant community of interest that acquired a shared understanding of the problem.

Several new methods for assessing information systems consequently emerged. Workshops sponsored by the Military Operations Research Society (MORS) spawned the Modular Command and Control Evaluation Structure (MCES), a framework for defining and evaluating measures of merit for assessing information systems.[4] This framework was subsequently adapted and extended by the NATO COBP (see below).

In the mid-1980s, the "mission oriented approach" (MOA) to C2 assessment was developed and applied; its key phases are summarized in Figure 11.2.[5] The approach addresses four questions:[6]

1. What are you trying to achieve operationally?
2. How are you trying to achieve the operational mission?
3. What technical capability is needed to support the operational mission?
4. How is the technical job to be accomplished?

---

[4]Ricki Sweet et al., *The Modular Command and Control Evaluation Structure (MCES): Applications of and Expansion to C3 Architectural Evaluation*, Naval Postgraduate School, September 1986; and Ricki Sweet, Morton Metersky, and Michael Sovereign, *Command and Control Evaluation Workshop* (revised June 1986), MORS C2 MOE Workshop, Naval Postgraduate School, January 1985.

[5]David T. Signori, Jr., and Stuart H. Starr, "The Mission Oriented Approach to NATO C2 Planning," *SIGNAL*, September 1987, pp. 119–127.

[6]The questions are posed from the perspective of the friendly coalition, which subsumes operational users, military information systems architects and developers, and the science and technology community.

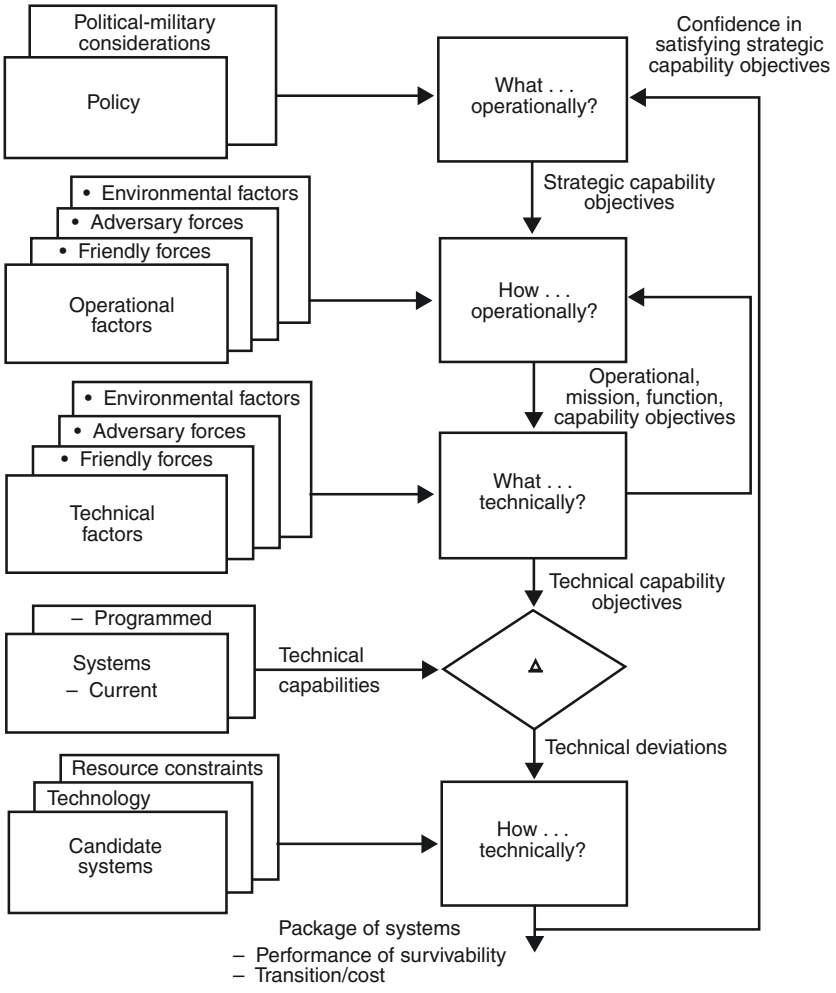

Figure 11.2—Phases of the Mission Oriented Approach

The MOA drove home the importance of assessing military information systems within the context of the missions they support. The process is implemented through top-down decomposition linking missions, functions, tasks, and systems. The "roll-up" process—in which analysts assess how candidate packages of military information systems satisfy mission objectives—remains a challenge.

One challenge of the roll-up process is understanding the performance of distributed teams of operational users under stress. To address this issue, manned simulator test-beds were developed to represent the specific weapons systems and military information systems supporting selected missions. An early example, the Theater Air Command and Control Simulation Facility (TACCSF) (originally, the Identification Friend Foe or Neutral [IFFN] test-bed), brought together teams of operators manning simulated weapons systems (e.g., airborne interceptors, high- to medium-range air defense systems) and associated military information systems (e.g., Airborne Warning and Control System [AWACS], associated ground-based C2 systems).[7] Such test-beds can flexibly assess a full range of doctrine, organization, training, materiel, leadership and education, personnel, and facilities issues associated with proposed systems-of-systems. (This combination of factors is characterized in *Joint Vision 2020*[8] by the infelicitous initialism "DOTML-PF".) Recent advances in computer science—e.g., the High Level Architecture (HLA)—have greatly helped such virtual simulations emerge and evolve.

New studies drew on these methods and tools to provide logical, systematic links between packages of military information systems and overall mission effectiveness. An early example of these products was developed as part of the NATO C3 Pilot Program in support of the Tri-Major NATO Commanders C3 Master Plan.[9]

CONTEXT FOR ASSESSING MILITARY INFORMATION SYSTEMS IN THE 21st CENTURY

Table 11.1 highlights some dramatic shifts that have occurred since the end of the Cold War. As is now commonplace to observe, the Soviet Union provided a sustained focus for intelligence gatherers and force planners during the Cold War. A few scenarios and types of

---

[7]J. E. Freeman and S. H. Starr, "Use of Simulation in the Evaluation of the IFFN Process," Paper 25, *AGARD Conference Proceedings*, No. 268 ("Modeling and Simulation of Avionics Systems and C3 Systems"), Paris, France, October 15–19, 1979.

[8]*Joint Vision 2020*, Chairman of the Joint Chiefs of Staff, Director for Strategic Plans and Policy, J5, Strategy Division, U.S. Government Printing Office, Washington, DC, June 2000.

[9]K. T. Hoegberg, "Toward a NATO C3 Master Plan," *SIGNAL*, October 1985.

Table 11.1

A New DoD Context

Area	Old	New
Threat	Relatively well-understood	New, uncertain
Missions	Established scenarios and operations	Broader range
Focus	DoD, alliance	National, coalition
Capability	Evolutionary	Revolutionary
Force	Overwhelming	Information/effects-based
Advantage	System-on-system	System-of-systems
Requirements	Relatively well-defined	Exploration/learning

operations sufficed for assessment and planning. Today's broader range of uncertain threats has made it difficult to anticipate issues and focus intelligence resources appropriately. The United States faces a variety of "new world disorder" missions, as well as the more conventional military missions (e.g., smaller-scale contingencies and major theater wars [MTWs]).

Alliances aside, DoD used to concern itself mainly with operations that involved only the U.S. military. Today's operations usually involve many other participants, such as ad hoc coalitions, various national government organizations, international organizations, and nongovernmental organizations (NGOs). Hitherto, warfighting capability evolved incrementally with the addition of each new weapons system. Now, information technology and precision weaponry may well change the nature of warfare in revolutionary ways.

Previously, success was thought to be determined by who could bring to bear overwhelming force. Today, the U.S. goal is to gather and exploit information about its adversaries so as to be able to apply the minimum force needed to achieve a specific effect, consistent with national policy. This force often transcends purely military action to include diplomatic, informational, and economic means. Advantage used to be measured in platform-centric terms—who had the best tank, ship, or plane. Today, networking sensors, C2, and weapons in a system-of-systems promise significant advantage through increased agility and more-discriminate application of force.

Finally, the stable, evolutionary environment of relatively well understood requirements has yielded to a period of experimentation and learning directed at understanding how to exploit new technologies and new concepts for competitive advantage. All told, such shifts mean a fundamentally different national security context for today's analysts, especially for those who assess information systems that play a newly critical role in force transformation. Table 11.2 highlights some of the key changes.

Analysts once could focus on ways to counter a specific threat; today, they must address capabilities that can be used in an agile manner to deal with a range of threats.[10] The stability of the threat and the evolutionary nature of military capability once permitted analysts to focus on refining established operational concepts and capabilities; today, they must explore completely new warfighting concepts, such as distributed C2 for a nonlinear battlespace. Cold War analysts could focus on the benefits of adding a new weapons system to the force mix; today's analysts must understand the fundamentals associated with networking the force or sharing information through a common relevant operational picture.

In the recent past, assessments focused on force mix/structure issues. Now, they must address *all* the elements of doctrine, organization, training, materiel, leadership and education, personnel, and

Table 11.2

New DoD Assessment Challenges

Area	Old	New
Planning	Threat-based	Capability-based
Focus	Refine established notions	Explore new possibilities
Objective	Identify benefits of incremental, new capabilities	Understand fundamentals
Assessment	Force structure	DOTML-PF
Issues	Ad hoc collection	Hierarchy of related issues
Complexity	Tractable	Exploding

[10]U.S. Department of Defense, *2001 Quadrennial Defense Review Report*, September 30, 2001, p. iv.

facilities (DOTML-PF). Whereas analysts used to concentrate on ad hoc issues arising in the programming and budgeting processes, they now must make systematic multilevel assessments of a comprehensive issue set.

Moreover, military information systems are themselves growing more complex. Table 11.3 highlights how emerging systems-of-systems and other integration proposals (e.g., the global information grid [GIG]) add further complexity. The challenge of assessing such systems reminds one of John Von Neumann's maxim: "A system is complex when it is easier to build than to describe mathematically."[11]

ADDITIONAL COMPLICATING AND SUPPORTING FACTORS

In assessing tomorrow's military information systems, additional factors must be considered: those that complicate the task (particular initiatives, especially by the services, and system trends) and those that can assist the analyst (such as new tools and new kinds of workshops).

Table 11.3

Simple Versus Complex Systems

Attributes	Simple Systems	Complex Systems
Number of elements	Few	Many
Interactions among elements	Few	Many
Attributes of elements	Predetermined	Not predetermined
Organization of interaction among elements	Tight	Loose
Laws governing behavior	Well-defined	Probabilistic
System evolves over time	No	Yes
Subsystems pursue their own goals	No	Yes
System affected by behavioral influences	No	Yes

SOURCE: R. Flood and M. Jackson, *Creative Problem Solving,* John Wiley, New York, 1991.

[11] J. Von Neumann, *Theory of Self-Replacing Automata,* University of Illinois Press, Urbana, IL, 1996.

Each service has undertaken activities to transform how it will operate.[12] The U.S. Army is transforming itself via the Stryker Brigade Combat Team (SBCT), the Future Combat System (FCS), and the Objective Force Warrior (OFW) to enhance deployability, sustainability, lethality, and survivability. These initiatives aim to dominate potential adversaries across the full conflict spectrum using information systems as the key force multiplier. The U.S. Air Force is creating an Expeditionary Aerospace Force, with enhanced responsiveness and global reach. These objectives are pursued through enhanced reach-back capability (e.g., using substantial resources in sanctuary to reduce the footprint in theater) and advanced collaboration tools (e.g., implementing the "virtual building" paradigm[13]). The U.S. Navy is pursuing the doctrine articulated in "Forward from the Sea," through the concept of network-centric warfare. Moving away from a platform-centric approach calls for the co-evolution of all the components of DOTML-PF (i.e., self-consistently modifying all aspects of the service's doctrine, organization, training, materiel, leadership and education, personnel, and facilities). A network-centric focus is promoted to enhance mission effectiveness through shared awareness and self-synchronization of the force. And, finally, the U.S. Marine Corps is using experimentation to refine "Marine Corps Strategy 21" through the innovative use of information systems to support small unit operations and urban warfare.

Information systems are perceived to be the key enablers for all these initiatives. From a joint perspective, the J-9 organization of Joint Forces Command (JFCOM) has an ambitious agenda to evaluate new joint concepts enabled by the revolution in information systems.

There is also growing interest in developing a joint, integrated information system infrastructure to underpin the operations of all missions. One aspect would be to design interoperability and security into the evolving systems-of-systems rather than treating them as add-ons. These initiatives include the Office of the Secretary of Defense (OSD)/Joint Staff efforts to have the GIG subsume the rele-

---

[12] *Service Visions*, available at http://www.dtic.mil/jv2020/jvsc.htm.

[13] Peter J. Spellman, Jane N. Mosier, Lucy M. Deus, and Jay A. Carlson, "Collaborative Virtual Workspace," *Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work: The Integration Challenge*, 1997, pp. 197–203.

vant service initiatives: the Air Force's Joint Battlespace Infosphere[14] and the Army's Tactical Infosphere.[15] The systemwide initiatives would exploit the power of Web-based architectures, commercial standards and protocols, and emerging information system markup languages based on the extensible markup language (XML).

However, many of the existing assessment tools for information systems are a poor fit for this class of systems, so several joint efforts are under way to develop better ones: the Joint Warfare System (JWARS) for joint assessment and the Joint Simulation System (JSIMS) for joint training. Although these tools seek to reflect information systems explicitly (and, in several cases, to interface with operational information systems), they are still immature and largely restrict themselves to the issues associated with conventional warfare.

Over the last decade, workshops—notably those by MORS—have advanced the understanding of challenges and opportunities associated with assessing military information systems. Recent MORS workshops have sought to identify the shortfalls in the community's ability to assess the impact of information systems[16] and to formulate a plan of action to ameliorate these shortfalls.[17]

NATO CODE OF BEST PRACTICE

In 1995, NATO established Research Study Group 19 to develop a code of best practice (COBP) for assessing C2 in conventional conflict; that COBP was issued under the newly formed NATO Studies, Analysis, and Simulations (SAS) panel.[18] A follow-up effort is extending the COBP to assess C2 for operations other than war (OOTWs).

---

[14]USAF Scientific Advisory Board, *Report on Building the Joint Battlespace Infosphere, Vol. 1: Summary,* SAB-TR-99-02, December 17, 1999.

[15]Army Science Board 2000 Summer Study, "Technical and Tactical Opportunities for Revolutionary Advances in Rapidly Deployable Joint Ground Forces in the 2015–2025 Era," Panel on Information Dominance, July 17–27, 2000.

[16]Russell F. Richards, "MORS Workshop on Analyzing C4ISR in 2010," *PHALANX,* Vol. 32, No. 2, June 1999, p. 10.

[17]Cy Staniec, Stuart Starr, and Charles Taylor, "MORS Workshop on Advancing C4ISR Assessment," *PHALANX,* Vol.34, No. 1, March 2001, pp. 29–33.

[18]*NATO Code of Best Practice on the Assessment of C2*.

Figure 11.3 portrays major elements of an effective assessment process for information systems that was identified in the NATO COBP. It highlights the major steps of the assessment and the products that should be developed in it. Despite the fact that the following discussion reflects this framework, however, it should be noted that meaningful assessments of information systems rarely follow such a linear process. Recent experience suggests that the way to best fit the problem at hand is to tailor and implement a nonlinear process that iterates among these steps.

Before the assessment process begins, the first issue is who will participate. Such undertakings generally require interdisciplinary teams of individuals skilled in operations research, modeling and simulation, information systems, and operations. Extensions of the COBP to OOTW also highlights the need to include those skilled in social sciences (e.g., political science and demography). Once a team is established, the process proceeds as follows, in line with Figure 11.3:

Problem Formulation. Military information system issues are complex, poorly defined, and hard to formulate sharply—especially when used in OOTWs, where cultural and historical context must be understood. Such issues are also hard to decompose into pieces that can be analyzed individually and then brought together coherently. Worse, posing options in strictly materiel terms is rarely acceptable. Issues associated with military transformation must address all the dimensions of DOTML-PF.

Human Factors and Organizational Issues. Information systems generally support distributed teams of people operating under stress; changing these systems often leads to altered tactics, techniques, procedures, and DOTML-PF—all of which must be considered in the assessment. These issues are often difficult to assess and are the subject of ongoing research efforts.[19] Factors such as belief (e.g., morale, unit cohesion), cognitive processes (e.g., naturalistic decisionmaking), and performance modulators (e.g., fear, fatigue, and sleep deprivation) are especially challenging to address.

---

[19]William G. Kemple et al., "Experimental Evaluation of Alternative and Adaptive Architectures in Command and Control," *Third International Symposium on Command and Control Research and Technology*, National Defense University, Fort McNair, Washington, DC, June 17–20, 1997, pp. 313–321.

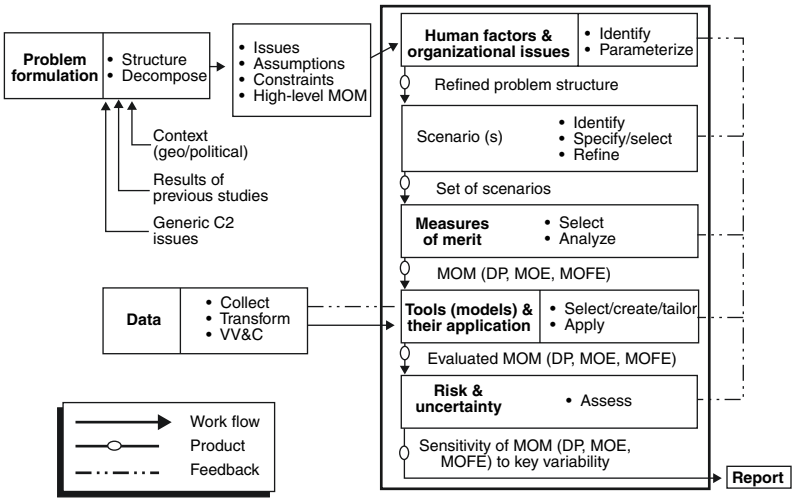

Figure 11.3—NATO COBP Assessment Methodology

Scenarios. The NATO COBP holds that military information systems can only be assessed relative to selected scenarios. Figure 11.4 identifies a scenario framework formulated in the NATO COBP; it is based on three major categories: external factors (e.g., political, military, and cultural situation), capabilities of actors (e.g., friendly forces, adversary forces, and noncombatants), and the environment (e.g., geography, terrain, and man-made structures). The challenge is to explore the scenario space rapidly and focus on its more "interesting" regions. Because military information systems are complex, looking at just one scenario is almost always a mistake. It is thus necessary to decompose the three major categories of the scenario framework, selecting a baseline scenario and interesting excursions.[20]

Measures of Merit. The NATO COBP states that no single measure exists by which the overall effectiveness or the performance of military information systems can be assessed. Drawing on prior MORS

[20]Stuart H. Starr, "Developing Scenarios to Support C3I Analyses," *Proceedings of the Cornwallis Group,* Pearson Peacekeeping Center, Nova Scotia, Canada, March 26–28, 1996.

External Factors	Political, military, and cultural situation	Mission objectives, mission constraints, rules of engagement	Mission tasks (e.g., military scope and intensity, joint/combined)
	National security interests		
Capabilities of Actors	• Organization, order of battle, C2, doctrine resources • Weapons, equipment • Logistics, skills, morale, etc.		
	Friendly forces	Adversary forces	Noncombatants
Environment	• Geography, region, terrain, accessibility, vegetation • Climate, weather • Civil infrastructure (e.g., transportation, telecommunications, energy generation/distribution)		

Figure 11.4—The Scenario Framework

workshops,[21] NATO recommended a multilevel hierarchy of measures of merit (MOMs), four levels of which are shown in Figure 11.5 and can be defined as follows:

- Measures of force effectiveness (MOFEs): how a force performs its mission (e.g., loss exchange ratios).
- Measures of C2 effectiveness (MOEs): impact of information systems within the operational context (e.g., the ability to generate a complete, accurate, timely common operating picture of the battlespace).
- Measures of C2 system performance (MOPs): performance of the internal system structure, characteristics, and behavior (e.g., timeliness, completeness, or accuracy).
- Dimensional parameters (DPs): properties or characteristics inherent in the information system itself (e.g., bandwidth).

Extending the NATO COBP to OOTW has demonstrated that the hierarchy of MOMs must be expanded to include measures of policy effectiveness. Since the military plays only a contributing role in such missions—ensuring that the environment is secure enough that

[21]Thomas J. Pawlowski III et al., *C3IEW Measures of Effectiveness Workshop*, Final Report, Military Operations Research Society (MORS), Fort Leavenworth, KS, October 20–23, 1993; and Sweet, Metersky, and Sovereign, "Command and Control Evaluation Workshop."

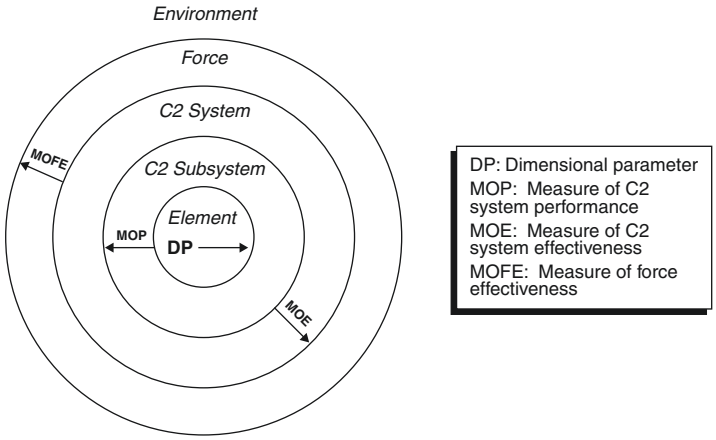

Figure 11.5—Relationships Among Classes of Measures of Merit

other organizations can function effectively—the contribution of international organizations and NGOs must be captured. Table 11.4 depicts representative MOMs for a hypothetical civil-military operations center (CMOC) that would provide the needed linkage between the military community and other organizations participating in the operation.

Historically, assessing what the MOMs at the top of the hierarchy implied for those measures at the bottom was a straightforward task. For instance, minimizing the leakage of incoming ballistic missiles creates a need for early warning to be extended and delays by military information systems to be minimized.[22] However, it is often more challenging to go "bottom-up" to estimate the effectiveness of mixes of weapons and information systems in the context of the operational scenario.

Data. At a MORS workshop in the late 1980s on simulation technology, Walt LaBerge, then principal deputy under secretary of defense (Research & Engineering), gave a presentation entitled "Without

[22]Signori and Starr, "The Mission Oriented Approach."

Table 11.4

Strawman MOMs for a Civil-Military Operations Center

Measures of policy effectiveness	Progress in transitioning from a failed state to a stable one (e.g., successful democratization and the ability to conduct a fair election; dealing with displaced persons and relocating displaced families)
Measures of force effectiveness	Ability of military to create and sustain a secure environment
Measures of C2 effectiveness	Quality of situational awareness and synchronization of effort
Measures of C2 performance	Ability to perform CMOC tasks and functions (e.g., time to complete a task)
Dimensional parameters	Communications (e.g., bandwidth and connectivity), automated data processing, support to personnel (e.g., quality and flexibility), collaboration tools (e.g., scalability, latency, and security)

Data We Are Nothing."[23] Unfortunately, the military's information system assessment community remains "data poor," despite repeated recommendations to establish a communitywide program to collect, transform, and verify, validate, and certify (VV&C) needed data. The problem is worse for OOTWs, because key information is controlled by NGOs (or even private corporations, such as insurance companies). Administratively, there is a need for a data dictionary/glossary at the outset of an assessment and a strategy for enhanced data management.

Tools and Their Application. Table 11.5 depicts a spectrum of assessment techniques. It discriminates among the various techniques by characterizing how they account for the systems, people, and operations/missions of interest. For example, in virtual modeling and simulation (M&S), real people are employed, interacting with simulated systems, in the context of a simulated operation. Conversely, in live M&S, real people are employed, interacting with real systems, in the context of a simulated operation. The COBP concluded that no

[23] *Proceedings of SIMTECH 97,* 1987–1988 (available through MORS office, Alexandria, VA).

Table 11.5

Spectrum of Assessment Techniques

	Assessment Techniques				
Key Factors	Analysis	Constructive M&S	Virtual M&S	Live M&S	Actual Operations
Typical application	Closed form, statistical	Force-on-force models; communications system models	Test-beds with humans in the loop	Command post exercises; field training exercises	After-action reports; lessons learned
Treatment of systems	Analytic	Simulated	Simulated	Real	Real
Treatment of people	Assumed or simulated	Assumed or simulated	Real	Real	Real
Treatment of operations/missions	Simulated	Simulated	Simulated	Real or simulated	Real
Resources	Relatively modest	Moderate to high	High to very high	Very high	Extremely high
Lead time to create	Weeks to months	Months to years	Years	Years	N/A
Lead time to use	Weeks to months	Weeks to months	Weeks to months	Weeks to months	N/A
Credibility	Fair to moderate	Moderate	Moderate to high	High	Very high

NOTE: M&S = modeling and simulation; N/A = not applicable.

single assessment technique would suffice for many issues of interest. A proper strategy must select and orchestrate a mix of techniques consistent with issues at hand and real-world constraints (e.g., resources, lead time). As concepts such as "information superiority" and "decision dominance" have gained interest, so has the need for tools to represent both friendly and adversary information processes. The need for discipline in applying these tools suggests that formal experimental design matrices should be employed to govern their application and support the generation of appropriate response

surfaces.[24] Fast-running tools can filter down to interesting segments of solution space, at which point fine-grained tools (e.g., virtual models and simulations) can provide more-focused, in-depth assessments.

Tools that have been formally verified, validated, and accredited are, of course, preferred, but few tools have undergone such stringent quality control processes. Confidence in results thus arises when independent assessments using varying tools nonetheless reach consistent findings. As an example, to provide an initial "cut" at a complex problem, analysts are beginning to develop and employ system dynamics models. These models (e.g., the C4ISR Analytic Performance Evaluation [CAPE] family of models[25]) evolve from influence diagrams that characterize factors such as model variables, inputs, outputs, and system parameters. They capture information system performance by explicitly representing sensors of interest, aggregate aspects of C3 (e.g., explicit constraints on communications capacity; time delays experienced by C2 nodes), and the phases of the intelligence cycle. CAPE was employed in OSD's C4ISR Mission Assessment to characterize the information systems that supported the engagement of time-critical targets.[26] Figure 11.6 depicts a representative output from CAPE characterizing the sensor-to-shooter string by estimating the probability of placing time-critical targets at risk as a function of target type (i.e., range and frequency of relocation).

Agent-based modeling represents another way to explore a solution space rapidly. It adopts a bottom-up approach to operations modeling by characterizing individual behavior (e.g., response to live or injured friendly or adversary entities; reaction to friendly or adversary objectives) and deriving emergent behavior from the resulting

---

[24]Starr, "Developing Scenarios."

[25]Jeremy S. Belldina, Henry A. Neimeier, Karen W. Pullen, and Richard C. Tepel, *An Application of the Dynamic C4ISR Analytic Performance Evaluation (CAPE) Model*, MITRE Technical Report 98W4, The MITRE Corporation, McLean, VA, December 1997.

[26]Russell F. Richards, Henry A. Neimeier, W. L. Hamm, and D. L. Alexander, "Analytical Modeling in Support of C4ISR Mission Assessment (CMA)," *Third International Symposium on Command and Control Research and Technology*, National Defense University, Fort McNair, Washington, DC, June 17–20, 1997, pp. 626–639.

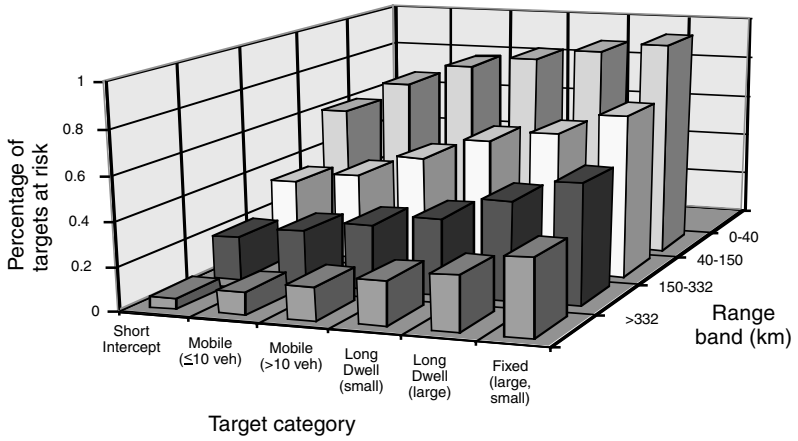

Figure 11.6—Representative CAPE Output: Targets at Risk

interactions.[27] Mana, a recent agent-based model developed by New Zealand's Defence Operational Support Establishment to prepare forces for peacekeeping operations in East Timor, has been employed to assess the risk to friendly personnel associated with alternative courses of action in OOTWs.[28]

Once the interesting parts of scenario space are identified, more-detailed simulations can explore them in greater depth. For example, to support the assessment of the time-critical target problem, the U.S. Defense Modeling and Simulation Organization (DMSO) developed Pegasus, a combination of three constructive simulations: the Extended Air Defense Simulation, Eagle, and the Navy Simulation System. JFCOM plans to use Pegasus and CAPE in its Model-Experiment-Model paradigm.

---

[27]Andrew Iiachinski, "Irreducible Semi-Autonomous Adaptive Combat (ISAAC): An Artificial-Life Approach to Land Combat," *MOR Journal*, Vol. 5, No. 3, 2000, pp. 29–46.

[28]Edward Brady and Stuart Starr, "Assessing C3I in Support of Dismounted Operations in Complex Terrain," *Proceedings of C2R&T Symposium*, NPS, Monterey, CA, June 11–13, 2002.

Other combinations are being developed that rely on virtual simulations to capture operators' response to a variety of stimuli. The Army is developing the Joint Virtual Battlespace (JVB) to assess and compare concepts proposed by contractors to implement the FCS, and the Air Force is developing the Joint Synthetic Battlespace to provide a context for acquiring a system-of-systems.

Risk and Uncertainty Assessment. The COBP notes that sensitivity analysis and risk assessment in C2 analyses often lack thoroughness because the issues are complex and the time and resources too limited. The need for and the results of sensitivity analyses should be stressed in discussions with decisionmakers. Analysts should at least test the robustness of the results against small excursions in the selected regions of scenario space. Ultimately, analysts must illuminate uncertainty, not suppress it.

Decisionmakers are also increasingly interested in getting risk-based instead of cost-benefit assessments. For example, the legislation mandating the 2001 Quadrennial Defense Review (QDR) specifically cast several questions in risk-based terms. This was echoed in the 2001 QDR itself, which introduced a new, broad approach to risk management.[29] The analysis community should also draw on the experience that financial planners and insurance actuaries have amassed in risk assessment.

This is the end of the process depicted in Figure 11.3. But, as discussed earlier, recent experience suggests that such a linear process rarely fits the needs of the situation. The last point is thus that an *iterative approach* is needed, since one pass through the assessment process is unlikely to generate meaningful answers. The first cut should be broad and shallow to identify key issues and relevant segments of scenario space, and subsequent iterations should then go narrower and deeper (drawing on suitable tools) to gain insight into key questions. Throughout this process, peer review is essential to provide adequate quality control.

---

[29] *2001 Quadrennial Defense Review Report*, Chapter VII, "Managing Risks," September 30, 2001.

ADVANCES OVER THE PAST 25 YEARS

Advances in the ability to assess military information systems are apparent in four areas. First and foremost, decisionmakers are now keenly aware that meaningful national security assessments require explicit consideration of military information systems. This awareness is apparent in recent products from the chairman of the Joint Chiefs of Staff, in which first "information superiority" and then "decision superiority" were placed at the foundation of DoD's strategic vision.[30] The easy, unknowing assumption that "information systems are perfect" is no longer acceptable.

Second, the processes for assessing military information systems have improved—a result of workshops (particularly those of MORS), individual studies (e.g., OSD's C4ISR Mission Assessment and Information Superiority Investment Strategy), and panels. Recent NATO panels have synthesized earlier efforts, promulgated COBPs, and identified the challenges associated with assessing military information systems in the context of "new world disorder" missions.

Third, considerable creativity has gone into developing new tools better suited to assessing information systems. Such advances have characterized system dynamics models (e.g., CAPE), agent-based modeling (e.g., Mana), constructive simulations (e.g., JWARS), federates of constructive simulations (e.g., Pegasus), and virtual simulations (e.g., JVB). The realization that no single tool or type of tool can adequately assess information systems has led to the creative orchestration of tools to exploit their strengths and compensate for their individual weaknesses.

Fourth, experiments that provide insights into the potential contribution of information systems to operational effectiveness are now deemed essential. New military information systems are recognized as a stimulus to new doctrine, organizations, training, leadership and education. These activities are the basis for acquiring the data and developing the models that the assessment community requires.

---

[30]See *Joint Vision 2010* and *Joint Vision 2020,* (both available at http://www.dtic.mil/jv2020).

RESIDUAL CHALLENGES: A NEW AGENDA

Despite all these advances, however, the assessment of military information systems is growing more difficult. Future missions will be much more varied than today's, yet there is great interest in an integrated system that would serve as the basis for all mission areas. And the information challenges are intermeshed with the broader transformation of the military. These changes have profound implications for the military's information system assessment community. A new agenda is needed, one with a more comprehensive analytic construct, new assessment capabilities, and a new culture/process for assessment.

A More Comprehensive Analytic Construct. The COBP makes a good start in describing how to assess a military information system. But DoD must extend it to deal with the full range of "new world disorder" missions. This will entail characterizing a broader range of scenarios, formulating new operational concepts, and deriving associated information needs. Consistent with the emerging interest in effects-based operations, the traditional hierarchy of measures of merit must be reevaluated, and new indications of operational success and failure will be needed. Finally, "soft factors," such as "sensemaking,"[31] must be represented better in community assessments.[32]

New Assessment Capabilities. DoD has historically placed great emphasis on the use of a single simulation to support major institutional decisionmaking processes (e.g., the use of TACWAR in the 1997 QDR). This is a Cold War artifact, one that is inadequate for meeting contemporary assessment needs. There is a growing need to assemble a "tool chest" that can be tailored to address the major

---

[31]Sensemaking is a process at the individual, group, organizational, and cultural level that builds on a "deep understanding" of a situation in order to deal with that situation more effectively, through better judgments, decisions, and actions (Dennis K. Leedem, *Final Report of Sensemaking Symposium*, Command & Control Research Program, OASD(C3I), Washington, DC, October 23–25, 2001 [also available at www.dodccrp.org]).

[32]David S. Alberts, John J. Garstka, Richard E. Hayes, and David A. Signori, *Understanding Information Age Warfare*, CCRP Publication Series, August 2001, p. 141.

problems of interest responsively, flexibly, and creatively. This tool chest must include a mix of exploratory tools (e.g., seminar games, influence diagrams, system dynamics models, agent-based models) that are well suited to effects-based analysis and can be used to identify and explore interesting parts of scenario space quickly and efficiently. The tool chest should also include JWARS, DoD's most recent effort to reflect military information systems and processes in a constructive simulation.

However, a tool such as JWARS will have only a supporting role to play as assessments grow narrower and deeper and thus inevitably require new virtual and live models and simulations, particularly to capture the role of the human in complex systems-of-systems. One of the associated challenges facing DoD is the development of consistent, verified databases, data dictionaries, and glossaries to link the components of the tool chest and ensure they are mutually self-consistent. This new tool chest and associated concepts of assessment will require new education and training for the assessment community.

A New Culture and Processes for Assessment. Military information system analysis must embrace a new culture of openness and cooperation that features rigorous peer review, information sharing, and collaboration across traditional organizational boundaries. In the area of transformation, new offices are emerging to stimulate the process—e.g., OSD's Office of Force Transformation and JFCOM's Project Alpha. The military information analysis community has an important role to play in linking these new entities with the traditional organizations that have been pursuing transformation (e.g., the service planning staffs and test and evaluation organizations).

Finally, with the emergence of homeland security and counterterrorism as major mission areas, additional participants must join the assessment process. These include analysts from other federal agencies, such as the new Department of Homeland Security, as well as from regional, state, and local organizations. The military analysis community must recognize that these other participants come to the problem with different frameworks and vocabularies, limited analytic tools, and little or no experience in dealing with classified

information. It will take mutual education and training to forge these disparate entities into an integrated community capable of performing creative, insightful analyses of proposed information systems.