Network-Centric Strategic-Level Deception

Philip B Erdie[1] and James B. Michael[2,*]

[1]*Marine Corps Systems Command, Quantico, Va., U.S.A. philip.erdie@usmc.mil*
[2]*Naval Postgraduate School, Monterey, Calif., U.S.A. bmichael@nps.edu*

*** Corresponding author**

Paper no. 254

Network-Centric Strategic-Level Deception

Captain Philip B. Erdie, USMC
Marine Corps Systems Command
Quantico, Virginia 22134 USA
philip.erdie@usmc.mil

James B. Michael
Department of Computer Science
Naval Postgraduate School
Monterey, California 93943 USA
bmichael@nps.edu

Abstract

This paper explores strategic-level deception in the context of network-centric information operations. Advances in information technology and the global connectedness of communications networks have created new opportunities and challenges for conducting strategic and operational level deception campaigns with significant utilization of cyberspace. Planning and executing concurrent strategic-level deceptions among distributed participants and against multiple targets requires speed, flexibility, and accurate situational assessment. This paper begins with a historical account of twentieth century use of strategic-level deception, followed by a definition of network deception, considerations for achieving network-based deception, and a proposed model for the planning and execution of network-centric deception campaigns. The command and control structure proposed in this paper is a framework that integrates complex elements of information infrastructures across public and private spectrums.

1. Introduction

Leading up to the 1973 Yom Kippur War, Egypt applied over 150 deception ploys in economic, political, and military form. Beginning in February of that year, a small team of people commenced planning the deception campaign for an invasion to occur eight months later. The actual combat that followed in October had been preceded by deceptive construction projects, false intelligence reports, and misinformation applied over a wide spectrum of noncombatant activities. However, few of the deceptions had any impact [3].

Some individuals believe that the tremendous growth in intelligence collection capabilities has diminished the possibility of deceiving a sophisticated opponent. An alternative perspective is that the more extensive the collection capability of an opponent, the greater the opportunity to feed the target specifically designed misinformation. Advances in information technology have created new opportunities to exploit the limitations on human information processing. The United States' public and private computer networks are probed by rogues (i.e., illegitimate users) on a frequent basis. Such probing activities result in varying degrees of network infiltration. In many cases, the targeted networks are compromised. Considering the existence of such adversarial activity and the growing importance of network-centric warfare, questions may be asked such as:

- Can such adversarial network attack activities be used for our own gain?
- Can we use our own networks and the information on these networks as a tool of deception?
- Can we initiate deceptive actions within our own C4I infrastructure?
- Can we conduct coordinated network deception operations?

This paper examines the potential value of network-centric strategic-level deception operations, which, if conducted during all phases of conflict, and in particular, during peacetime, would strengthen national C4I assets, support geo-political and military operations, and potentially deter future conflict.

1.1 Problem Definition

The purpose of this paper is to examine the potential value of stratagem conducted in the modern network-centric environment. The proprietors of the rapidly growing communications infrastructures include government agencies, military commands, financial institutions, and corporations. The question explored in this paper is, "How do we conduct and manage network deception operations in support of the action of national objectives?" The answers to the following questions provide a background for this explanation:

- What is network-centric strategic-level deception (NSD)?
- What is involved in planning and executing network deception?
- How should the command and control structure be organized to support NSD?

1.2 Scope

The scope of this paper includes developing a definition for network-centric strategic-level deception in support of national security strategies and subsequent military and diplomatic activities. This paper also introduces an organizational model for the planning and executing network-centric deception campaigns but detailed analysis of the proposed command structure is left for future work.

1.3 Significance of Paper

NSD is a sequence of computer network activities or measures taken to manipulate adversarial perceptions regarding computing and communication capabilities. Network-centric deception campaigns can facilitate strategic and operational objectives of the U.S. Government. NSD is an instrument for influencing the perceptions and subsequent actions of adversaries with regard to economic, military, and information resources. The aim of NSD is to protect the national security interests of the United States. NSD enabled exploitation facilitates strategic and operational objectives by influencing adversarial actions and creating opportunity for tactical gain or diplomatic leverage.

Second, NSD may make possible sustained network access even if adversarial sensors monitor network activities. If an adversary is able to compromise a communications network, most likely that network becomes a liability with regard to operation specific security. Continued use of the network may not be an option. However, if crafted properly, an adversary would have difficulty discerning between legitimate and deceptive data collected from the network. Data that is transmitted across the communications infrastructure by legitimate users is "accompanied by a bodyguard of lies" [1] via deceptive data in the "noise" of the deception. This, in turn, can degrade the ability of the adversary to exploit the networks for their gain while legitimate users can use the infrastructure to conduct business.

Third, NSD may mislead or persuade adversaries to opt for disadvantageous courses of action. The aim of this stratagem is to guide an opponent to an unfavorable course of action [15] and eventually that adversary will fall victim to surprise. Deceptive measures are a type of counterintelligence activity for misleading or confounding the adversary. Contradictory indicators, missing data, fast moving events, time lags between data collection and analysis, and simple chance all inhibit accurate intelligence assessment and potentially lead to successful deception efforts.

Fourth, NSD is a tool to gain operational advantage. Historically, deception is the least expensive and most effective means of manipulating an opponent's military, economic, and diplomatic resources [9] below. The objective of network deception, conducted at the strategic and operational levels, is to influence adversarial decision makers before conflict occurs. NSD may thwart adversarial intelligence operations resulting in inefficient allocation of enemy assets and personnel creating diplomatic leverage and delaying an adversary's military or political decisions and perhaps avoiding conflict altogether.

Lastly, NSD can preserve C4I assets. Military planners, adversarial and friendly alike, often plan for worst-case scenarios that generally lead to inflated projections about the opponent's capabilities. False projections about a nation's communication infrastructure and computing ability will influence an enemy's assessment of that opponent's command and control capability. An adversary's inflated assessments can be used to the strategic advantage of the opposing side. By forcing an adversary to allocate minimal intelligence assets to what is perceived to be a tertiary effort, enemy intelligence-gathering operations will be reduced in effectiveness. This economy-of-force concept translates to communication network activities and is applicable to both defensive and offensive operations. Small measures of successful network deception have the potential to compensate for or hide gross failures of operational security.

2. Case Studies

Within recent history, there have been several well-documented examples of meticulously planned and executed strategic-level deception campaigns that complimented long-term military operations. Two well-known exploits of deception were Plan Bodyguard during World War II and Operation Badr, which preceded the Yom Kippur War of 1973. The organizations responsible for the deception efforts were the United Kingdom's London Control Section and the Egyptian political leadership, respectively. For an in depth histories of Plan Bodyguard and Operation Badr, see [8] and [12], respectively.

2.1 The London Control Section

The London Control Section (LCS) was a secret bureau established by Britain's Prime Minister Winston Churchill. Considered the first national government organization formally tasked to conduct strategic-level deception campaigns, the LCS conceived and coordinated stratagems to deceive Hitler and his General Staff [1]. The British tool of deception was "special means," covert activities designed to compliment military operations. "Special means" was indeed Britain's strength considering the fact that Britain had maintained its vast empire for hundreds of years. Deception, considered the pursuit of gentlemen [1], achieves great victories through "subtle means and good brains." Through the LCS,

Churchill made deception an integral part of conducting military and statecraft affairs. The members of the LCS used every medium of deception: "whispers, rumors, double and triple agents, sacrificial and clandestine operations" [1]. Also, Churchill made sweeping changes to Britain's intelligence community by centralizing the coordination of campaigns conducted by military and intelligence organizations. Churchill recognized that a single repository of intelligence was necessary for his war of special means. A single source of intelligence would allow Churchill and the LCS to possess the sum of all available intelligence in order to deliberate the minute details of Britain's deception campaigns.

The Chief of the LCS was Colonel John Bevan. Bevan was from a family of financiers that had connections and assets worldwide. Deputy to Colonel Bevan was Colonel Sir Evelyn Leslie Wingate. Wingate had served as a political officer throughout the British Empire. He was fluent in Greek, Arabic, French, and Urdu. Only Colonels Bevan and Wingate were privy to all details of the intertwining activities of the LCS. Other members of the LCS came from unique and broadly varying backgrounds: financiers, politicians, diplomats, scientists, writers, and artists all scattered abroad and gentlemen of special means. From this core of men radiated connections [1] to military commands and intelligence agencies, enemy and friendly alike.

> Thus, the structure of the LCS was such that a stone cast at Storey's gate rippled in ever widening circles of political, financial, civilian, diplomatic, scientific, military influence. [1]

The LCS was not concerned with tactics or with execution of the operational plans. The focus of the LCS was strategic. The activities of the LCS transpired nowhere near the physical battlefields. Their campaigns were waged via the communications infrastructure used by financial institutions, manufacturing facilities, diplomatic circles, and scientific forums. The LCS was able to transmit instructions in a fast, secure, reliable, and synchronized manner. A story planted in Lisbon circles could be substantiated by a political move in Washington, a news story from Stockholm, military action along the Syrian-Turkish border, a calculated leak at Madrid, a rumor in Cairo, and the statement of a high commander in New Delhi. Through these communication channels, Bevan could "ring his carillon at will" [1].

Fortitude South is perhaps the best example of the LCS ability to influence Germany's military operations. The objective of Fortitude South was to mislead the Germans as to the time and place of an Allied invasion: the aim was to trick the German leadership into believing that Allied forces would land at Pas de Calais, France. The LCS already had a well-established operation known as Jael. This particular operation involved spreading rumors at diplomatic posts around the world in an effort to shift Germany's focus anywhere other than the coast of Northwestern France. The LCS knew that Germany had three primary means of intelligence collection: aerial reconnaissance, spies, and signals intelligence. The LCS orchestrated the release of deception cues so that the pieces of the Fortitude South puzzle would create the desired perception to Germany's High Command. Knowing the Luftwaffe had limited aerial reconnaissance capability, the LCS had to ensure what little imagery obtained by Germany would support the deception storyline. The Allied deception force constructed dummy tanks, airfields, and landing craft that appeared authentic to airborne observers. Next, the LCS turned its Double Cross (XX) Committee. The most successful double agent, Garbo, was able to influence German leadership from the top-down to include Adolf Hitler. Also, an important factor of Fortitude South was Ultra, a code name for intelligence obtained from intercepts of German radio traffic. Ultra provided timely feedback. Through the Ultra radio intercepts obtained, the LCS was able to verify the varying degrees of success achieved by XX agents. The content of radio intercepts supported the belief that the Pas de Calais was the main target of the pending Allied invasion.

Signals deception also played a significant role in the overall plan of Fortitude South. To convince the Germans that the Allies were forming an Army in Kent, radio message traffic was transmitted that would confirm such suspicion. Also, the Allies used chaff to simulate the ships of an invasion fleet headed toward Pas de Calais. In anticipation of an Allied landing, Germany's leadership positioned significant military forces at Pas de Calais. Instead, Allied forces landed farther South at Normandy. Fortitude South proved so successful that those German forces remained at Pas de Calais for almost a week awaiting a landing that never happened.

2.2 Yom Kippur War

In January 1973, Egypt accelerated its preparations for a long-anticipated attack on Israel. Arab leaders at the highest political levels understood that obtaining at least a partial surprise was essential to military success. In order to offset Israel's overwhelming military superiority, Egypt and Syria initiated Operation Badr. The Egyptian leadership devised a sophisticated deception plan that encompassed both political and military elements. Worthy of note, Egypt's subsequent military campaign was in large measure built around the elaborate deception plan. The purpose was to disguise Egypt's intentions by conditioning the Israelis to continuous Arab troop build-ups along the borders of the occupied territories. Forcing the Israelis to operate at a high state of alert with an added element of uncertainty would fatigue Israeli forces.

Further, such operations conducted for long periods of time would place considerable financial burdens on the Israeli economy. Israel could not afford to reassemble its forces every time Egypt and Syria conducted defensive exercises. Perpetual defensive exercises, President Sadat believed, would ultimately condition the Israelis to perceive mass movements as routine, offering Israel a false sense of security.

In support of the deception plan, Egypt built defensive positions along the west bank of the Suez Canal. Egypt's deception, a shrewd combination of political and military maneuvering, had an audience that went far beyond neighboring countries of the Middle East. Arabs wanted other diplomatic powers, including the United States, to believe an attack from Israel was expected by Egypt. Units conducted endless defensive exercises to lull the Israelis into complacency. The Egyptians stepped-up their deception plan and the Israelis watched the monthly movements of men, equipment, and supplies progressively grow to division-size formations. In 1973 alone, some Egyptian reserve units were mobilized and released as many as twenty times. These mobilizations were publicized in Egyptian newspapers. By the end of September 1973, all classes of reservists were activated. Carefully emphasized in a few Egyptian newspapers was the announcement that reserve exercises would end by October 8th. However, unlike previous exercises, civil defense organizations were not activated. In September alone, the Egyptian formations moved up to the canal six times and then withdrew. Egyptian planners were confident that Israel was now interpreting large force movement as routine.

Another facet of the deception plan called for Egypt to depict its military as operationally unready. The Egyptian Navy made arrangements for submarines to receive repairs in Pakistan. Months earlier, Sadat had dismissed thousands of Soviet military advisors who were providing training to the Egyptian forces. The Israeli leadership believed that Egypt could not operate newly acquired weapons without proper training. Further, the Egyptian government made public announcements that its Naval forces had performed poorly during exercises and would need to undergo further training. Consequently, Israeli intelligence estimations were that Egypt could not launch attacks until 1975. The Egyptian leadership shrewdly utilized the media in the days immediately prior to October 7th. For example, an announcement was printed that officers could request to make the Oomrah to Mecca. Also, several Egyptian news sources publicized that two thousand reservists were to be demobilized on October 3rd, just four days before the pending attack. To avoid any tone of imminence, diplomatic elements of the deception plan were carefully orchestrated by President Sadat, himself. In February 1973, Sadat dispatched his national security advisor to numerous foreign capitals including Moscow, Bonn, London, and Washington. He also sent Egypt's foreign minister to New Delhi and Peking to lobby support for Sadat's peace plan. Sadat's bogus pursuit of peace failed but the political impression was that Sadat wanted a peaceful solution to Egypt's conflict with Israel. In the days immediately before the war, continuing diplomatic squabbling between Egypt and Libya was perceived to be business as usual. Also, Egypt continued preparations for a pending visit from Princess Margaret and visits from Romanian dignitaries were conducted as scheduled. On October 5th, several of Sadat's ministers were on diplomatic missions abroad offering no indication of attack. Israel's, as well as the United States', perception was that of Egypt conducting only defensive maneuvers and that Syria was fortifying defenses. The Arab deception plan was so successful, that as late as the morning of October 5, 1973, Israeli intelligence advisors briefed Prime Minister Golda Meir that the risk of an attack was low. On October 6, 1973, Egypt and Syria opened a coordinated surprise attack against Israel.

2.3 Discussion

The deception campaigns of Plan Bodyguard and Operation Badr clearly illustrate many important details involved in a deception campaign. First, the critical activities of a deception campaign can be far removed from the physical battlefield. Both Sadat and Churchill understood that diplomacy, economics, and information are essential tools of deception. Second, these deception campaigns were driven by leadership involvement at the highest levels. In each of the aforementioned case studies, the top leaders from each nation had directly participated in their deception campaigns. Third, in both instances, military operations were tailored around the greater deception campaign plan. Finally, secrecy was paramount for both deception campaigns. The existence of LCS was more guarded than the U.S. project to develop the atomic bomb. In fact, the details of the LCS were not revealed until almost thirty years after WWII. The Egyptian leadership was so successful with their operational security (OPSEC) efforts that an overwhelming percentage of Egyptian and Syrian soldiers did not know of the offensive until hostilities commenced. Israel conducted interrogation of over 8,000 Egyptian and Syrian POWs. Ninety-five percent of the captives learned of the attack only on the first day of the war. Of Egypt's eighteen captured lieutenant colonels and colonels, only four knew on October 4th that war would break out, but these POWs did not know when. One colonel learned the specifics on October 5th. The remaining thirteen high-ranking officers were informed the morning of the operations. During all phases of war, to include peace, deception should be the most secret of secret operations [15]. However, Feer [5] notes that

> The Egyptians did indeed surprise the Israelis, but they were never within a

> mile of defeating the Israelis. Thanks to some tactical innovations of their own and the Israelis mistakes, the Egyptians did give the Israelis a fright and a very bloody nose. More to the point, however, Sadat's success was in realizing that politics is war carried out by other means—having demonstrated his seriousness and a level of competence by his military, he changed the political calculation. The situation was analogous to the political impact versus military impact of the 1968 Tet Offensive.

3. Planning and Execution of Deception

3.1 Background

A network-centric strategic-level deception (NSD) campaign can be described as a coordinated wrapping of many small, elements of misinformation and deceptive actions within a scheme across multiple computer networks. In other words, many deceptive operations constitute a network deception campaign. Network deception can be compared to that of a theatrical production. Fundamental elements of theater include such things as dialogue, characters, scenery, and props [4]. Similarly, a detailed script for Network Deception would include elements of users, computers, intranets, organizations, and most importantly, information. These elements alone have little meaning. However, if combined in a complimentary manner, a coherent storyline can be conveyed.

3.1.1 What is Network-Centric Strategic Level Deception? This paper defines network-centric strategic-level deception as a sequence of computer network activities or actions taken to manipulate adversarial perceptions regarding computing and communication capabilities. NSD may serve multiple purposes. One possible purpose is employing coordinated NSD to compliment the conventional elements of a broad deception. In other words, a network deception campaign may be a component of a more comprehensive and multifaceted strategic campaign that includes complimentary diplomatic, economic, and military elements spanning organizational boundaries (e.g., across military units, government agencies, and even nation-states). The activities associated with this particular type of network deception include masking the extent and disposition of network activities, fabricating mock data networks, and creating the impression of authentic information with associated processes where none will actually occur. A second possible type of network deception, which this paper will not address, is to provide a layer of protection to information within networks. This purpose of this type of network deception activity is to conceal the intent to conceal or shroud the information on a network or perhaps even cloak the true purpose for which that network is used.

Practically all ruses and stratagems of war according to [15] "are variations or developments of a few simple tricks that have been practiced by man since man was hunted by man." Techniques of deception come in many forms to include ruses, decoys, camouflage, and feints. These deception concepts may be employed within communication networks in order to deceive or condition a target's perception about the intent or purpose of communication activities. In this paper we refer to deception concepts that are specific to network operations as deceptors. Specific network activities intended to manipulate adversarial perceptions and influence actions are called deceptors. The term "deceptor" is applicable to deceptive data, network components, or possibly an entire network. Table 1 lists and describes various forms of deceptors.

A communication channel that broadcasts relevant and authentic data can also transmit irrelevant and false data. Network-centric deception supports any operation, which has objectives that are a function of communication networks, both adversarial and friendly. In other words, if an adversary relies on communication networks to obtain, process, and analyze the common operational picture (COP), that COP may be skewed or altered through NSD.

In conventional warfare, successful deception operations evolve in three distinct phases: 1) manipulate beliefs, 2) affect action based on altered perceptions, and 3) exploit and benefit from subsequent actions. NSD has a useful role in this three-phase process. Within the first phase, it can be conducted to either generate or reaffirm an enemy's preexisting bias and beliefs. Affecting an adversary's belief system is a process that may take considerable time. In this paper, altering a target's beliefs and perception is considered a strategic activity. The second phase of the deception process is to precipitate adversarial action. Conducting NSD to facilitate action by an opponent should be executed within specific operations, and thus, contemplated at the operational level of conflict. The third phase of deception in warfare is the exploitation of adversarial action for the purpose of gain. The third phase, exploiting an opponent's action for gain, is conducted at the tactical level. This paper will not address exploitation for gain because this phase is removed from the information domain. However, tactical aspects must be noted when discussing conflict because operational victory is a product of tactical successes.

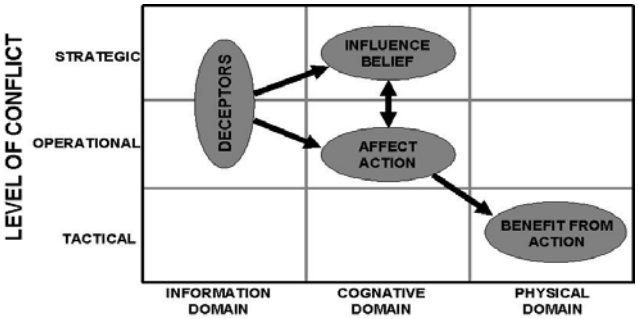

Figure 1. Network Deception and Levels of Conflict

3.1.2 Strategic and Operational-Level Network-Centric Deception. NSD is of value if a country makes use of computing and communication networks to facilitate its long-term military and geo-political goals. In order for a network deception campaign to be developed and initiated, operational if not strategic objectives must exist to provide the context for that deception. Strategically, successful network deception results from an array of deceptors designed to influence adversarial perceptions of friendly capabilities and intentions in such a manner as to support already-established strategic objectives.

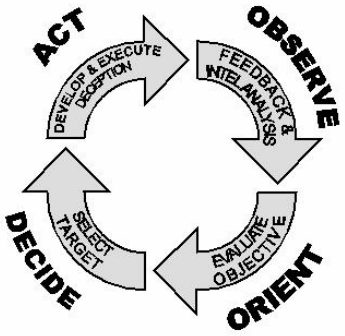

Figure 2. Deception Process and OODA Loop

Historically, attempts at strategic deceptions have relied on circumstances that are difficult if not unlikely to anticipate [13]. In other words, there is a certain amount of luck required for strategic deception to be successfully executed. Operation Mincemeat of World War II, perhaps the most famous deception operation ever mounted in warfare, also documented in the book [11] and movie [14] "The Man that Never Was," highlights the critical role chance plays in strategic deception. Operation Mincemeat involved British intelligence using a human corpse as a means to convince Hitler and his High Command that the objective of a pending Allied invasion of southern Europe was to land in Sardinia. In actuality, the Allies had selected Sicily as the real target. British intelligence went to great efforts to prepare and plant the corpse. "Major Martin" the corpse, was a junior staff officer, supposedly killed in a plane crash on his way to Allied HQ in North Africa. The deception planning was so complete in detail that British intelligence officers created a personality for "Martin," planting on the body letters from a fictional girlfriend, theatre tickets, and even a memo from his bank manager. Also, attached to the corpse were cleverly forged documents designed to convince Germany's military intelligence that plans for an attack on Sicily were decoys from the real target. The corpse of "Martin" was set adrift by a submarine off the Spanish coast. Once Major Martin was set adrift, the British could only hope the body would wash ashore and be recovered by Nazi authorities. Circumstances favored the Allies. Major Martin's body washed up on a Spanish shore and was intercepted by Nazi intelligence services. From a historical perspective, repeated instances of plain luck, necessary for successful strategic deception, are rare. Regardless, this paper will discuss NSD at the strategic as well as operational levels of conflict, with the aim of influencing not only network attacks, but the national and ideological leaders who direct such attacks.

3.2 Requirements for NSD

3.2.1 Central Organization and Control. In order for the storyline of a NSD campaign to unfold in its intended manner, the command of coordination, timing, and tempo must be focused at the strategic level. However, command and control of a deception may shift to the operational level during conflict. A NSD campaign will involve various organizations with multiple systems across numerous networks. If a deceptor is applied at one node of the network, the other deceptors need to be formulated and positioned to make the first deceptor seem plausible. Centralized management is necessary to maintain a plausible degree of continuity and avoid conflicting details within the storyline. Also, centralized management is necessary for the operational security of the entire campaign. In order to maintain the integrity of the network deception campaign, the number of people involved in planning needs be kept to an absolute minimum. Maintaining a balance of effective management and campaign secrecy is best accomplished by centralized organization and control.

3.2.2 Planning, Preparation, and Timing. As in the stage production analogy previously described, in order for the story to unfold in the desired manner, each element of the NSD campaign must be coordinated with the proper timing of signals [7] and tempo of content. All of these elements play to the perceptions of the target or adversarial decision maker. Formulating a deception campaign must begin in the initial planning phase of the core strategy for which the long-term deception campaign is intended to support. Also, the deception must be acutely integrated into core communication network operations. Successful and authentic network activities are creativity, imaginative, unusual, and believed to be impossible by an adversary. However, the storyline that the deception conveys must be sensible and obvious to its intended target. In other words, friendly network

operations to be viewed by the enemy must be plausible and appear authentic. In order to understand what an enemy may or may not consider authentic, the elements of the target's decision and intelligence cycle must be understood. Further, the deception storyline should be doctrinally consistent with known friendly capabilities. Planning and preparation issues to remain cognizant of when planning a network deception campaign include but are not limited to:

- Accessibility of network to the adversary
- Network resources relied upon by the adversary intelligence gathering organizations
- Deceptors needed to provide confirmation to the adversary

Lastly, timing of signals and tempo of content of the deception storyline is critical to a successful campaign. A proper sequencing planted signal with necessary content provides a degree of plausibility to the story being conveyed.

3.2.3 Credibility, Confirmation, and Flexibility. Long-term NSD operations must involve three key aspects: credibility, confirmation, and flexibility. Credibility preys upon the target's belief base. Non-deceptive network activities aside, the NSD must be straightforward, sensible and obvious in order not to be ignored by the adversary. Network deception should be rooted in truth and play on the expectations of the adversary by reinforcing what the enemy already believes. Initial credibility will draw the necessary attention of the adversary. Once indicators are interpreted to be credible, providing confirmation is the next consideration for the deception campaign. Again, this intermediate step of providing confirmation to the adversary will lead to the opponent taking action--the final step in the deception process. Confirmation lends itself to manipulating the target's actions. The third and final step of a deception campaign is to gain advantage from the adversarial actions. Therefore, a deception plan must allow for some degree of freedom with regard to subsequent actions to seize any chance of opportunity.

4. Network-Centric Strategic Deception (NSD) Model

4.1 NSD Management Model

The NSD Management Model described in this chapter is a framework for organizations cooperating to conduct strategic-level deception and exchange information in a manner comparable to a flattened network. In other words, the suggested model provides a process for a labyrinth of public and private organizations to disseminate information in a timely manner, bypassing bureaucratic obstacles and circumventing organizational hindrances. The NSD Management Model shown below encompasses the hierarchy of government organizations to include the National Security Council, the Office of the Secretary of Defense, the Joint Chiefs of Staff, numerous Combat Support Agencies, and elements of the Global Information Infrastructure.

Many of the elements that fall within this hierarchal pyramid have already established formal relationships and doctrine. A new concept introduced by this model is the network deception-planning cell. The deception cell added to the existing bureaucratic structure creates a viable scheme for managing network deception in the highly dynamic environment of the National and Global Information Infrastructures.

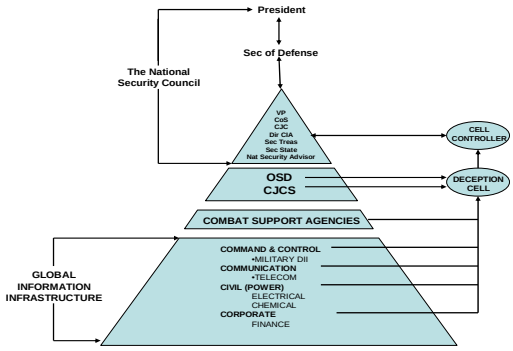

Figure 3. NSD Management Model

4.1.1 National Security Council. The National Security Council (NSC) is a small assembly, chaired by the President, which contemplates national security issues, sets foreign policy, and develops geo-political objectives that support national security. The NSC also serves as the President's primary instrument for coordinating policies among various government agencies. With respect to the NSD management model, the NSC is a critical tool from which the President and the deception coordinator have direct influence to not only military affairs, but more importantly, complimentary diplomatic and economic resources which are necessary to complete the deception picture. Permanent members of the NSC include the following:

- The President
- The Vice President
- Secretary of State
- Secretary of Defense
- Secretary of the Treasury
- Chairman of the Joint Chiefs of Staff
- National Security Advisor
- Director of the Central Intelligence
- Chief of Staff to the President
- Assistant to the President for the Economic Policy

The heads of other executive departments and agencies, as well as other senior officials, attend meetings of the NSC as needed. An important document developed by the NSC is the National Security Strategy (NSS). The NSS is the text that outlines the long-term objectives that best serves the interests of the United States. Once complete, the NSS is then passed to the Joint Chiefs of Staff (JSC). The JCS draws on the NSS as the primary guide to develop the National Military Strategy (NMS).

4.1.2 Joint Chiefs of Staff and Office of the Secretary of Defense. The JCS includes the Chairman, Vice Chairman, Chiefs of the four armed services, and the Joint Chiefs Directorates, J1-J8. These specific directorates are:

- J1: Manpower and Personnel
- J2: Intelligence
- J3: Operations
- J4: Logistics
- J5: Strategic Plans
- J6: C4I
- J7: Operational Planning
- J8: Force Structure

The primary function of the JCS is to develop the NMS as directed by the President and the Secretary of Defense. Developed from the NSS and its objectives, the NMS supports the policies and directives of the NSC from a strategic outlook, which is doctrinally five to seven years. Also involved in the development and execution of the NMS is the Office of the Secretary of Defense (OSD). The OSD is the principle staff element of the Secretary of Defense responsible for policy development, resource and fiscal management, to include program evaluation. Within the proposed NSD management model, the OSD and JCS are critical yet unsuspecting participants oblivious to any deception campaigns. The OSD and JCS directorates are able to arrange and project deception storyline indicators that are associated with the military industrial complex.

4.1.3 Combat Support Agencies. The Combat Support Agencies are agencies that serve the NSD management model in either of two capacities. The first purpose of the CSAs is projecting pieces of specifically tailored information. This information may be in the form of human, signal, technical, or possibly optical intelligence. The second capacity of the CSAs is to provide a means of feedback for a deception operation. Again, this feedback may be in the form of human, signal, technical, and optical intelligence.

a) Defense Intelligence Agency

The DIA is a major producer of foreign military intelligence. The DIA provides military intelligence to warfighters, defense policy makers, and force planners, in the Department of Defense and the Intelligence Community, in support of U.S. military planning and operations and weapon systems acquisition. Also, the DIA coordinates activities of the defense intelligence community. The DIA is versed in the areas of military history and doctrine, economics, physics, chemistry, world history, political science, bio-sciences, and computer sciences.

b) Defense Information System Agency

The DISA is a combat-support agency responsible for planning, engineering, acquiring, fielding, and supporting the Defense Information System Network that serves the needs of the President, the Secretary of Defense, and the other DoD Components.

c) Defense Logistics Agency

The DLA Director reports to the Under Secretary of Defense for Acquisition, Technology and Logistics through the Deputy Under Secretary of Defense (Logistics and Materiel Readiness). DLA provides worldwide logistics support for the missions of the Military Departments and the Unified Combatant Commands. The DLA also provides logistics support to other DoD Components and certain Federal agencies, foreign governments, international organizations, and others as authorized.

d) National Geospatial-Intelligence Agency

Formed from several different defense and intelligence agencies, the NGA merges imagery, maps, charts, and environmental data into geospatial intelligence. Using the latest technology, the NGA renders imagery and geospatial data into visual representations. This capability aids in multiple applications for homeland defense and national security, serving military, civil, and international needs.

e) National Security Agency

NSA has two primary missions. First, its information assurance mission provides the solutions, products, and services needed to achieve information assurance for information infrastructures critical to national security. Second, the foreign signals intelligence (SIGINT) mission allows for effective organization and control of all the foreign signals collection and processing activities of the United States. NSA is authorized to produce SIGINT in accordance with objectives, requirements, and priorities established by the Director of Central Intelligence with the advice of the National Foreign Intelligence Board.

4.1.4 Global Information Infrastructure. The Global Information Infrastructure (GII) is the transnational communications system that facilitates communication across the entire globe including telecommunications and com-

puter networks. The physical links of the GII are trans-oceanic cables, terrestrial communications systems, and layered satellite constellations. The GII is dynamic and constantly evolving characterized by private and public ownership as well as private and public users.

In contrast, a National Information Infrastructures (NII) is composed of communication networks that fall within the influence and control of a nation state. Multiple NIIs constitute the greater GII. The numerous elements of a nation's communication infrastructure include public, private, and corporate communication networks used to regulate:

- Finance - Banking, payment services, investment institutions, securities and commodities exchanges, transaction networks, and record storage.
- Energy - Power production, distribution, storage, efficient management, and grid status. Worthy of note, the NII is dependent on the national power infrastructure, and likewise, the electrical grid is regulated through the NII.
- Chemical - Production and distribution for transportation and manufacturing needs.
- Transportation - Physical distribution surface shipping, rail systems, and air traffic.
- Government Services - Critical services at all levels of government to include public health, emergency response, social security payments, and record storage.

These various networks within the NII serve completely different purposes but are all dependent on efficient and timely communication.

The Defense Information Infrastructure (DII) is the infrastructure utilized by the military and intelligence organizations of the nation. The United States DII is maintained by DISA. The DII is an information grid of networks, computers, databases, weapon interfaces, and security systems that process and transport the information needed by the DoD. The DII can be divided into three subgroups: Program and Technical Activities, C4I, and DII applications. These elements are becoming increasingly integrated into the NII and GII via commercial services. As networked digital systems become ubiquitous, it is ever more difficult to differentiate between public, private, and military networks. These networks use the same physical infrastructure.

4.2 The Deception Cell

In our model of the command structure, the network deception cell is a select collective of leaders who are tasked with the development, planning, coordination, and execution of network deception campaigns. Numbering less than one dozen permanent members, the deception cell is comprised of leaders of public corporations, private organizations, government agencies, military commands, financial institutions, and academic institutions. These cell members have direct influence over the various elements that comprise the NII, if not the GII. The premise of the deception cell is to flatten or horizontally integrate the large and complex hierarchy of organizations that comprise the NII. The most critical undertakings of a network-deception campaign are the selection of a deception cell leader, the selection of the deception cell members, and the subsequent coordination or organization of these cell members.

4.2.1 Coordinating Officer. The coordinating officer leads the deception cell. Acting as the manager of the deception cell, the coordinating officer supervises the execution of network deception activities by the cell members and their respective establishments. Additionally, the coordinating officer works in conjunction with the Joint Planning Staff and briefs the NSC when required. In working with the JCS, the coordinating officer ensures that cover plans prepared by the JCS and NSC compliment strategic, as well as operational plans and activities. Further, this individual has direct access to all members of the NSC, to include the President of the United States and the Secretary of Defense. When deemed necessary, the coordinating officer may exercise the authority of the President and the Secretary of Defense. This measure is necessary to resolve or subvert bureaucratic conflicts. Also, the coordinating officer is to direct the establishment of working relations with the leadership of public and private organizations that may not be organic to the deception cell. Other details of the coordinating officer's job description include the support of network deception schemes by information leakage and the perpetuation of network propaganda. Also, the coordinating officer will oversee the selection and departure of cell members.

4.2.2 Cell Members. These members, permanent as well as temporary, are drawn from the various sectors that rely on the NII. These sectors include but are not limited to:

- Banking and Finance
- Transportation
- Manufacturing
- Telecommunications
- Government agencies
- Military
- Civil infrastructure
- Academia

This group must be kept small and organized in a manner that facilitates communication and promotes creativity among the members and their respective organizations.

4.2.3 Cell Organization. Equally important is the assembly of the cell members. With respect to time and information, the national and global information infrastructures are dynamic, if not volatile environments. The cell members must be able to organize in a manner that is conducive to creativity, communication, and coordination. However, network-centric deception campaigns hinge on a paradoxical relationship of intelligence sharing and operations security. The organization of the network deception cell must be structured in a manner that considers these three pillars of a successful deception campaign. Intelligence assessments establish a starting point to incorporate strategic-level network deception measures into normal network operations. Efficient communication among cell members is an absolute necessity to maintain proper content and timing among the numerous elements of a strategic deception campaign. The second important consideration when organizing the deception cell is full integration and synchronization into the planning and execution phases of an operation. Synchronization entails obtaining, interpreting, and disseminating intelligence to the planners [6] of the deception and operational campaigns to coordinate deception related activities. The activities between the intelligence organizations and operational planners must be conducted in a complementary and synchronized manner: This is the purpose of the deception cell. Perhaps the most important element of a network deception campaign is that of operational security. Operational security is essential to the successes of the deception as it establishes the base of secrecy necessary for success. Strong operational security, however, not only shrouds the deception operation but also protects the integrity of the true operation.

The structure of the deception cell must be elastic enough to plan and execute deceptions in a volatile environment. The coordination officer must be given the ability to alter the framework in which the members are allowed to interact. There are three possible organizational structures; open forum, compartmental, and hybrid. An open forum has no formal order. Such a structure would facilitate communication and creativity among the cell members. The flexibility of altering campaign plans and an open forum would also advance coordination. However, the premise of an open forum runs counter to operational security. Less favorable to communication and synergy is compartmentalization of the deception cell. The primary advantage of compartmentalization is that such a structure would limit damage in the case that the integrity of the deception cell is compromised. The third possible organization structure is a hybrid of open forum and compartmentalization. This combination could be of any varying degree that is a function of the need for communication among specific members, while maintaining an appropriate level of secrecy about operations.

4.3 Model Validation

Suppose a country X has the ability to detonate a nuclear device at high altitude. Such a nuclear device could produce an electromagnetic pulse (EMP) that would seriously disrupt and degrade the command and control (C2) capabilities of U.S. military forces within distances as great as one thousand miles. Given this threat, the U.S. could initiate a deception campaign intended to convince X, as well as other adversaries, that the United States has successfully developed and tested integrated circuitry technology that demonstrates resistance to EMP pulses with intensity comparable to close proximity nuclear detonations.

In this strategic-level deception campaign, specific networks within the U.S. NII will serve as the primary instrument of deception. The objective of this deception campaign is to deter any future military confrontation with X. The target is the military and civilian leadership of X at the highest levels. The story line is that the United States has developed integrated circuit technology that is completely impervious to high intensity EMP discharges. Further, the U.S. Government has completed extensive field testing and this new circuitry technology allows electrical components such as tactical communication and data equipment to be exposed to an intense EMP such as that of a nuclear blast and remain operational. The primary consequence of this revolutionary technological is that the U.S. military command and control infrastructure is no longer vulnerable to EMP associated with directed energy weapons and high-altitude nuclear detonations.

To the best of our knowledge, this technology may not exist. However, key indicators associated with development, fabrication, and fielding of this EMP-resistant technology could be placed throughout cyberspace. By implementing concepts of NSD on the U.S. NII, an adversary such as X might be shown the way to conclude that EMP/HEMP weapons will not be effective against critical U.S. communications assets. If such a technology was developed, a broad range of organizations to include DoD, academic, financial, government, and commercial corporations would have direct involvement in the development, testing, and subsequent fielding. To convince the military and leadership of X, a comprehensive deception plan would have to be implemented. Coordinating an intricate computer-based deception among academic institutions, research facilities, military commands, government offices, and commercial business would present geographic, technological, and bureaucratic barriers. To provide a plausible story that numerous organizations contributed to the development and production of EMP resistant electrical components, many communication networks will need specific deceptors put in place. In order to convey a convincing

story, these deceptors compliment one another with respect to content and timing.

As suggested by the model, personal relationships existing within the network deception cell would be the most expeditious and secure way to facilitate placement of deceptors within applicable networks. The members of the network deception cell would develop, plan, and initiate the execution of the specific details of the NSD campaign. For example, DoD networks would need to indicate that programs for EMP-resistant circuitry were being sponsored by DoD. These programs would require financial support. Financial transactions would need to be conducted to validate the existence of EMP-resistant product development. Further, if such product development were conducted, universities, national laboratories, and manufactures would produce significant amounts of data concerning product research and development. The cell members, having direct influence over particular military, financial, academic, and commercial communication networks have the task of putting deceptors into operation. The coordinating officer, who has direct oversight over network deception cell activities, would serve as the liaison between network-cell activities and governmental organizations such as the NSC and JCS. The coordinating officer would ensure that the cell's NSD activities remain consistent and in support of national strategic and operational objectives and also compliment deception activities that may involve diplomatic and military efforts.

However, the fact that X has highly sophisticated communications capabilities and systematic intelligence collection is a two-edge sword. One must assume that X does a good job of tracking the state of the art in the development of weapons and countermeasures, making it difficult to maintain such a deception campaign for a long period of time. Second, what if it turns out that it is possible to develop such circuits? Is the campaign worth the risk of encouraging X to succeed, or for X to turn the deception around on the U.S. by hinting that X has been successful at developing the circuits?

4.4 Discussion

The model described in this chapter suggests a general framework for planning and executing network-centric deception actions within complex hierarchies of organizations. This model offers several advantages. First, this framework provides for a small number of key personnel a means for integrating and synchronizing the tangle of public and government organizations that constitute the NII. Without restructuring or augmenting existing government agencies, strategic and operational level network deception can be planned, coordinated, and executed with the involvement of national leadership at the highest levels. Also of importance, this model integrates all elements of statecraft: military force, economics, diplomacy, and information. Horizontal integration is necessary to minimize the broad range of barriers and subsequent friction associated with multi-organizational interaction. These barriers may be technical, monetary, geographic, cultural, lingual, and legal. Legal issues are outside the scope of this paper. For an introduction to legal and societal issues regarding the use of deception, consult [10].

Moreover, the network-centric deception model allows for operational flexibility. The deception cell, members as well as organizational structure, may need to change as strategic and operational circumstances dictate. Flexibility with regard to cell organization becomes more important as a campaign progresses through developmental, planning, and execution phases. Specific details such as interaction and communication among cell members must be left to the discretion of the deception cell. In particular, this model allows the cell leadership to have direct control of cell members, cell structure, campaign scope and direction. Lastly, since this model is centered on a small cadre, there is an inherent element of operational security. To summarize, network-centric strategic-level deception campaign is characterized by organizations targeting other organizations in which timeliness, synchronization, and operational secrecy are necessary.

5. Conclusion

5.1 Summary

Growth in global communications and the subsequent reliance on information technology has created new opportunities for strategic and operational-level deception campaigns. Offered in this paper is the concept of planning and executing strategic-level deceptions among multiple global communication networks. This concept is known as network-centric strategic-level deception (NSD). NSD is a succession of computer network measures conducted to manipulate perceptions held by adversaries in support of complex strategic or operational deception campaigns that incorporate diplomatic, economic, and military elements. Specific network activities intended to manipulate adversarial perceptions and influence actions are called deceptors.

Historical accounts of deception discussed in this paper emphasized four fundamental aspects necessary for a successful deception campaign. First, deception operations cannot be considered a responsibility of the military leadership. Successful strategic-level deception involves economic, diplomatic, and information activities much more so than military actions. Second, deception campaigns require aggressive involvement of a nation's highest leadership. Next, to achieve success, military operations must be planned and executed around information campaigns

to include deception. Fourth, secrecy is the utmost priority in all campaign planning activities. Deception operations as well as other operations depend on maintaining operational security to the highest degree.

NSD serves a process that has three distinct phases. These three phases involve manipulating adversarial perceptions, precipitating action, and eventual exploitation of resultant action. NSD offers a means to manipulate perception and affect action. Also, this NSD process must be centrally organized and completely synchronized with primary operations beginning at the earliest phase. The proposed NSD command structure in this paper is a framework that facilitates a process for public and private organizations to conduct coordinated deceptive network activities in a timely manner, circumventing bureaucratic conflict. The network deception model offered for planning and executing NSD incorporates centralized control, broad integration (of the complex elements of information infrastructures), and operational secrecy.

5.2 Future Work

The concept of network-centric strategic-level deception offers many avenues for research. For example, implementing deception techniques and deceptors specific to communication networks, such as a feint or decoy networks, remains to be explored. The specific attributes of the deceptor concept needs to be further detailed. Another possible area of research is the development of an authoritative structure for coordinating NSD activities among civilian communication networks under the control of public and private organizations. Also, another research area involves extending the NSD model to the participation of allied nations in U.S. led deception campaigns and incorporating methods of influence and network exploitation on the GII not controlled by the United States. The President's Commission on Critical Infrastructure Protection (PCCIP) has established partnerships among public, private, and governmental sectors, such as the Information Sharing and Analysis Centers (ISAC) and Cross-Sector Partnerships (CSPs). Something similar might be done for NSD but it remains to be determined how to create ISAC or CSP-like groups in which secrecy can be maintained. It is necessary to develop further the theory underlying the NSD management model, from the perspective of organizational design. A starting point would be to build on the theories about levels and span of control described in [2]. Lastly, an area of future work is the incorporation NSD into the Department of Defense's vision for a Global Information Grid (GIG). In order to facilitate information superiority worldwide, the GIG concept encompasses communication systems both owned by the U.S. Government and leased from corporate entities. NSD could be used in a complimentary manner with the GIG to provide not only a measure of protection for the GIG but also use the GIG to conduct deception campaigns.

Acknowledgements

We thank Mr. Fred Feer for his comments on an earlier version of this manuscript. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright annotations thereon.

References

[1] Brown, A. C. *Bodyguard of Lies*. New York: Bantam Books, 1976.

[2] Carley, K. M. Computational and mathematical organization theory: Perspective and directions, *Computational and Mathematical Theory* 1,1 (1995), pp. 39-56.

[3] Cockburn, A. and Cockburn, L. *Dangerous Liaison: The Inside Story of the U.S.-Israeli Covert Relationship*. New York: HarperCollins, 1991.

[4] Daniel, D. C. and Herbig, K. L. Propositions on military deception. In Daniel, D. C. and Herbig, K. L., eds., *Strategic Military Deception*. New York: Pergamon Press, 1982, pp. 3-30.

[5] Feer, F. Private communication, Mar. 29, 2005.

[6] Field Manual 90-02: Battlefield Deception, 1998.

[7] Fowler, C. A. and Nesbit, R. F. Tactical deception in air-land warfare, *J. Electronic Defense* 18, 6 (June 1995), pp. 37-44, 76-79.

[8] Hinsley, F. H. *British Intelligence in the Second World War*. Abridged version. New York: Cambridge University Press, 1993.

[9] Joint Publication 3-58, Doctrine for Military Deception. Washington, D.C.: Joint Staff, 31 May 1996.

[10] Michael, J. B. and Wingfield, T. C. Lawful cyber decoy policy. In Gritzalis, D., di Vimercati, S. D. C., Samarati, P., and Katsikas, S., eds. *Security and Privacy in the Age of Uncertainty*. Norwell, Mass.: Kluwer Academic Publishers, 2003, pp. 483-488.

[11] Montagu, E. *The Man Who Never Was*. Philadelphia, Penn: J. B. Lippincott Co., 1954.

[12] Rabinovich, A. *The Yom Kippur War: The Epic Encounter that Transformed the Middle East*. New York: Schocken Books, Inc., 2004.

[13] Sherwin, R. G. The organizational approach to strategic deception: Implications for theory and policy., In Daniel, D. C. and Herbig, K. L., eds., *Strategic Military Deception*. New York: Pergamon Press, 1982, pp. 70-98.

[14] *The Man Who Never Was*. Dir. R. Neame. Perfs. C. Webb, G. Grahame. Twentieth Century Fox Film, 1956.

[15] Whaley, B. *Stratagem, Deception and Surprise in War*. Cambridge, Mass.: M.I.T. Center for Int. Studies, 1969.

Table 1. Deception Techniques and Deceptors

Deception Technique	Battlespace Deception	Deceptor
Camouflage & Concealment	Use of terrain and environment features in an effort to hide, blend, or disguise tactical assets and personnel.	Cloaked information, communication assets, or networks which are undetectable or indistinguishable from adjacent superficial networks.
Demonstrations, Feints, or Diversions	Exhibition of military force intended to delude the enemy to an unfavorable course of action.	A network action intended to distract or draw adversarial attention away from an intended target of information.
Displays, Decoys, or Dummy	Authentic or imitation tactical assets and personnel statically displayed to enemy intelligence sensors.	Fictitious network or sub-components serving as a static front or cover purposely exposed to observation.
Mimic, Simulations, Spoofs	Tactical systems and assets that do not exist are projected onto the battlefield for enemy observation.	A network activity conducted to assume resemblance of a trusted relationship in order to either protect or exploit information, computers, or networks.
Dazzle or Sensor Saturation	Screening activity that causes temporary loss of visual or sensor surveillance degrading enemy targeting ability.	Screening action that disrupts sensor acuity, temporarily degrading an opponent's intelligence collection ability.
Disinformation or Ruses	Tactical action involving fraudulent information or maneuvers intended to deceive adversarial intelligence collection and leadership.	Fraudulent network assets or information purposely exposed to adversarial sensors in order to exploit or gain advantage.
Conditioning	Tactical actions that generate and subsequently exploit a target's preexisting bias, belief, or habit.	Network operations or communication activities intended to establish, reaffirm, and exploit adversarial bias and beliefs.