Synthetic Economies: The Application of Distributed Interactive Computing Environments for Policy and Management Decision Making

Richard White, IDA Project Manager
Alok Chaturvedi, Purdue Project Manager
Edward Smith, IDA
Robert Clover, IDA
Shailendra Mehta, Purdue
Chandrajit Bajaj, Purdue
PREFACE

This paper is the product of an internally funded IDA independent research project, looking at the application of distributed interactive simulation techniques to policy decision making, an approach we have termed "synthetic economies." In addition to this paper, the CRP was also used to host a joint IDA-Purdue Conference on Synthetic Economies, which included a demonstration policy game, at IDA on 23 and 24 July, 1997. An annotated briefing describing the policy game is contained in Appendix B; the proceedings from the conference are being produced under separate cover.

The authors would like to thank General Larry Welch, Dr. Robert Roberts, Mr. Michael Leonard, Mr. Thomas Christie, and Mr. Neal Cosby of IDA, and Drs. Dennis Weidenaar and Luis Proenza of Purdue for their continued interest in extending the application of distributed interactive simulation techniques beyond their origins in military wargaming. In addition, the authors would like to express their appreciation for the tireless support of Daniel Seals, Ian Rehmert, Wyatt Crossin and Marc Samuels of IDA, and Chris Foutz, Vidyanand Choudhary, Wei T. Yue, Steve Cutchin, and Martin Hillgrove of Purdue.
This paper explains how distributed, interactive computing can be used to assist decision makers to investigate alternative courses of action in complex, dynamic business and policy environments. The military’s use of computer-generated synthetic battlefields for training is the metaphor; the creation of synthetic economies within which to practice policy and management prerogatives is the goal. Exposition proceeds by example, while methodological excursions and underlying theory are provided in supporting appendices.

A. SETTING THE STAGE

For the past three years, Chris Foutz, the CEO of a large U.S.-based transnational, has deftly out-maneuvered his corporate adversaries. First expanding into Europe, then Asia, the company’s profits have risen sharply in the past two quarters due to strong sales and maturing technology investments. However, all is not bright. Along with greater international market exposure have come ancillary problems of operating in less-developed, non-western economies. Right now, however, his biggest problem is not poor roads, unreliable utilities, and corrupt officials. Right now, a terrorist group demanding better working conditions for local employees is making good on one of their threats. Right now, the corporate intranet is failing and the entire enterprise is coming to a screeching halt.

When the first ransom note threatening a cyber attack was received over a year earlier, Chris’s immediate reaction was to seek help from the U.S. government—to no avail. He was informed that while various agencies would be willing to give him some protection for domestic operations, outside American borders the company was on its own. As a result, Chris decided to bolster corporate information assurance beyond that provided through government programs by increasing his firm’s level of investment in computer security.

Making what he thought at the time was a rational trade-off between risk and cost, Chris opted to raise the overall security for his foreign and domestic operations to modest levels. The measures taken were intended to be commensurate with the risks that had been reported to him—primarily threat assessments he had received via government connections. He was told that the most sophisticated threats he would encounter would
be radical groups not yet capable of conducting serious information warfare-style attacks. For a year, it appeared that he had made the right choice in not going overboard. However, he did not count on attracting the interest of a state-backed terrorist cell.

Of course, the first attack did not come as a complete surprise. U.S. intelligence had informed him that, as one of their people dramatically put it, “there now exist[ed] a foreign-nation-backed information security threat of the highest order to foreign-based subsidiaries of U.S. transnationals that constituted a ‘clear and present danger’ to assets abroad.” Chris’ first reaction was that someone had been reading a little bit too much “Clancy.” Nevertheless, he took the threat seriously and again began to increase his computer security levels, this time investing an additional $20 million.

The first hint that his firm was under attack was subtle and seemingly innocuous. A second ransom demand was received that threatened to temporarily shut down his firm’s computers. Believing that his systems were safe due to recent improvements in security, Chris refused to pay the $2 million. He relied on a sort of perverse logic that the potential harm from a successful attack would somehow be of the same order of magnitude as the ransom demand. Again, as with the first ransom demand, nothing seemed to happen immediately. For a short while, he believed that he had beaten the odds. Nothing, however, could have prepared him for what was to come next.

When the cyber attack arrived, the idea that the consequences would be on par with the ransom demand proved tragically wrong. The terrorist group responsible for unleashing the assault used the most advanced techniques available to a nation-state engaged in an information war. It literally brought the company to a standstill. Based on potential down time, the estimates of total losses from eroded market share and foregone sales were projected at upwards of 17 percent of annual revenues. After three successive years of rapid growth, Chris’ firm was suddenly mired in deep financial trouble.

To their credit, the U.S. and host nation governments did their best to try to catch and punish the terrorists. However, because of only tenuous links and no hard evidence, the governments were reluctant to carry their insinuations too far. Who knew, perhaps the rogue state that had supported the terrorists was threatening to do harm to even more firms. All Chris knew was that the next time he played this game, he would pay much more attention to information assurance and not be lulled into a false sense of security by incomplete intelligence reports.

On to the afternoon session . . .
B. WHAT IS A SYNTHETIC ECONOMY?

The game that Chris played was the result of a close collaboration between the Krannert School of Management at Purdue University and the Institute for Defense Analyses (henceforth, the Purdue/IDA game). In fact, it is a computer-facilitated, distributed interactive simulation—a “synthetic economy”—so termed because the underlying rules are based upon economic principles to derive costs, benefits, and utilities from simultaneous player interactions. Similar to computerized wargames used by the military, this synthetic economy is a virtual framework that relates the actions of participants to one-another through a set of carefully crafted interdependencies customized to explore the confluence of business, policy, and national security issues.

In its most inclusive sense, a synthetic economy is an extension of the more general concept of synthetic environments. It is the application of computer-generated modeling techniques, here-to-fore used to render virtual realities (e.g., 3-D computer representations such as wire framing; rendering; texture, reflection, and environment mapping; ray tracing, and animation) to create virtual economies in which investigators may participate and conduct experiments. These economies are situation-specific and based upon mathematical rule-sets derived from theoretical and empirical work. As with current synthetic environments, extensions of the basic synthetic economy paradigm could ultimately take advantage of multi-sensory human interfaces such as data gloves, stereoscopic glasses, and data body suits to immerse the participant in a virtual economic world.

In recent times, many innovative applications of synthetic environments have emerged. For example, the Department of Defense uses synthetic environments for training, acquisition, mission planning, and wargaming; the Department of Energy is developing synthetic environments for simulating nuclear explosions; the aerospace industry has synthetic wind tunnels; the automotive industry is undertaking virtual prototyping; the healthcare industry is pursuing tele-medicine and surgical planning; and some currency and securities trading companies are now applying these techniques to visualize continually changing data in “real-time” to spot trends in currency and price movements.

The particular scenario in which Chris was involved was a multi-level game combining nation-states, transnational firms, and a terrorist organization. In many ways it was a game within a game. Governments and terrorists were engaged in attempting to
defend and attack, respectively, the transnational firms. The firms, in addition to defending themselves, sought to maximize profits and growth (see Figure 1).

![Figure 1: Interactions Among Participants](image)

Of course, the scope of this game could be expanded considerably by adding more players, computing power, and relationships. Many different, interrelated games could be played simultaneously, each representative of a particular tactical or strategic situation. Perhaps most important, however, is that this computing environment allows policymakers to explicitly address the economic dimensions of important issues along with their security and military implications. This means that unique incentives can be built into the games to reflect different circumstances and decision criteria.

C. HOW REALISTIC ARE SYNTHETIC ECONOMIES?

Frequently the question is asked, why an interactive simulation rather than an autonomous, pre-programmed simulation (e.g., system dynamics)? The answer is that, while a "hard-wired" simulation offers advantages of repeatability and, hence, some
semblance of rigor, interactive simulation offers unpredictability and uncertainty closely mimicking reality. The trade-off is one of intent, application, and flexibility. Interactive simulations can offer bounded solutions for complex problems where autonomous simulations degenerate or explode.

For analytical purposes where model structure, stochastic rigor, and tractability are desirable, more traditional approaches such as system dynamics or econometrics are most appropriate. However, when it becomes desirable to allow underlying relationships to "evolve" in ways not captured by extant data, interactive simulation or game playing is useful. Relatively new fields, such as "experimental economics," combine the attributes of both to yield interactive simulations where underlying structures are pre-programmed as the rules of play.

The basis for a policy game in which "extra-market" players are inserted into the synthetic economy is the creation of a rule set that models the costs, benefits, and utilities derivative from different courses of action. For instance, government players who are able to adjust tax rates, pass laws, impose regulations, and punish "rule breakers" can be included. This would be done by creating a rule set for government players that rewards or penalizes them for individual or overall "societal" outcomes resulting from their actions. Similarly, antagonists, such as terrorists, rogue nations, or cartels can be included by developing alternative rule sets that would affect other players directly through their bottom line, or indirectly through access to resources, production costs, access to technology, and so forth.

A good indication of the level of realism of synthetic economy games played so far is the degree of involvement by participants. Based upon our own observations, the level of engagement is intense. Players use every available minute of time to make deals, review corporate strategies, trade information, and consummate transactions. Some complain that the simulation can be too slow, response times to bids and offers in auctions are not sufficiently "real time," and that insufficient amounts of market information are available. Amusingly, these complaints about the unrealistic aspects of the simulation are the very types of problems faced by real businesses and governments.

Based upon the reaction of participants, the Purdue/IDA game is realistic in the sense that it provides role players with experiences analogous to those found in the worlds of business and government policy. That is, in the sense that virtual battlefield simulations are realistic representations of military engagements, interactive synthetic
economy gaming creates an environment that presents participants with problems similar to those that might be encountered in the marketplace as well as by government organizations. While it may be argued that the environment is not nearly as elegant or seamless as one might find in an actual business, or as rigorous as policy deliberations by public decision makers, the problems that confront the participants are characteristic of and similar in complexity to those found in such situations.

The scope of what can be gamed using a synthetic economy is therefore a function of our ability to conceive of ways to express relationships in economic terms—to develop appropriate rules and incentives. The level of realism is a function of the resources committed, the detail built into the system, and the length of play. Too much detail is distracting; too little and the game is devoid of context. Basic motivations and fundamental relationships must be present, but many of the ancillary features of the real world that would overwhelm players must be excluded. A "realistic" game is therefore one that encourages participants to use their imaginations and create alternative futures in real time within an atmosphere of learning.

D. EXTENSIONS

The quest for one single, overarching, economy-wide or global modeling framework has been pervasive in economics. The two primary approaches to date have been through the application of simultaneous equation systems methods in the fields of econometrics and computable general equilibrium models. Unfortunately, neither provides a complete description of economic reality. One major reason is that investigators feel compelled to create these models from scratch. While economic theories evolve cumulatively, economic models seem to evolve individually. What is needed is a modular approach, where researchers in different fields create a whole collection of sub-models in their individual areas of expertise, which then function together to replicate large parts of actual economies.

As we move into the next century, the effectiveness and viability of the U.S. business enterprise will depend upon our understanding of the complex and ever-changing international business environment. The research community, industry, and government do not currently have comprehensive access to the many advanced tools necessary to address these problems in an integrated way. Clearly, there is a need to develop a standards-based synthetic economy with fully integrated goods, labor, assets, bonds, and currency markets. Such a synthetic economy should be able to allow very
large numbers of individual agents, both real and artificial, to interact simultaneously and
continuously using information very similar to what would be encountered in the real
world. Human actors would be provided with sophisticated tools that would enable them
to improve their decision processes.

In addition to the business and government policy applications mentioned above,
the pursuit of a synthetic economic modeling and simulation framework could potentially
open up new avenues for research. For example, repeatable complex economic
interactions could lead to behavioral investigations that were previously impossible using
traditional empirical techniques. Extremely complex events could be instrumented,
simulated, and analyzed. Questions pertaining to the rationality of human players could
be addressed with renewed vigor and repeatability. Different sorts of rule-based trading
algorithms, including finite automata and neural networks, could be arrayed to perform
against human players under a variety of circumstances.

Using a synthetic economic framework we could begin to apply advances in
artificial intelligence and autonomous agents to address a variety of fundamental issues in
economic modeling and simulation. For instance, under what circumstances do different
kinds of artificial agents mimic the behavior of human beings very closely? Can one
separate the agents in an economy into different classes that may be adequately
represented by artificial agents? Can an artificial, agent-based economic simulation
replicate observed economic phenomena on a large scale? Can we begin to create
extensive, realistic economies which could run on a continuous basis and which could be
modified to answer the important questions of the day?

E. OPPORTUNITIES

Properly structured, the pursuit of synthetic economies should be able to provide a
constructive basis for exploring potential business, economic, and national security
outcomes across a broad spectrum of organizations. For instance:

- Department of Defense interest in economic and business simulations would
  likely come from efforts involved with industrial base issues such as dual-use,
  Title III, prime contractor consolidation, and technology investments/incentives.
  The opportunities here would be to play games that challenge the conventional
  wisdom of government decision makers to alert them of possible outcomes from
  policy changes. Other simulations could also be developed for more traditional
  strategic and tactical decision making purposes.
The intelligence community may have an interest in simulations that could help predict the responses of world leaders to economic sanctions, the proliferation of conventional and unconventional arms, and possibly the affects of government policies on drug trades.

Agencies such as the Department of Commerce and the Office of the U.S. Special Trade Representative might be interested for the purpose of developing international trading simulations involving both countries and transnational firms. These simulations might seek to resolve questions of national interest, the impacts of embargoes, or responses to changes in most favored nation status, to mention a few.

Assessments of infrastructure security and preparedness to defend against cyber or physical attacks could be conducted. This would involve the development of collaborative/competitive games functioning simultaneously at different levels of granularity, and would involve representatives of the national security, law enforcement, and civil sectors.

Because of their pedagogical dimension, synthetic economies should find a natural employment for training and education purposes. The Global War Game, conducted each summer by the U.S. Navy War College, could be hosted via a distributed, interactive simulation, the foundation of which would be a synthetic economy. Similar to wargaming, other games could be used to train senior decision makers, such as general officers, government executives, and program managers. There are even opportunities to use such games as a way to assess the impacts from government reorganizations.

There are likely to be many other applications and potential sponsors. To initiate a constructive dialog with interested parties in the public sector, IDA will need to do more than provide information briefings. Ideally, to convey potential synthetic economy applications, an in-house capability to periodically host a gaming session will be needed, because the full range of opportunities for the approach can only be understood through immersion in the gaming process itself.
Appendix A

A Short Note on Purdue’s SEAS
(Synthetic Economies for Analysis and Strategy)
The base synthetic economy developed at Purdue University contains three sectors: industrial producers, firms, and households. Each is initially endowed with resources (cash or income) and behavioral assumptions:

- Industrial producers and firms have cost functions and product lines.
- Households have utility functions and income endowments.

Industrial producers supply "raw materials" in the form of intermediate industrial products, which are used by firms to produce consumables. Consumables, in turn, are purchased by households from which they derive utility. Households are stratified, and provisions have been made for players to move between "classes."

Firms are able to issue stock, which may be purchased by anyone in the economy. Goods and services are also purchasable by anyone, but households are precluded from making sales (no secondary goods' or services' markets exist for households). In addition to goods, some firms have been established to provide consulting services that serve as surrogates for R&D, and therefore allow modification of production functions.

The model of the economy is not "closed" with respect to households; that is, it is not a circular system. Rather, it is open so that demand functions from households drive the demand for antecedent production.

The simulation is played as a competitive "game" among the students at the business school. To ensure that all are properly engaged and committed, results from the game are used to determine part of the semester's grade. While the relative scale of resources commanded by households, firms, and industrial consumers varies, the stakes are real.

Up to 60 separate teams of students have been engaged simultaneously, interacting and making decisions which are processed on an interdependent basis to give immediate results. Decisions include what to produce and/or purchase, whether or not to buy or sell stock, and how to maximize utility from consumption.
Appendix B

Transnationals, Governments, and Terrorists:
A Synthetic Economy Game
Transnationals, Governments, and Terrorists: A Synthetic Economy Game

Alok Chaturvedi, Shailendra Mehta, Chandrajit Bajaj
Richard White, Edward Smith

Purdue University and the Institute for Defense Analyses
July 24, 1997

At the July Conference on Synthetic Economies held at the Institute for Defense Analyses (IDA), a synthetic economy game combining transnational firms, governments, and terrorists was played by conference participants. The purpose of the game was to demonstrate the feasibility of combining quantitative and qualitative elements into a single, end-to-end distributed interactive simulation. The game was developed jointly by IDA and the Krannert School of Management at Purdue University, and was based upon Purdue’s Synthetic Economies for Analysis and Strategy (SEAS) simulation environment. IDA contributed to the national security and information warfare aspects of the game, while Purdue contributed elements dealing with economic and business environments and interactions.
A simplified representation of transnational interactions was used as a basis for the game. Five "countries," five "transnational firms," and one "terrorist organization" were constructed and employed in the gaming scenario.
Some of the types of interactions possible among the “players” included:

- Governments provided security to and collected taxes from transnational firms. They also engaged in intelligence gathering activities, invested in national security to prevent information warfare attacks, and could assist firms to recover from terrorist incidents.

- Transnational firms competed in the marketplace by producing and selling commodities, defended against terrorist attacks, and made investments in foreign countries.

- Terrorists perpetrated attacks on transnational firms and governments, and attempted to elude discovery by concealing their activities.
Each of the transnational firms began with an initial endowment of factors of production as well as cash. These resources were used to produce goods by investing in capital, and to create the opportunity to produce new types of goods through technology (R&D) investments. Factors of production considered but not included in the game were labor and education.

Governments focused on the protection of firms from terrorist attacks as well as the maximization of GDP and adjustment of tax rates. Terrorist incidents and foreign direct investment were not included as variables to be maximized by governments, although GDP did suffer as a result of successful terrorist attacks on domestically based firms.

For the scenario, factors such as interest rates and financial markets were not included so as to retain focus on information warfare and security issues. The game could be expanded to handle these and many other types of markets and non-market factors in the future.
To assist players in keeping track of the course of events unfolding during scenarios, a visualization was employed that showed each transaction (including terrorist attacks) in near real time. The following player icons were used:

**Green Icons = Governments**
- Big West = North America
- Europa = Europe
- Great East = Asia
- Badguysia = Rogue Nation
- Developiya = Developing Nations

**Red Icons = Transnational Firms**
- Megacorp = North American Firm
- Euro Ltd. = European Firm
- Kirebol = Asian Firm
- GL Inc. = Rogue Nation Firm
- HM LLC. = Developing Nation Firm

- PFLE = Terrorist Organization

For each of the player icons, the visualization also provided graphical (bar graph format) quantitative data. Such information was available to the respective players for their own organizations, as well as to rivals and governments willing to spend large amounts of monies on intelligence gathering activities.
Icons were employed in the visualization to show the types of transactions taking place. As a transaction occurred, it was rendered by the visualization as the icon moving along an arc from between the two parties to the transaction. In cases of successful terrorist attacks, the arrival of the attack icon (lit bomb) was followed by a large orange flash to depict an explosion.
Transnationals

Goal: Maximize end of game cash balance (revenues - costs)

Production
- Firms begin with assigned product lines, market shares, and prices
- A firm may compete in any market after its home government establishes an embassy in that market
- All 5 commodities may be produced and sold by a firm in any market once a core competency has been established through R&D product investments
- Entry barriers to markets exist (entry costs); there are no exit costs

Security
- Successful terrorist attacks affect firm bottom lines
- Firms may purchase security as a cost of doing business
- Government security efforts assist all firms within same-nation equally
- Sectoral dependencies exist so successful attacks in one sector affect other sectors to some degree
- The severity of terrorist attacks is carried as an impact on the bottom line and as a denial of service (access to the game)

Taxes
- Government taxes all firms in a nation at the same rate to provide for security
- Government allocates its infrastructure investments according to sectors

Each of the four types of players (transnationals, governments, rogue nation, and terrorists) had specific objective functions they attempted to maximize. These functions were kept simple to provide players with clear goals during the course of play. In the case of transnational firms, the primary goal was to maximize the end of game cash balance (revenues minus costs). In addition, firms had to consider production, security, and taxes as part of their play.
Mainstream Governments

Goal: Maximize end of game GDP (see below)

Production
- Make infrastructure investments to improve productivity of domestically based firms

Security
- Invest to raise overall level of national security
- Invest in intelligence to provide warning
- Invest in law enforcement to pursue perpetrators

Budgets
- Collect taxes to finance investments in security, intelligence, and law enforcement
- Run budget deficits or surpluses
- Tax revenues reduced as a result of successful terrorist attacks

GDP
- GDP is calculated as: (firm revenues + taxes - [intelligence + infrastructure + security + law enforcement])

The primary goal set for governments was to maximize end of game GDP. To keep the game simple, GDP was measured as the aggregate revenues of firms operating domestically plus taxes, less government expenditures. As a result, governments had an incentive to attract firms to produce within their borders, protect the firms, and make investments in infrastructures that would boost firm revenues.
Rogue Nation Government

Goal: Maximize end of game GDP + Damage (see below)

Production
• Make infrastructure investments to improve productivity of domestically based firms

Security
• Invest to raise overall level of national security
• Invest in intelligence to provide warning
• Invest in law enforcement to pursue perpetrators

Budgets
• Collect taxes to finance investments in security, intelligence, and law enforcement
• Run budget deficits or surpluses
• Tax revenues reduced as a result of successful terrorist attacks

GDP & Damage
• GDP is calculated as: (firm revenues + taxes - [intelligence + infrastructure + security + law enforcement])
• Damage is calculated as the sum of all damage inflicted by terrorists

The rogue nation government had the same incentives as the other government described in the previous slide. In addition, to incentive the rogue nation to support terrorist attacks the sum of all terrorist damage inflicted worldwide was made part of the objective function of the rogue nation.
Terrorists

Goal: Maximize end of game Ransom and Damage

Ransom and Damage
• Ransom is exacted through threats to do harm to transnationals
• The monetary value of damage is a function of the severity of an attack and the cash balance on hand of the firm attacked
• Terrorists gain utility through successful attacks on transnational firms
• Attacks are nation- or firm-specific
• Probability of success of an attack is a function of the resources committed and the combined national and firm defenses committed to defending against the attack
• Terrorists given a set amount of resources per period, augmented by ransom and reduced by successful law enforcement efforts

Finally, the primary raison d'être for the terrorists was to maximize the total revenues collected through ransom demands plus the overall damage inflicted on firms. The total damage to a firm from a terrorist attack was calculated based upon the difference between the firm’s security level and the severity level of the terrorist attack.
Synthetic Economies: The Application of Distributed Interactive Computing Environments for Policy and Management Decision Making

Richard H. White, IDA Project Manager; Alok Chaturvedi, Purdue Project Manager; Edward F. Smith, IDA; Robert Clover, IDA; Shailendra Mehta, Purdue; Chandrajit Bajaj, Purdue

Institute for Defense Analyses
1801 N. Beauregad Street
Alexandria, VA 22311

This paper explains how distributed, interactive computing can be used to assist decision makers to investigate alternative courses of action in complex, dynamic business and policy environments. The military's use of computer-generated synthetic battlefields for training is the metaphor; the creation of synthetic economies within which to practice policy and management prerogatives is the goal. Exposition proceeds by example, while methodological excursions and underlying theory are provided in supporting appendices.

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

13. ABSTRACT (Maximum 200 words)

14. SUBJECT TERMS
synthetic economies, global economy, interactive simulation

15. NUMBER OF PAGES
28

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
UNCLASSIFIED

18. SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19. SECURITY CLASSIFICATION OF ABSTRACT
UNCLASSIFIED

20. LIMITATION OF ABSTRACT
UL

NSN 7540-01-280-5500

Form Approved
OMB No. 0704-0188