

The Critical Link

Financial Implications of National Security Threats

Co-sponsored by
United States
Naval War College
and

Cantor Fitzgerald



EXERCISE REPORT

Economic Security Exercise II

June 1998



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 1998		2. REPORT TYPE		3. DATES COVERED -	
4. TITLE AND SUBTITLE The Critical Link: Financial Implications of National Security Threats				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval War College, Newport, Ri, 02841				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT see report					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 79	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Economic Security Exercise II

June 1998

DISCLAIMER

This report was prepared by staff of the U.S. Naval War College, Newport, Rhode Island, with input from experts within and outside the U.S. government. The information was designed expressly for use in the Economic Security Exercise of 1 June 1998 and should not be utilized for any other purpose. The postulated scenario was formulated expressly to challenge exercise participants with situations and issues that could pose major problems for U.S. economic interests and national security. The scenario should not be inferred to represent expected or desired future conditions and does not constitute an official position of the U.S. Naval War College or any other U.S. government agency.

Cover illustration of tiger: Reprinted by permission from UPSIDE MAGAZINE, March 1998, www.upside.com. Illustration by Richard Merchan.

THE CRITICAL LINK:
Financial Implications of National Security Threats

A Report of
ECONOMIC SECURITY EXERCISE II

01 June 1998

Prepared by
Bradd C. Hayes

The contents of this report reflect the views of the author and are not necessarily endorsed by Cantor Fitzgerald, the Naval War College, or any other department or agency of the United States Government.

ACKNOWLEDGMENTS

The author expresses his gratitude for the thoughtful review and comments provided by Theophilos Gemelas, Lawrence Modisett, Paul Taylor, Andres Vaart, Jim Hart, Stuart Starr and John Woodward. Gregory Hoffman and Professor Gemelas also provided valuable analytical assistance. Any errors contained in the report, however, are solely the responsibility of the author.

Table of Contents

I. The Economic Security Exercise Series	1
Background	1
Purpose and Objectives	1
Report Outline	2
II. Basic Scenario and Economic Benchmarks	3
Background	3
Benchmarks	3
III. Phase One – Regional Crisis 1998–99	4
Response to Phase One	7
IV. Phase Two — US Intervention	8
Response to Phase Two	9
V. Phase Three — Information Crises	11
Background	11
Initial Cyber-attacks	12
Response to Initial Cyber-attack	12
Follow-on Cyber-attack	13
Response to Follow-on Cyber-attack	14
VI. Phase Four — Possible End States	15
End State One — Restoration of Order by Moderate Military Regime	15
Response to End State One	15
End State Two — Islamic Nationalist State	16
Response to End State Two	16
End State Three — Balkanization of Indonesia	17
Response to End State Three	18
VII. Exercise Analysis and Observations	19
Voting	19
General Observations and Policy Implications	24
General Observations	24
Policy Implications	25

Appendix A	27
Participants	27
Appendix B	30
Department of State Background Notes on Indonesia.....	30
Appendix C	45
The Importance of the Straits and Spratly Islands Region	45
Appendix D	51
PDD 63 Fact Sheet & White Paper	51
Appendix E	68
Polling Data.....	68

I. The Economic Security Exercise Series

Background

For most of the past century, the Naval War College has helped the national security community examine potential consequences of a wide range of crisis scenarios. Historically military and diplomatic responses were the focus of these activities. Because the number and types of issues affecting national security continues to grow, however, national security is no longer the special enclave of diplomats and soldiers. It was less than a decade ago that economic issues were first addressed in the President's *National Security Strategy*, and they were shortly joined by environmental issues as challenges that could adversely affect the nation. In October 1997, the Naval War College, in partnership with Cantor Fitzgerald, conducted the initial Economic Security Exercise exploring the link between maritime security issues and global financial markets.



Since economic issues have not been a central focus of most games or decision events conducted at the Naval War College, pursuing a partnership with the financial community was a logical course. Several senior members of Cantor Fitzgerald have close professional ties with the United States Navy, making this a natural partnership. Cantor Fitzgerald provides a broad spectrum of institutional brokerage and execution services to global financial markets. It operates the world's largest electronic marketplace for G-10 sovereign debt, emerging markets and Eurobonds and is one of the largest "third market" equity operations in the US stock market. The success of the first Economic Security Exercise encouraged both institutions to conduct a follow-on event in order to broaden and deepen the discussion.

Like the initial Economic Security Exercise, this workshop brought together key figures from the national security, governmental, and financial communities to explore and test the relationships between international events, national security, and financial markets. Participants (see Appendix A) included currency, commodity, fixed income, and securities traders. The overall purposes of the exercise were to draw insights and, where possible, explore options about how the various communities can work together to mitigate the unexpected effects of crises.

Purpose and Objectives

For much of the past decade, analysts have insisted that America's economic future is closely tied to Asia. They have noted that over the past 10 years most of the 3 billion people who have joined the international market economy live in that region. Such predictions seemed reasonable as one emerging "Asian

tiger” after another reported impressive economic growth and development. But the troubling events of 1997 demonstrated that a future tied to a stagnant or shrinking Asian economy could contain grave financial risks for the US. Hence, during this exercise participants were asked to:

- ◆ explore the financial implications of a security crisis in Southeast Asia involving violence and US forces, and
- ◆ discuss measures that could be taken to prevent or mitigate the consequences of a disruption in international financial markets.

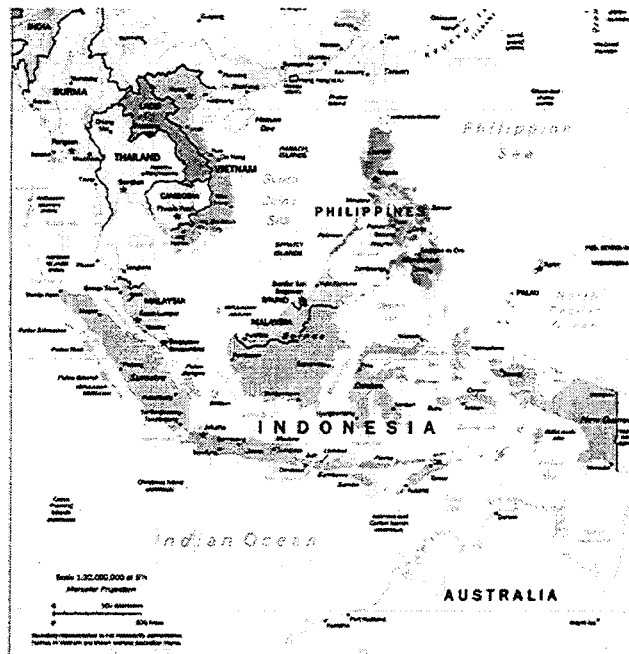
Report Outline

This report:

- ◆ details the scenario used during the exercise,
- ◆ notes participant responses, and
- ◆ analyzes exercise results.

The appendices provide:

- ◆ a participant list,
- ◆ other background data given to the players, and
- ◆ voting data.



Map 1. Southeast Asia

II. Basic Scenario and Economic Benchmarks

Background

When this scenario was selected, many Asian economies were already in a financial morass, but Indonesia had not yet experienced widespread violence or political upheaval. The timeliness of the exercise became evident when the fictional scenario was almost overtaken by events. The exercise focused on a regional crisis in Southeast Asia that unfolded over four phases. Phase One was the onset of the crisis. Phase Two posited the intervention of US forces. Phase Three saw the crisis spread when a serious blow was dealt to the regional infrastructure used to exchange global financial data. Phase Four looked at three alternative end states. The timeframe for the scenario was late 1998–early 1999. The scenario was selected because it presented real challenges in what recent events proved to be an all too plausible setting. Even so, it was not intended to be predictive. As a recent *New York Times* article noted, businesses are using scenarios to examine their options precisely because the future cannot be predicted.¹

One of the objectives of this exercise was to obtain expert opinions on how various financial indicators would react to hypothetical security events, using Delphi polling techniques. Eight indicators were selected: the price of gold and oil, the Dow Jones Industrial Average, the Nikkei average, the values of the yen and Deutsche mark against the dollar, and the yields on 3-month Treasury bills and 30-year Treasury bonds. Table 1 shows the notional benchmarks that were established for these indicators at the beginning of the game, against which participants' reactions could be measured.

Benchmarks

Gold and Oil

Gold and oil prices generally are the most sensitive commodity values to international crisis scenarios. Gold was expected to change because there is often a “flight to quality” when other types of investment are unsure or at risk. Oil was selected because the scenario involved strait closures that could triple its delivery costs.

¹ Steve Lohr, “Long Boom or Bust,” *The New York Times*, 2 June 1998, p. D1.

Dow Jones and Nikkei Averages

Although many of the world's stock markets would react to the crisis, the Dow Jones and Nikkei were selected because they measured the impact on two of the world's most important economies. The expectation was that the Nikkei would fluctuate the most in this scenario because a significant portion of Japanese trade passes through Southeast Asia, including over 80 percent of its oil imports.

Currency Exchange Rates

A number of currencies could have served as indicators of the effects of the crisis. The yen and Deutsche mark exchange rates against the dollar were selected because of their global importance. The exercise's timeframe was before the euro is scheduled to be placed into wide circulation; therefore, the Deutsche mark was selected to indicate the effect on the European economy.

US Treasury Securities

US Treasury securities (3-month T-bills and 30-year bonds) were selected to determine what the short- and long-term effects of the crisis might be on the US economy. Yield to maturity, rather than discount, rates were used.

Indicator	Benchmark
Gold	US\$300/ounce
Oil	US\$15/barrel
Dow Jones	10000
Nikkei	15000
Yen	125/\$
Deutsche Mark	1.75/\$
3-Month Treasury Bill	5.75% yield to maturity
30-Year Treasury Bond	6.00% yield to maturity

Table 1: Notional benchmarks for economic indicators

III. Phase One – Regional Crisis 1998–99

With the Indonesian economy mired in a region-wide recession that began in 1997, President Haji Mohamed Suharto, who faced increasing pressure to step aside from both his supporters and detractors, announced in May 1998 his decision to retire from public life. His controversial deputy, Dr. Bucharuddin Jusuf Habibie, with the putative backing of the military, was named interim

president to serve out the remaining three years of Suharto's term. See Appendix B for more information about Indonesia.

The exercise scenario postulated that opposition forces seized this opportunity to mount successful rebellions in Sumatra and parts of Java. Buoyed by their success, leaders of this opposition movement declared themselves the legitimate government and stated that their intention was to seize Jakarta.

President Habibie tried to strengthen his position by promoting his strongest supporters — former hard-line Suharto loyalists — to the highest positions in Indonesia's defense community. In doing so, he marginalized the moderate head of the armed forces, General Wiranto. This caused a deep rift in the military and many former Wiranto supporters, including the Indonesian Navy, defected to the opposition movement.



President B. J. Habibie

Faced with a devalued currency (see Figure 1) and continued high (if not hyper-) inflation, leaders of the "opposition government" repudiated the conditions established by the International Monetary Fund (IMF), asserting that such programs unduly infringed on the nation's sovereignty. This stand was embraced by Indonesia's suffering population, and the opposition leadership promised to find a new, self-reliant way of solving the economic crisis.

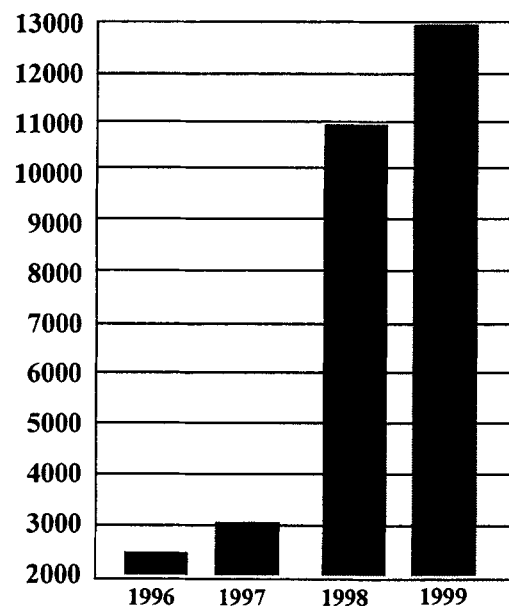


Figure 1. Devaluation of the rupiah versus the dollar.

Asserting that the onerous requirement to service foreign debt was the primary weapon in a conspiracy to keep emerging Asian nations from joining the upper tier of industrialized states, opposition leaders threatened to default on foreign loans. They also heightened racial tensions by accusing ethnic Chinese and foreigners living in Indonesia of being accomplices in this conspiracy. The ethnic Chinese were singled out because they controlled the vast majority of investment capital in the country (see Figure 2). Violence against these groups rose sharply. To raise working capital, the rebel leadership declared passages through the Indonesian archipelago (the Malacca, Sunda, and Lombok Straits – see Appendix C) to be sovereign territorial waters and stated its intention to levy tariffs on shipping using these vital waterways.²

Widespread violence resulted in thousands of refugees fleeing into Singapore, the Philippines, Australia, and Malaysia. The sitting interim government in Jakarta appealed for international (particularly US) help. Australia and Singapore also encouraged the US to increase its naval presence to help stem refugee flows, assist in non-combatant evacuation operations, and help restore order in Indonesia. Malaysia, on the other hand, viewed the crisis as an opportunity to raise much needed foreign capital to help further its recovery. It became the first state to recognize the opposition government and declared its intention to help enforce and share in collecting tariffs on ships desiring transit through the Strait of Malacca. Hoping to influence the Singaporean government to back off its request for US assistance and from providing assistance to US warships, Malaysia deployed forces along its border with Singapore.

The rebel Indonesian government made good on its threats by stopping a Japanese supertanker and a US Maritime Administration ship in the Malacca Strait. During the operation, the master of the Japanese ship was killed. Smaller ships were also boarded in other straits. A press bulletin from the White House decried this turn of events and announced that the National Security Council had taken the matter under consideration.

Although concerned about the treatment of ethnic Chinese in Indonesia, the Peoples' Republic of China (PRC) declined to become actively involved in regional events—fearing such involvement would be contrary to policy decisions made by the 1998 National Peoples' Congress and would interfere with ongoing talks with Taiwan. Despite the threat to its economy, Japan limited its activities to non-military measures because of constitutional constraints on its use of armed forces as well as regional sensitivities to Japanese military activity. Other Asian nations (such as the Philippines, Thailand, and South Korea) also remained aloof, fearing involvement could disrupt their own economic recoveries.

² For some time, Indonesia has been seeking control of its waterways under a policy of having them declared “archipelagic sea lanes.”

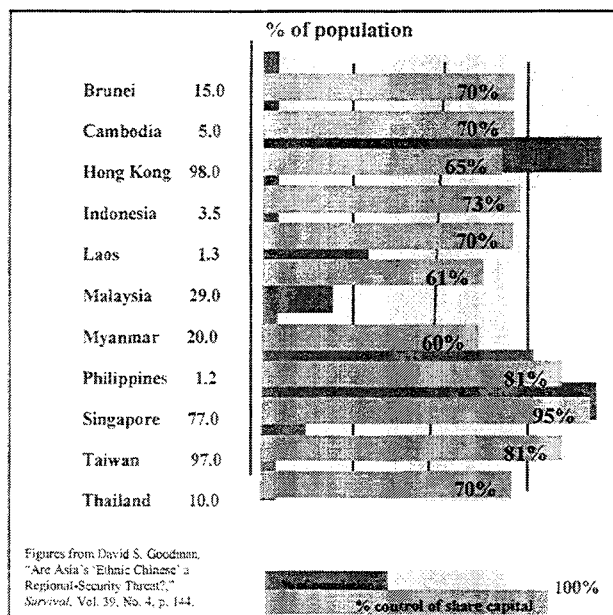


Figure 2. Ethnic Chinese and their control of wealth in Southeast Asia

Response to Phase One

Participants were interested in exploring the motivation behind the insurgent action in the straits (money and international recognition of their authority); the reaction of other oil producing Muslim states (wait and see); the prospects for a regional coalition forming to oppose the rebels (one did); and why China assumed a hands off policy—especially since ethnic Chinese were targets of violence (see above). Some participants were troubled by Malaysia's support for the rebels, noting that this would signal the end to cooperation among the Association of Southeast Asian Nations (ASEAN).

A government participant noted that hikes in the price of oil would go beyond those necessary to offset increased transportation costs, which alone could raise oil prices \$1 to \$2 a barrel. If the straits were closed, Japan, rather than dipping into its strategic reserves, would turn to Alaska and Venezuela as alternative sources of oil. Since this oil would normally have gone to US markets, competition for it would also drive crude prices higher. Closure of the Malacca Strait would also affect Singapore, which supplies refined petroleum products to the region. According to one analyst, Singapore does not hold large reserves and a shortage of petroleum products would undoubtedly be felt throughout Southeast Asia. An opposing view was that despite initial crude oil price hikes, long-term prices would decline because the supply/demand balance would continue to be favorable to consumers.

Figure 3 shows the percentage change for each of the indicators following participant voting. For US securities, the figure represents the change in yields. *Only participants from the financial community were asked to vote.*

Several voters expressed the view that even though oil prices would spike they did not expect the long-term trend to be inflationary. Hence, there was virtually no movement in long bonds. One participant believed the vote underestimated the amount of money that would flow into T-bills. Voters also believed, as demonstrated by the stability of the Deutsche mark, that the crisis would have little initial effect on Europe. Since the crisis would have the greatest impact on Japan's economy, both the Nikkei and the yen were adversely affected, with the Nikkei falling nearly ten percent and the yen losing almost seven percent against the dollar.

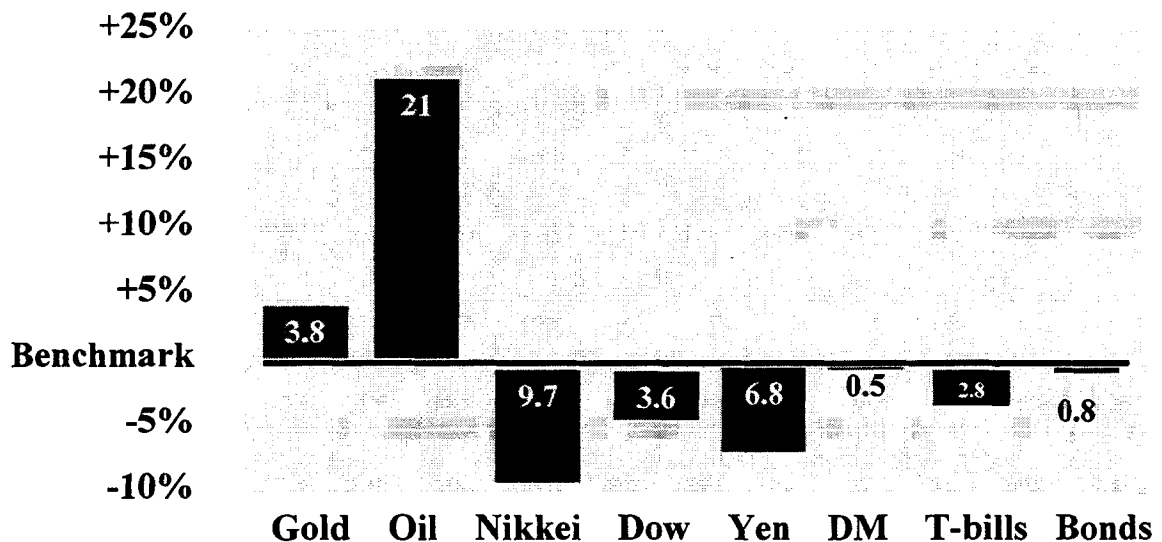
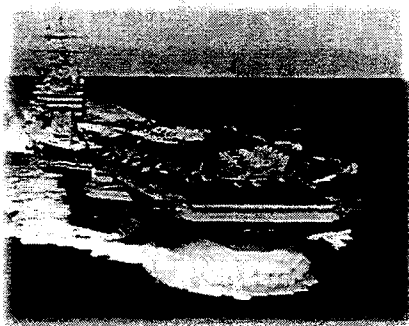


Figure 3. Percentage change in indicators following Phase One voting

Although there was some variation in voter numbers, all participants were on the same side of the benchmark for the first five indicators. Participants had mixed views concerning the effect of the crisis on the European and US economies. This uncertainty was reflected in the fact that they placed votes on both sides of the benchmarks for the last three indicators (Deutsche marks, T-bills, and long bonds).

IV. Phase Two — US Intervention



Phase Two posited a military intervention by the United States in response to ongoing events in Indonesia and the straits. Violence continued to increase, especially in Jakarta. Habibie supporters were reported to have fired on demonstrators throughout the archipelago. Forces responding to the crisis included a carrier battle group, an amphibious ready group, and selected Air Force units. They were able to free held vessels, but not before insurgents,

frustrated at losing control of the straits, effectively closed the straits by scuttling ships in shallow transit lanes. Smaller vessels that managed to get through were attacked by small boats using rocket-propelled grenades and by land-based aircraft. Mining of critical channels was also reported. On the Singapore/Malaysia border, gunfire was regularly exchanged and aircraft routinely flew threatening patrols. China continued to acquiesce to US leadership. Japan, Singapore, and Australia offered naval and other units in support.

Response to Phase Two

One government participant noted that during this phase the United States would be actively collaborating with China (first and foremost), Japan, Australia, and other members in the Asia-Pacific Economic Cooperation process. He indicated that US concerns, in order of priority, would be protection of American citizens, economic considerations, and broader strategic issues (such as freedom of navigation and other law of the sea matters). He insisted that the US would not act unilaterally in this matter, except if an evacuation of US citizens became necessary, preferring to take a broad-based multilateral approach. He also indicated that the US would be looking for ways to deny the rebels benefits from their activity. The least desirable would be “shooting options.”

One military participant noted that scuttled ships and straits closures indicated that the intervention had not gone well—a situation that he would have found disappointing had he been in command. He believed that the military could have prevented the straits from being closed, thus averting the economic crisis such action would cause. He asserted that, if necessary, the US could act unilaterally in the strait in accordance with the Law of the Sea agreement. His comments reassured one financial community participant who asked if an insurrection group could really challenge the world’s largest navy and succeed in disrupting global markets. Another military participant noted that hostile conditions could considerably lengthen salvage operations (perhaps taking months to complete). It was also noted that piracy and other acts of violence against shipping would complicate the military’s challenge.

A government analyst indicated that closure of the Malacca Strait would mean that all excess tanker capacity would quickly disappear. He indicated that the Saudis could increase production to make up for any loss of Indonesian oil, but he anticipated that oil prices would nonetheless rise between three and five dollars per barrel. Another government participant noted that this scenario would be taking place during the period when most analysts have predicted that an economic recovery in Asia would begin, effectively putting a stop to that recovery.

Figure 4 shows how participants believed economic indicators would react to Phase Two developments. The benchmark used was the consensus vote from the previous phase. In comparison to Phase One results, Phase Two voting showed much less change. One participant commented that developments in this phase did not significantly alter the situation. Another was surprised, however, that the Nikkei did not drop further.

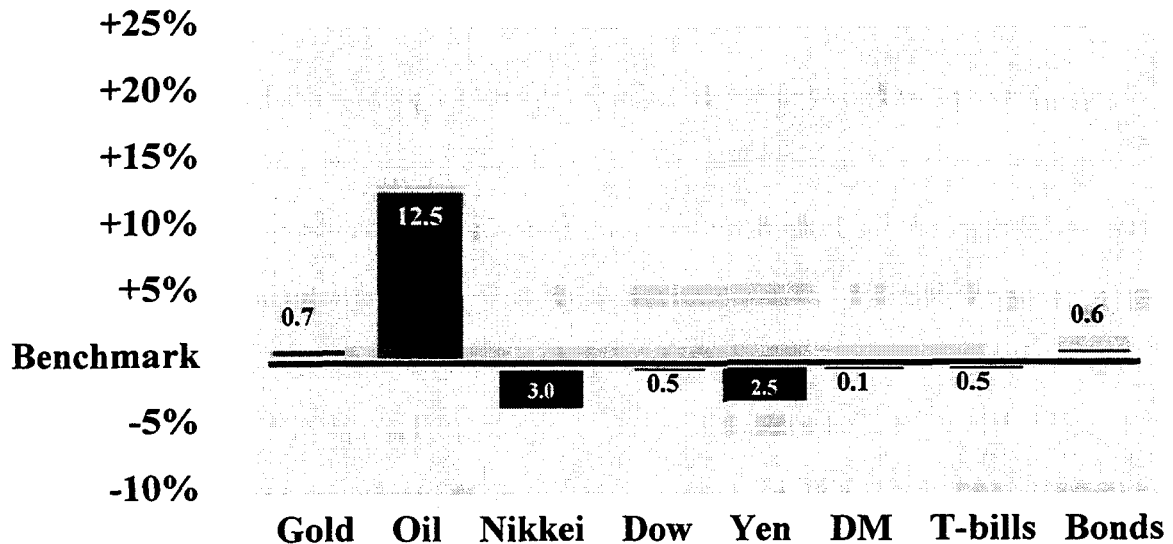


Figure 4. Percentage change in indicators following Phase Two voting

The most dramatic outcome of Phase Two voting was another 12.5 percent hike in the price of oil. One participant pointed out that increased crude prices could remain in place for a lengthy period; he was therefore surprised that the security market remained stable. Another participant speculated that this crisis could prompt a withdrawal of investment money from emerging markets, including Russia. This, in turn, would have a much greater effect on Europe than the votes on the Deutsche mark (which stayed remarkably stable) would lead one to conclude. One financial analyst believed the variable that would have the greatest effect on markets was how decisively the US Government addressed the crisis. If it quickly assumed a strong leadership role, he believed only short-term spikes in the indicators would result. If it hesitated or forfeited leadership, he believed long-term inflationary reactions would result.

Another analyst speculated that with Japan in trouble and Hong Kong feeling the effects of the crisis, China would be forced to consider devaluation of its currency. He feared that such an event would be the catalyst for a renewed region-wide economic crisis.

V. Phase Three — Information Crises

Background

Non-voting participants from the Mitre Corporation presented the information warfare (IW) phase of the exercise.³ They began their presentation by reviewing conclusions of a task force that examined critical infrastructures in the United States. They noted that more and more sectors of society are linked by critical relationships that are vulnerable to cyber-attacks (see Figure 5). Particularly critical are the interlinking vulnerabilities of the information and electric power infrastructure.

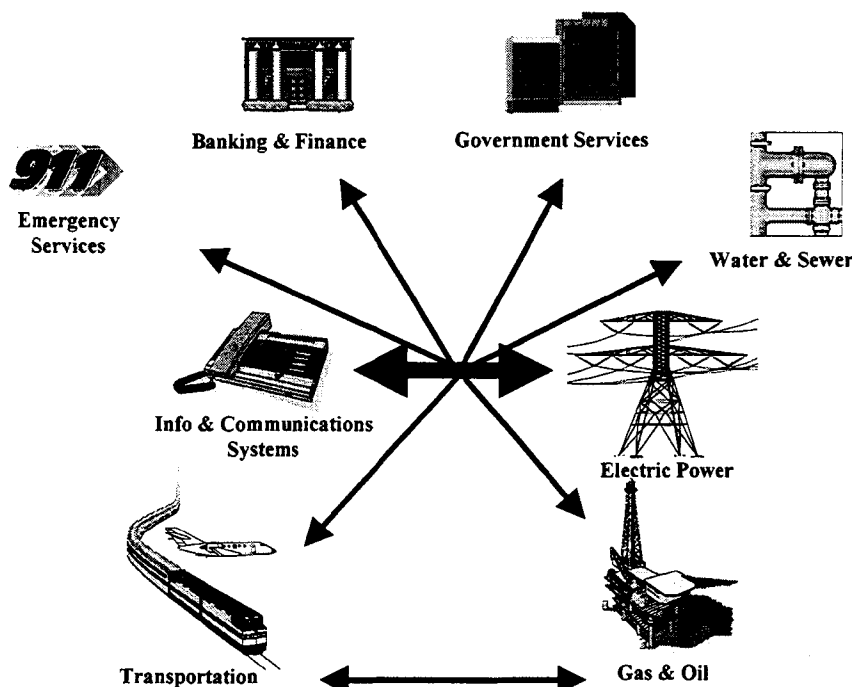


Figure 5. Critical infrastructure relationships.

They also presented background material and case studies to demonstrate that the attacks proposed in the scenario were plausible. Less than two weeks prior to the exercise, "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63" (PDD 63) had been signed (see Appendix D). The directive's proposal for government/community cooperation was briefly discussed.

³ Information Warfare is a catch-all phrase for a number of concepts. IW attacks can be mounted against the military, the government, or society. Among the areas covered by this phrase are: Command and Control Warfare, Electronic Warfare, Intelligence-based Warfare, Hackerwar, Cyberwar, Economic Info-warfare, and Psychological Warfare. For additional information, see Martin C. Libicki, "What is Information Warfare?" *Strategic Forum*, No. 28, May 1995, National Defense University, Institute for Strategic Studies.

Initial Cyber-attacks

The information crisis occurred several weeks after the beginning of widespread unrest in Indonesia. The weakened central government was unable to quell insurgents, whose primary goals became overthrowing the Habibie government and punishing the financial markets that the insurgents believed served to oppress the people. These goals were viewed as mutually supportive in that a downturn in one area would be mirrored in the other.

The insurgents had several secondary aims as well. First, they needed to acquire resources in order to fund their activities. Second, they wanted to minimize the role of foreign financial institutions in the region, believing that Indonesia's future would be brighter if left alone. Finally, they wanted to deter other nations from supporting the Habibie regime.

The insurgents managed to attract supporters among younger members of the educated elite in key software management and financial institutions. Those dealing in software specialized in solving the "Year 2000 Problem" (Y2K).⁴ These individuals launched coordinated insider attacks against Singapore on 19 March 1999.

The initial attack targeted selected Singapore financial institutions. Using the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system, malevolent insiders in Malaysia and Indonesia transmitted a large number of apparently legitimate, but actually bogus, transactions. The result was widespread confusion in Singapore's financial community. Shortly after the initial attack, Singapore's electric power and telecommunications systems were disrupted so that targeted firms were unable to close or reconcile their accounts. The electric power sector was forced off line using dial-up access to distribution sub-station power control networks to create surges that damaged critical high-voltage transformers. Signal Transfer Point (STP) computers were the critical nodes in the telecommunications sector attacks. They were spoofed to halt power generation by repeatedly sending them "kill" commands on the signaling channel. As a result, network services throughout the area were either intermittent or non-existent.

Response to Initial Cyber-attack

Figure 6 provides the results of the voting that took place at the end of this phase. Once again the benchmark represents the consensus vote from the previous phase.

⁴ The Y2K problem deals with the challenge created by some computer systems that manipulate data using only the last two digits of the year. Hence, these programs cannot differentiate between 1900 and 2000 and may create havoc in data bases maintained by these programs.

One analyst was surprised that others believed investors would continue to show confidence in the markets following the attacks. Hence, he placed the price of gold much higher than most. Others agreed that the anxiety that would be created throughout the financial community was probably not accurately reflected in the votes. Under these conditions, one participant indicated he would have advised his clients to place their money in short-term securities until circumstances sorted themselves out.

On the other hand, many believed that because investors would flee emerging markets and put their assets in more stable portfolios, the Dow would rise rather than decline as money moved towards American investments. Some non-voting participants wondered why a cyber-attack would affect the price of oil. Several voting members explained that they raised oil prices because these attacks meant that the insurgents were much more powerful and clever than previous events indicated.

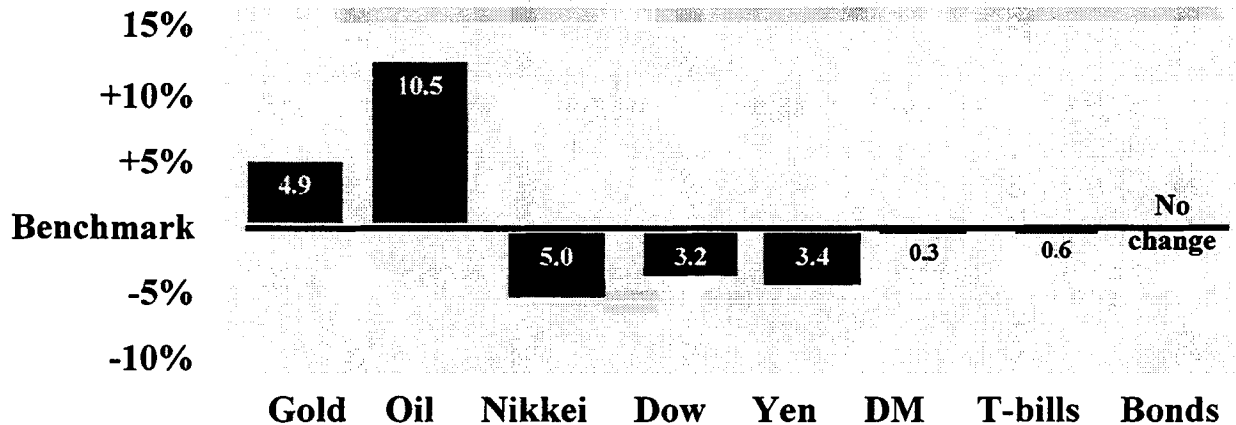


Figure 6. Percentage change in indicators following initial cyber-attack

Follow-on Cyber-attack

Ten days later, two days before the end of Japan's fiscal year, another info-attack was launched against financial institutions in Japan that had strong ties to businesses in Indonesia. During these attacks, the accounts of targeted Indonesian businesses were looted, and the funds transferred into accounts controlled by the rebels. To cover these lost holdings, Japanese financial institutions were compelled to auction off major holdings in US Treasury securities. These attacks resulted from programmers sympathetic to the rebels planting malicious code in software used to resolve the "Year 2000 Problem." When triggered, this software caused massive, illicit shifting of funds from accounts of Indonesia's "capitalist cronies" into those of the insurgent leaders.

Response to Follow-on Cyber-attack

An interesting discussion concerning the Y2K problem followed the presentation of this phase of the exercise. It was stated that many of the systems requiring a fix are written in COBOL, and since COBOL is an older programming language, those knowing it are in short supply. Hence, many companies hiring programmers are less concerned about background checks than professional skills. Malicious code has already been discovered in software purchased overseas by American companies. Their reliance on imported code is likely to increase. One government participant noted that the malicious code problem is becoming more difficult because many software companies are leaving old code in upgraded programs rather than removing it. Another participant noted that his organization has set up a test site and runs new programs on it before introducing them into actual operation. He was told, however, that testing software does not necessarily uncover malicious code. Only an examination of code line-by-line is likely to uncover potentially damaging code.

Figure 7 provides the voting results for this phase. The benchmarks were the consensus figures from the previous phase's voting.

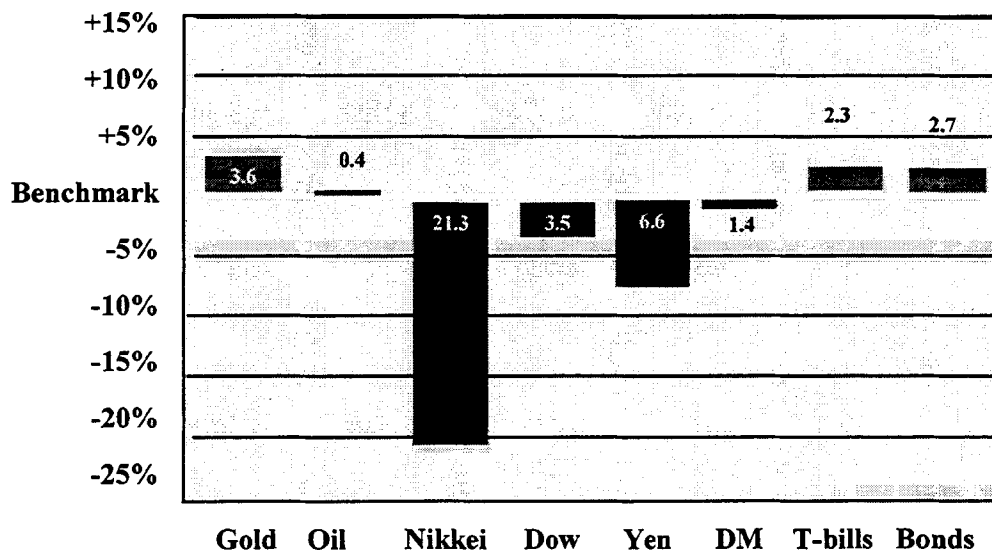


Figure 7. Percentage change in indicators following second cyber-attack

As dramatic as the decline of the Nikkei was in the consensus vote, some participants believed it would have fallen even further as a result of the loss of investor confidence. Some believed that the only companies holding Japanese equities at this time would be Japanese companies. There was some discussion about the relationship between the sell-off of US securities by Japanese institutions and the exchange rate of the yen. At least one participant believed that this sell-off would have stabilized the yen. He also believed the Bank of Japan would have been very active in trying to protect the yen. However,

another participant observed that it might have been wise for the Bank of Japan to elect not to defend the yen, noting that if it tried and failed, the yen would truly go into “free fall.”

The view was also expressed that at the 150 yen to the dollar level, China would be compelled to devalue its currency and this would cause a new round of devaluations throughout the region.

One voter believed that long bonds would have reacted more strongly as a result of investors fleeing to quality because of uncertainty.

VI. Phase Four — Possible End States

Following scenario discussions, participants were asked to consider three possible end states for the crisis—none of which, it was pointed out, were very sanguine. All end states were briefed as occurring approximately six months after the cyber-attacks. It was noted that they were end states in name only, since none represented a return to stability.

End State One — Restoration of Order by Moderate Military Regime

This end state posited the post-Suharto government losing control of the country. Fearing anarchy and violence, the moderate wing of the military felt compelled to restore order. A moderate interim military government was installed whose aim was to reestablish civilian rule as soon as possible. The new government had to walk a fine line between implementing IMF reforms on the one hand and quelling internal dissatisfaction on the other. The government often pled for concessions and selective relief from IMF conditions. The new government found it difficult to end cronyism and dismantle the commercial empire established by the Suharto family. It tried to sustain high technology programs initiated under Suharto, but was only partially successful. Violence and refugees remained a problem. Encouraged by the short-lived rebellion, separatists in East Timor and West Sumatra remained active. US military forces were withdrawn as the straits opened and violence receded, but piracy and other activities that impeded the flow of shipping remained a problem.

Response to End State One

Some participants noted that, as dismal as it was, this was the best of the end states. Figure 8 details the results of voting. The benchmark for this and all other end states was the consensus vote following the second cyber-attack.

Since it was the most optimistic of the end states, almost all of the indicators moved toward pre-crisis levels. The most vociferous discussion following the

voting concerned oil. Some participants believed that crude prices would not decline as quickly as the voting suggested.

Some participants believed that this end state would help draw the world recession to a close and that all sectors would begin to concentrate on development. They stated that this would have a significant effect on sovereign securities. US instruments should be more attractive and bond rates should decline.

Other participants believed that the rapid return to normalization was an artifact of the exercise and that normalization would not be so quick in returning.

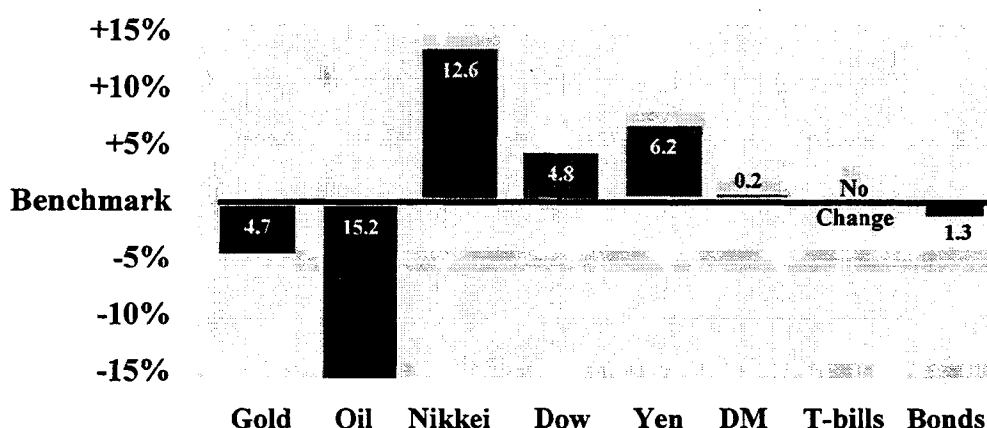


Figure 8. Percentage change in indicators following End State One voting

End State Two — Islamic Nationalist State

End state two posited that Islamic nationalists managed to oust the successor government. A populist, Muslim leader took control and halted violence against foreigners and non-ethnic Indonesians, but Westerners were asked to leave. The country eased into a barter economy and the government made the currency non-convertible. Foreign debt payments were suspended, bringing an end to IMF assistance. Free passage through the straits was restored, but the new government was unable to stop harassment by pirates and others who routinely impeded the flow of shipping. Following the initial flight of non-ethnic Indonesians and Suharto supporters, refugee flows were reduced dramatically. US military forces were withdrawn as the straits opened and violence receded. Since high oil prices persisted, South Korea, the Philippines, and Thailand all faced renewed balance of payment problems, and China was compelled to devalue the renminbi.

Response to End State Two

Throughout the game some participants urged US policymakers to push for sanctions against the Indonesia rebels. They believed this takeover could have

provided enough impetus for sanctions finally to be considered. Participants also believed that the establishment of a barter economy would result in an increase in economic refugees. Unlike the wealthy ethnic Chinese that fled earlier in the scenario, these refugees would have difficulty finding sanctuary. Some participants believed that this end state would result in the Chinese devaluing their currency by as much as 30 percent.

Figure 9 details the results of voting. Once again the benchmark was the consensus vote following the second cyber-attack.

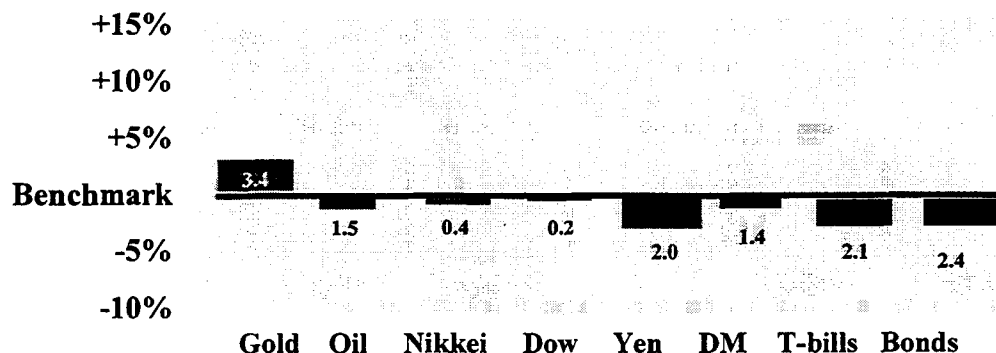


Figure 9. Percentage change in indicators following End State Two voting

One analyst was surprised that oil prices remained stable. He believed this stability meant that most voters assumed oil prices would remain high. He then wondered why they also believed long bonds would maintain a six percent yield. Another participant indicated that the crisis would produce a “fixed bump” in oil prices and that the world would remain in recession. Several agreed that the outlook for long-term stability would not be good. The counter argument was that the devaluation of the Chinese currency would drive prices down, partially offsetting the increase in oil prices.

Looking at the voting results, one government analyst agreed with voters that the uncertainty created by this end state would cause a flight to gold.

End State Three — Balkanization of Indonesia

The final end state posited an on-going crisis in which neither side was able to gain the upper hand. The weak central government lost control of the archipelago. Independence movements in East Timor and elsewhere gained strength and achieved autonomy. Violence continued against ethnic Chinese and foreigners as well as government representatives. As a result, refugee movements remained high. The collapse of a centralized economy resulted in the suspension of debt payments and an end of IMF support. A barter economy emerged. Although tolls were no longer demanded, movement through the straits was routinely impeded by pirates. US military forces were asked to remain by regional states to protect foreigners, safeguard

humanitarian assistance, and keep the straits open. Like End State Two, high oil prices persisted, which meant South Korea, the Philippines, and Thailand all faced renewed balance of payment problems. Several major Japanese banks were forced either into bankruptcy or restructuring as investments at home and throughout Asia failed with increasing frequency.

Response to End State Three

One of the military participants indicated it was no surprise that the US military found itself remaining. He noted that it is much easier to intervene in these situations than to withdraw from them. All participants saw this as the bleakest situation because of the uncertainty it created. (Although one broker noted that uncertainty was good for his business because it created volatility and increased transactions!)

Some participants believed that the world is getting used to Asian economic crises and as a result this end state might not generate as big an effect on the US economy as the consensus vote indicated.

Figure 10 details the results of voting.

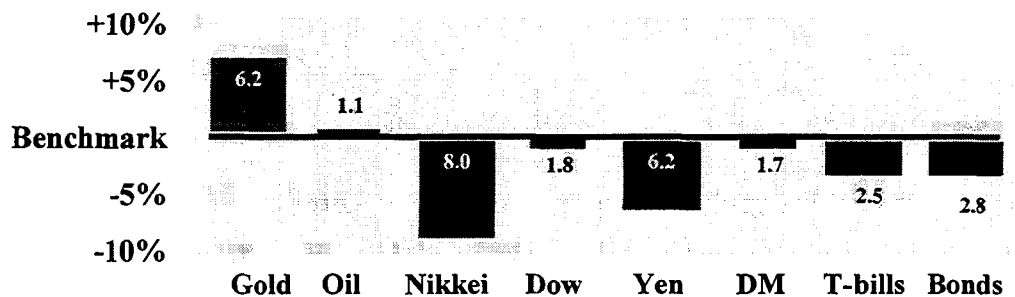


Figure 10. Percentage change in indicators following End State Three voting

To put this final vote in perspective, compared with the initial benchmarks, the price of gold rose over 20 percent; the price of oil soared over 50 percent; the Nikkei declined 32 percent; the Dow Jones fell 18 percent; the yen lost over 28 percent of its value against the dollar; the Deutsche mark remained stable; and T-bill yields declined slightly, as did long bonds.

VII. Exercise Analysis and Observations

Because events in Indonesia moved rapidly in the weeks prior to the exercise, game sponsors were concerned that actual market reactions to real-world events might preclude lively debate among participants. Those fears proved unwarranted. One reason was that there was a natural tension felt throughout the exercise that pitted an appreciation of the economic benefits of global integration against a growing concern that integration brings with it a number of risks.

A related theme that wove its way through the game was the complexity and inter-relatedness of the global economy. Although the stability of the Deutsche mark and US fixed income securities during this exercise would appear to belie that verity, that result was probably more an indication of the necessity to bound the game (i.e., keep the focus on Asia) than a reflection of reality. For one thing, China was lightly played during the exercise, even though it was clear that China's reaction to the crisis would have a major impact on any outcome. Appendix E contains charts showing the level of agreement (or disagreement) among voters on each indicator throughout the exercise.

This section looks first at the results of the voting and concludes with several observations drawn from the exercise. There was general agreement among participants that events of this kind, that bring together individuals from the private, military, and government sectors, enable important connections to be made and new ideas to be fleshed out. They also underscore the importance of taking a broader based approach to dealing with crises.

Voting

The figures below give an overall sense of how each indicator changed over time. The first four columns in each figure represent exercise phases in chronological order. The last three columns represent the three end states presented during the exercise; each is chronologically connected to the fourth column.

Commodities. Figures 11 and 12 show the changes in gold and oil through each phase of the crisis. As expected, gold prices increased as other investments became more risky. This flight to quality was most prominent during End State Three (represented in the final column) when conditions were most uncertain. Over the course of the crisis, gold prices rose from the benchmark of \$300 to \$362 in End State Three — a 20 percent increase — although End State One, a more favorable situation, resulted in a modest increase of only 8.2 percent.

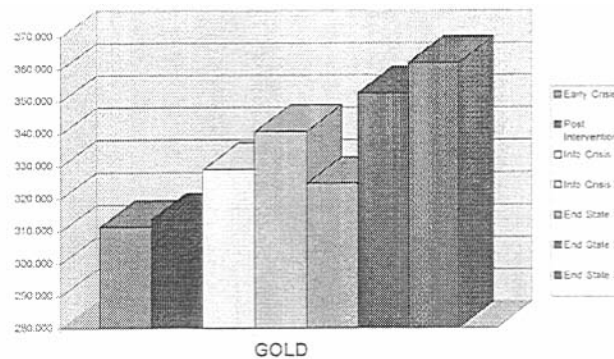


Figure 11. Changes in gold prices

Figure 12 shows that participants believed the price of oil could increase from five to seven dollars per barrel from the initial benchmark of \$15. If the price stabilized at this level, as many participants believed it could, an annualized decrease of half a percent in the US gross domestic product (or approximately 38 billion dollars per year) could result. Crude oil rose to \$22.98 per barrel during End State Three — a 53 percent increase. Some voting participants believed it could go as high as \$26 per barrel — a 73 percent increase over the initial benchmark. One government analyst felt that even that price might be optimistic. The most optimistic end state (End State One) saw the price of oil remain 28 percent higher than the pre-crisis level.

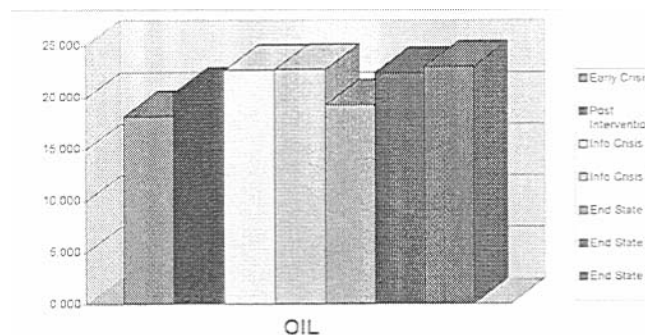


Figure 12. Changes in oil prices

Stock Exchanges. Figures 13 and 14 present consensus votes for the Nikkei and Dow Jones averages. Figure 13 shows how dramatically the Nikkei was affected. From the 15000 benchmark, the Nikkei fell to 10215 during End State Three — a 32 percent decrease in value. The fact that the value of the Nikkei remained 17 percent lower than the initial benchmark during End State One, the most optimistic, reflected the continuing internal problems many participants believed Japan has yet to overcome.

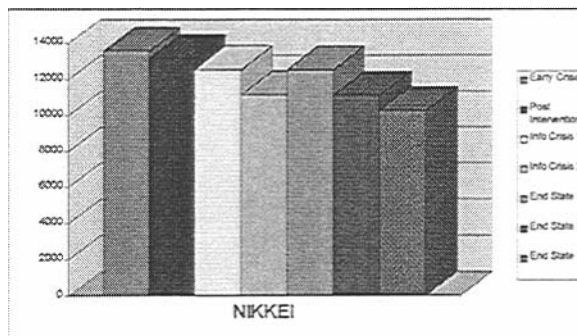


Figure 13. Changes in the Nikkei average

The Dow Jones also showed a steady decline as seen in Figure 14. The 12 percent decline (from the 10000 benchmark to 8812 during End State Three), however, was just over a third of the relative loss suffered by the Nikkei. During End State One, the Dow remained down 6 percent. What was not captured in the voting was the effect that a widespread lack of confidence in stock markets would have. Although mentioned in passing by several participants, a contagious lack of confidence, beginning with emerging market investments then spreading, could have a great deal more impact than the voter consensus indicated.

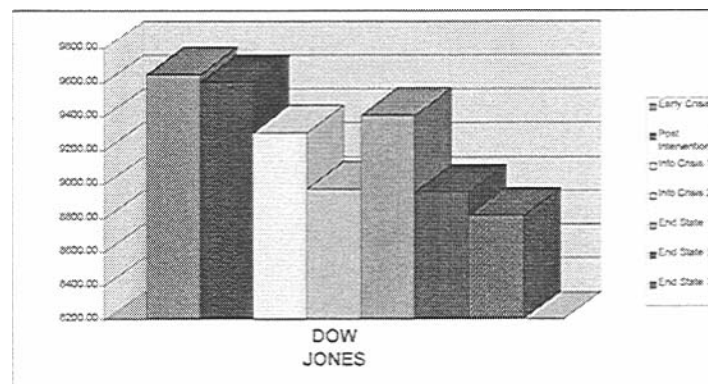


Figure 14. Changes in the Dow Jones average

Currency Exchange Rates. Figures 15 and 16 reflect the exchange rates of the Deutsche mark and the yen against the dollar. As mentioned earlier, the Deutsche mark remained remarkably stable during the exercise, despite the fact that some participants believed events in Asia would affect all corners of the globe. The greatest variation of the Deutsche mark never exceeded 1.5 percent, and during the second information crisis phase, it actually gained against the dollar.

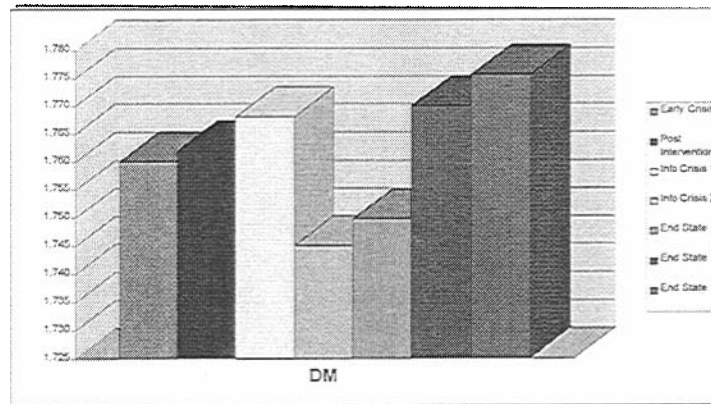


Figure 15. Changes in the exchange rate for the Deutsche mark

The yen nearly matched the volatility of the Nikkei, falling 28 percent against the dollar (to 160.29 during End State Three) from the pre-crisis benchmark rate of 125. One participant predicted we would see more volatility in commodities than in currencies because the latter were subject to national policies. His prediction was only partially correct. Oil was, in fact, a more volatile indicator than either the DM or the yen, but the yen proved more volatile than gold.

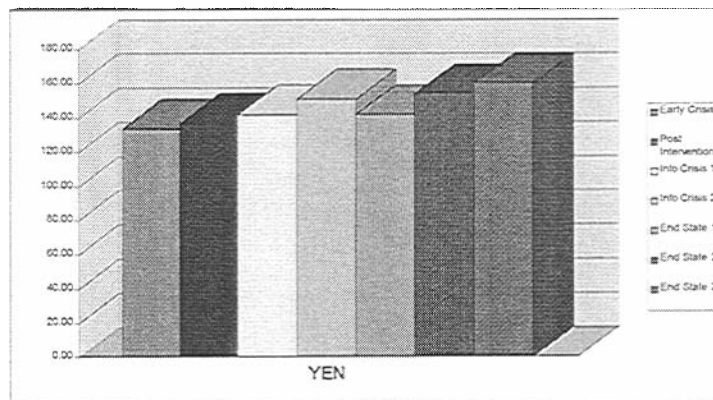


Figure 16. Changes in the exchange rate for the yen

US Treasury Securities. Figures 17 and 18 show the changes in US Treasury instruments during the course of the exercise. Both 3-month T-bills and 30-year bonds were remarkably stable. As Figure 17 shows, the lowest yield for T-bills occurred during End State Three, when participants believed a lot of money would flow into US investments as a result of chaotic conditions in Asia. Even so, the 5.55 percent yield was down only 4 percent from the pre-crisis benchmark of 5.75 percent. T-bill yields never increased above the initial benchmark during the crisis, demonstrating both investor risk aversion and confidence in the US Government.

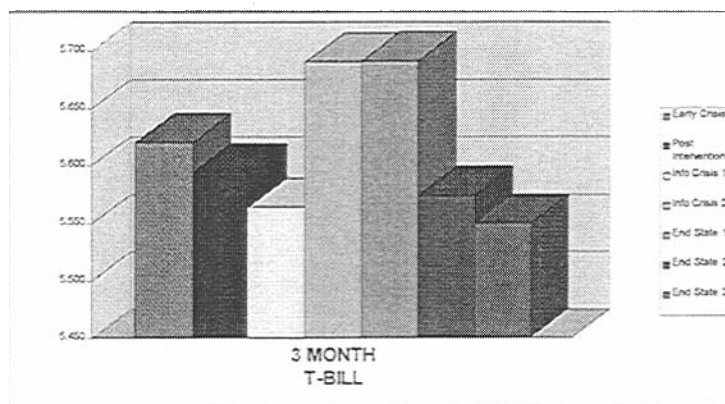


Figure 17. Changes in 3-month T-bill yields

Unlike T-bills, long bond yields increased slightly during several phases of the crisis. The most prominent rise was during the second phase of the information attacks, when confidence in the markets was shaken and Japan was compelled to sell off a significant amount of US securities. Assuming those securities were sold at an attractive discount price, long bond yields could expect to rise to meet the competition. Although this increase was only 2.5 percent over the benchmark yield of 6 percent, it was significant enough to demonstrate participant concern about across-the-board investor confidence. It also increased during End States One and Two, when short-term investments were estimated to provide a greater return. During End State Three, however, when the long-term outlook for the global economy was most in question, it took a dip, down about a half a percent from the pre-crisis benchmark, as investors moved to hedge against a long-term recession.

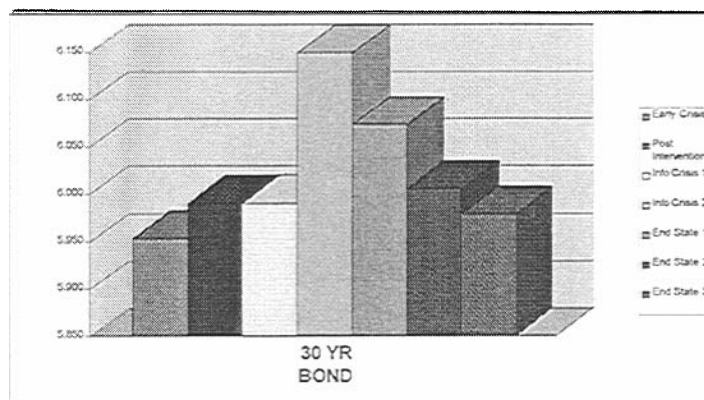


Figure 18. Changes in 30-year bond yields

General Observations and Policy Implications

Discussions during the exercise covered a diverse array of topics, from policy implementation to marketing strategies. The following observations and policy implications are offered in no particular order.

General Observations

Fear of insider attacks. The biggest concern raised during the IW portion of the exercise was the issue of insider attacks on databases, accounts and wire transactions. Mitre representatives noted that deregulation of industries such as electric power generation has increased the risk of such attacks because individuals or groups with malevolent motives can become insiders for a nominal cost.

Cyber Security is a selling point. Military participants noted that the Department of Defense solution to cyber-attacks has been to isolate critical information and systems on separate networks. As the commercial world becomes more integrated, this solution becomes less feasible to it. Hence, in the future, the ability to ensure client security may become a big selling point for companies.

Impact of Information Warfare. Voting on indicators and comments by participants indicated that the introduction of cyber-attacks substantially increased participants' concern over the breadth of the crisis. The resulting loss of confidence in markets threatened to bring economic repercussions well beyond even those resulting from higher oil prices and impeded movement of commerce. Whether the cyber-attack was a "one-of-a-kind" event or not, perceptions could lead to investor panic and widespread loss of confidence in the financial community.

Emerging markets are strongly linked. A downturn in one emerging could affect others. When money fled emerging markets in Asia, participants did not believe it would flow into other emerging markets (such as Latin America). In fact, they believed investors in all emerging market would look for more secure areas for their assets under the uncertainty passed. They felt Russian investments would be particularly hard hit.

Freedom of navigation issues were downplayed. The game book posited that one reason the United States would respond was to ensure historical freedom of navigation claims were reinforced. However, one government participant said that those concerns would be low on the list of reasons that would motivate the US to intervene. Another government participant indicated that the transit toll introduced into the scenario had been set at a level that shippers could absorb without disrupting maritime traffic.

Policy Implications

China has become a major political/economic player. Participants from all sectors agreed that China is becoming an increasingly important player in diverse ways. Although the exercise deliberately kept China on the periphery of the action, participants constantly reminded one another that how China responded would have a major impact on developments. They noted that devaluation of its currency could ignite another setback in Asia; it now has an out-of-area naval capability; and its ties with a large and wealthy diaspora of ethnic Chinese connect it to every aspect of the global economy.

Cooperation not regulation. It was evident during the exercise that some form of government/private cooperation is required if infrastructure vulnerabilities are to be reduced. The commercial sector's fear is that cooperation could result in regulation. Analysts noted that governments must be involved in solving some of the legal issues (such as jurisdiction and property rights), but that assistance, not oversight, was the goal.

Coordinating bodies are required. Most participants agreed that a centralized organization is necessary in order to standardize security measures, provide information, and issue warnings. Few believed that such a group would be established within the timelines set in PDD 63. Moreover, PDD 63 is focused on attacks against United States infrastructure. How the US government would respond to attacks on systems overseas that created ripple effects in the US is an open question. The recommendation was that international coordinating bodies might be required.

Forfeiture of US leadership could be disastrous. Financial participants said they looked to the US Government to provide strong leadership during crises. Several participants believed that a scenario such as the one presented could lead to the remilitarization of Japan were the US to sit on the sidelines. Others believed that China would fill any leadership vacuum and press its agenda on the region (which could lead to an unhealthy arms race). One participant stressed that the degree to which the US Government appeared to act promptly and decisively would be the most important consideration in his assessment of the crisis.

Military forward presence remains vital. US leadership must be backed by credible force. As one government participant noted, diplomacy backed by force is the preferred course of action for most crises of this type. Participant comments made it clear that the financial community is much more likely to act confidently in a situation if the crisis has the full attention of the government and the government has the means to act in accordance with public expectations. Incapable or ineffective forces undermine US credibility and leadership.

The nature of the IW problem. The key cyber-threats were perceived to be: intrusion (where the financial sector is making reasonable progress); the insider problem (which is much tougher); and the malicious code problem (which is potentially horrendous). When asked to rate the severity of the problem, a government official characterized it as, "Bad. There is no room full of cyber experts ready to stem attacks." This was amended by a senior military official who said, "It's even worse. PDD 63 just kicks off the effort." This was augmented by an IW expert who stated, "It's EVEN WORSE. We haven't begun to attack the international problem."

Appendix A

Participants

Participants
(in alphabetical order)

*John Bocchi	Cantor Fitzgerald
Joe Bouchard	National Security Council
Mead Briggs	CS First Boston
VADM Art Cebrowski	US Navy Staff
**Art Cubbler	USMC Public Affairs Officer, New York
VADM Jim Ellis	US Navy Staff
ADM (ret) Wm. "Bud" Flanagan	Cantor Fitzgerald
Craig Foster	CS First Boston
**MGEN (ret) Don Gardner	Intrepid Museum
Theophilos Gemelas	Naval War College
Phil Ginsberg	Cantor Fitzgerald
Jim Harris	Central Intelligence Agency
Jim Hart	Department of Energy
Bradd Hayes	Naval War College
*Andy Hecht	Cantor Fitzgerald
Gregg Hoffman	Naval War College
Kent Karosen	Cantor Fitzgerald
Aproova Koticha	Citibank
*Dave Lavecchia	Cantor Fitzgerald
Howard Lutnick	Cantor Fitzgerald
Lawrence Modisett	Naval War College
Ed Mount	SBC Warburg Dillon Read
Alan Palazzo	Naval War College
LTG (ret) Roger Peterson	SBC Warburg Dillon Read
Tom Piersanti	Banque Nationale de Paris
Mackin Pulsifer	Fiduciary Trust International

Gary Rasmussen	Department of the Treasury
*Peter Rogers	Cantor Fitzgerald
Gary Shrout	Naval War College
Adam Schwarz	Council on Foreign Relations
RADM James Stark	Naval War College
Stuart Starr	Mitre
Lisa Schwartzman	Cantor Fitzgerald
Paul Taylor	Naval War College
James Thorpe	Morgan Stanley
*Angelo Toglia	Cantor Fitzgerald
Andres Vaart	Naval War College
John Woodward	Mitre
**Llew Lewis	US Navy Staff

***Dinner only**

****Observer**

Appendix B

Department of State Background Notes on Indonesia



U.S. Department of State

Background Notes: Indonesia, November 1997⁵

Released by the Bureau of East Asian and Pacific Affairs.

Official Name: Republic of Indonesia

PROFILE

Geography

Area: 2 million sq. km. (736,000 sq. mi), about three times the size of Texas; maritime area: 7,900,000 sq. km.

Cities: Capital--Jakarta (est. 8.8 million). Other cities--Surabaya 3.0 million, Medan 2.5 million, Bandung 2.5 million plus an additional 3 million in the surrounding area

Terrain: More than 17,000 islands but only 1,000 permanently settled. Large islands consist of coastal plains with mountainous interiors.

Climate: Equatorial but cooler in the highlands.

People

Nationality: Noun and adjective--Indonesian(s).

Population: 206.6 million.

Annual growth rate: 1.5%.

Ethnic groups: Javanese 45%, Sundanese 14%, Madurese 7.5%, coastal Malays 7.5%, others 26%.

Religions: Islam 87%, Protestant 6%, Catholic 3%, Hindu 2%, Buddhist and other 1%.

Languages: Indonesian (official), local languages, the most important of which is Javanese.

Education: Years compulsory--9. Enrollment--92% of eligible primary school-age children. Literacy--85%.

Health: Infant mortality rate--63/1000 live births. Life expectancy at birth--men 60 years, women 64 years

Work force: 71 million. Agriculture--50.1.5%, trade and restaurants--15.0, public services--13.7%, manufacturing--11.6%.

⁵ Downloaded from http://www.state.gov/www/background_notes/indonesia_971100_bgn.html/

Government

Type: Independent republic.

Independence: August 17, 1945 proclaimed.

Constitution: 1945. Embodies five principals of the state philosophy, called Pancasila, namely monotheism, humanitarianism, national unity, representative democracy by consensus, and social justice.

Branches of Government: Executive--president (head of government and chief of state) chosen for a 5-year term by the 1,000-member People's

Consultative Assembly. Legislature--500-member House of Representatives elected for a 5-year term. Judicial--Supreme Court.

Economy (1995)

GDP: \$197.8 billion.

Annual growth rate: 7.5%.

Per capita income: \$1,013.

Natural resources (8.4% of GDP): Oil and gas, bauxite, silver, tin, copper, gold, coal.

Agriculture (17.2% of GDP): Products--timber, rubber, rice, palm oil, coffee. Land--17% cultivated.

Manufacturing (24.3% of GDP): Garments, footwear, electronic goods, furniture, paper products.

Trade: Exports--\$45.4 billion including oil, natural gas, plywood, manufactured goods.

Major markets--Japan, Singapore, Taiwan, Korea, U.S.

Imports: \$33.8 billion including food, chemicals, capital goods, consumer goods. Major suppliers--Japan, U.S., Thailand.

PEOPLE

Indonesia's 206 million people make it the world's fourth-most populous nation. The island of Java is one of the most densely populated areas in the world, with more than 107 million people living in an area the size of New York State.

Indonesia includes numerous related but distinct cultural and linguistic groups, many of which are ethnically Malay. Since independence, Indonesian (the national language, a form of Malay) has spread throughout the archipelago and has become the language of all written communication, education, government, and business. Many local languages are still important in many areas, however. English is the most widely spoken foreign language.

Education is free and compulsory for children between ages 6 and 12. Although about 92% of eligible children are enrolled in primary school, a much smaller percentage attend full time. About 44% of secondary school-age children attend junior high school, and some others of this age group attend vocational schools.

Constitutional guarantees of religious freedom apply to the five religions recognized by the state, namely Islam (87%), Protestantism (6%), Catholicism (3%), Buddhism (2%), and Hinduism (1%). In some remote areas, animism is still practiced.

HISTORY

By the time of the Renaissance, the islands of Java and Sumatra had already enjoyed a 1,000-year heritage of advanced civilization spanning two major empires. During the 7th-14th centuries, the Buddhist kingdom of Srivijaya flourished on Sumatra. At its peak, the Srivijaya Empire reached as far as West Java and the Malay Peninsula. Also by the 14th century, the Hindu Kingdom of Majapahit had risen in eastern Java. Gadjah Mada, the empire's chief minister from 1331 to 1364, succeeded in gaining allegiance from most of what is now modern Indonesia and much of the Malay archipelago as well. Legacies from Gadjah Mada's time include a codification of law and an epic poem.

Islam arrived in Indonesia sometime during the 12th century and, through assimilation, supplanted Hinduism by the end of the 16th century in Java and Sumatra. Bali, however, remains overwhelmingly Hindu. In the eastern archipelago, both Christian and Islamic proselytizing took place in the 16th and 17th centuries and, currently, there are large communities of both religions on these islands.

Beginning in 1602, the Dutch slowly established themselves as rulers of present-day Indonesia, exploiting the weakness of the small kingdoms that had replaced that of Majapahit. The only exception was East Timor which remained under Portugal until 1975. During 300 years of Dutch rule, the Dutch developed the Netherlands East Indies into one of the world's richest colonial possessions.

During the first decade of this century, an Indonesian independence movement began and expanded rapidly, particularly between the two World Wars. Its leaders came from a small group of young professionals and students, some of whom had been educated in the Netherlands. Many, including Indonesia's first president, Sukarno, were imprisoned for political activities.

The Japanese occupied Indonesia for 3 years during World War II and, for their own purposes, encouraged the nationalist movement. Many Indonesians took up positions in the civil administration which had been closed to all but token rulers under the Dutch. On August 17, 1945, 3 days after the Japanese surrender to the Allies, a small group of Indonesians, led by Sukarno -- the country's first truly national figure and first president (1945-1967) -- proclaimed independence and established the Republic of Indonesia. Dutch efforts to reestablish complete control met strong resistance. After 4 years of warfare and negotiations, the Dutch transferred sovereignty to a federal Indonesian Government. In 1950, Indonesia became the 60th member of the United Nations.

Shortly after hostilities with the Dutch ended in 1949, Indonesia adopted a new constitution providing for a parliamentary system of government in which the executive was chosen by and made responsible to parliament. Parliament was divided among many political parties before and after the country's first nationwide election in 1955, and stable governmental coalitions were difficult to achieve.

At the time of independence, the Dutch retained control over the western half of New Guinea, known as Irian Jaya. Negotiations with the Dutch on the incorporation of West Irian into Indonesia failed, and armed clashes broke out between Indonesian and Dutch troops in 1961. In August 1962, the two sides reached an agreement, and Indonesia assumed administrative responsibility for Irian Jaya on May 1, 1963. An Act of Free Choice, held in Irian Jaya under UN supervision in 1969, confirmed the transfer of sovereignty to Indonesia.

From 1524 to 1975, East Timor was a Portuguese colony on the island of Timor, separated from Australia's north coast by the Timor Sea. As a result of political events in Portugal, Portuguese authorities abruptly withdrew from Timor in 1975, exacerbating power struggles among several Timorese political factions. An avowedly Marxist faction called "Fretilin" achieved military superiority. Fretilin's ascent in an area contiguous to Indonesian territory alarmed the Indonesian Government, which regarded it as a threatening movement. Following appeals from some of Fretilin's Timorese opponents, Indonesian military forces intervened in East Timor and overcame Fretilin's regular forces in 1975-1976. Small-scale guerrilla activity persists to the present. Indonesia declared East Timor its 27th province in 1976.

Unsuccessful rebellions on Sumatra, Sulawesi, and other islands beginning in 1958 plus a long succession of short-lived national governments weakened the parliamentary system. Consequently, in 1959, when President Sukarno revived the 1945 constitution, which gave broad presidential powers, he met little resistance.

From 1956 to 1965, President Sukarno imposed an authoritarian regime under the label of "Guided Democracy." He also moved Indonesia's foreign policy toward nonalignment. Advocated by the leaders of other former colonies, these nonaligned countries became known as the Non-Aligned Movement. President Sukarno closely worked with Asian communist states and increasingly tilted toward the Indonesian Communist Party (PKI) in domestic affairs.

By 1965, the PKI controlled many of the mass organizations that Sukarno had established to mobilize support for his regime and, with Sukarno's acquiescence, embarked on a campaign to establish a "fifth armed force" by arming its supporters. Army leaders resisted this campaign. On October 1, 1965, PKI sympathizers within the military, including elements from Sukarno's palace guards, occupied key locations in Jakarta and kidnapped and murdered six senior generals.

The army executed the coup plotters within a few days, but unsettled conditions persisted through 1966. Violence swept throughout Indonesia. Rightist gangs killed tens of thousands of alleged communists in rural areas. Estimates of the number of deaths range between 160,000 and 500,000. The violence was especially brutal in Java and Bali. The emotions and fears of instability created by this crisis persist.

In the aftermath, President Sukarno vainly attempted to restore his political position and shift the country back to its pre-October 1965 position. Although he remained president, in March 1966, Sukarno had to transfer key political and military powers to General Soeharto, the general who rallied the military to defeat the coup attempt. In March 1967, the People's Consultative Assembly (MPR) named General Soeharto acting president. Sukarno ceased to be a political force and lived quietly until his death in 1970.

President Soeharto proclaimed a "New Order" in Indonesian politics and dramatically shifted foreign and domestic policies away from the course set in Sukarno's final years. The New Order established economic rehabilitation and development as its primary goals and pursued its policies through an administrative structure dominated by the military but with advice from Western-educated economic experts.

In 1968, the MPR formally selected Soeharto to a full 5-year term as President, and he was reselected to additional 5-year terms in 1973, 1978, 1983, 1988, and 1993. It is likely that he will again be selected President in March 1998.

GOVERNMENT AND POLITICAL CONDITIONS

Indonesia is a republic based on the 1945 constitution providing for a limited separation of executive, legislative, and judicial power. The president, elected for a 5-year term, is the overwhelmingly dominant government and political figure and is the highest executive office of the state. He is selected along with the vice president by the MPR. The president has the authority to conduct the administration of the government and is accountable only to the MPR. The President appoints a 41-member Cabinet to assist him.

The People's Consultative Assembly (MPR) consists of 1,000 members of whom 500 are appointed by the president and 500 are members of the House of People's Representatives. The assembly selects the president and vice president and establishes governmental guidelines for the next 5 years.

The House of People's Representatives (DPR) is a 500-member body that serves as the legislative arm of the government and is empowered to approve all statutes and the national budget and to initiate legislation. Of the 500 members, 425 are elected to office every 5 years and 75 are selected by the president from Indonesia's armed forces.

Although nominally independent, the judiciary is strongly influenced by the executive branch of government.

Although Indonesia is a unitary state, there are 24 provinces, 2 special territories and 1 capital city district (Jakarta). These are further divided into 243 districts and 55 municipalities, 16 administrative municipalities, 35 administrative cities, and 3,841 subdistricts. Provincial governors are selected by the president.

By law there are only three legal political parties: Golkar, a federation of groups including civil servants, youth, labor, farmers, and women; United Development Party (PPP), composed of various Muslim groups; and the Indonesian Democracy Party (PDI) composed of Christian, socialist, and nationalist elements. The party system reflects the Soeharto Government's determination to shift the political focus from Indonesia's deep ethnic, religious, and ideological differences, which contributed to the collapse of an earlier experiment in parliamentary democracy. Soeharto's preferred strategy is authoritarian, program-based, development-oriented politics.

In elections held in 1997, Golkar received a 74% majority, PPP 24%, and PDI only 3%. PDI's poor showing reflected a year long struggle over who the chairman of the party should be.

The armed forces have shaped and staffed Soeharto's New Order since it came to power in the wake of the abortive 1965 uprising. Military officers, especially from the army, have been key advisers to Soeharto and have great influence on policy. Under the dual function concept, military officers serve in the civilian bureaucracy at all government levels, although there has been a recent tendency to somewhat reduce the military's direct involvement in the civilian bureaucracies.

Principal Government Officials

President--Soeharto

Vice President--Try Sutrisno

Minister of Foreign Affairs--Ali Alatas

Ambassador to the United States--Arifin Siregar

Ambassador to the United Nations--Makarim Wibisono

The embassy of Indonesia is at 2020 Massachusetts Avenue NW., Washington, DC 20036 (tel. 202-775-5200-5207; FAX: 202-775-5365). Consulates General are in New York (5 East 68th Street, New York, NY 10021, tel. 212-879-0600/0615; FAX: 212-570-6206); Los Angeles (3457 Wilshire Blvd., Los Angeles, CA 90010; tel. 213-383-5126; FAX: 213-487-3971); Houston (10900 Richmond Ave., Houston, TX 77042; tel. 713-785-1691; FAX: 713-780-9644). Consulates are in San Francisco (1111 Columbus Avenue, San Francisco, CA 94133; tel. 415-474-9571; FAX: 415-441-4320); and Chicago (2 Illinois Center, Suite 1422233 N. Michigan Avenue, Chicago, IL 60601; tel. 312-938-0101/4; 312-938-0311/0312; FAX: 312-938-3148).

ECONOMY

Indonesia has a free-market economy that is dominated by the private sector. The government still plays a significant role in the economy, however, through state-owned firms and the imposition of price controls in selected industries.

Since President Soeharto took power in 1966, Indonesia's economy has grown steadily, from a per capita GNP of \$70 to a per capita GNP of about \$900. It is recognized as a newly industrializing economy. Real GDP growth has averaged 6.7% over the last 5 years. By employing a restrictive monetary policy and a conservative fiscal stance, the government has held inflation in the 5%-10% range. With strong export performance and manageable import growth, Indonesia saw a trade surplus of about \$3 billion in 1995.

Petroleum is one of Indonesia's major exports. Indonesia endured a difficult economic period in the early 1980s because of falling oil prices but has successfully managed to diversify its economy and to attract manufacturing to create a more stable economic climate.

In the mid-1980s, the government began eliminating regulatory obstacles to economic activity. These steps primarily have been directed at the external and financial sectors and were designed to stimulate growth in non-oil exports and revenues and to strip away import substitution barriers. The May 1994 and May 1995 deregulation packages helped level the playing field for competition. The January 1996 package helped cut tariffs. The most important, unfinished deregulation steps are removal of nontariff barriers and associated domestic regulations reducing tariff protection on vehicles, the opening up of the strategic industries, and the removal of domestic subsidies and export restrictions.

In late 1997, Indonesia concluded a 3-year stabilization/structural adjustment program with the international financial institutions. Under this program the rupiah will be stabilized in foreign exchange markets by the government adopting tight fiscal and monetary policies. Non-viable banks will be closed, and a broad range of structural reforms will be implemented including liberalization of foreign trade and investment; dismantling of domestic monopolies, allowing greater private sector participation in provision of infrastructure; and expanding the privatization program.

Indonesia's foreign debt at the end of 1995 was about \$95 billion of which approximately \$65 billion was official. Most of the government's foreign debt is medium to long term, predominantly on concessional terms from multilateral and bilateral donors.

Oil and Minerals Sector

The oil and gas sector, including refining, constitutes about 10% of GDP. Although the sector's share of export earnings and government revenue has dropped to about 10%, it remains an important part of the economy. Many U.S. companies participate. Crude and condensate output averaged 1.6 million barrels per day (bpd) in 1995. With domestic

demand for petroleum fuels expanding, Indonesia will become a net importer of oil by the next decade unless new reserves are found.

The state owns all oil and mineral rights. Foreign firms participate through production sharing and work contracts. Contractors are required to finance all exploration, production, and development costs in their contract areas; they are entitled to recover operating, exploration, and development costs out of the oil and gas produced.

Although traditionally known for bauxite, silver, and tin production, Indonesia is expanding its copper, nickel, gold, and coal output for export markets. Total coal production reached 41 million tons in 1996, including exports of 27 million tons. In mid-1993, the Department of Mines and Energy reopened the coal sector to foreign investment. Indonesian coal production in the range of 70-80 million tons by the end of the decade is possible.

Investment

The Indonesian Government actively encourages foreign investment. Burgeoning infrastructure requirements and the desire to contain the increase of foreign commercial indebtedness have reinforced that pro-investment attitude. The value of domestic investments approved by the BKPM grew 65% in 1995 to a total of \$31 billion, while foreign investment approvals increased five-fold to a total of \$40 billion. Most approved investment during the last 5 years have been in manufacturing, especially in textile, pulp and paper, and chemical industries. While the United States is by far the largest participant in the oil and gas sector, Japan has traditionally been the leader in terms of value of BKPM-approved investment. Japan remains the biggest foreign investor in Indonesia. Other major foreign investors include Singapore, Hong Kong, Taiwan, and South Korea.

Over the past few years, Indonesia has made numerous changes in its regulatory framework to improve the business climate and encourage increased foreign investment. In addition to the deregulation measures noted earlier, the recent passage of intellectual property protection laws and a movement to privatize previously restricted sectors such as road, electric power, and telecommunications have improved the investment climate in Indonesia.

FOREIGN RELATIONS

Since independence, Indonesia has espoused a "free and active" foreign policy, seeking to play a role in regional affairs commensurate with its size and location but avoiding involvement in conflicts among major powers.

Indonesian foreign policy under the "New Order" government of President Soeharto has moved from the stridently anti-Western, anti-American posturing which characterized the

Sukarno era. Indonesia preserves a non-aligned position while seeking constructive, responsible relations with many nations.

A cornerstone of Indonesia's contemporary foreign policy is its participation in the Association of Southeast Asian Nations (ASEAN), of which it was a founding member in 1967 with Thailand, Malaysia, Singapore, and the Philippines. Since then, Brunei, Vietnam, Laos, and Burma also have joined ASEAN. While organized to promote common economic, social, and cultural goals, ASEAN acquired a security dimension after Vietnam's invasion of Cambodia in 1979; this aspect of ASEAN expanded with the establishment of the ASEAN Regional Forum in 1994, which comprises 18 countries, including the U.S.

Indonesia was also one of the founders of the Non-Aligned Movement (NAM) and has taken moderate positions in its councils. As NAM Chairman in 1992-95, it led NAM positions away from the rhetoric of North-South confrontation, advocating instead the broadening of North-South cooperation in the area of development.

Indonesia has the world's largest Muslim population, but it is a secular state. It is a member and current chairman of the Organization of the Islamic Conference (OIC), and while it carefully considers the interests of Islamic solidarity in its foreign policy decisions, it has been an influence for moderation in the OIC.

Since 1966, Indonesia has welcomed and maintained close relations concerning economic assistance with the United States, Western Europe, Australia, and Japan, from which, through the Intergovernmental Group on Indonesia (IGGI) and its successor, the Consultative Group on Indonesia (CGI), it has received substantial foreign economic assistance. Indonesia has no diplomatic relations with Portugal, due to their inability to reach agreement over the decolonization and subsequent Indonesian incorporation of East Timor, but the two countries are discussing the issue under the auspices of the United Nations.

Indonesia restored diplomatic relations with China in 1989 and, with the end of the Cold War, has supported efforts to gradually expand a regional security dialogue under the aegis of the ASEAN Regional Forum to all Asia-Pacific nations. Indonesia has advocated the eventual expansion of ASEAN to include all the nations of Southeast Asia.

Indonesia has been a strong supporter of the Asia-Pacific Economic Cooperation forum (APEC). Largely through the efforts of President Soeharto, APEC members agreed to implement free trade in the region by 2010 for industrialized economies and 2020 for developing economies at the 1994 meeting in Bogor, Indonesia.

National Security

Indonesia's armed forces total about 420,000 members, including the national police and the traditional services (army, navy, marines, and air force). The army is by far the

largest, with 215,000 active-duty personnel. Various paramilitary, civil defense, and other auxiliary units supplement the official armed forces. With defense spending at 1.48% of GDP for 1995-96, Indonesia ranks among those countries that spend least on their armed forces.

The Indonesian military sees itself as a unifying force among the various ethnic, religious, and political elements in Indonesia. Thus, the military views its prime mission as assuring internal security. The president, vice president, and many members of the cabinet have military backgrounds. Furthermore, active duty and retired military personnel occupy a large number of seats in the House of Representatives and the MPR. Under the government's dual-function concept, many military personnel occupy positions in regional government.

Commanders of the various territorial commands also are very influential in the politics of their respective regions. Local military units can and do respond quickly with force if necessary.

Indonesia is at peace with its neighbors. The P.R.C. claims in the South China Sea, where Indonesia has large natural gas reserves, concern the Indonesians, however. Economic development has taken priority over the military budget in the Soeharto years. Recently, however, the armed forces, particularly the navy, have undertaken some small but significant improvements of their external capabilities.

U.S.-INDONESIAN RELATIONS

The United States has important economic, commercial, and security interests in Indonesia because of its growing economy and markets and its strategic location astride a number of key international maritime straits. Relations between Indonesia and the U.S. are good. The U.S. played an important role in Indonesian independence in the late 1940s, and appreciated Indonesia's role as a staunch anti-communist bulwark during the Cold War, and maintains cordial and cooperative security arrangements today, although the two countries are not bound by any formal security treaties.

The United States and Indonesia share the common goal of maintaining peace, security, and stability in the region and engaging in a dialogue on threats to regional security. The United States has welcomed Indonesia's contributions to regional security, especially its leading role in helping restore democracy in Cambodia and in mediating among the many territorial claimants in the South China Sea. The United States and Indonesia maintain a modest, fruitful program of military cooperation which includes military training, ship and aircraft visits, joint exercises, and mutual visits of ranking military officers.

Friction points in the bilateral political relationship in recent years have centered on human rights, especially in East Timor, and also on the rights of workers. The U.S. Congress cut off grant military training assistance (IMET) to Indonesia in 1992 in response to a November 12, 1991, shooting incident in East Timor involving Indonesian

security forces and peaceful Timorese demonstrators; this restriction was partially lifted in 1995. The U.S. strongly supports UN efforts to promote a dialogue between Indonesia and Portugal to resolve their differences regarding the political status of East Timor.

On worker rights, Indonesia was the target of two 1992 petitions filed under the Generalized System of Preferences (GSP) legislation. The petitions argued that Indonesia did not meet recognized labor standards of excessive military involvement in legitimate labor activity and severe restraints on the right of association regarding organizing unions. A formal GSP review was suspended in February 1994 without terminating GSP benefits for Indonesia, but an active dialogue continues on worker rights issues.

Economic Relations With the United States

U.S. exports to Indonesia in 1995 totaled \$3.4 billion. The main exports were construction equipment, machinery, aviation parts, and agricultural products. U.S. imports from Indonesia totaled \$7.4 billion and consisted mainly of natural rubber and footwear.

Economic assistance to Indonesia is coordinated through the Consultative Group on Indonesia (CGI), formed in 1989. It includes 19 donor countries and 13 international organizations and meets annually to coordinate donor assistance. The July 1997 meetings resulted in pledges of \$5.2 billion. Japan's contribution of \$1.76 billion provided the largest share of this total. The United States pledged about \$92 million for fiscal year 1995.

The U.S. Agency for International Development (USAID) has provided development assistance to Indonesia since 1950. Initial assistance focused on the most urgent needs of the new republic, including food aid, infrastructure rehabilitation, health care, and training. After the 1965 turmoil, during which time U.S. aid was curtailed, USAID responded to the Indonesian Government's request to reactivate the overseas training program, assist in rebuilding infrastructure, invigorate the fledgling private sector, and help curb the country's exploding population growth rate. Through the 1970s, a time of great economic growth in Indonesia, USAID played a major role in helping the country achieve self-sufficiency in rice production and in reducing the birth rate.

By the mid-1980s, a drop in oil prices led Indonesia to undertake far-reaching economic policy reforms aimed at improving economic efficiency and reducing dependency on oil revenues. USAID supported this process with technical and financial assistance. USAID's current program, which supports Indonesia's goal of achieving a per capita income of \$1,000 by the year 2000, focuses on developing a more competitive, participatory economy, improving health and reducing fertility, reducing the rate of environmental degradation, and strengthening key institutions which support citizen's rights and civic participation. Total U.S. grant and loan assistance in fiscal year 1996 was \$52 million.

Principal U.S. Embassy Officials

Ambassador--J. Stapleton Roy
Deputy Chief of Mission--Michael Owens
Political Counselor--Edmund McWilliams Jr.
Economic Counselor--Judith Fergin
Administrative Counselor--Maurice Kralnek
USAID Director--Vivikka Moldrem
Defense Attaché--Col. Charles McFetridge
Consul General--William H. Barkell
Public Affairs Officer--Steven J. Monblatt
Agricultural Counselor--Rubin Tilsworth-Rude
Commercial Counselor--Michael Hand

The U.S. Embassy in Indonesia is located at Jalan Medan Merdeka Selatan 5, Jakarta (tel. (62-21) 344-2211). U.S. mail to the embassy may be addressed to APO AP 96520.

The U.S. Consulate General in Surabaya is located at Jalan Dr. Sutomo 33, Surabaya East Java (tel. (62-31) 568-2287). Principal Officer—William Pierce

For information on economic trends, commercial development, production, trade regulations, and tariff rates, contact the International Trade Administration, U.S. Department of Commerce, Washington, DC 20230.

TRAVEL AND BUSINESS INFORMATION

The U.S. Department of State's Consular Information Program provides Travel Warnings and Consular Information Sheets. Travel Warnings are issued when the State Department recommends that Americans avoid travel to a certain country. Consular Information Sheets exist for all countries and include information on immigration practices, currency regulations, health conditions, areas of instability, crime and security, political disturbances, and the addresses of the U.S. posts in the country. Public Announcements are issued as a means to disseminate information quickly about terrorist threats and other relatively short-term conditions overseas which pose significant risks to the security of American travelers. Free copies of this information are available by calling the Bureau of Consular Affairs at 202-647-5225 or via the fax-on-demand system: 202-647-3000. Travel Warnings and Consular Information Sheets also are available on the Consular Affairs Internet home page: <http://travel.state.gov> and the Consular Affairs Bulletin Board (CABB). To access CABB, dial the modem number: (301-946-4400 (it will accommodate up to 33,600 bps), set terminal communications program to N-8-1 (no parity, 8 bits, 1 stop bit); and terminal emulation to VT100. The login is travel and the password is info (Note: Lower case is required). The CABB also carries international security information from the Overseas Security Advisory Council and Department's Bureau of Diplomatic Security. Consular Affairs Trips for Travelers publication series, which contain information on obtaining passports and planning a safe trip abroad, can be

purchased from the Superintendent of Documents, U.S. Government Printing Office, P.O. Box 371954, Pittsburgh, PA 15250-7954; telephone: 202-512-1800; fax 202-512-2250.

Emergency information concerning Americans traveling abroad may be obtained from the Office of Overseas Citizens Services at (202) 647-5225. For after-hours emergencies, Sundays and holidays, call 202-647-4000.

Passport Services information can be obtained by calling the 24-hour, 7-day a week automated system (\$.35 per minute) or live operators 8 a.m. to 8 p.m. (EST) Monday-Friday (\$1.05 per minute). The number is 1-900-225-5674 (TDD: 1-900-225-7778). Major credit card users (for a flat rate of \$4.95) may call 1-888-362-8668 (TDD: 1-888-498-3648)

Travelers can check the latest health information with the U.S. Centers for Disease Control and Prevention in Atlanta, Georgia. A hotline at (404) 332-4559 gives the most recent health advisories, immunization recommendations or requirements, and advice on food and drinking water safety for regions and countries. A booklet entitled Health Information for International Travel (HHS publication number CDC-95-8280) is available from the U.S. Government Printing Office, Washington, DC 20402, tel. (202) 512-1800.

Information on travel conditions, visa requirements, currency and customs regulations, legal holidays, and other items of interest to travelers also may be obtained before your departure from a country's embassy and/or consulates in the U.S. (for this country, see "Principal Government Officials" listing in this publication).

U.S. citizens who are long-term visitors or traveling in dangerous areas are encouraged to register at the U.S. embassy upon arrival in a country (see "Principal U.S. Embassy Officials" listing in this publication). This may help family members contact you in case of an emergency.

Further Electronic Information:

Department of State Foreign Affairs Network. Available on the Internet, DOSFAN provides timely, global access to official U.S. foreign policy information. Updated daily, DOSFAN includes Background Notes; Dispatch, the official magazine of U.S. foreign policy; daily press briefings; Country Commercial Guides; directories of key officers of foreign service posts; etc. DOSFAN's World Wide Web site is at <http://www.state.gov>.

U.S. Foreign Affairs on CD-ROM (USFAC). Published on a semi-annual basis by the U.S. Department of State, USFAC archives information on the Department of State Foreign Affairs Network, and includes an array of official foreign policy information from 1990 to the present. Contact the Superintendent of Documents, U.S. Government Printing Office, P.O. Box 371954, Pittsburgh, PA 15250-7954. To order, call (202) 512-1800 or fax (202) 512-2250.

National Trade Data Bank (NTDB). Operated by the U.S. Department of Commerce, the NTDB contains a wealth of trade-related information. It is available on the Internet (www.stat-usa.gov) and on CD-ROM. Call the NTDB Help-Line at (202) 482-1986 for more information.

Appendix C

The Importance of the Straits and Spratly Islands Region

According to a 1996 National Defense University/Center for Naval Analyses study, “over half of the world’s merchant fleet capacity—more than one-third of the world’s ships— sailed through the Straits of Malacca, Sunda, or Lombok, or sailed past the Spratly Islands” in 1993, and their cargoes included “over one-half trillion dollars of long-haul interregional seaborne shipments.”⁶ Approximately 40 percent of the seaborne trade of Japan, Australia, and Southeast Asian states transits these straits. Nearly one-quarter of seaborne trade of Hong Kong, Taiwan, and South Korea also uses the straits.⁷ Although alternate routes are available, closure of the straits would be extremely expensive for some states, and disastrous for others (see Table C-1).

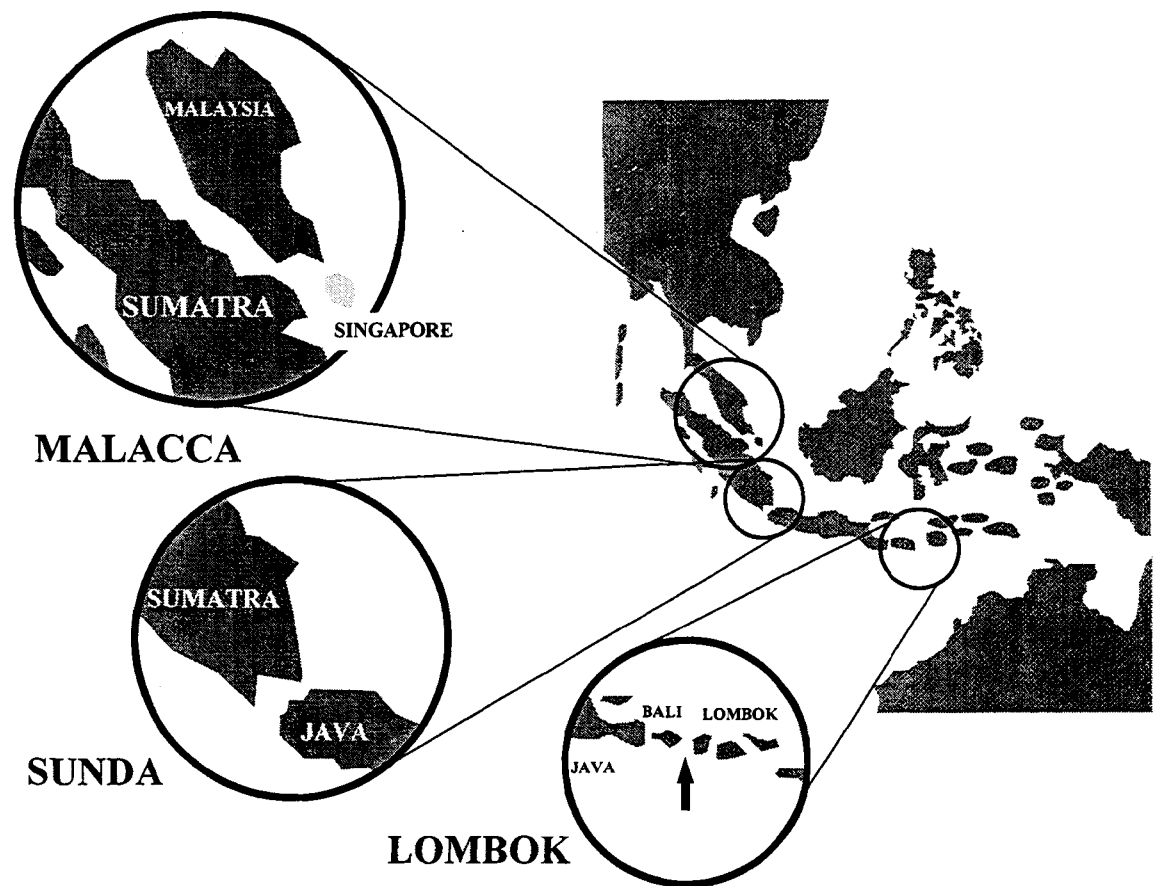


Figure C-1. Location of Vital Straits

⁶ John H. Noer with David Gregory, *Chokepoints: Maritime Economic Concerns in Southeast Asia* (Washington, DC: National Defense University, 1996), pp. 3–4.

⁷ *Ibid.*, p. 4.

Although Japan, Greece, the United States, the United Kingdom, and Singapore own most of the capacity-carrying ships passing through the straits, most of them fly flags of convenience (Panamanian and Liberian flags being the most prevalent).⁸ Often these ships carry cargoes owned by nationals from a third state, making shipping through the straits a truly international enterprise. Having to divert these cargoes around the archipelago would increase shipping rates, decrease annual available cargo capacity, and eventually affect consumer prices. Over half of the interregional tonnage passing through the Malacca Strait is either coming from or going to the Persian Gulf.

Although a quick glance at a map appears to show a number of courses through the Indonesian archipelago, water depth in these passages is extremely restrictive. Large crude oil carriers typically draw from 19 to 22 meters when fully laden. This draft challenges even the Malacca Strait, whose depth ranges from 21.1 to 22.9 meters. These ships are confined to a carefully marked channel and are unable to deviate to avoid other traffic.

These restrictions on navigation make it operationally feasible for an entity with even modest military capabilities to close the straits to deep-draft vessels. Often just the threat of violence can cause maritime insurers to refuse to cover vessels sailing in "war zones" or, alternatively, cause them to raise their rates exorbitantly. The narrow confines of the straits in question would make ships transiting them particularly susceptible to threats. Increased piracy could also cause insurers to increase coverage costs. If all of the straits were closed, shipping traffic would have to take the much longer southern route around Australia (see Figure B-2). The southern route around Australia from the Persian Gulf to Japan is approximately 5000 nautical miles longer than the route through the Malacca Strait. At 14 knots, this represents an additional 15 steaming days.

The study cited above estimates that *short-term* closure of the straits would have little impact on the global economy.⁹ Participants in this workshop were not so sanguine. They believed a short-term closure could be the catalyst for a far deeper Asian recession. The ripple effect created by the closure would be felt immediately in Singapore, one of the world's largest refining centers. It exports approximately 1 million barrels of product per day. Since it has relatively small stockpiles, refined products would soon be had only at a premium. A *lengthy* closure would probably result in a capacity shortage, but over time it would disappear, since there is typically an oversupply of vessel capacity on the market.¹⁰

⁸ Ibid., p. 5.

⁹ Ibid., p. 36.

¹⁰ Ibid., p. 38.

Commodity	Volume (millions of tons)	Value (billions of SUS)
Coal and coke	15.0	0.7
Consumer/electrical/other	90.5	149.4
Crude oil	309.9	40.1
Dry bulk	14.3	3.1
Food/agriculture/wood	38.6	29.0
Industrial goods	13.8	46.2
Iron ore	31.6	0.9
Metal and machinery	29.9	98.7
Petroleum products and chem.	72.2	23.4
Total	534.8	391.6
Destination region	Volume (millions of tons)	Value (billions of SUS)
Africa	1.8	4.6
Arab Gulf	5.2	12.3
Asia NIEs	123.3	61.7
Australia	6.3	10.8
Canada	0.1	10.8
China	6.7	9.1
Europe & Mediterranean	40.1	156.6
Indian sub-continent	9.3	8.1
Japan	240.1	70.4
South America	0.9	5.3
Southeast Asia	99.6	49.6
United States	1.5	2.7
Total	534.8	391.6
Source region	Volume (millions of tons)	Value (billions of SUS)
Africa	8.1	2.7
Arab Gulf	334.6	46.6
Asia NIEs	12.7	57.9
Australia	12.9	6.0
Canada	2.0	0.3
Caribbean	0.1	0.0
China	5.4	9.1
Europe & Mediterranean	45.4	109.2
Indian sub-continent	26.8	6.8
Japan	12.2	99.6
South America	8.2	0.3
Southeast Asia	62.0	47.5
United States	4.4	5.5
Total	534.8	391.6

Table B-1. Interregional cargo flows via Strait of Malacca, 1993¹¹

If sustained increased costs did result, it would be because of the extra ship-days required to transport goods. Extra fuel costs would be the primary cost driver. In the short run freight rates could triple (especially for crude oil), adding between three and five dollars to the price of crude.¹² An annualized detour cost could reach 7.4 billion dollars.¹³ The *direct* effect of straits closure

¹¹ Table 21 in Noer, op. cit., p. 59. Estimates include only interregional maritime shipments.

¹² Discussions with Department of Energy analyst, 9 June 1998.

¹³ Noer, op. cit., p. 45 (1993 dollars).

on the US economy would not be too severe, since only 3.3 percent of American exports and 4.5 percent of its imports travel these routes.¹⁴ The real significance would be the trickle down effects from the impact on the economies of US Asian trading partners and possible sustained high oil prices.

Japanese energy costs alone would rise an estimated \$1.5 billion annually as a result of increased shipping costs.¹⁵ But the long-term effect on its economy could prove much greater if oil shortages caused a significant slow-down in Japanese production.¹⁶ In 1997, Japan's crude oil imports from Middle East countries accounted for over 82 percent of its total crude oil imports (or approximately 1.71 billion barrels).¹⁷ Japan is reluctant to tap its strategic reserves and, according to one participant, "would open its checkbook" and start buying Pacific crude from Alaska and Venezuela at inflated prices.

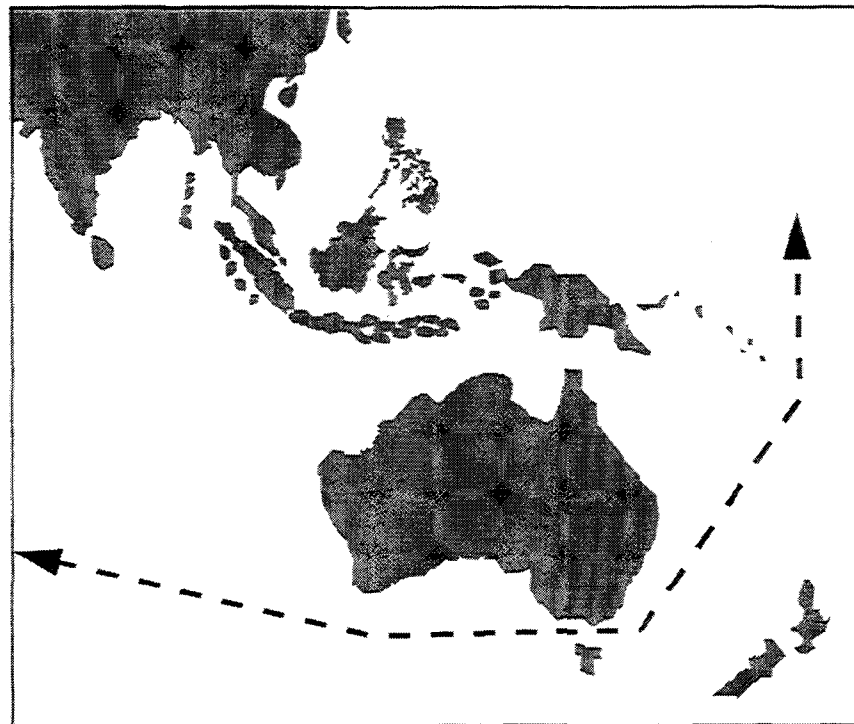


Figure B-2. Southern route around Australia

¹⁴ Ibid., p. 25.

¹⁵ Ibid., p. 45 (1993 dollars).

¹⁶ According to a 6 April 1994 report on the Japanese energy budget from the American Embassy in Tokyo, Japan has a national stockpile goal of 50 million kiloliters of crude oil (approximately 67 days worth at 1997 import rates). The same report indicates that private stockpiles also have about a 70-day supply. <www.gwjapan.com/ftp/pub/business/imi/apr/im940406.n03>

¹⁷ "In Japan . . .," *Platt's Oilgram News*, Vol. 76, No. 21, 2 February 1998, p. 6 (Lexis/Nexis)

If the production of Indonesian oil was stopped due to a crisis, another three to five dollar per barrel increase in oil prices could be expected. When added to similar increases caused by shipping rates, oil prices could go up between six and ten dollars per barrel. This would result in a one-half to one percent slow down in the US gross domestic product, or a resulting loss of anywhere from 38 to 72 billion dollars a year. Indonesia also supplies Japan with liquified natural gas that produces nearly ten percent of Japan's electrical power. Loss of that natural gas could also put pressure on crude oil prices. What is true for Japan is also true for South Korea.

Since 15 percent of the world's interregional seaborne shipments of all cargo types pass through this region, the broader global impact of having to divert around it could be billions more in price hikes and lost revenue.

Appendix D

PDD 63 Fact Sheet & White Paper

THE WHITE HOUSE

Office of the Press Secretary
(Annapolis, Maryland)

For Immediate Release

May 22, 1998

FACT SHEET

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURES: PDD 63

This Presidential Directive builds on the recommendations of the President's Commission on Critical Infrastructure Protection. In October 1997, the Commission issued its report calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, banking and finance, energy, transportation, and essential government services.

Presidential Decision Directive 63 is the culmination of an intense, interagency effort to evaluate those recommendations and produce a workable and innovative framework for critical infrastructure protection. The President's policy:

- ◆ Sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003, and significantly increased security to government systems by the year 2000, by:

Immediately establishing a national center to warn of and respond to attacks.

Ensuring the capability to protect critical infrastructures from intentional acts by 2003.

- ◆ Addresses the cyber and physical infrastructure vulnerabilities of the Federal government by requiring each department and agency to work to reduce its exposure to new threats;
- ◆ Requires the Federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained;
- ◆ Seeks the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships;
- ◆ Protects privacy rights and seeks to utilize market forces. It is meant to strengthen and protect the nation's economic power, not to stifle it.

- ◆ Seeks full participation and input from the Congress.

PDD-63 sets up a new structure to deal with this important challenge:

- ◆ A National Coordinator whose scope will include not only critical infrastructure but also foreign terrorism and threats of domestic mass destruction (including biological weapons) because attacks on the US may not come labeled in neat jurisdictional boxes;
- ◆ The National Infrastructure Protection Center (NIPC) at the FBI which will fuse representatives from FBI, DOD, USSS, Energy, Transportation, the Intelligence Community, and the private sector in an unprecedented attempt at information sharing among agencies in collaboration with the private sector. The NIPC will also provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts;
- ◆ Information Sharing and Analysis Centers (ISACs) are encouraged to be set up by the private sector in cooperation with the Federal government and modeled on the Centers for Disease Control and Prevention;
- ◆ A National Infrastructure Assurance Council drawn from private sector leaders and state/local officials to provide guidance to the policy formulation of a National Plan;

The Critical Infrastructure Assurance Office will provide support to the National Coordinator's work with government agencies and the private sector in developing a national plan. The office will also help coordinate a national education and awareness program, and legislative and public affairs.

For more detailed information on this Presidential Decision Directive, contact the Critical Infrastructure Assurance Office (703) 696-9395 for copies of the White Paper on Critical Infrastructure Protection.

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

May 22, 1998

WHITE PAPER

The Clinton Administration's Policy
on Critical Infrastructure Protection:
Presidential Decision Directive 63
May 22, 1998

This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. It is intended for dissemination to all interested parties in both the private and public sectors. It will also be used in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for course work and exercises on interagency practices and procedures. Wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government.

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- ◆ the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- ◆ state and local governments to maintain order and to deliver minimum essential public services;
- ◆ the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison

Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- ◆ assessing the vulnerabilities of the sector to cyber or physical attacks;
- ◆ recommending a plan to eliminate significant vulnerabilities;
- ◆ proposing a system for identifying and preventing attempted major attacks;
- ◆ developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns.

We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.

The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.

Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.

The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people.

In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.

The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.

The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.

The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.

We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.

Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. Structure and Organization

The Federal Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A).

Lead Agencies for Sector Liaison: For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the

Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

Lead Agencies for Special Functions: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.

Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.

National Infrastructure Assurance Council: On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish

procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.

Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.

Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.

Response: A system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.

Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.

Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding

the importance of security and to train them in security standards, particularly regarding cyber systems.

Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.

Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.

International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.

Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.

The CICG shall also review and schedule the taskings listed in Annex B.

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

Annex A: Structure and Organization

Lead Agencies: Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

Lead Agencies for Sector Liaison:

Commerce

Information and communications

Treasury	Banking and finance
EPA	Water supply
Transportation	Aviation Highways (including trucking and intelligent transportation systems) Mass transit Pipelines Rail Waterborne commerce
Justice/FBI	Emergency law enforcement services
FEMA	Emergency fire service Continuity of government services
HHS	Public health services, including prevention, surveillance, laboratory services and personal health services
Energy	Electric power Oil and gas production and storage

Lead Agencies for Special Functions:

Justice/FBI	Law enforcement and internal security
CIA	Foreign intelligence
State	Foreign affairs
Defense	National defense

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and communication, the Department of Defense will retain its Executive Agent responsibilities for the National Communications System and support of the President's National Security Telecommunications Advisory Committee.

National Coordinator: The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs. The National Coordinator will also

participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison Officials and Special Function Coordinators shall attend the CICG's meetings. Departments and agencies shall each appoint to the CICG a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. Beginning in FY99, the NPC shall be an office of the Commerce Department. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive.

Warning and Information Centers

As part of a national warning and information sharing system, the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, the President also directs the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government,

including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIPC will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community.

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the National Coordinator, with the

assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

Annex B: Additional Taskings

Studies

The National Coordinator shall commission studies on the following subjects:

- ◆ Liability issues arising from participation by private sector companies in the information sharing process.
- ◆ Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.
- ◆ The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.
- ◆ The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national

security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.

- ◆ The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.
- ◆ The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.

Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken:

- ◆ The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.
- ◆ The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.
- ◆ The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.
- ◆ The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

Internal Federal Government Actions

In order for the Federal Government to improve its infrastructure security, these immediate steps shall be taken:

- ◆ The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.
- ◆ The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.
- ◆ All federal agencies shall make clear designations regarding who may authorize access to their computer systems.
- ◆ The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.
- ◆ The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.
- ◆ The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.
- ◆ The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.
- ◆ GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.

- ◆ OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.
- ◆ The NSA, in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations.

Assisting the Private Sector

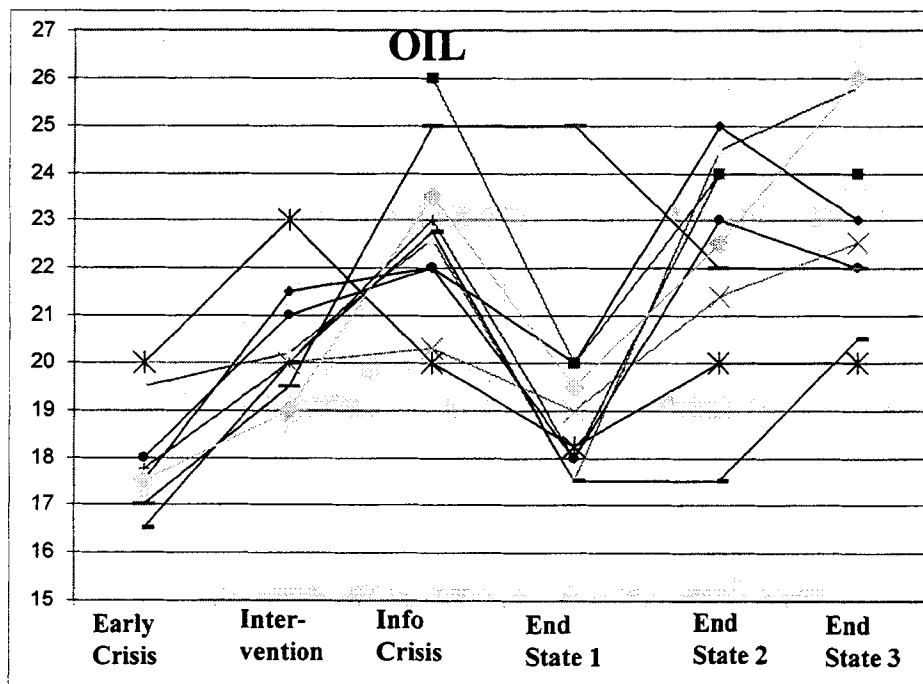
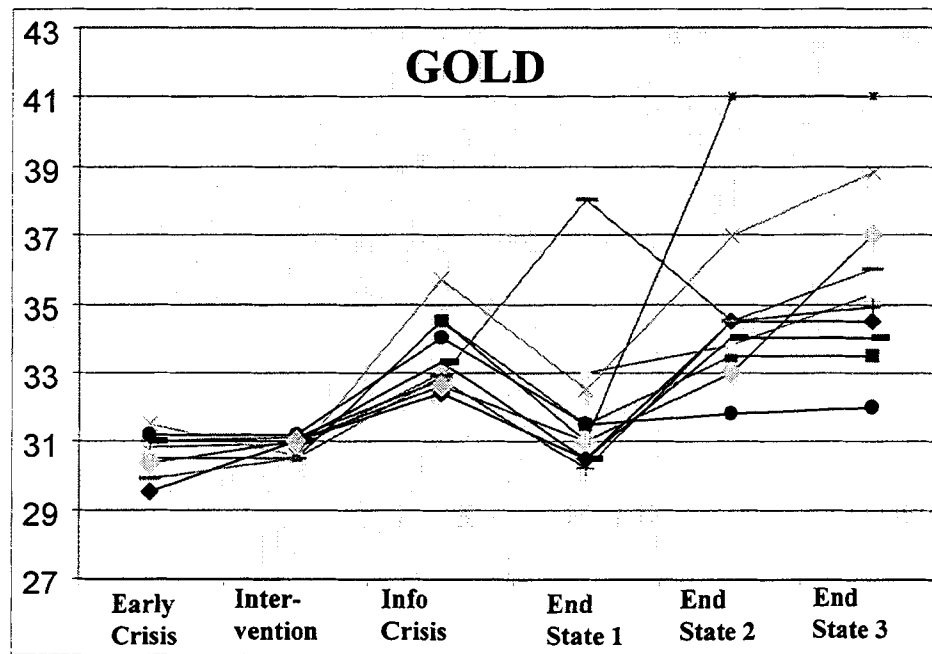
In order to assist the private sector in achieving and maintaining infrastructure security:

- ◆ The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.
- ◆ The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.
- ◆ The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles.

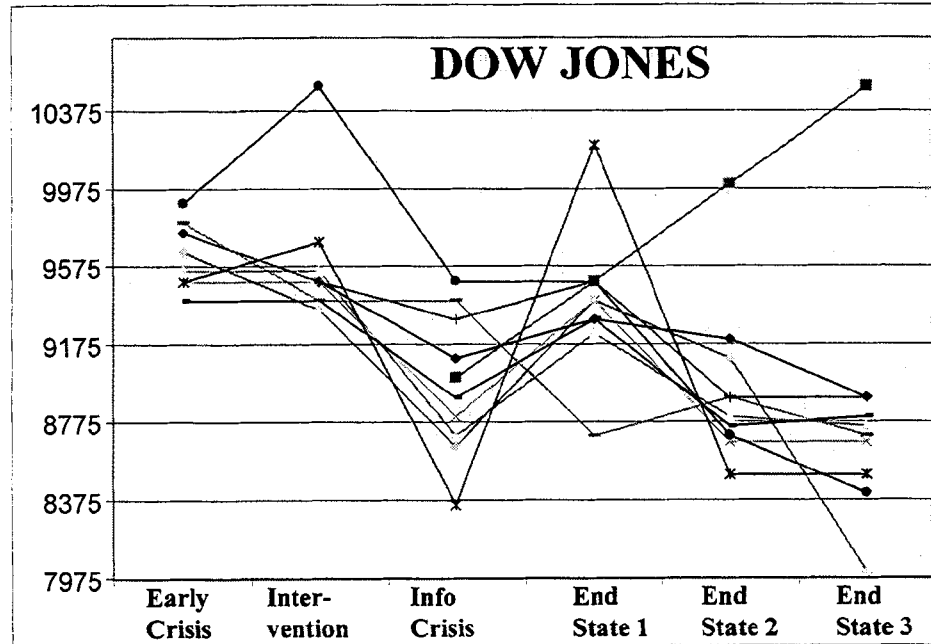
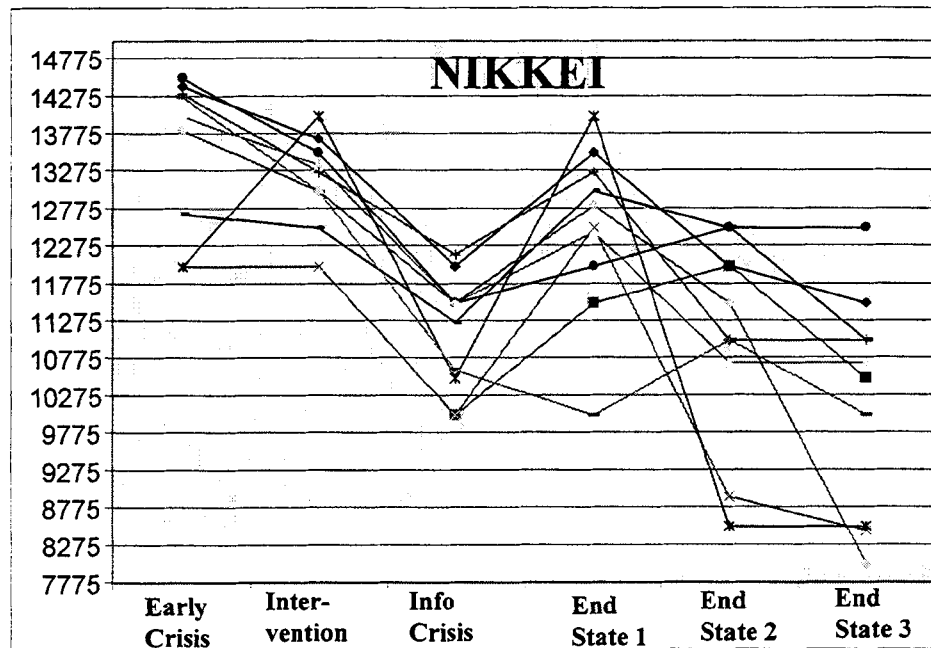
Appendix E

Polling Data

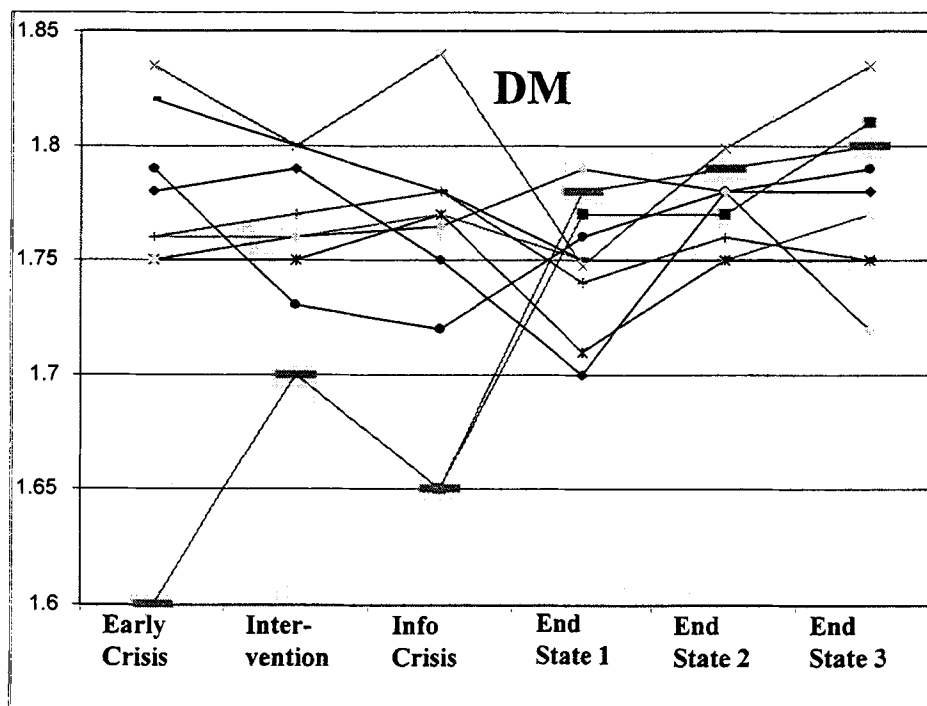
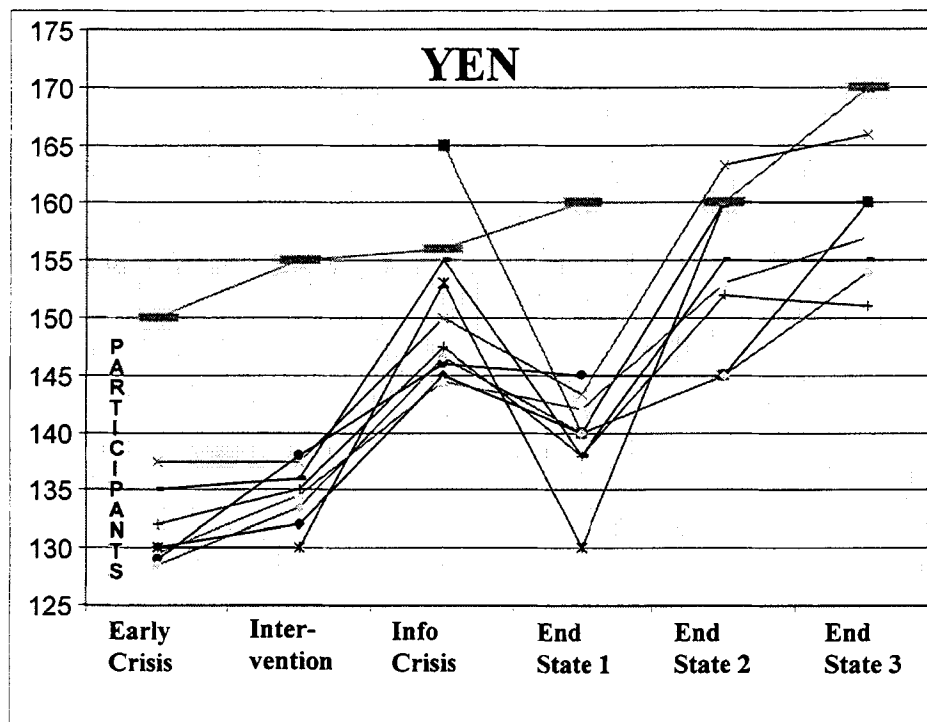
COMMODITIES



STOCK EXCHANGES



CURRENCIES



SECURITIES

