Environ Syst Decis
DOI 10.1007/s10669-013-9479-9

Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks

Andjelka Kelic · Zachary A. Collier · Christopher Brown · Walter E. Beyeler · Alexander V. Outkin · Vanessa N. Vargas · Mark A. Ehlen · Christopher Judson · Ali Zaidi · Billy Leung · Igor Linkov

Abstract Increased reliance on the Internet for critical infrastructure and the global nature of supply chains provides an opportunity for adversaries to leverage dependencies and gain access to vital infrastructure. Traditional approaches to assessing risk in the cyber domain, including estimation of impacts, fall short due to uncertainty in how interconnected systems react to cyber attack. This paper describes a method to represent the pathways of disruption propagation, evaluate the macroeconomic impact of cyber threats and aid in selecting among various cybersecurity policies. Based on state of the art agent-based modeling, multicriteria decision analysis, and macroeconomic modeling tools, this framework provides dynamic macroeconomic, demographic and fiscal insights regarding shocks caused by cyber attacks to the regional economy over time. The interlinkage of these models will provide a robust and adaptive system that allows policy makers to evaluate complex issues such as cybersecurity threats and their impacts on the geopolitical, social, environmental, and macroeconomic landscape.

Keywords Agent-based modeling · Multicriteria decision analysis · Input/output modeling · Cybersecurity · Macroeconomics · Critical infrastructure

A. Kelic (✉) · W. E. Beyeler · A. V. Outkin · V. N. Vargas · M. A. Ehlen
Sandia National Laboratories, Albuquerque, NM, USA
e-mail: akelic@sandia.gov

Z. A. Collier · I. Linkov
US Army Engineer Research and Development Center, Vicksburg, MS, USA

C. Brown · C. Judson · A. Zaidi · B. Leung
Regional Economic Models, Inc., Amherst, MA, USA

1 Introduction

With increasing global reliance on the Internet as a medium to make transactions and transmit information comes an increased risk of cyber attack. Global cyber infrastructure is interconnected with and instrumental to economic prosperity and national security. However, most cyber infrastructure is not secure and is vulnerable to attacks from malicious actors potentially leading to failure of critical infrastructure, exploitation of sensitive information, and loss of intellectual property (US White House 2009). For example, cyber attacks on our banking and infrastructure systems are increasing in both frequency and sophistication, continually advancing to bypass firewalls and other detection systems (US Senate 2010).

Cybersecurity breaches can infect one computer or entire computer networks and can be launched by a variety of actors ranging from individuals to well-resourced organized crime syndicates or nation states. Motivations for compromising cyber systems include terrorism, criminal profiteering, and mischief. Results of compromise can vary depending on the intent of the actor and potentially include localized damage to hardware, destruction or theft of data (identity theft or industrial espionage), or disabling or controlling critical infrastructure.

From an economic perspective, a targeted cyber attack could cause massive losses that cascade through multiple infrastructure sectors (such as energy, transportation, health care, finance) given that cyberspace has increased the interconnectedness among them (Rinaldi et al. 2001). Direct and indirect costs could include the following:

business interruption costs, replacement of hardware, customer reimbursements, spending on cyber defense, criminal use of credit card numbers, stolen identities, fines, infrastructure replacement, and cyber risk insurance (Hachman 2011; Associated Press 2013; Moore 2010).

The US Defense Science Board concluded that cybersecurity is a major national security concern, especially since foreign-built components are increasingly deployed in the nation's cyber and communications infrastructure, and the Department of Defense (DoD) is currently not at the level of readiness required to adequately defend against cyber attacks (DSB 2013). The US military has identified cyberspace as a new operational domain that is embedded within all of the traditional physical domains (land, sea, air, space) (Welch 2011).

Recognizing the criticality of securing the nation against cyber attacks, President Obama signed Executive Order 13636—Improving Critical Infrastructure Cybersecurity, which calls for the establishment of risk-based standards for the protection of critical infrastructure (EO 13636 2013). However, cyber risks are especially difficult to assess given the substantial uncertainty surrounding the identification of hazards, assessment of exposure, and quantification of effects (Cox 2008). Given the significant uncertainty and rapid increase in sophistication and intensity of cyber threats, traditional quantitative risk assessment methods are insufficient (Frick 2012). Furthermore, in the global economic and financial arena, actions of decision makers are key to influencing the consequences of events. Those actions sometimes are coordinated (global central bank intervention) and sometimes competitive (currency devaluations). Therefore, there is a need for global economic tools that allow representation of this global decentralized interaction and evaluation of its effects on finance and the underlying economy.

This paper describes an analytical framework tailored to the requirements of cybersecurity risk analysis. It leverages multicriteria decision analysis (MCDA), agent-based modeling, and macroeconomic modeling. These tools are combined to evaluate the effects of various cybersecurity threats and large systemic risks.

The framework is intended to capture the actions of individual decision makers in financial, business, and public policy environments, and the economic and policy factors influence and follow from these decisions. While substantial advances have been made in these fields independently (discussed further in the next section), the authors are not aware of any other unified framework that combines the causal pathways of disruption propagation with evaluation of macroeconomic impacts and ranking of the effects of different mitigation and response strategies. As such, we believe this approach is unique.

In response to Executive Order 13636 and other policy directives, the framework can be used to aid policy makers by informing them about the delayed and indirect consequences of monetary and business decisions. This provides a clear and defensible basis for designing cybersecurity-related risk measures and safeguards, improving crisis management and promoting national security.

The remainder of the paper is organized as follows. Section 2 provides background on the kinds of models available for estimating different aspects of the consequences of cyber disruption, integrating those estimates in a way that can inform decision making. Section 3 discusses the specific modeling tools adopted in our framework and the processes they represent. Sections 4 and 5 discuss the use of the framework to analyze two different cyber attack scenarios: disruption of a significant oil production system and regulation of integrated circuit acquisition for critical infrastructures. Section 6 concludes.

2 Existing modeling approaches

Cyber attacks and counter measure simulation techniques have been studied extensively, and numerous modeling and simulation tools are available (Cayirci and Ghergherehchi 2006). The proposed framework not only captures the effects of an attack or counter measure on financial markets and decision-making processes at an agent level, but also conveys to policy makers the dynamic economic implications of such events and decisions on regional, domestic, and global economies. These downstream effects propagate across multiple industry sectors and regions to ultimately impact the competiveness of domestic firms (Clayton and Segal 2013; Parfomak 2013). The following sections describe prior work in agent-based and macroeconomic modeling and multicriteria decision analysis.

2.1 Agent-based models

Agent-based modeling is an excellent tool for understanding and representing disruption mechanisms, the effects of changes in market participant strategies, and the effects market rules and government intervention may have on outcomes. Agent-based modeling capabilities have been used for understanding disruption propagation in financial and other domains.[1] Understanding such mechanisms is crucial for representing the path of novel disruptions and may be necessary for determining the end state of the system once the disruption has propagated. This involves

[1] These capabilities were developed for the National Infrastructure Simulation and Analysis Center (NISAC) and the Complex Adaptive System of Systems group (CASoS) at Sandia National Laboratories.

understanding the decisions and interactions of producers, consumers, traders, governments, and other parties.

These capabilities include the Securities Market Model (NISAC 2011), the NISAC Payment Systems modeling project (Renault et al. 2009), the Global Finance (NISAC 2013) tools, and chemical supply chain (Ehlen and Vargas 2013) models developed for NISAC as well as earlier work in payment systems (Outkin et al. 2008) and financial markets modeling (Darley and Outkin 2007). Combined, these capabilities allow representation of investors', trading agents', producers', and consumers' behaviors and responses to a disruption, effects of information flow disruptions, and effects of actual or perceived commodity shortages.

The consequences of large-scale disruption will depend on the consequent reallocation of supply through commodities markets. Market models that can be used to explore possible reallocations must connect expectations of availability to market behavior. Most current work in modeling markets in general and commodity markets in particular is not concerned with this problem. The seminal model of Schwartz and Smith (2000), for example, is a stochastic representation of the evolution of market prices, including parameters describing expected short- and long-term variability; however, these parameters are estimated from historical price signals. It is not appropriate for anticipating reactions to novel supply shocks.

Agent-based models can be used to forecast the large-scale market consequences of unprecedented stresses because they derive those consequences from the individual decisions of traders. These decisions are generally modeled as a kind of goal seeking given the agent's information and resources. The effects of unprecedented events can therefore be derived by changing the information or resources available to each agent. Agent-based market models have been developed for many applications (Tesfatsion 2006), including creating an environment for training commodities traders (Cheng and Lim 2009).

Agent-based models can also capture a number of important supply chain dynamics not represented in traditional models. Traditional approaches often determine optimal strategic or operational resource allocations within or between manufacturing facilities (Perea-Lopez et al. 2001; Chen and Lee 2004; Lababidi et al. 2004) and treat tactical concerns with models of uncertainty (Petkov and Maranas 1997; Applequist et al. 2000; Timpe and Kallrath 2000; Kallrath 2002; Levis and Papageorgiou 2004; Guillen et al. 2006). In comparison, agent-based supply chain models allow decision makers to consider a fuller set of dynamics associated with, for example, tactically managing the operations of a fabrication plant that must adapt its own operations, its suppliers, and its logistics to ensure output of final product.

2.2 Macroeconomic modeling

Approaches taken to quantify the macroeconomic impact of cyber attacks often have relied on strict input/output tools to generate linear impacts related to demand or supply disruptions (Andrijcic and Horowitz 2006; Santos et al. 2007). Regional Economic Models, Inc. (REMI) PI^+ is a tool that captures similar inter-industry relationships, but also includes computable general equilibrium principles and domestic trade flows which allow for dynamic changes over time (Shao and Treyz 1993). The REMI PI^+ model allows for insight into macroeconomic consequences and the propagation across regions and industry sectors. Cyber attacks that disrupt critical infrastructure could have the effect of reducing demand, changing market prices, or eliminating parts of a supply chain. PI^+ can include inputs which represent each one of these direct economic shocks. The model generates year-by-year results across individual counties, states, or larger regions across over 150 North American Industrial Classification System (NAICS) categories.

2.3 Multicriteria decision analysis

Individuals are faced with numerous decision problems every day. Sometimes these decisions can be made intuitively, but especially in high-stakes situations, decision problems may be poorly defined or may involve substantial uncertainty (von Winterfeldt and Edwards 2007). In these situations, ad-hoc decision making may not be sufficient, and the use of a decision aid may be valuable. Decision Analysis is a broad field of study offering an array of deterministic and stochastic tools and processes, which aid in structuring and assessing decision problems. Providing a normative, formalized and systematic approach to complex problems, it is "a logical procedure for the balancing of the factors that influence a decision. The procedure incorporates uncertainties, values, and preferences in a basic structure that models the decision" (Howard 2007).

Explicit in this definition is the process of building a decision model in which courses of action can be assessed based on the objectives and preferences of the decision maker. A variety of modeling tools exist within the umbrella of Decision Analysis such as decision trees and influence diagrams. For example, decision trees (Kirkwood 2002) mathematically combine the values of different outcomes with subjective probability assessments of the occurrence of future events. The decision tree generally presents results in terms of expected monetary value or expected utility. However, this can be limiting when there are multiple, dissimilar, and difficult to quantify criteria (Belton and Stewart 2002; Linkov and Moberg 2011). The field of Multi-Criteria Decision Analysis (MCDA) extends

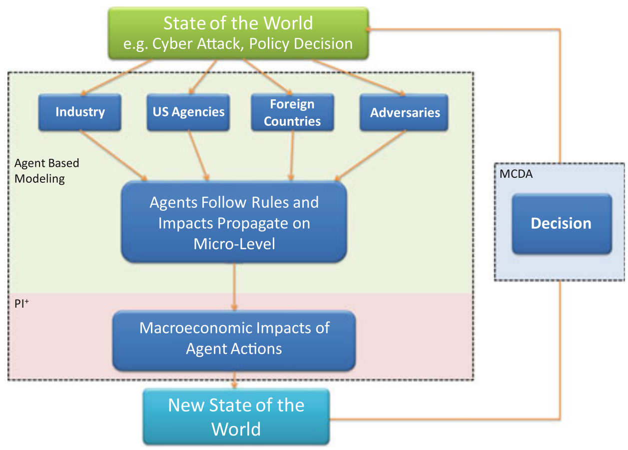


Fig. 1 Structure of the overall framework

the field of Decision Analysis by providing a collection of methods in which trade-offs can be made across performance criteria above and beyond simple monetary or utility-based measures, such as those that would be encountered during a cybersecurity scenario.

MCDA methods generally contain similar structural elements, including an objective (or objectives), a number of alternatives, a set of criteria in which the alternatives are assessed, and weights placed on criteria that represent the relative importance or preferences of the decision maker. Methods differ widely in their underlying algorithms for how to elicit and combine values (Huang et al. 2011). Examples of MCDA methods include Multi-Attribute Utility Theory (MAUT), in which scores are transformed into utilities (Keeney and Raiffa 1976), Analytic Hierarchy Process (AHP) which assesses criteria based upon pairwise comparisons (Saaty 1980), and outranking, a family of methods in which alternatives are comparatively ranked across a number of dimensions. These methods can incorporate stochastic, fuzzy, or other such inputs. Thus, MCDA allows decision makers to formally and rigorously frame and structure information and select among several courses of action.

3 General framework and its components

The multicriteria, macroeconomic, agent-based framework is a decision support tool for analyzing the effects of disruptions on global economic and financial systems. It is composed of several classes of model that capture realistic pathways of cyber-based disruption propagation through physical, financial, economic, and decision-based systems (Fig. 1).

The framework begins with a description of the state of the world that is being modeled. This could include information about the current state of the economy as well as the disruption of interest, such as a cyber attack or enacting a new piece of legislation. It is possible to set the quantity (how much) and quality (accuracy) of the information about the world each modeled decision maker (or agent) knows since the case of perfect information is highly unrealistic.

This information is transferred to the agent-based models, which simulate the decisions and interactions of individual decision makers at a micro-level within the economy and government. These actions (e.g., trading strategies, supply chain decisions, alternate public policy) allow the modeler to investigate how cyber events propagate at the micro-levels of the economy and government.

Next, the impacts of these micro-level actions are fed into the REMI PI$^+$ macroeconomic impact model to assess the macro-scale economic implications of the disruptions. These impacts, representing a new state of the world, can either be taken as the results of the model, or iteratively fed back to the agents for numerous rounds of decision making and impact assessment.

Finally, the economic impacts can be fed into the MCDA model, representing a decision maker using the results of the analysis. Based on the impacts to the economy, the particular objectives of the decision maker, and the relative preferences of some decision criteria over others (e.g., prevent unemployment vs. prevent inflation), these decision models can determine the preferred course of action (such as policy measures or business decisions) for the agent to take that maximizes their overall utility or value score. This decision has an effect on the state of the world, which in turn causes the agents to react and economic impacts to follow. This process can be iterated as many times as needed to capture the desired effects. The MCDA step can be skipped as an alternative if the user wishes to forego the normative alternative assessment phase and focus solely on descriptive assessments of impacts.

3.1 Selected models for inclusion in the framework

3.1.1 Securities market model

The Securities Market Model (SMM) (NISAC 2011) estimates the responses of traders in securities markets to disruptions to the financial system. The model represents decisions by traders in financial markets to buy and sell assets based on their perceptions of various factors affecting the asset value. These factors include some inherent value assigned to the asset, observed asset prices and price trends, and expected fixed or variable returns. The reliability and latency of the systems used to trade assets are among the factors considered. Individual traders

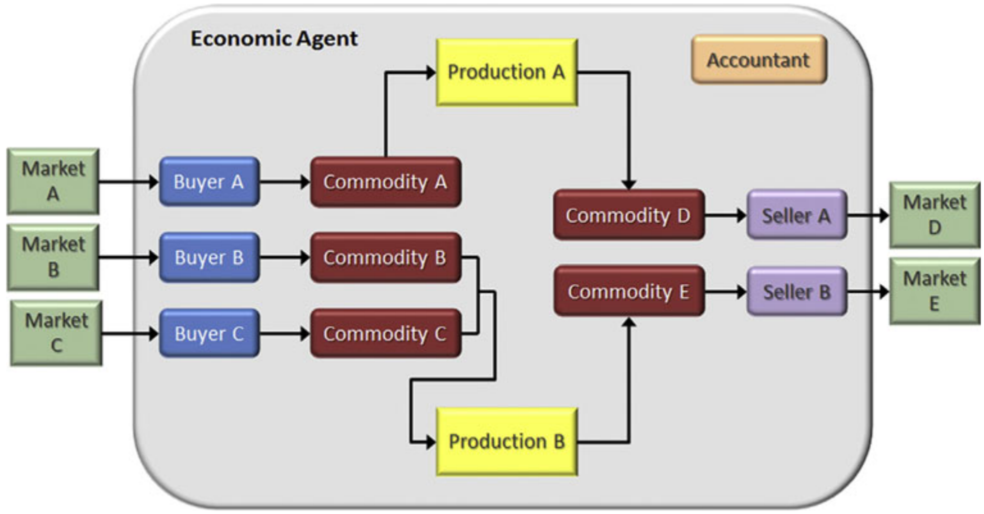


Fig. 2 N-ABLE economic Agent (adapted from Ehlen et al. 2014)

Fig. 3 N-ABLE modeling of buyer-to-seller markets (*arcs*) and transportation (*spider-lines*) (adapted from Ehlen and Vargas 2013)

place different weights on these factors, and have different risk dispositions. This system allows the effects of a cyber disruption on multiple financial assets to be estimated, including the potential for cascading effects from sudden changes in risk perception.

Changes to traders' behavioral parameters represent the effect of cyber disruptions on trader attitudes. These changes lead to changes in traders' valuation of assets, which are then reflected in their buying and selling behavior. Changes in behavior by individual traders can change asset prices and trends, which then feed back to influence other traders whether or not the initial disruption directly affected those traders. In addition to changes in risk perception, systematic changes in the expected returns of specific assets can be postulated as a direct consequence of a shock to production facilities.

3.1.2 N-ABLE

The N-ABLE model is a large-scale agent-based economic model of firms, supply chains, and household sectors (Ehlen et al. 2008, 2010, 2014; Ehlen and Vargas 2013). N-ABLE agents are detailed enterprises (Fig. 2) that purchase materials, produce, and sell in markets. These enterprises interact with one another in markets and in their use of critical infrastructure systems (Fig. 3).

Disruptions to these modeled supply chains caused by natural and man-made disasters cascade through the simulated economy based on: firms' individual decisions about their internal operations and uses of markets and infrastructure; the abilities of the firms to substitute alternate suppliers and buyers, adjust productions (schedules, lines) and inventories (onsite, in-transit) to mitigate impact; and government actions to mitigate if not prevent disruption effects. The modeling of thousands of such firms in supply chains subject to disruptions informs decision makers on the risks to and resilience of economy-related critical infrastructure.

As discussed in Sect. 5, US firms that may be subject to a new cyber-based integrated circuit policy must consider a range of complex business factors that influence their operations, profitability, and business resilience over the near and long term. These factors include the availability, location, cost, and quality of labor, material suppliers, and supporting infrastructure (energy, communications, transportation); and the effects of these components on their overall supply chain logistics and profitability. Integrated circuit manufacturers are often reliant on nearby suppliers of high purity metals, chemicals, and other components; such supply chain details are essential to day-to-day operations, logistics continuity, and long-term profitability.

New policies that limit the business and supply chain options of manufacturers could have unintended economic consequences: manufactures could simply divest and outsource their IC needs to foreign companies, resulting in lost US output, employment, and income. As such, these manufacturing business and investment factors, dynamics, and potential impacts are an essential component of public-sector policy analysis.

3.1.3 PI$^+$

PI$^+$ is a dynamic structural economic forecast and policy analysis model. It captures the framework of how regional economies both operate and interact within a national and international marketplace. Within the structure are defined and quantified linkages between producers and both intermediate and final consumers (Treyz 1993; Treyz and Treyz 1997). It measures population growth over time, accounting for both natural growth as well as migratory transfers in and out of a region (Treyz et al. 1993; Greenwood et al. 1991). The model describes the market structure of interest and allows for exogenous shocks to affect market interactions. Built largely on publicly available data, an independent short-run national forecast and its internal linkages structure, PI$^+$ is able to generate a year-by-year baseline forecast to the year 2060.

Within the framework PI$^+$ is constrained by several factors. PI$^+$, as a model which requires user inputs, is subject to bias and poor assumptions. It is also constrained to displaying annual impacts. Within the framework, PI$^+$ takes outputs from SMM and N-ABLE agent-based models as inputs. By using other robust tools to develop inputs to PI$^+$ the expectation is that the simulations will be more appropriate and accurate and allows the analyst to clearly express what the key drivers are.

PI$^+$ includes four different quantitative methods in its framework, which makes the model more flexible by allowing them to highlight each others' strengths and compensate for their weaknesses. The first methodology is input/output tabulation (I/O), which looks for transactions between industries and households in the economy (Leontief 1986). The second, Econometrics, provides statistical parameters for behavioral patterns and responses inside of the economy. Computable General Equilibrium (CGE) and New Economic Geography, the third and fourth methodologies, add market-level concepts and the principles of equilibrium economics to the linkages within the structure of PI$^+$, and include concepts of agglomeration, labor pooling, and economies of scale, respectively (Fan et al. 2000; Fujita et al. 1999).

I/O modeling includes the flow of goods from firm-to-firm through supply chains, final sales to households, and then wages paid to and spent by individuals and families. Included in the model's adjustments from year to year is the notion that markets take time to "clear" after a shock, returning to relative stability of prices and quantity and a balance between supply and demand. Elasticity of price and wealth—the response of households and firms to changes in prices and wages—and the "rate of adjustment" from a shock to a new stability inside of the economy are all computed before an eventual result is reached. PI$^+$ is unique for integrating the characteristics of I/O and CGE modeling together, taking into account equilibrium entities including, but not limited to, markets for labor, housing and consumer goods, composite inputs for firms, and market shares for local industry. PI$^+$ also incorporates the recognition that labor-intensive industries, such as healthcare or professional services, tend to cluster in urban centers with an educated labor force with specializations in their exact areas. The same is true of goods-producing industries, which tend to locate themselves near customers, input suppliers, transport hubs, and other "environmental" factors that help them lower their costs or increase productivity. These concepts are endogenous to PI$^+$, adjusting for clusters by region.

PI$^+$ employs a block structure, representing different parts of the economy (Fig. 4). Each block has its own "perspective." Through the model software, model users manipulate policy variables that directly "shock" one or multiple parts of the model structure. The model then simultaneously solves for a new equilibrium. Block 1 is final demand and final production; it is the "macroeconomy" in terms of its total aggregates. Block 2 is the business perspective of the economy, where industries need to

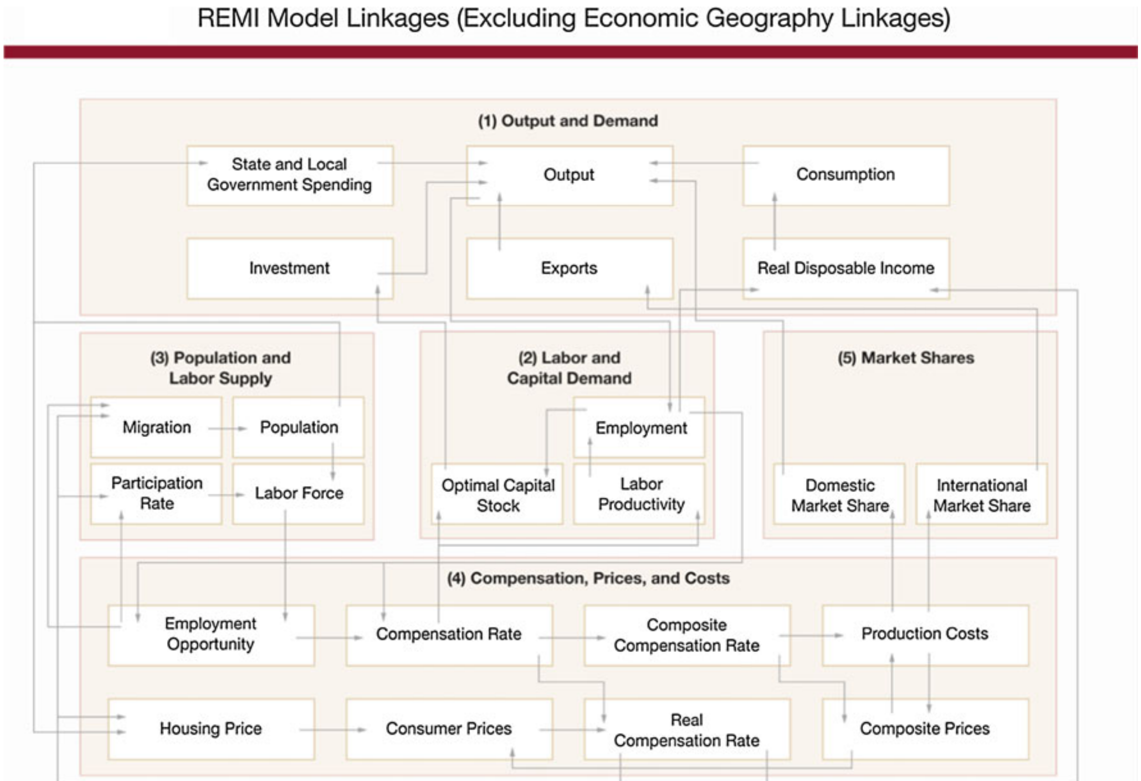


Fig. 4 Block structure of PI$^+$

Fig. 5 General MCDA approach

produce a certain amount of output. To do this, they need inputs (which include labor, capital, and fuel), but they will also try to minimize costs when adjusting for productivity. The household concept in PI$^+$ is Block 3, which includes how consumers spend by region, how they choose to participate in the labor market, and how migration changes a regional economy over time. Block 4 includes market concepts for labor, housing, consumer goods, costs of living, and the cost of doing business in an area for firms. Block 5 measures competitiveness for a region on the domestic and international marketplace. This includes how "skilled" an area is at keeping away imports, as well as how much it is able to export to other locales (REMI 2013). These model linkages, using outputs from the agent-based models, form the structural basis for determining how micro-scale decisions in response to a disruption would manifest in the macroeconomic landscape.

3.1.4 Multicriteria decision analysis (MCDA)

MCDA, unlike the previously discussed models, is not a specific model, but rather a broad approach to problem solving and decision making. Following a Value-Focused Thinking approach (Keeney 1994; Parnell 2007), MCDA breaks the decision-making process down into the following major steps (summarized in Fig. 5).

- Determine the overall objective of the decision—in this case, to choose the best alternative for securing against a cyber attack and maintaining economic stability.
- Identify the evaluation criteria. Criteria represent what are important to the decision maker and stakeholders. Criteria may contain several nested sub-criteria.
- Identify measurements for evaluation criteria. Measurement endpoints (i.e., metrics) may include physical data, modeling results, and qualitative measurements such as expert judgment. These metrics are used to score each alternative on how it performs on each criterion.
- Assign weights to evaluation criteria. Weights determine the relative importance of the evaluation criteria in comparing the alternatives. There are many types of weighting methods, including rank-based methods, swing weights, and pair-wise comparisons (Linkov and Moberg 2011).
- Identify and score alternatives that meet the management objective. The alternatives may include different policy options or response strategies for preventing a future cyber attack or mitigating the effects after a successful attack.
- Synthesize results and conduct a sensitivity analysis. Generally speaking, alternatives are compared by calculating an overall value score of the form $V = \Sigma_i \cdot w_i x_i$, where w represents the weight assigned to criterion x, and where $\Sigma_i \cdot w_i = 1$. Sensitivity analyses provide insight on the superiority of the optimal alternative relative to the others. The contribution of assigned weights and the various measured endpoints to the determination of the optimal alternative can be measured.

4 Scenario 1: cyber attack on oil industry

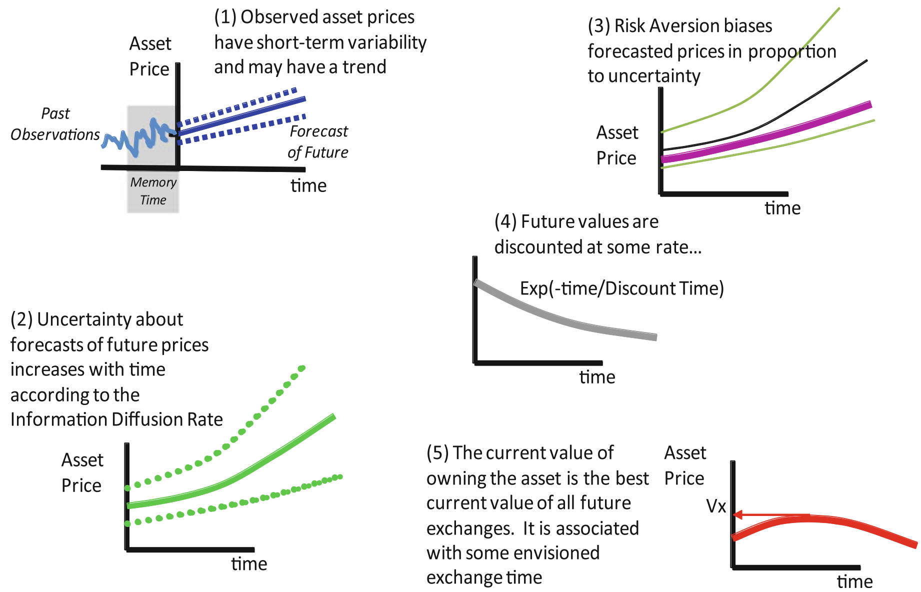
The cyber attack on 30,000 computers at Saudi Aramco on August 15, 2012 was aimed at disabling the production of crude oil and natural gas as well as accessing proprietary data (New York Times 2012). The computer virus did wipe hard drives of data and documents but did not affect the process control systems software. Since control systems software remained untouched, the cyber intrusion did not halt crude oil and natural gas production as initially feared.

For our analysis we posit a cyber attack, similar to the one on Saudi Aramco, conducted against a foreign oil producing entity. Unlike the Saudi Aramco attack, which only affected business systems, this attack spills over into the control systems that govern oil production. Oil production at the entity is disrupted creating a production shock that affects the availability of oil and the associated financial markets.

A successful attack disrupting oil production creates a supply shock and a perception of increased risk associated with oil availability and future prices. There are multiple historic examples of oil production disruption and numerous studies analyzing their effects. We illustrate the mechanisms of the supply shock propagation on the example of the cessation of the Iranian oil exports in 1978 following the Iranian revolution. Yergin (1990) reports that oil production in the first quarter of 1979 following the Iranian revolution was about 2 million barrels per day lower than the last quarter of 1978. This production decline represented no more than 4–5 percent of the total world demand of 50 million barrels per day. Yet, the oil price increased by 150 % percent in the same time period. Yergin (1990) attributes that amplification to the following factors:

- Oil consumption growth and a perception that the oil consumption will continue to rise.
- Disruption of oil industry contractual arrangements following the Iranian revolution.
- "… contradictory and conflicting policies of consumer governments"
- Successful attempts by the oil exporters to increase their rents, by such mechanisms as manipulation of supplies.
- Effects of "uncertainty, anxiety, confusion, fear, pessimism" on the consumer and trader decisions. According to Yergin, the panic-buying "… more than doubled the actual shortage and further fueled the panic."

Fig. 6 Formulation of trader's Asset valuation function in SMM



As Yergin illustrates, there are multiple mechanisms through which a production disruption will affect the financial markets. Those mechanisms involve not only the initial effects, such as the traders' and consumers' reactions, but also the delayed feedback effects, such as increased spending on fuel due to higher gas prices.

4.1 Model overview, parameters and agent behaviors

4.1.1 Scenario overview

We initially treat this cyber-caused disruption the same as a physical disruption resulting in the local shortage of crude oil and incorporate the estimates of shortages into the SMM (NISAC 2011). In this scenario, the supply of crude oil is instantaneously reduced following the disruption. Actual physical flows of oil both via the pipelines and the tankers will be affected by the disruption. This physical disruption component is defined exogenously. It affects the quantity of trading contracts available and the price and risk expectations for them.

Following the attack, the producer, consumer, and trader expectations of price and availability of oil will change as a result of the disruption. In particular, the perceived shortage will affect the trading strategies or their parameters, which in turn translate into likely effects on the spot and the futures prices. The trader reactions and changes in the outlook are represented in SMM, by changing the traders' expectation of the future asset (crude oil futures in this case) returns and perceived risks and by changing the traders' assessment of supply conditions or even the perceived reliability of trading platforms. The SMM formulation of trader evaluations, shown in Fig. 6 below, allows sudden changes in information and uncertainty to be imposed on commodity traders.

This capability to change the trader strategies in response to disruptions applies across a broad range of attacks on the institutional or technological underpinnings of production systems or financial markets. Furthermore, in addition to representing the propagation of disruption through the commodities markets, the SMM also estimates the concomitant effects on other asset classes, such as stocks and bonds.

4.1.2 Entities in the simulation

The SMM represents the market structure, the agents, their decisions and interactions, and some of the corresponding physical flows of oil. The agents in the model include traders as well as the consumption and production agents. The model generates prices of the securities based on the continuous double auction, where traders submit bids and asks that are continuously matched by the exchange. Additional trading rules include margin requirements that can be changed in the event of disruption to reflect the enhanced risks or risk perceptions. The physical flows of oil can be represented by flows over pipelines or by the movements of the tanker fleet or both depending on scenario requirements. As a result, the SMM generates oil price dynamics and volumes traded by representing the interaction of trading strategies and physical components of the system over time.

4.1.3 Traders decision making

The traders in commodities and financial markets buy and sell assets based on their expectations of future prices and perceptions of risks affecting the asset value. Specifically for oil trading those risks will include the new perceived threats to production facilities, highlighted by the disruption. If the cyber attack extends beyond the production facilities, the risk perception will be affected by the compromise of the institutions and facilities used in trading.

For this scenario, the SMM will include a population of heterogeneous traders, who buy and sell in commodities, stocks, and bonds (commercial and government bonds) markets. Traders have different initial allocations of assets and cash, and can have different values for each of the parameters that describe behavior. These parameters allow trader agents to be configured to represent a spectrum of market participants, from individual investors to pension funds. Statistical descriptions of the traders and of the financial assets are model input.

The model uses a few basic parameters to describe traders' behavior. Each trader has a *discount rate* used to translate future income to the present. Each uses information about past asset prices to estimate the trend and variability of future prices. A trader's *memory time* determines how much past price information they use to estimate future prices. Traders have uncertainty about their estimates of future prices, and this uncertainty is larger for longer-term forecasts. A trader's *information diffusion rate* describes the tendency for uncertainty to increase as the length of the forecast increases. Traders place different weights on their uncertainty: risk-averse traders place a lower value on assets with large uncertainty compared with a similarly priced asset with less uncertainty. The *risk aversion* parameter describes this effect.

Following the oil production disruption, the traders' perceived risk of extreme asset price variations increases. This increase in traders' perceived risk is reflected by an increase in the value of their information diffusion parameter in SMM. Increased uncertainty about future prices may increase the amount of cash required in leveraged deals, thus affecting the traders' decision-making process and the capital available for trading.

4.2 Estimating the disruption effects on prices

The price response in the SMM is affected by sudden changes in traders' perceptions, and in the longer term by the readjustment of actual demand and supply. Production shortages can be covered through existing inventories until those inventories are drawn down. Unaffected producers may increase their production to make up for the lost capacity. Consumption may have to decrease if the disruption persists for a sufficiently long time or if unaffected producers cannot make up for the lost capacity.

The granularity and the details of the specific version of the SMM created for this scenario will be affected by the data available and the specification of the scenario, such as the disruption duration. In general, for each of the basic asset types, many specific assets (for example stocks in specific companies) can be created for traders to exchange. The asset types differ in their mechanisms for providing returns to investors and in the variability of these returns. Stocks may pay dividends at specified periods; however, the size of these dividends is variable and may be zero in some periods. Bonds pay fixed yields at specified periods. Commercial bonds are subject to default, which eliminates future payments to bond holders. Government bonds are assumed to be free of default risk.

We represent oil trading via the futures contracts. Given the fixed duration of such contracts, the traders have to ensure that they close their positions before the contract maturity date if they do not plan to take delivery of the underlying asset (oil in this case). All asset types can be sold at some future time until their maturity, and the prospect of increases or decreases in price is another factor in the way traders value assets. These characteristics capture the basic properties of real assets, and offer traders a spectrum of options for balancing risk and income.

The actual price of oil in the model is determined by traders expressing their intentions by limit orders. The new and existing orders are matched at every time step of the simulation in the double auction process. The matched orders result in actual trades that determine the security price at a particular time step. The actual quantities of oil consumed and produced are determined by the corresponding agents, based on the price information and other parameters in the model.

Prices set in markets influence resource allocation decisions in the real economy. This influence is captured through two kinds of price signals sent from the SMM to PI^+. The prices determined in the market model of commodity-based securities determine the costs of basic inputs in PI^+. Prices of corporate bonds determine the capital costs confronting different sectors of the economy and therefore influence growth rate. Because individual market transactions are simulated, prices and capital costs are produced at a very short time scale. These have to be averaged over longer time periods (quarters or years) to correspond to the time scale used in PI^+.

4.3 Estimating the effect of price shocks on the economy

As a structural forecasting model, PI^+ contains policy variables that allow the modeler to directly interact with any particular block or linkage of the structure. By modifying those variables, PI^+ generates an alternate forecast that can then be compared with the baseline. The price and cost shocks enter into the model through the third model block in Fig. 4, the "compensation, prices and costs" block. The variables here modify equilibrium prices and force both supply and demand to adjust to the new cost reality. The inputs distinguish between residential consumers as purchasers of gasoline, and industries as consumers of fuel (as an input to the factors of production). Thus, the price shocks generated by the SMM will be separated. The first separation defines how the price shocks impact industries in different sectors (by NAICS code), which will directly impact each individual sector's cost of production; the other separation will define how the price shocks impact individuals through higher gas prices, thereby affecting disposable income. Given that the market for oil is globalized, there will not be strong regional differences in the relative cost change. However, given some regions' and industries' relative intensities of oil or gas use, there may be changes in relative competiveness. The same is true for the industry change in capital costs: the financial market will change costs across various countries somewhat uniformly, but will impact capital intensive industries more than others.

The macroeconomic impact of higher gas prices is a reduction in disposable income available for other goods and services. PI^{+} contains 79 consumption categories with regional spending elasticities for each commodity. The model will capture the increased spending on gas and allocate spending away from all other goods and services. This fall in aggregate demand will have an impact on the production of domestic and imported goods. Depending on the length of the disruption and sustained higher prices, the drop in sales and output could lead to reductions in hiring, and even job losses across all sectors.

The effect of changes to both fuel and capital costs in industry sectors will cascade through the production channel of the model, which determines each industry's relative competiveness across all regions within the United States, or the rest of the world. The relative competiveness concept determines relative delivered prices and therefore determines the industry's market share. The market share determines each industry's relative growth, as well as the long-run output and employment growth. Each industry's production function consists of capital, labor and fuel as components of value added. If the cost of any one of these factors is impacted, not only will the overall production cost be impacted, but because substitutability exists among factors of production, there will also be substitution between capital to labor depending on the market and availability.

Changing the cost of capital also impacts the level of residential and non-residential capital investment. Capital investment contributes to long-run level of capital stock, but also directly to final demand.

The model runs a single simulation with each one of the various inputs included. This way, all direct effects are appropriately captured. The model then solves for and generates a new forecast given the policy shock. Given that the price effects of cyber attacks contain uncertainty, the modeler can run multiple scenarios adjusting for a range of inputs.

5 Scenario 2: policy analysis for hardware security

In addition to cyber attacks via networks and software, the economy is also vulnerable to attacks via counterfeit electronic hardware. Parts that are relabeled, refurbished, or repackaged to misrepresent their authenticity (Sood et al. 2011) have been found throughout the global supply chain, and their prevalence is on the rise. The US Government Accountability Office (GAO) found that counterfeit parts, even those misrepresented as military grade, were easily purchased from online vendors (GAO 2012). The US Department of Commerce (DOC) conducted a study of counterfeit electronics within the US Department of Defense (DoD) supply chain, and found that over a 4-year period the number of reported incidents increased by 141 percent, with over 8,000 incidents in a single year (DOC 2010).

These counterfeit electronic parts have potentially serious consequences ranging from damage to brand identity and increased security risks. Products made from these parts may have degraded product reliability and raised safety concerns for consumers. Firms producing these products would incur decreased profits and damage to their brand identity (Pecht and Tiku 2006). Hardware Trojan horses (HTHs), or malicious modifications of electronic circuitry, can compromise sensitive information and cause product failure (Tehranipoor and Koushanfar 2010).

5.1 Policy alternatives

In this scenario, the US Federal Government decides that the foreign manufacture of integrated circuits (ICs) used in critical infrastructure is an unacceptable risk to national security. To mitigate these risks, the government mandates the procurement of these ICs from acceptable-risk sources, starting on a certain date. Acceptable-risk sources include: (1) mandating procurement from domestic production facilities, to replace foreign-made components[2]; and (2) developing a certification program to allow select offshore producers and facilities to be deemed equivalent to a

[2] This mandate could, for example, be promulgated via the Defense Production Act.

domestically sourced product. We focus discussion on the first: mandating procurement from domestic production.

This potential policy has a complex set of private- and public-industry decisions that need to be made, ones that have potentially negative impacts on US regional and national economies. Within industry, key decision makers are the fabrication (or "fab") companies that physically make the ICs. Given a new policy requiring domestically produced ICs, a fab company needs to assess the relative tradeoffs associated with at least the following factors:

- If they do not currently produce these ICs domestically, where to locate a new domestic fab plant, which must be carefully placed near the supporting suppliers of subcomponent, metals, and chemicals.
- Whether to divest the particular IC product market entirely, and reinvest their resources in other markets that are potentially more profitable than domestic IC production.

From a federal government standpoint, this policy would not likely include additional provisions to incentivize private-sector plant investments. State governments, however, have incentives to attract these domestic fabrication plants to their own state. In the auto industry, for example, incentives to create or maintain local production include tax subsidies, loans, and even stock purchase. The potential economic impacts of the proposed cybersecurity policy occur at two basic decision-maker levels: the individual manufacturing companies; and local, state, and federal governments. Each is considered in turn.

5.2 Decision-making process

5.2.1 IC fabricator decision process

At the level of the manufacturing firm, decisions about where and how to manufacture or acquire IC components are made through careful risk analysis of the business and economic conditions that affect profitability. In considering a change in production facility investments, there are three basic supply chain concerns:

1. Strategic decisions—how does this facility affect overall production, marketing, and profitability for the company;
2. Operational decisions—what will be the day-to-day operations of the facility and its role in the larger IC supply chain; and
3. Tactical decisions—how well can the facilities operations adapt to changing, unforeseen conditions so as to meet the longer-term strategic objectives.

Many of the strategic and operational decisions are modeled with existing, non-agent paradigms. The tactical decisions are complex enough to need a larger decision process such as MCDA. Figure 7 illustrates a decision framework for an IC fabricator considering two options: invest in the new production facility or divest from the IC product line. The basic criteria for this decision are profitability and market share, two related but distinct business objectives. Each is affected by three sub-criteria: operational factors such as actual day-to-day operations; tactical factors such as the ability to address and adapt to unforeseen disruptions and other uncertainties; and strategic or long-term factors.

The N-ABLE supply chain model of the IC fabricator includes the following components:

- The fabricator's enterprise operations, including the purchase, store, and use of inputs, and the production of outputs;
- The first-tier suppliers of sub-assemblies;
- The lower-tier suppliers to the sub-assemblies, and so on; and
- The transportation and other critical infrastructure systems upon which the IC supply chain relies.

The supply chain measurements and dynamics modeled would include:

Operational factors Although raw commodities can be provided from outside of the US, the government policy would require significant sections of a firm's supply chain to be located within the United States. The fab needs close and reliable component suppliers, to ensure quality and just-in-time efficiencies. The firm's labor force and many of its supplier's labor force may require security clearances, adding to industry production costs and government service requirements. The security requirements would prevent international migrants from being able to provide the required jobs. The PI^+ model will assume firms obtain their supply chain and labor force based on relative distance to the fab plant and relative costs of goods and labor required. PI^+ can be parameterized to account for requirements set in the site selection process and agreements set with local and State entities.

Tactical factors Disruptions in supplier, buyer, or transportation conditions can affect the "throughput" of the IC manufacturing supply chain. Changes in the IC cyber policy in the short to medium term could adversely affect the fab's long-term profitability; the particular supply chain configuration would need to be sufficiently adaptable to these and other cyber-related threats and policies.

Strategic factors The complete onshore procurement of critical infrastructure IC components would require the IC fab to identify the most profitable and secure supply chain. If the current domestic labor market is not sufficient to

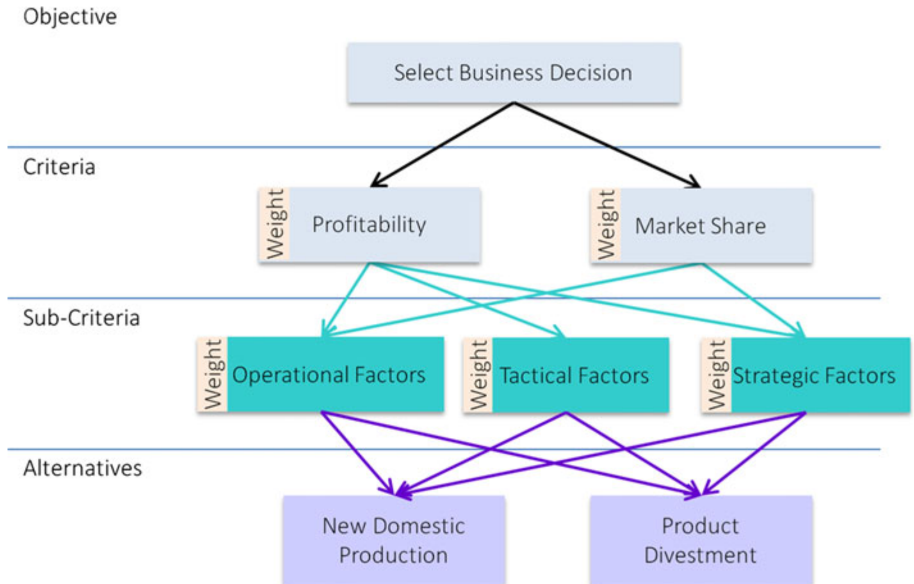


Fig. 7 Hardware security decision problem: fabricator

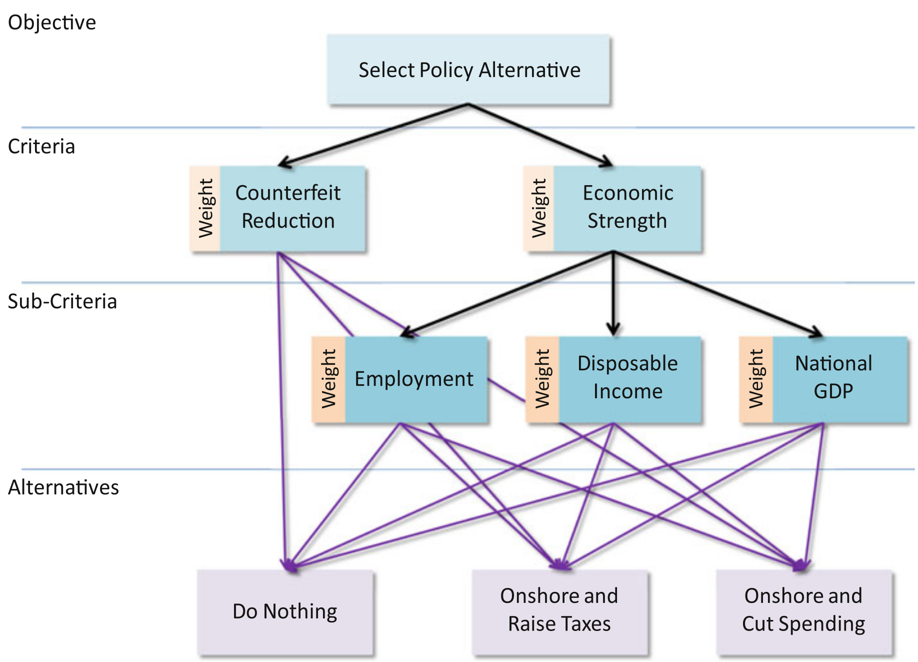


Fig. 8 Hardware security decision problem: government

provide the jobs required, firms will attempt to substitute toward capital investments or will be required to limit the total amount of IC components they can provide to the federal government and critical infrastructure.

The N-ABLE agent-based framework is particularly well-suited to all three decision-targeted modeling sub-factors and their contribution to profitability and market share. The resulting decision or decision-probability space that would include the estimated change in economic activity (output, employment, income) that affects the state and federal decision process outlined in Fig. 8.

5.2.2 *Government decision process*

A government official or policy advisor responsible for providing guidance on this issue has several decisions to make. First, there is the decision as to whether or not to mandate the on-shoring in the first place as compared to a "doing nothing" strategy. While doing nothing is technically a feasible option, there may be pressure to take action from a number of stakeholders and constituents by implementing the on-shoring alternative.

However, these policy mandates carry intended and unintended downstream benefits and costs. For example, requiring that private industry, without incentives or other actions, use specific domestic suppliers could have the unintended effect of incentivizing those suppliers to off-shore parts of their supply chain, making the cyber risks the same if not higher. On-shoring IC components could increase the cost of the component, thus requiring the US government to allocate more funding to purchase these goods. The US government would then be required to face a new decision problem: cut spending in other areas or levy taxes to cover the increased costs. If the US government levied new taxes, then consumers and industry would pay the cost. Alternatively, the US government could cut spending in other areas, leading to decreased services provided to the public and fewer government jobs. The increased manufacturing activity of IC components within the US would create jobs and inject money into that sector of the economy. Other nations may negatively react to the US onshore procurement mandate and could jeopardize US exports to the rest of the world or stop providing vital commodities. Depending on production costs, labor and commodity access, the overall onshore procurement could have a net positive or considerably negative economic impact on total employment, real disposable income, and GDP.

At the level of state or federal government, action to restrict access to foreign IC component production for critical infrastructure would likely have significant economic implications on government agencies, industry, and consumers. A study by Rose et al. (2009) using PI^+ concluded that a complete closure of the US border to outside trade and travel due to a security or health threat would have significant overall negative economic effects. The US economy relies heavily on access to global markets to obtain goods and labor; without access to lower priced and foreign-made goods and decreased access to a skilled labor force from international migrants, US firms paid higher component costs and wage rates. Despite select labor markets receiving new employment opportunities and higher wage rates, the overall cost to businesses and the final consumer in conjunction with decreased access to vital commodities caused the overall gross domestic product (GDP) growth rate to diminish significantly. Import bans on US goods and the absence of international travelers injecting money into the US economy lead to further degradation. The effects of import prohibition imports of specific goods would presumably be less severe, but qualitatively similar to the results reported in the study.

Faced with competing objectives in this simplified case, namely to choose a policy alternative to minimize counterfeit electronics from the supply chain and maximize economic prosperity, one can see that the different policy decisions may have potentially profound impacts on the stated objectives. While the agent-based modeling approaches can model the propagation of disruptions and the PI^+ model can forecast the results in terms of an array of economic indicators, this still leaves the decision maker faced with the challenge of choosing a course of action.

To this point, we have clearly articulated a set of objectives and identified several alternatives. In addition, criteria have been identified in which one can measure the effectiveness of the alternatives in meeting the objectives. For instance, employment, disposable income levels, and GDP were mentioned above as potential indicators of economic wellbeing. In addition, there must be a criterion that can assess whether the policy of on-shoring is achieving the goal of protecting against counterfeit parts—an example of such a criterion could be number of yearly incident reports of counterfeits found within the supply chain.

These criteria can then be weighted to reflect their relative importance to the decision maker. For instance, a general in the military may weigh the criterion of counterfeit parts avoidance heavily since that directly affects their mission effectiveness, whereas an economist may weigh the economic criteria most heavily since there are many other factors that govern the overall health of the economy. A representative of the semiconductor industry may choose a more even distribution of weights among the criteria, since both counterfeit avoidance and economic strength are important to the performance of the industry and individual firms within it. Figure 8 shows a general schematic of the decision-making process.

Through the PI^+ model, we may estimate the ultimate impacts of different policy measures on the economy in terms of the criteria identified above. In terms of counterfeit reduction, estimates from subject matter experts (e.g., number of identified counterfeit incident reports would likely fall to 50 per year) may be used. With these criteria weights and scores, alternatives can be comparatively ranked using MCDA algorithms, generally taking the linear additive form described above. In this way, alternative courses of action can be compared relative to one another based on a composite weighted score that considers not only the estimated performance of each alternative, but also the relative importance the decision maker or stakeholder group places on the relevant criteria.

6 Discussion and conclusions

One of the benefits of the framework is that it has multiple uses—both descriptive and normative. Descriptively, the combination of agent-based modeling and PI^+ can provide predictive insights on the impacts of disruptions within the cyber domain, such as in the first scenario. From a normative policy perspective, the inclusion of multi-decision criteria analysis can aid policymakers in assessing the trade-offs among multiple risks and downstream consequences associated with cybersecurity policy decisions, demonstrated in the second scenario. This trade-off analysis could be made in the first scenario as well with respect to different recovery efforts or policy actions that could make the economy more or less vulnerable to the cyber attack. Therefore, users have the option to include MCDA for decision support, or skip that step to descriptively assess the impacts of disruptions. Thus, this framework has the option to answer two critical questions: "What will the likely impacts be?" and "What should be done about it?" These answers can aid planners and policymakers in fortifying the gaps in budget allocation and vulnerabilities in infrastructure spending that are exposed by cyber attacks.

The uncertainty for some of the parameters used in the simulations will be significant. For example, precise quantities for parameters such as amount of risk aversion, lost production capacity due to a cyber attack or mitigation measure will not be possible to obtain. The flexibility of the modeling framework allows for the representation of uncertainty by running multiple instances of any given scenario and varying the simulation parameters for the precipitating event as well as the behavior of agents within the models through a bounded set of possibilities. However, this uncertainty in potential risk points toward future research in a complementary *resilience*-based approach, in which systems are designed within a cycle of preparation, absorption, recovery, and adaptation to not only defend against known threats, but bounce back from unknown threats (Linkov et al. 2013).

The scenarios presented in this paper are a conceptual study designed to illustrate the flexibility of the framework for exploring mitigation and policy options related to cyber attacks and cybersecurity by linking the options to economic consequences. Decision makers could use the framework in war-gaming exercises or preparedness studies (e.g., McCreight 2013) to explore policy options and mitigation strategies for cyber attacks. Future direction for this work includes moving from conceptual linkages between the modeling constructs to more formal and automated links where appropriate.

This modeling framework is critical in aiding the fulfillment of EO 13636 (2013) and other policy directives in that it will aid policy makers by allowing for the assessment of cyber attack scenarios and cybersecurity policies linked to their potential economic consequences. The link to consequences will aid in designing cybersecurity-related measures and safeguards. It will also help decision makers understand the lagged and indirect macroeconomic consequences of policy moves and mitigation measures, such as maintaining exchange rate targets or controlling capital inflows and outflows, within a powerful predictive decision framework.

Acknowledgments Permission was granted by the USACE Chief of Engineers to publish this material. The views and opinions expressed in this paper are those of the individual authors and not those of the US Army, or other sponsor organizations. Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the US Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Regional Economic Models, Inc. is a privately held company based in Amherst, MA and Washington, DC PI$^+$ is a licensed trademark of REMI.

References

Andrijcic E, Horowitz B (2006) A macro-economic framework for evaluation of cyber security risk related to protection of intellectual property. Risk Anal 26(4):907–923

Applequist GE, Pekny JF, Reklaitis GV (2000) Risk and uncertainty in man-aging chemical manufacturing supply chains. Comput Chem Eng 24(9–10):2211–2222

Associated Press (2013) Sony fined in UK over PlayStation cyber attack. http://abclocal.go.com/ktrk/story?section=news/technology&id=8966259 Accessed 8 April 2013

Belton V, Stewart T (2002) Multiple criteria decision analysis: an integrated approach. Springer, Boston

Cayirci E, Ghergherehchi R (2006) Modeling cyber attacks and their effects on decision process. In: Jain S, Creasey RR, Himmelspach J, White KP, Fu M (eds.) Proceedings of the IEEE 2011 winter simulation conference

Chen CL, Lee WC (2004) Multi-objective optimization of multi-echelon supply chain networks with uncertain product demands and prices. Comput Chem Eng 28(6–7):1131–1144

Cheng S-F, Lim YP (2009) An agent-based commodity trading simulation. Research Collection School of Information Systems (Open Access). Paper 838. http://ink.library.smu.edu.sg/sis_research/838

Clayton B, Segal A (2013) Addressing cyber threats to oil and gas suppliers. Council on foreign relations. http://www.cfr.org/cybersecurity/addressing-cyber-threats-oil-gas-suppliers/p30977

Cox LA Jr (2008) Some limitations of "risk = threat x vulnerability x consequence" for risk analysis of terrorist attacks. Risk Anal 28:1749–1761

Darley VM, Outkin AV (2007) A Nasdaq market simulation: insights on a major market from the science of complex adaptive systems. World Scientific Publishing, Singapore

Defense Science Board (DSB) (2013) Task force report: resilient military systems and the advanced cyber threat

Ehlen MA, Vargas VN (2013) Multi-hazard, multi-infrastructure, economic scenario analysis. Environ Syst Decis 33(1):60–75

Ehlen MA, Downes PS, Scholand AJ (2008) A mesoeconomic model of the regional impacts of natural and man-made disruptive events. Sandia National Laboratories SAND2009-0206 Report

Ehlen MA, Loose VW, Smith BJ, Vargas VN, Warren DE, Downes PS, Eidson ED, Mackey GE (2010) Economics definitions, methods, models, and analysis procedures for homeland security applications, Sandia National Laboratories Report SAND2010-4315, July 2010

Ehlen MA, Sun AC, Pepple M, Eidson ED, Jones BS (2014) Chemical supply chain modeling for analysis of homeland security events. Comput Chem Eng 60: 102–111 (forthcoming)

EO 13636 (2013) Executive Order 13636—improving critical infrastructure cybersecurity. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity. Accessed 8 April 2013

Fan W, Treyz F, Treyz G (2000) An evolutionary new economic geography model. J Reg Sci 40(4):671–695

Frick DE (2012) The fallacy of quantifying risk. Def AT&L 228:18–21

Fujita M, Krugman P, Venables AJ (1999) The spatial economy: cities, regions, and international trade. MIT Press, Cambridge, MA

Government Accountability Office (2012) Suspect counterfeit electronic parts can be found on internet purchasing platforms. GAO-12-375

Greenwood MJ, Hunt GL, Rickman DS, Treyz GI (1991) Migration, regional equilibrium, and the estimation of compensating differentials. Am Econ Rev 81(5):1382–1390

Guillen G, Mele FD, Espuna A, Puigjaner L (2006) Addressing the design of chemical supply chains under demand uncertainty. Ind Eng Chem Res 45(22):7566–7581

Hachman M (2011) PlayStation hack to cost Sony $171 million: quake costs far higher. http://www.pcmag.com/article2/0,2817,2385790,00.asp Accessed 8 April 2013

Howard RA (2007) The foundations of decision analysis revisited. In: Miles RF, von Winterfeldt D, Edwards W (eds) Advances in decision analysis. Cambridge University Press, Cambridge

Huang I, Keisler J, Linkov I (2011) Multicriteria decision analysis in environmental sciences: ten years of applications and trends. Sci Total Environ 409:3578–3594

Kallrath J (2002) Combined strategic and operational planning—an MILP success story in chemical industry. OR Spectr 24(3): 315–341

Keeney R (1994) Creativity in decision making with value focused thinking. Sloan Manag Rev 35:33–41

Keeney R, Raiffa H (1976) Decisions with multiple objectives; preferences and value trade-offs. Wiley, New York

Kirkwood CW (2002) Decision tree primer. http://www.public.asu.edu/~kirkwood/DAStuff/decisiontrees/index.html. Accessed 11 April 2013

Lababidi HMS, Ahmed MA, Alatiqi IM, Al Enzi AF (2004) Optimizing the supply chain of a petrochemical company under uncertain operating and economic conditions. J Eng Chem Res 43(1):63–73

Leontief WW (1986) Input-output economics, 2nd edn. Oxford University Press, New York

Levis AA, Papageorgiou LG (2004) A hierarchical solution approach for multi-site capacity planning under uncertainty in the pharmaceutical industry. Comput Chem Eng 28(5):707–725

Linkov I, Moberg E (2011) Multi-criteria decision analysis: environmental applications and case studies. CRC Press, Boca Raton, FL

Linkov I, Eisenberg DA, Bates ME, Chang D, Convertino M, Allen JH, Flynn SE, Seager TP (2013) Measurable resilience for actionable policy. Environ Sci Technol 47(18):10108–10110

McCreight R (2013) Scenario development: using geopolitical wargames and strategic simulations. Environ Syst Decis 33(1): 21–32

Moore T (2010) The economics of cybersecurity: principles and policy options. Int J Crit Infra Prot 3:103–117

National Infrastructure Simulation and Analysis Center (NISAC) (2011) Banking and finance capability development

National Infrastructure Simulation and Analysis Center (NISAC) (2013) Global finance capability development report

New York Times (2012) Aramco says cyberattack was aimed at production. http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0. Accessed 9 April 2013

Outkin A, Flaim S, Seirp A, Gavrilov J (2008) FinSim: a framework for modeling financial system interdependencies. In: Yang A, Shan Y (eds) Applications of complex adaptive systems. IGI Global, Hershey

Parfomak PW (2013) Keeping America's pipelines safe and secure: key issues for congress. Congressional Research Service R41536

Parnell G (2007) Value-focused thinking using multiple objective decision analysis. In: Lorech A, Rainey L (eds) Methods for conducting military operational analysis: best practices in use throughout the department of defense. Military Operations Research Society, Arlington

Pecht M, Tiku S (2006) Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectr 43(5):37–46

Perea-Lopez E, Grossmann IE, Ydtsi BE, Tahmassebi T (2001) Dynamic modeling and decentralised control of supply chains. Ind Eng Chem Res 40:3369–3383

Petkov SB, Maranas CD (1997) Multiperiod planning and scheduling of multiproduct batch plants under demand uncertainty. Ind Eng Chem Res 36(11):4864–4881

Regional Economic Models, Inc. (REMI) (2013) Model equations. http://www.remi.com/download/documentation/pi+/pi+_version_1.5/REMI_PI+_v1.5.pdf. Accessed 12 July 2013

Renault F, Beyeler WE, Glass RJ, Soramaki K, Bech ML (2009) Congestion and cascades in interdependent payment systems. Sandia National Laboratories SAND 2009-2175 J Report

Rinaldi S, Peerenboom J, Kelly T (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag 21(6):11–25

Rose AZ, Leung B, Beeler GR, Wei D (2009) Macroeconomic impacts of shutting down the US borders in Response to a security or health threat. In: Gordon P, Moore JE II, Richardson HW (eds) Global business and the terrorist threat. Edward Elgar Publishing Limited, Cheltenham

Saaty T (1980) The analytic hierarchy process. McGraw Hill, New York

Santos JR, Haimes YY, Lian C (2007) A framework for linking cybersecurity metrics to the modeling of macroeconomic interdependencies. Risk Anal 27(5):1283–1297

Schwartz E, Smith JE (2000) Short-term variations and long-term dynamics in commodity prices. Manage Sci 46(7):893–911

US White House (2009) Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. Accessed 12 July 2013

US Senate (2010) Senate report 111-384, Cybersecurity Act of 2010, Report of the Committee on Commerce, Science, and Transportation on S. 773, December 22, 2010

Shao G, Treyz GI (1993) Building US National and regional forecasting and simulation models. Econ Syst Res 5(1):63–76

Sood B, Das D, Pecht M (2011) Screening for counterfeit electronic parts. J Mater Sci: Mater Electron 22:1511–1522

Tehranipoor M, Koushanfar F (2010) A survey of hardware Trojan taxonomy and detection. IEEE Des Test Comput 27(1):10–25

Tesfatsion L (2006) Agent-based computational economics: a constructive approach to economic theory. In: Tesfatsion L, Judd KL (eds) Handbook of computational economics, vol 2: agent-based computational economics. Elsevier, Amsterdam

Timpe CH, Kallrath J (2000) Optimal planning in large multi-site production networks. Eur J Oper Res 126:422–435

Treyz GI (1993) Regional economic modeling: a systematic approach to economic forecasting and policy analysis. Kluwer Academic Publishers, Norwell, MA

Treyz GI, Treyz F (1997) The REMI multi-regional U.S. policy analysis model. North American Regional Science Association

Treyz GI, Rickman DS, Hunt GL, Greenwood MJ (1993) The dynamics of U.S. internal migration. Rev Econ Stat 75(2):209–214

US Department of Commerce (2010) Defense industrial base assessment: counterfeit electronics. http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf. Accessed 11 April 2013

von Winterfeldt D, Edwards W (2007) Defining a decision analytic structure. In: Miles RF, von Winterfeldt D, Edwards W (eds) Advances in decision analysis. Cambridge University Press, Cambridge

Welch LD (2011) Cyberspace—the fifth operational domain. IDA Research Notes. https://www.ida.org/upload/research%20notes/researchnotessummer2011.pdf. Accessed 12 July 2013

Yergin D (1990) The prize: the epic quest for oil money & power. Free Press, New York