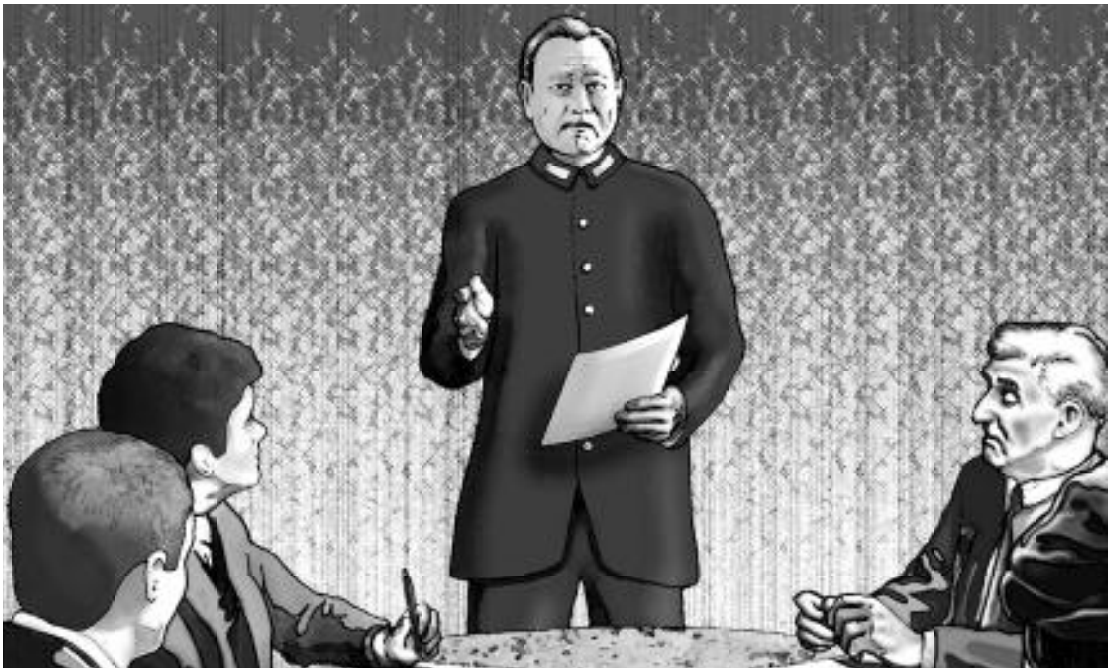
DISTRIBUTION A:
Approved for public release; distribution is unlimited.

A Failure of Vision

Retrospective*

CAPT FRED KENNEDY, USAF
CAPT RORY WELCH, USAF
CAPT BRYON FESSLER, USAF

PYONGYANG, KOREA, 2013. "Defeating the United States was a much easier task than we thought possible," Col Myong Joo Kim said in precise English. Educated at Harvard and CalTech, the haggard 45-year-old North Korean stood at the head of a small table around which sat interested representatives from nine nations. The room was harshly lit, without windows, and electronically screened from the outside world by systems "borrowed" from their prostrate foe. Colonel Kim's speech would never be heard again outside this forum, and the representatives would rapidly disperse after the briefing. However, it was essential for each representative to understand the nature of the successful campaign against the Americans and the implications for his nation. Colonel Kim announced:



*This article was written in the fall of 1997, before the present Iraqi crisis over UN inspections and the recent anthrax scare in Las Vegas. It appears that we are at least beginning to take biological warfare seriously. The authors would like to thank the following individuals for their invaluable assistance in producing this work: Capt Daniel Dant and Capt John Shaw, who provided excellent insight into what kind of story to tell; Capt Kathy "Gus" Viksne, who gave us some useful pointers on air defense; Capt Bryan Haderlie, who enlightened us on the subject of optical systems for space surveillance; Col Chris Waln, USAF, Retired, who provided the seeds for the Decapitation scenario; and Col Michael Mantz.

> Our plan has succeeded. We have inflicted—to paraphrase the words of an American airpower theorist—a "strategic paralysis" on the United States so that it is incapable of acting.[1] Following our attack on their homeland, the Americans have become defensive, turning decidedly inward. Their influence is rapidly waning around the globe; no longer do they deserve the title, "superpower." The remainder of the twenty-first century is wide open.

Some congratulatory glances were exchanged. Colonel Kim noticed these, then glanced down at his notepad. He spoke louder:

> Please do not make the mistake of assuming that this outcome was a foregone conclusion. The United States remains very powerful. There were specific steps that the Americans could have taken that might have prevented us from succeeding, or stopped our efforts in the planning stage. However, to be blunt, they suffer from a rather distressing lack of vision. Their own military strategy documents of the late 1990s anticipated much of the multipolarity and rapid change that have shaped the world of the twenty-first century—something that we in part helped to precipitate. As the world's last superpower, they acknowledged the dangers posed by aspiring regional powers, the proliferation of advanced weapons, terrorists, and attacks on their homeland.[2] However accurate their predictions of the future might have been, they made the mistake of continuing to structure their armed forces for combat between large numbers of conventional forces[3] while paying only lip service to the threat of asymmetric attack. Their arrogance blinded them to the possibility that a potential adversary might actually try to achieve their ends by other than a direct military confrontation. Their folly allowed us to exploit vulnerabilities in their most vital high-technology systems, making the dominance of their conventional forces irrelevant.[4] We should not fault them too much. Events have proceeded apace. Without an easily understood and measurable foe, the Americans have floundered for almost 20 years. It is certainly true that they have upgraded their systems along the way, but they never were able to fully realize the true value of their most technologically advanced systems, those that operate in two closely coupled media—space and information. We were able to take maximum advantage of their plodding and uncertainty. Let me start at the beginning.

Like any other nation, the United States is a complex system, and despite its many protests to the contrary, it has systemic weaknesses and leverage points that can be exploited by a knowledgeable adversary.

The Plan

Rangoon, Myanmar, 2009. The first meeting was shrouded in the utmost secrecy. The principals, with a suspicion verging on outright paranoia, shuttled through several unlikely ports of call before finally arriving at their destination. Initial communications were by word of mouth. There would be no "smoking gun" in the form of a document or cellular phone call to betray those involved. All participants prepared decoys who appeared prominently in foreign cities to distract the attention of the American intelligence-collection system. One joked nervously that he was less concerned with potential Central Intelligence Agency (CIA) ferrets than with the ubiquitous representatives of the US media. One reporter might suspect a ruse and inadvertently stumble on a story larger than he or she could easily imagine.

The Iranian envoy spoke first. He had not only originated the initial plan but had taken the potentially risky step of personally contacting the other members—representatives from North Korea, China, Iraq, and several multinational corporate concerns. He spoke of the "artificial restraints" currently imposed upon the world by American might, the inability of nation-states to exercise their freedom, and the absolute preeminence of the United States in the technical, industrial, and military realms. "Rome was no greater a power in its day," he remarked, "and Rome

endured for centuries. The Pax Americana is less than a century old. How long must we endure it?"

Nods and shrugs. The discussion quickly turned to the magnitude of the problem facing the cabal. The Iraqi envoy noted that his country had attempted to stand its ground with the best weapons it could afford only a generation previously but that it had been thoroughly trounced by the American war machine. The Iranian countered that the Iraqi challenge had been foolhardy, based as it was on meeting American strength directly. "Let us not tempt their stealth fighters and their carrier battle groups. We cannot best them. We are not—with the possible exception of my able Chinese friend—'peer competitors.' "[5]

"What, then?" asked the North Korean. "Terrorist attacks? Car bombs and suicide squads? What you seem to be suggesting is a route that has been attempted but that is felt to be no more than a pinprick by such a giant." The Iranian smiled and gave his reply:

> Like any other nation, the United States is a complex system, and despite its many protests to the contrary, it has systemic weaknesses and leverage points that can be exploited by a knowledgeable adversary. First, we will attack its leadership directly and audaciously. We will then undertake to seriously damage its command, control, and communications infrastructure. Finally, we will assault the economic infrastructure of several major cities.
>
> Some of you are clearly asking, To what end? The answer is simply put: to make them withdraw, to turn inward. The Americans are insular by nature, and they are still not entirely comfortable with the leadership role history has thrust upon them. Our attack will exceed their "cost-tolerance"[6] for continued conflict, at which point they will retreat to North America and wall themselves in. Such a course of events will permit us a free hand to take what is rightfully ours, unhindered by American intervention.

There were nervous shuffles and uncomfortable looks around the table. The Chinese representative spoke up. "We must not provide the United States with a valid target. They will want to lash out, and may perhaps do so irrationally. Therefore, all strikes must be covert strikes. We shall undertake no high-profile efforts that could warrant direct retribution against a specific nation."

"That is precisely what I have in mind."

Stage 1 (Decapitation)

11 July 2012, 8:35 A.M. EST. The day dawned hot, humid, and calm, typical of this time of year in the Washington area. Commuters inching north along I-395 glanced up through sunroofs to notice a low-flying twin-engined plane following the freeway at an altitude of only 100 feet. Of these, only four had the presence of mind to call in complaints on their cellular phones, but these calls were ignored by dispatchers as likely cranks. The aging 1972 Beechcraft King Air E-90 had already been airborne for over three hours, angling northeast across farmland and forested hills after an uneventful predawn takeoff from a private field east of Roanoke, Virginia. This course had been selected after only the most careful consideration of the alternatives—including a launch from one of the numerous supertankers plying their way up and down the East Coast. The conspirators had decided that the US air defense network of phased-array radars, Air National Guard and Customs patrols, aerostats, and the occasional overflight by low-orbit satellites carrying synthetic aperture radars (all enlisted in the continuing war on drug trafficking) was sufficiently daunting to make an unnoticed approach to the coast a chancy proposition. However, one member of the team pointed out that the North American Aerospace Defense Command (NORAD) was not nearly as interested in happenings within the interior of the country. Furthermore, US air traffic controllers often viewed only their transponder data, not bothering with the cluttered and headache-inducing radar return. A light plane running low and with its transponder off could thus be virtually invisible. Acquiring the plane and smuggling in the "munition" became the largest stumbling blocks, but the North Korean "team" overcame these

obstacles with relative ease.[7] All had dispersed within minutes of the plane's takeoff and were headed for international flights from several different airports in the Southeast.

Guided by a vastly improved global positioning system (GPS) network[8] and assisted by sophisticated terrain-mapping software[9] (downloaded from a French web site), the King Air carried no living human cargo—although a freshly thawed corpse was strapped into the pilot seat. The air plane dipped to under 50 feet as it passed between the Pentagon and Washington National Airport, cruising within the ground clutter, and then it abruptly began climbing, dispensing innumerable spores of multiply resistant *Bacillus anthracis* across much of the central capital area.

Suddenly alerted to the small plane's presence, air traffic controllers at the airport and at Andrews AFB, Maryland, tried at first to contact the aircraft and then began to narrowcast warnings to the Secret Service and other agencies. After several minutes, however, the aircraft veered to the northwest, dove rapidly, and crashed into the bluffs above the Maryland side of the Potomac, across from CIA Headquarters. The resulting fireball was extremely hot, leaving eager investigators and media little evidence other than melted wreckage and charred bone fragments. One observer reported weeks later that she had seen the small aircraft drop a cylindrical object as it flew over the Potomac, just prior to impact.

"Inhalation anthrax"[10] announces itself with initial symptoms easily mistaken for the flu or a common cold. Within two days, approximately 250,000 people—including the president, the vice president and her husband, 160 senators and representatives, senior leaders from numerous federal agencies, three service chiefs, and more than 11,000 Pentagon employees began to experience low-grade fever, fatigue, and a slight cough. Of the few that bothered to notify their doctors in the critical hours following the attack, none received the correct—and fatal—diagnosis. Ninety percent of those infected would die within a single week. The ensuing chaos would plunge the entire country into confusion.

Colonel Kim continued:

> We killed a significant portion of their national leadership with a single blow—the president, vice president, and several cabinet members, along with a host of their military leadership. Yet we left no traces for them to follow, and there was little opportunity for a coordinated investigation in any event, given our next actions. Now, the Americans could have prevented this if, for instance, they had carried out their plans for a space-based radar or global air traffic control system. Their current surveillance is spotty at best—and despite their professed concern about terrorism, they are egregiously poor at deterring internal threats. Even a fairly rudimentary low- or medium-orbit constellation of radar satellites providing continuous wide-area coverage could have detected our aircraft in time to take action.

The Iranian envoy frowned and said, "We had initially thought that their space systems were among their strongest assets." Kim replied,

> Yes, and you were correct to think so. However, we quickly discovered significant gaps in their existing reconnaissance and surveillance architecture. Certainly, they were—and are—able to detect virtually anything that moves on or above the earth, but in very circumscribed regions, and for only short periods of time. Without a global network, they must deduce which areas are of interest for observation, and either wait for their satellites to pass over the target or command them to modify their orbits. The first is time-consuming, while the second wastes precious fuel.

US leaders never succeeded in developing either the doctrine or the systems required for space denial and space protection. In fact, their national policy proscribed such activities, despite the obvious vulnerabilities of their vital space assets.

In short, the United States failed to capitalize on its initial investment—and continued to rely on an immature intelligence architecture. It hid behind its superior technology but failed to close the gaping holes in its systems.

Stage 2 (Disruption)

15 July 2012, 11:40 A.M. EST. Thousands of cases of severe respiratory distress were being reported all across the national capital region—alarming doctors and patients alike. Some two thousand people had already succumbed to "an unknown viral or bacterial infection." Widespread panic engulfed the District of Columbia metro area following the Center for Disease Control's (CDC) announcement of a regional quarantine on travel. With very little yet to go on, investigators from the CDC and the Army's Institute for Infectious Diseases were out in force, searching for answers. A regional manhunt was on, with few obvious suspects. Even as it was becoming clear that the national capital had been subjected to a catastrophic biological attack, it was evident that there was very little that could be done for the victims. The president was said to be gravely ill and several of his advisors incapacitated. Major news outlets were scrambling for information. Cable News Network (CNN) placed the story at the top of the lineup for its midday news summary, despite the skimpy nature of the material. Most other networks followed their lead. These reports were destined to never make it on the air.

Some 35,000 kilometers overhead, a nondescript Chinese telecommunications satellite, Dong Fang Hong (DFH) 91, sat idle in a "supersynchronous" orbit.[11] The Chinese had launched the satellite over a year and a half earlier, but it had suffered a series of highly publicized technical problems and was grudgingly relegated to the "junk belt" beyond geosynchronous earth orbit (GEO) in January 2012. Perhaps as a final insult to its builders, DFH 91 failed completely after performing its apogee boost and now revolved in a "useless" 26-hour orbit, returning to geosynchronous altitude at a slightly different longitude every day.

In reality, DFH 91's status as a derelict applied only to its ability to transmit digital TV to Chinese viewers on the planet below. Beginning in April, an observer positioned near the satellite would have noticed something out of the ordinary. Upon each descent of DFH 91 to the geosynchronous belt, a small dark object not much larger than a football would be ejected from a rear panel of the satellite. As it floated away from its parent, the small object would flare brightly and begin to recede, braking its way into a true geosynchronous orbit.[12] DFH 91's patient ground con-trollers would time these events to occur only over the daylit side of the planet; after all, even an enterprising amateur astronomer might have spotted the brief but brilliant pulse during an evening's comet hunting.

By late June, nearly 90 of these odd vehicles had been deposited around the GEO ring like so many space borne mines. All had benefited from the GPS's recent addition of "aft horns," allowing satellites in GEO to take advantage of America's premier navigation system to find their way. All had performed coorbital approaches and were scant meters from their targets, awaiting the final order to rendezvous. The targets, 86 diverse satellites built and launched by a half dozen nations, sat blissfully unaware, most receiving and transmitting video and voice data to waiting customers on the planet below. Other "birds" gathered weather data or listened to the encoded electronic whispers of a billion conver-

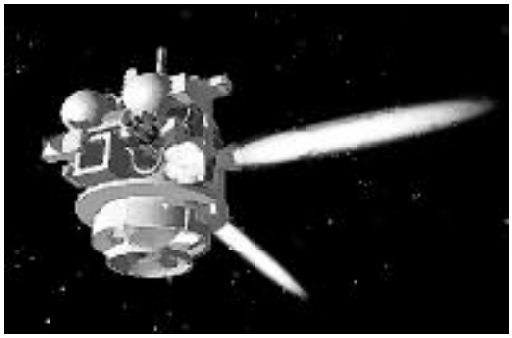
sations. Some waited patiently to report the telltale bloom of a ballistic missile launch or nuclear detonation.

The targeting itself was indiscriminate—and purposefully so. The Chinese knew that they would lose three satellites of their own in the attack. This was deemed an acceptable loss, and a useful misdirection. After all, there were still fewer than 20 states that could have managed the launch of a geostationary satellite, and suspicion would quickly settle on just one or two.

The final order was in fact no order at all. In the event of an abort, DFH 91 would have suddenly and surprisingly come to life, broadcasting a strong encrypted message to its kill vehicles strewn throughout the GEO ring. The vehicles would have immediately shut down, and the Chinese would explain the anomalous event as one more example of the satellite's bizarre behavior.

No abort was issued; the kill vehicles obligingly proceeded to "dock" with their targets. Most satellites are "hardened" against the severe radiation environment of space; some are further hardened to withstand the radiation concomitant with a nuclear blast. Few are armored against physical assault, other than to mitigate the effects of continuous micrometeoroid bombardment. After all, armor is heavy, and weight is at a significant premium when the cost of lifting a single kilo to orbit exceeds $50,000.[13] Thus, it was quite unnecessary to construct sophisticated kill vehicles. The simple devices simply exploded in close proximity to their satellites, sending shrapnel through solar arrays, battery systems, onboard computers, guidance systems, and sensors alike.

Sixty-two satellites were completely destroyed. Ten more were severely damaged and able to provide only marginal capability. Fourteen were apparently undamaged—most likely due to a faulty trigger on the kill vehicle or badly executed terminal maneuvers. The roster of casualties included Intelsat 919 (broadcasting 20 channels of video to various Arab nations), Thaisat 7 (providing mobile communications to Southeast Asia), and Go-



rizont 80 (a Russian military communications satellite).

None of these losses were made immediately apparent to Americans. However, at 9:43 A.M., Mountain Standard Time, controllers at the Space Based Infrared Systems (SBIRS) II[14] ground station at Falcon AFB, Colorado, were startled by the simultaneous loss of signal from fully three of their GEO birds. These satellites surveilled the planet for the infrared signature of ballistic missile launches. Without them, the United States would have to rely entirely on its groundside radar sites for detection of incoming missiles. A mad search for answers began to leap up the chain of command. A similar panic was setting in at the control center for Milstar III[15] communications satellites, where half of their birds had suddenly gone dark. Automatic rerouting systems looked for the next satellite in line to relay the growing backlog of message traffic, and, finding none, began sending queries and alarms to the control centers. Secure communications were crashing across the planet. In the anarchy that followed, the secretary of defense was forced to use land lines, ordering US military forces around the globe to their highest state of alert. No opponent had yet bothered to raise its head.

As the military scrambled to respond to an unknown threat, civilian controllers watched in horror as CNN's five network broadcasts went down simultaneously. Iran's Voice of the Islamic Republic, broadcast on nine channels, vanished into static. Viewers in Southern California lost all 460 channels of GlobalNet LA. Local television affiliates, adrift without their normal satellite feeds, began

What the United States needed was a few simple systems and the doctrine to tie them together.

placing calls to network broadcast centers, looking for answers that were simply unavailable. In a matter of minutes, the United States had lost 43 of its satellites in GEO, devastating military and civilian constellations alike. Fully two-thirds of the data shuttling between GEO and earth suddenly had nowhere to go.

Despite this, none of the personal communication and mobile telephone systems, provided by satellites orbiting at much lower altitudes, were destroyed. Between 11:30 A.M. and 1:30 P.M., call volume over these systems tripled, then quadrupled. By early evening, it was virtually impossible to secure a phone line anywhere in the country. The ubiquitous World Wide Web, repeatedly overhauled and massively enhanced during the first decade of the twenty-first century, was suddenly jammed with billions of demands for news. The information flow first slowed, then stopped. There was little enough to be had in any event.

Colonel Kim pointed to the statistics flowing down the wallscreen behind him:

> In all of this, we never engaged a single American weapon system. US leaders never succeeded in developing either the doctrine or the systems required for space denial and space protection. In fact, their national policy proscribed such activities, despite the obvious vulnerabilities of their vital space assets. The unspoken consensus among their commanders was clearly that space itself was too vast and the technologies needed were sufficiently difficult to develop that few other nations could devote the necessary resources to acquiring them.[16] Further, it is now clear that the United States was confident that it could spot a "rogue" launch and antisatellite attempt, trace it to the offending nation, and mete out punishment through more conventional means—via air strikes, for instance. The highly clandestine nature of the Chinese attack thwarted this, and left the United States without an adversary on which to concentrate.

"Yet we must certainly be high on their list of suspects," the Chinese representative pointed out. Kim nodded and said:

> Yes, and for this very reason we insisted on a plan which would foil even a determined investigation. Even so, discovery after the fact was not our greatest fear. In the midst of the confusion we created, with the chain of command disrupted, it was entirely possible that the United States might jump to conclusions and lash out blindly.

Colonel Kim shook his head in mock concern, then continued:

> The biological attack might have been seen as domestic terrorism, but an attack on space assets could be attributed to none other than a foreign power. Yet, even today, US leaders remain uncertain. Their ground-based assets were able to tell them that their satellites had been physically damaged or destroyed, but the lack of space-based reconnaissance systems has severely hampered their attempts to identify their foe.
>
> What the United States needed was a few simple systems and the doctrine to tie them together: a highly mobile reconnaissance platform to perform on-demand, close-in imagery; perhaps a variant of the same platform to damage a hostile satellite or tow it to a nonthreatening orbit; some form of proximity detection and defense for their most prized assets, such as their early warning satellites; and a rapid, ultra-low-cost launch capability to replenish constellations during a crisis. Finally, and most importantly, there was the need for an overarching concept of operations to integrate these basic missions. Without these elements, the US space architecture was immature, completely wedded to remote sensing and communication—in essence, subservient to their information architecture. Unable to conduct either offensive or defensive space operations, the existing American space order of battle—if we can so dignify it—calls to mind nothing so much as their Civil War–era ballooning efforts, the first crude attempts at overhead reconnaissance: virtually unmaneuverable, vulnerable to fire from below but unable to return fire. And yet, the United

> States was eventually able to achieve a fearsome mastery of air warfare, despite a somewhat unpromising beginning. In space, however, it remained stubbornly unwilling to make the logical leap.

The Iraqi piped up irritably, "For what purpose do you tell us where the Americans failed?" Kim pointed a finger at the Iraqi and said:

> I tell you this because our coalition must now begin to consider these very issues if we wish to someday gain hegemony. We have learned much from the US defeat, and if we do not take advantage of this momentary lapse in American attention, our efforts will have been for naught. In a very real way, we have surpassed them.
>
> They believed themselves to be, technologically, several generations ahead of their competition, which made them complacent. They chose to forget that a true revolution in military affairs—I use their terminology—requires not just the systems but a sophisticated operational doctrine to support them.

Stage 3 (Pandemonium)

15 July 2012, 1:54 P.M. EST. The CDC issued a sporadically heard statement at this hour, declaring the capital a victim of a biological attack. Emergency Broadcast System messages began playing at local Washington, D.C., affiliates just before 2:00 P.M., asking the populace to remain calm and stay in their homes. This warning went unheeded. Highways around the region were closed to inbound traffic entirely, freeing up additional lanes to the fleeing public. National guardsmen from Virginia and Maryland, requested by the president early in the afternoon as riots began to erupt around the District, found themselves stranded along the shoulders of major arteries, waiting out the passage of hundreds of thousands of panicked residents in the D.C. area.

As panic gripped the national capital region and the military groped for answers, the final phase of the coalition attack began. It had already been initiated by a scrambled cellular call, placed from Teheran to Norway at just after 9:50 P.M. Iranian time. In a quiet Oslo suburb, a "go" was given. Led by the notorious hacker "Whisper," three seasoned programmers set to work, bouncing the ignition signal of a particularly potent virus off three telephone switching stations in Britain, and finally through commercial web sites on both the East and West Coasts of the United States. The effect was immediate: automated teller networks in six major cities—Los Angeles, San Francisco, Seattle, New York City, Miami, and Washington—were instantly brought down. Those that returned to service began to behave erratically, releasing thousands of dollars at the touch of a button. Los Angeles–based banks responded almost instantly, closing their doors on mobs of angry account holders in the early afternoon. Lending institutions across the country began to follow California's lead, creating a growing ripple of uneasiness. The run on hard currency was beginning. The New York Stock Exchange suspended trading half an hour before the closing bell; the market had already slipped an ominous 15 percent. Despite the frustrating communications backlog, realization was spreading that the United States appeared to be under some form of diverse, coordinated assault. In Oslo, Whisper prepared to unleash a second attack.[17]

They [the Americans] chose to forget that a true revolution in military affairs . . . requires not just the systems but a sophisti- cated operational doctrine to support them.

The target was the already overloaded US telephone network and its collection of switching and routing stations.[18] Cellular grids and telephone exchanges in the D.C. area received special attention, although outages were initiated in seemingly random locales from Colorado Springs to Charleston. The net effect of the attack was to bring nationwide commercial telecommunications to

a standstill. Coupled to the crippling blow dealt the banking industry, economic transactions ground to a halt. In contrast, vital national communications were left untouched. The military's workhorse Defense Switching Network (DSN), the Joint Chiefs of Staff Alert Network (JCSAN), and the Secure Voice Teleconferencing System (SVTS) remained fully operable.[19] Information warfare experts were awakening to the fact that they had been as effectively bypassed as the Maginot Line in 1940.[20] What none had yet understood was the magnitude of the disaster. Whisper's viruses would confound some of the best American programmers for months. The heavily encrypted Iranian software had been designed to resist the most concerted decoding attempts.

Word of the president's death by severe respiratory distress arrived shortly after the dinner hour on the East Coast, and reached the rest of the nation and the world primarily through shortwave radio transmissions. With the vice president already dead, the Speaker of the House, a senior Democrat from Pennsylvania, was transferred by helicopter to Andrews AFB. At 6:55 P.M., the Speaker boarded the nation's single E-5D, a highly modified Boeing 777, and the latest in a long line of aircraft that had waited to perform this mission. As the plane became airborne, one of the three surviving Supreme Court justices administered the oath of office to the badly shaken congressman, whose first act was the declaration of martial law nationwide. His second act, perhaps more controversial, transferred the official seat of government from Washington to Philadelphia "for the duration of the crisis."

Americans in all walks of life awaited their opponent's next move. Colonel Kim pointed to the Iraqi envoy:

> In 1990, the United States perceived your incursion into Kuwait as a serious threat to its national security. Why? Your nation hadn't fired on any Americans. Your crime was to endanger their oil supplies. They responded with prompt action, and you and your countrymen were humiliated.
>
> The Americans saw the threat to their information networks even as they were constructing them. Their military built elaborate security measures to resist intrusions into secure areas, protecting sensitive data and preventing unwelcome visitors from wresting control. Yet even as they strengthened these defenses, they did not pay sufficient attention to the massive growth of their nation's commercial information infrastructure, and their economic reliance upon it. The analogy between oil and information could not be clearer—banking networks and telecommunications systems are, if anything, more essential to the day-to-day operation of their country, and far more vulnerable to disruption.
>
> Our Iranian allies chose well, attacking vulnerable civilian systems and ignoring the heavily protected government networks. By itself, such an effort would have resulted in irritation and annoyance. Coming on the heels of the other attacks, however, our information strike resulted in a mass hysteria which, for all practical purposes, temporarily shut down the United States. While they were able to reconstitute their government fairly quickly, they have still failed to fully recover. Their citizenry is up in arms and demanding answers. For the past year, their legislators have been calling for a "retrenchment."

"I trust that you all understand why I am spending some time on how the Americans might have defeated us?" Kim asked. There were nods of assent around the table.

> One lesson we have learned is that information warfare is not to be applied in a vacuum.[21] In concert with other forms of war, it can have useful synergistic effects. Taking out a city's electrical power is an inconvenience, but is not typically life-threatening. But to the same city gripped in the throes of rioting, such a move can be devastating.
>
> Countering our information strikes would have required a coordinated effort on the part of the American military establishment to protect "critical sectors"[22] of the commercial information infrastructure. This would have been a daunting task. American corporations are noted for their fierce independence; they would have chafed under any form of regulatory guidance the government imposed.

> Yet forgoing any form of protection is foolishness—after all, one should not depend on that which one cannot defend.

Colonel Kim switched off the wallscreen. In a grave tone, he continued:

> The United States was able to marshal its enormous scientific and engineering expertise to create invention after invention for space and information applications. Americans built high-technology houses of cards and congratulated themselves on their innovation without taking the time to fully understand the full implications of what they had wrought. They dabbled in remote sensing, providing themselves an illusory sense of security at odds with their actual capabilities, and leaving themselves open to unconventional attack. They refused to apply their own lessons of airpower to space power, preferring to maintain a fragile and highly vulnerable information architecture in the sky. Lastly, they chose not to tackle the admittedly difficult problem of safeguarding their civilian information infrastructure. Taken in isolation, each of our attacks was painful but not threatening to their national integrity. Together, however, they very nearly brought the United States to its knees.

The North Korean envoy rose and bowed expansively, "Thank you, Colonel Kim. Your analysis is a cogent one, and I assure you it is greatly appreciated by each of us. I apologize for not remaining; I go now to oversee the last of the mopping-up operations around Pusan. Please, know my gratitude and that of your nation."

Epilogue

History will record that the United States suffered a resounding defeat in 2012 by an anonymous adversary employing a combination of low- and high-technology thrusts that skillfully brought the world's last superpower to its knees. Emboldened by the emergence of this power vacuum, numerous nation-states rushed to pursue territorial expansions that would have been unthinkable in another era. North Korea, hanging on long after pundits had predicted its fall from famine, brutally seized the South with chemical and biological weapons in 2013; three years later, China moved southward into the newly emergent industrial powers—Laos, Cambodia, and Vietnam—of the Asian Dynamo. After initially threatening a nuclear response, an exhausted Israel capitulated to a combined Islamic force in 2029. In all of these crises, the worldwide question was the same: Where were the Western powers? Without strong US backing, Europe was essentially impotent, unable or unwilling to come to consensus decisions. Russia, continually wracked by internal civil strife, could not shift its focus away from preserving the remains of its shattered empire. While the United States was able to recover and rebuild itself following the initial shock, it was simply incapable of responding to foreign crises. Fortress America had been breached, and the citizenry was adamant that it would never happen again. The rest of the world would, for the most part, be left to its own devices. □

Notes

1. John A. Warden, "Air Power for the 21st Century," in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues* (Maxwell AFB, Ala.: Air University Press, 1995).

2. These potential threats to US interests are discussed in the *Report of the Quadrennial Defense Review (QDR*) (Washington, D.C.: Department of Defense, 1997), 3–4. The full text is on-line at http://www.defenselink.mil/pubs/qdr/.

3. Ibid., v.

4. The *Report of the QDR* did acknowledge that future adversaries may use terrorism; nuclear, chemical, and biological (NBC) threats; information warfare, or environmental sabotage to attack our forces or interests overseas and at home. However, such threats were viewed only in the context of how they might adversely impact our conventional military operations (p. 4).

5. The *Report of the QDR* notes, "The security environment between now and 2015 will also likely be marked by the absence of a "global peer competitor" able to challenge the United States militarily around the world as the Soviet Union did during the cold war. Furthermore, it is likely that no regional power or coalition will amass sufficient conventional military strength in the next 10 to 15 years to defeat our armed forces, once the full military potential of the United States is mobilized and deployed to the region of conflict" (p. 5).

6. *Cost-tolerance* is defined as the point at which the cost of accepting an adversary's policies, in terms of deprivation and

suffering, is less than the cost of continued resistance. Dennis M. Drew and Donald M. Snow, *The Eagle's Talons: The American Experience at War*(Maxwell AFB, Ala.: Air University Press, 1988), 6–7.

7. Airplanes On-Line advertises numerous light planes for sale (http://www.airplane.com/). One of the authors was easily able to locate several aircraft with the necessary range, one right over the Virginia border in North Carolina, and the asking price was not exorbitant.

8. The US Naval Observatory's web site (http://tycho.usno.navy.mil/gpsinfo.html/) speaks to current GPS capabilities. The Standard Positioning Service (SPS) permits a vertical fix accurate to approximately 156 meters (511 feet), insufficient to fly "nap-of-the-earth." GPS's Precise Positioning Service (PPS) provides substantially improved performance, allowing for a fix of 28 meters (92 feet) or better. Originally, PPS was to be made available to nonmilitary users on a case-by-case basis; however, a 1996 presi- dential directive specifically called for the more accurate signal to be made available to civilian users by 2006. Differential GPS—using ground reference receivers—makes "sub-meter" determination possible, without any of the additional enhancements currently planned by the NAVSTAR GPS Joint Program Office for its Block IIF satellites. Some discussion of this can be found at http://www.arpa.mil/ARPATech-96/slides/ganz/100.

9. Digital terrain modeling software is easily available today via the Internet through numerous commercial outlets. The authors were able to download demonstration versions of both American and New Zealand models. It is not unlikely that 12 years from today highly accurate terrain maps, updated via imaging satellites (such as France's SPOT) will be available for perusal almost in real-time. This practice is not limited to commercial concerns; the US Geological Survey maintains a web site (http://www-nmd.usgs.com) where precise topological maps of the nation's countryside can be purchased.

10. Part II (Biological) of the *Handbook on the Medical Aspects of NBC (Nuclear/Biological/ Chemical) Defensive Operations* describes the effects of inhalation anthrax as well as the woeful state of potential countermeasures. It can be found on the World Wide Web at http://www.nbc-med.org/amedp6/PART II. A more detailed discussion is available in Dr. Malcolm Dando's*Biological Warfare in the 21st Century* (London: Brassey's [UK], 1994). On page 34, Dando notes, "Infection through the lungs is particularly dangerous . . . [inhalation anthrax] has a mortality rate approaching 100 percent."

11. Dong Fang Hong 91 is depicted as the latest of an existing series of Chinese satellites. For instance, DFH 41, a telecommunications satellite launched 29 November 1994, was retired only a few months later, ostensibly due to a fuel leak. Numerous satellites sit in the "junk belt" beyond GEO, moved out of their precious slots to make room for other, newer assets. These moribund devices are said to have been "supersynched." For an excellent description of current satellites on orbit, point your web browser at http://www.telesatellit.com/tse/online/, the on-line edition of the *Satellite Encyclopedia.*

12. Boeing's Kinetic Energy Anti-Satellite Technology (KE-ASAT) program is a potential prototype of the Chinese "kill vehicles" aboard DFH 91. See "KE-ASAT Prototype Tracks Target in Edwards Hover Test," *Aerospace Daily*, 13 August 1997, 239.

13. The Developmental Planning Directorate at Air Force Materiel Command's (AFMC) Space and Missile Systems Center (SMC/XR) estimates the current cost of a Titan IV launch to approximate $500 million. Since Titan IV, coupled with a Centaur upper stage, can deliver 5,200 kg to geosynchronous orbit, the cost per kilogram to GEO is slightly more than $95,000 per kilo.

14. SBIRS (Space-Based InfraRed Systems) is the follow-on to the Defense Support Program (DSP) series of satellites, and is intended to provide missile warning, missile defense, and "battlefield characterization" information to earthside users. SBIRS is currently considering a bifurcated architecture of "high" (GEO- and Molniya-based) and "low" (low earth orbit-based) vehicles. The first SBIRS high satellites is likely to come on-line in early 2002. Mission and schedule information were found on the SBIRS web site http://www.laafb.afmil/SMC/MT/sbirs.htm.

15. Milstar III is a fictional extrapolation of the existing series of secure military communications satellites. More information can be found at http://www.laafb.af.mil/SMC/MC/Milstar/.

16. These commanders were also supported by the pacifistic nature of extant space law: "States Parties to the Treaty undertake not to place in orbit around the earth any objects carrying nuclear weapo ns or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner." Taken from Article IV of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bo d ies, signed 27 January 1967. Liberally interpreted, this passage has been used to attack the emplacement of any form of weapon in space. The full text of the "Outer Space Treaty" is on-line at http://www.spfo.unibo.it/spolfo/SPACELAW.htm.

17. Spectre-Press's web site (http://www.spectre-press.com/) offers its customers a "monumental" instruction book on a vast array of dubious activities, including guidance on sending fake electronic mail messages, "cracking" Novell Netware, and getting into all manner of systems (from credit bureaus and banks to government networks). Numerous other hacker sites exist, catering to a growing subculture of covert cyber-criminals.

18. Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995). Colonel Szafranski notes on pages 61–62, "In the case of advanced societies or groups, attacks against telecommunications systems can wreak havoc with an adversary's ability to make effective decisions in warfare." This article can be found at the College of Aerospace Doctrine, Research, and Education (CADRE) site (http://www.cdsar.af.mil/apj/szfran.html).

19. The Defense Information Systems Agency (DISA) maintains a list for these and other frequently used acronyms at http://www.disa.mil/org/acronym.html. JCSAN permits the joint chiefs access to secure, on-call voice communications with all specified and unified commands. SVTS is described as an executive-level network (president/White House to secretaries) that includes packetized data networking, broadcasting, and video teleconferencing capabilities. Systems such as these are likely candidates for enhancement and expansion over the next decade.

20. Martin C. Libicki echoes this concern in the introduction to his excellent *Defending Cyberspace, and other Metaphors* (Washington, D.C.: National Defense University Press, 1997). He states, "Global computer and media networking carries risks, even if these risks are easily exaggerated. Computer networks might permit enemies to use hackers to attack the information infrastructure of the United States, rather than its military forces. The conventional defense establishment has been described as a Maginot Line, in which hackers are equivalent to Guderian's Panzer Korps, wheeling past prepared defenses to strike at the nation's unguarded flanks." The full text is available at the Institute for National Strategic Studies' home page on NDU's web site, http://www.ndu.edu/.

21. Ibid. The author rightly wonders, "How much damage could a digital Pearl Harbor cause? Suppose hackers shut down all phone service (and, say, all credit card purchases) nationwide. That would certainly prove disruptive and costly, but as long as recovery times are measured in hours or even days, such an attack would be less costly than such natural events as a hurricane, snowstorm, flood, or earthquake — events that have yet to bring the country to its knees."

22. Ibid. Key sectors should include telecommunications, energy, funds distribution, and safety systems.