Spring 2017

Constrained Cognition: Information Management and the Practical Limits of Nuclear Escalation Control

Luke James O'Brien

CONSTRAINED COGNITION: INFORMATION MANAGEMENT AND THE PRACTICAL LIMITS OF NUCLEAR ESCALATION CONTROL

A Master's Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Defense and Strategic Studies

By

Luke J. O'Brien

May 2017

CONSTRAINED COGNITION: INFORMATION MANAGEMENT AND THE PRACTICAL LIMITS OF NUCLEAR ESCALATION CONTROL

Defense and Strategic Studies

Missouri State University, May 2017

Master of Science, Defense and Strategic Studies

Luke J. O'Brien

ABSTRACT

Nuclear escalation control theory rests on the idea that decision makers, in a limited nuclear war scenario, will choose their actions based on a rational assessment of the available information. That information essentially consists of intelligence reports about one's adversary and information reporting the status of one's own forces' ability to execute offensive actions and the damage level of vital national targets. Yet the practical limits of managing the flow and quality of this information, coupled with the fog and friction inherent in human analyses, significantly affect the decision-making process vis-à-vis nuclear escalation. Hence, these limitations cast a pall over any military doctrine that relies heavily on the assumption that nuclear escalation can be controlled with precision. Examining information management during the Cuban Missile Crisis shows the practical limits of managing this information flow, which in turn limits the ability of national leaders to make such decisions properly.

KEYWORDS: nuclear escalation control, limited nuclear war, intelligence analysis, intelligence management, cuban missile crisis.

This abstract is approved as to form and content

_____

John Mark Mattox, Ph.D.
Chair, Advisory Committee
Missouri State University

CONSTRAINED COGNITION: INFORMATION MANAGEMENT AND THE PRACTICAL LIMITS OF NUCLEAR ESCALATION CONTROL

By

Luke J. O'Brien

A Masters Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
For the Degree of Masters of Science, Defense and Strategic Studies

May 2017

Approved:

_____
John Mark Mattox, PhD: Thesis Chair

_____
John Rose, PhD

_____
David Trachtenberg, MS

_____
Julie Masterson, PhD: Dean, Graduate College

ACKNOWLEDGEMENTS

To my wife, Crysti. I love you. Thank you for all your love and encouragement. Without your support, I would never have accomplished this thesis. I look forward to our future adventures, personal, professional, and academic, over the many years ahead.

…oh, and Crysti? Now this is done, that doesn't mean I'm done buying books. I'm totally buying more books. Just figured I'd put that disclaimer in here, for posterities sake.

TABLE OF CONTENTS

1. INTRODUCTION

Ever since the Soviet Union developed its own nuclear weapon and, in doing so, shattered the US nuclear monopoly, nuclear theorists have tried to reconcile existing international relations theory with a world that possesses weapons of unprecedented power. The power of nuclear weapons, in turn, gave rise to the short-lived doctrine of "massive retaliation." This controversial theory, embraced by President Dwight D. Eisenhower, posited that the threat of a devastating nuclear attack could deter any military provocation because the sheer destructive potential of such an attack would give pause to any potential adversary.

Massive retaliation, however, quickly found itself challenged by national security theorists. Senior US Army officials in particular took issue with the idea that strategic nuclear weapons would so threaten the survival of an adversary that it would refrain from offensive actions. Recognizing that there is likely a range of potential conflicts between total nuclear war and peace, thinkers pushed for a new conception of military strategy that relied on numerous options built around so-called “limited war.”[1]

Limited War

The concept of limited war evolved over the course of several decades. As theorists in the 1960s defined it, individual belligerents exchanged nuclear attacks against targets of tactical, operational, and strategic value. These attacks used “strategic or long-range weapons,” in such a way that is “deliberately and voluntarily limited in the total

[1] Taylor, Maxwell D. *The Uncertain Trumpet*. New York: Harper, 1960. p. 27.

amount of damage threatened, planned, and done as well as in the kinds of targets attacked."[2] Such conflicts, in theory, focus on much simpler objectives of much-reduced stakes.

By the conclusion of the Kennedy and Johnson Administrations, exactly how limited those nuclear options proved to be in practice was open to debate. The US military received its policy guidance from the National Strategic Targeting and Attack Policy (NSTAP), which identified three core missions for the US strategic forces in the event of conflict. The first core task was to destroy both the political leadership and the strategic forces located outside of urban areas of both the Soviet Union and China. The second task was to destroy the non-urban conventional military capabilities of the Soviet Union and China. The third and final task was to destroy those strategic capabilities of the Soviet Union and China located within urban areas[3].

These tasks, then, were integrated into the Single Integrated Operations Plan (SIOP) as "five attack options against the Soviet Union and other communist countries" which included some variations of each targeting task, some of which were pre-emptive and some of which were retaliatory[4]. In addition to these five options, US decision makers would be given the ability to exclude, or "withhold" some targets from consideration, including exempting certain major targets (such as national capitals), as well as individual countries (as an example, the United States could exclude

---

[2] Read, Thornton, and Klaus Knorr. *Limited Strategic War*. New York: Published for the Center of International Studies, Princeton University, by Praeger, 1962. p 3.

[3] Kaplan, Fred M. The wizards of Armageddon. Stanford, CA: Stanford University Press, 1991. pp. 267-268

[4] Burr, William. The Nixon Administration, the SIOP, and the Search for Limited Nuclear Options, 1969-1974. November 23, 2005. Accessed April 17, 2017. http://nsarchive.gwu.edu/NSAEBB/NSAEBB173/.

Czechoslovakia)[5]. In doing so, then, decision makers would be granted limited options to engage in nuclear operations at a level below general war. In doing so, the hope was US decision makers would be able to negotiate war termination at a level agreeable to US interests.

At the beginning of the Nixon Administration, however, it was decided that these options were insufficient. Aiming to further develop a "broad range of limited options aimed at terminating war on terms acceptable to the U.S. at the lowest levels of conflict feasible"[6] the new policy sought to "control escalation by setting clear boundaries on the scale of the attack."[7] As Kissinger would observe during the formulation of this strategy, large inflexible options would portend massive destruction, and as such "smaller packages will be used to avoid going to larger ones."[8]

This doctrine, later known as the Schlesinger Doctrine[9], sought to avoid catastrophic damage during a nuclear confrontation by creating smaller and more discrete targeting packages, so that a decision maker could engage some finite targets while avoiding others, in the hope that the adversary would reciprocate. In this regard, then, the emphasis on "limited war" shifted from one of whole-target sets to even smaller options, such as "selected economic and military resources of the enemy critical to post-war

[5] Ibid

[6] US White House. Office of the National Security Advisor. Memorandum for the President "Nuclear Policy." Henry A. Kissinger. January 7, 1974. Office of the President, Washington, D.C.

[7] Ibid.

[8] US National Security Council. "Notes on NSC Meeting 14 February 1969." Washington, D.C.

[9] Garthoff, Raymond L. Detente and confrontation: American-Soviet relations from Nixon to Reagan. Washington, D.C.: Brookings Institution, 1994. p. 466

recovery" or "those enemy military forces which otherwise could exercise internal control over…post-attack recovery."[10]

A good example of how these kinds of options would proceed is Exercise ABLE ARCHER, a notable Cold War exercise that rehearsed such a limited nuclear war in 1983. Exercise planners envisioned that death in the Soviet leadership led to political turmoil within the Soviet Union and the Warsaw Pact. Yugoslavia, during this chaos, turned to the West for financial and military assistance to counteract its stagnating economy. The Soviet Politburo, fearing that Yugoslavia's action might prompt other Warsaw Pact nations to abandon the Soviet Union, launched an invasion of Yugoslavia, hoping to quell dissent as it had in the Hungarian Revolution and Prague Spring.

This invasion, however, mobilized NATO. In response, the Soviet Union then invaded Norway, Finland, and Greece. As NATO attempted to repel these attacks, the bulk of the Soviet Forces in Germany attacked through the Fulda Gap. The fighting went badly for NATO. After several days of battle, which included air strikes and Army Special Forces infiltrations into Crimea, NATO employed a nuclear weapon against a target within the Soviet Union. This employment was intended to signal that the NATO was willing to escalate the conflict to terminate the conflict, hoping that such a signal would persuade the Soviet Union to sue for peace in a manner favorable to NATO. This nuclear weapon, targeted against Kiev, marked the conclusion of the exercise (and presumably, in the minds of the designers, the limited war)[11].

---

10 US Department of Defense. Office of the Secretary of Defense. "Nuclear Weapons Employment Policy." 10 April 1974. Washington, D.C.

11 Houghton, Vince, and Nate Jones. "Able Archer 83: An Interview with Nate Jones · SpyCast." Spycast. November 15, 2016. Accessed November 28, 2016.

Such limited nuclear conflicts, while obviously more ideal than a general nuclear war, are far more subjective and prone to overall misperception. Indeed, as the Cold War continued, there was a recognition that limited war, while better than a general nuclear war, was still not an ideal option. As nuclear theorist Paul Bracken observe in the 1980s:

> Some may not like the theory of limited war, especially in its nuclear variety, and there is no guarantee that the theory actually will work in practice. Nuclear war once begun may escalate to nearly complete levels of national destruction. For this reason, any principles and incentives that indicate a way for a nuclear war to end short of these damage levels can be criticized. But having at least some basis for believing war could end before massive casualties is better than not having any basis for believing this.[12]

Escalation

A necessary part of limited war is the concept of "escalation", or "an increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants…. Escalation can be unilateral, but it is often reciprocal, as each combatant struggles ever harder to achieve victory or avoid defeat."[13] US Air Force styles this doctrine as "escalation dominance," namely "the ability to increase the adversaries' cost of defiance while denying them the opportunity to neutralize those costs (e.g., the threat of a major increase in the tempo of operations against them)."[14] Such an ability

---

https://www.spymuseum.org/multimedia/spycast/episode/able-archer-83-an-interview-with-nate-jones/.

12 Carter, Ashton B., John D. Steinbruner, and Charles A. Zraket. Managing Nuclear Operations. Washington, D.C.: Brookings Institution, 1987. p 199.

13 Morgan, Forrest E. Dangerous Thresholds: Managing Escalation in the 21st Century. Santa Monica, CA: RAND Project Air Force, 2008.

14 US Department of the Air Force. Curtis E. LeMay Center for Doctrine Development. Practical Design: The Coercion Continuum.

requires an understanding of both the "total resolve" and "relative resolve" of the participants of a crisis. A state's *total resolve* consists of three key components:

- Stakes: "Strategic objectives or national interests."
- Credible Capabilities: "The relevant factors of time, space, and forces...that enhance the perception that escalation is possible."
- Risk Tolerance: "Inherent aggressiveness or boldness."

Relative resolve is "how one actor perceives the other actor's resolve relative to its own, and is calculated as the difference between the challenger's resolve and the defender's resolve."[15] However, for a decision maker to assess relative resolve requires an understanding of each participant's total resolve. Without such an understanding, a decision maker may misread the overall situation and select actions that may worsen a crisis.

Such an understanding is often elusive, leading to imperfect decision making. As will be argued hereafter, the Cuban Missile Crisis of October, 1962, provides a useful rubric for understanding the sources of such imperfections.

National Decision-Making

Escalation requires action on the part of a crisis participant. As such, it is helpful to have a methodological framework to understand leadership decision making. Though many models exist, perhaps the most useful for this task is the Observe-Orient-Decide-Act (OODA) Loop.

Fighter pilot and military theorist John Boyd created the OODA Loop, which has given the loop the alternate name of "The Boyd Loop." This concept was fleshed out in *Creation and Destruction*, an unpublished paper, as well as in "Discourses on Winning

15 Ducharme, Douglas R. "Measuring Strategic Deterrence: A Wargaming Approach." Joint Forces Quarterly, July 2016, pp. 40-46.

and Losing," and "Patterns of Conflict," briefings Boyd created and gave to explain the theory to government decision makers. Boyd posits that conflict is a "time-competitive cycle" in which both sides attempt to impose their will on their adversary by responding to their decision making the fastest.[16]

Imagine a boxer during a prize fight. In the "Observe" phase, the fighter is amassing as much information about his adversary as possible as well as about the ring itself. He might observe what direction his opponent is approaching from, if he is favoring one side of his body over the other, where he has his footing, if there is a puddle of water in the middle of the ring, etc.

In the second phase, "Orient," the boxer pairs his observation of his adversary with an understanding of that opponent's background: What is that adversary's fighting style? What kind of advice is his coach likely giving him? Is he prone to rash actions if pressured? Does he favor a particular kind of punch? This phase is the most critical and most difficult of all those in the OODA loop.[17] "Orient" cannot be achieved through simple modeling or organizational changes; it requires an individual decision maker to not only acquire a thorough understanding of the adversary but to reach that understanding at an almost unconscious level. Boyd himself recognized that a potentially vast array of factors must be understood to "actually understand" an opponent, including such concepts as "cultural traditions", "previous experiences", and "genetic heritage". [18]

The third phase is "Decide", namely, to settle upon an action to engage the adversary. Taking the information he has gathered about his opponent and the

16 Lind, William S. Maneuver Warfare Handbook. Boulder, CO: Westview Press, 1985. p. 5.
17 Coram, Robert. Boyd: The Fighter Pilot Who Changed the Art of War. Boston: Little, Brown, 2002. pp. 334-335.
18 Coram, p. 335.

environment from the "Observe" phase, and then pairing that with a holistic understanding of that adversary in the "Decide" phase, the boxer decides what kind of punch to use. Perhaps a right hook would be the best punch to deliver to his opponent because that opponent is favoring one side of his body due to blows sustained earlier in the fight. Or, the boxer might rely on the knowledge that the gym where the opponent trains does a poor job of teaching its boxers on how to defend against such a strike.

The final phase is "Act", is where a decision maker carries out the action decided upon in the previous phase. In the context of the ongoing boxing example, the boxer then delivers a right hook to his adversary. Once complete, the cycle begins again, with the boxer observing how his opponent responded to the strike and planning his next move accordingly. The goal of the OODA loop is to run through this cycle as quickly and efficiently as possible (and, in any case, more efficiently than one's adversary). Doing so allows a decision-maker to better manage the chaos and uncertainty implicit within conflict and cause the adversary's ability to resist to collapse—in effect "out-OODA-ing" the adversary.[19]

Military historians who are critical of Boyd's theory, such as Daniel Bolger, argue that the theory is overly abstract and idealized.[20] Others, like Robert R. Leonard, argue that Boyd's theory is difficult to apply in practice given modern organizational and societal constraints.[21] Despite these critiques, as a framework for understanding human decision making during a conflict, the OODA-Loop should not be summarily dismissed;

19 Polk, Robert B. "A Critique of the Boyd Theory: Is It Applicable to the Army." M.A. thesis, School of Advanced Military Studies, 1999.
20 Daniel P. Bolger, "Maneuver Warfare Reconsidered," in Maneuver Warfare Anthology ed. Richard D. Hooker, Jr. (CA: Presidio Press, 1993), 21-22.
21 Polk, p 36.

for, although properly moving through the Loop in real time might be difficult to train for and accomplish in practice, it can be useful in understanding past decision making or hypothetical decision making in the future.

Information management has a significant role to play within the Boyd Loop, both for the "observe" and "orient" phases. For decision makers to make decisions, they require the information needed to make those decisions accurately. That information must be collected, selected for relevance, properly analyzed, and transmitted to proper decision makers. Yet as military theorists have observed for centuries, this process of information management is not perfect. Information that is incorrect, misunderstood, or simply absent is a constant fixture of warfare. Writing in 1832, in the wake of the Napoleonic Wars, Carl von Clausewitz observed that:

> If we pursue the demands that war makes on those who practice it, we come to the region dominated by the powers of intellect. War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth.[22]

This "fog" is where the "fog of war" concept has its roots. The fog of war posits that "[w]ar is inherently volatile, uncertain, complex and ambiguous."[23] In doing so, it asserts that commanders are not omniscient. As one analyst attempting to capture the essence of the problem remarked:

> "Whether he is a rookie fighter pilot, a silver-haired fleet admiral, or an aging politician, the commander of a military force wants to know more than [he or she]

22 Von Clausewitz, Carl, Michael Howard, and Peter Paret. On war. Norwalk, CT: Easton Press, 1991. p. 101

23 Kiesling, Eugina C. ""On War: Without the Fog"." Military Review, Sept. & Oct. 2001, 85-87.

> usually gets told about the enemy. Commanders in the field, whether of an army or an airplane, generally also want to know more about the environment - weather, for example, or the relevant terrain. Finally, much as it pains a bureaucracy like an armed service to admit it, a commander often lacks the ability to get [his or her] own organization to report adequately about its own status to carry out [his or her] orders. Even in an Army of smokeless powder and ball bearings, the fog and friction of war dominate the battlefield and make the vanquished easy prey for armchair historians[.]"[24]

Human conflict, then, is enshrouded in this fog. From the platoon leader attempting to maneuver his unit onto an objective to the commander of a carrier battle group attempting to maneuver his force into position for a strike, commanders must analyze their situation, make the best decision he or she is able and have that decision carried out despite the gaps in their overall understanding of a situation. Nuclear escalation control is not exempt from this; it too must contend with the fog of war.

At its heart, the fog of war is a problem of information management. As such, we must understand the dynamics of that information management to judge how effectively it can overcome the fog of war. A key aspect of information management is intelligence collection. During escalation management, there are three key intelligence functions. First, decision makers require "intelligence warning," which is the "process of communicating judgments about threats to US security or policy interests to decision-makers."[25] Second, decision makers must have a clear "situational awareness," or the understanding of the enemy situation, consisting both of where an adversary is physical located and of what capabilities the adversary has at its disposal. Decision makers must also have a clear vision of their opponents as human beings as opposed to mere

24 Setear, J. K. Simulating the Fog of War. Santa Monica: Rand Corporation, 1989. p. 1
25 Mary McCarthy, "The National Warning System: Striving for an Elusive Goal," Defense Intelligence Journal 3 (1994).

abstractions and, on that basis, consider what, namely what they might actually intend to do and how they might actually react to any action taken by decision makers.

Yet the fog of war demonstrates that gulf exists between limited war in theory, and limited war in practice. Examining the information management during the Cuban Missile Crisis shows the practical limits of managing this information flow limit the ability of national leaders to make such decisions properly. Using the Cuban Missile Crisis as a vehicle to study the analytic pathologies that can affect information management, it will examine:

- *Collection Failure.* Critical information is missed by the intelligence community. Such oversights can come from the sheer volume of available information, due to a technical fault or oversight, or simply due to deliberate obfuscation by an adversary. It can also result from human errors in operating intelligence collection equipment or from equipment malfunctions, resulting in the presentation of false data for analysts.
- *Analytic Bias.* Information can be misinterpreted, misused, or dismissed due to existing preconceptions on the part of both analysts and decision makers, and overly granular reports given in parallel can often fail to provide decision makers with the proper understanding of the situation that could have been achieved by combining them into a more holistic assessment, resulting in an *analytic failure*.
- *Vulnerabilities to the Command, Control, Communications, Computers and Intelligence (C4I) Infrastructure.* The delicate networks and facilities required for passing information and making assessments for decision makers are finite and vulnerable to destruction; and overreliance upon such systems can, in the case of their major disruption or destruction, render impossible the task of analyzing incoming information, making decisions, and transmitting those decisions to the proper recipients.

The following chapters will address each of these concepts. Chapter 2 will explore collection failure in the context of the Cuban Missile Crisis, determining why information that could have allowed the United States to escalate while the Soviet Union's total resolve was low was not detected. It will examine the challenges facing

analysts and decision makers caused by large information volume, and adversary denial and deception activities, and errors in collection and information management equipment.

Chapter 3 will explore the various analytic biases that compounded the collection failures during the Cuban Missile Crisis and nearly led to fatal misjudgments about Soviet resolve. These analytic failures include poor analytic tradecraft on the part of intelligence analysts as well as bureaucratic interference on the part of intelligence managers and the senior advisors surrounding decision makers.

Chapter 4 will explore how the vulnerable C4I Infrastructure would have made effective decision making during an escalation difficult, due to the destruction of infrastructure critical to that decision making. This vulnerable infrastructure can be broken down into three distinct types: communications infrastructure, analytical infrastructure, and command facilities.

Finally, Chapter 5 will explore how the problems in the previous three chapters not only remain relevant today but have become far worse. Advances in technology, often thought of as the cure-alls to problems within government, are double-edged swords: Just as much as technology relieves problems, it also exacerbates them.

The Cuban Missile Crisis is a frequently used case study, in part because of the wealth of available documents. It is entirely possible that other crisis periods, such as the 1983 Soviet War Scare, may have brought the world closer to war than the Cuban Missile Crisis, and that historians lack access to the same amount of classified materials to confirm this assessment. In any case, the Cuban Missile Crisis offers remarkable insights concerning limited nuclear escalation control that remain applicable today.

2. COLLECTION FAILURE

Because it is typically thought of by many analysts and observers as the key intelligence requirement within escalation control, "warning" consumes much of the intelligence community's time and resources. At a minimum, the ability to detect that an attack is in progress has been a core mission of the nuclear enterprise for almost its entirety of its existence. Warning is the "process of communicating judgments about threats to US security or policy interests to decision-makers."[26] Warning is divided into three distinct types. "Strategic Warning" is looking out to the "distant future" and is primarily used to identify emerging threats to national security. "Operational warning" is more granular and seeks to "identify indicators that an attack is in preparation." Finally, "tactical warning" exists to serve as the "immediate alerting function" that a specific attack is underway.[27]

To better understand the differences in the three kinds of warning, consider the familiar example of the Japanese attack on Pearl Harbor on December 7, 1941. Strategic Warning indicators would have included growing Japanese belligerence and the fact that their reliance on supplies of oil were vulnerable to US embargo. Operational warning indicators would have included the Japanese assembling a carrier task force and submarines and moving them toward Pearl Harbor. Tactical warning would have been the actual sightings of Japanese strike aircraft flying from their aircraft carriers and towards the island.

---

26 McCarthy.

27 Cooper, Jeffrey R. Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis. Washington, DC.: Center for the Study of Intelligence, 2005. p. 16.

During the Cuban Missile Crisis, strategic and operational warning proved elusive for three primary reasons:

1. *Information volume*, namely that the information collected was so voluminous as to overwhelm analysts.
2. Robust Soviet *denial and deception,* or actions by the Soviet Union which served to obscure much of the signs that a significant movement was underway.
3. *Collection errors* resulting from equipment needed for intelligence collection not working as intended, either due to mechanical failure or misuse by its operators.

Information Volume

Cuba had become a rapidly denied environment for intelligence collection, one where the intelligence community had little in the way of taskable assets. Especially after the failed Bay of Pigs in April, 1961, the Central Intelligence Agency rapidly found itself with few agents that could be tasked to find answers to specific intelligence queries from analysts. The CIA maintained two major intelligence networks inside Cuba, known as "AMTORRID" and "COBRA." AMTORRID was located in the Cuba's eastern Oriente Province, while COBRA operated in the western Pinar del Rio Province. These networks were primarily focused on paramilitary operations aimed at sabotage, and though ran several dozen subagents and claimed to have over 2,000 informants[28].

Because of a lack of taskable agents in key positions, the CIA was forced to rely upon debriefing the flood of middle-class refugees fleeing Cuba. By October, 1962, approximately 155,000 Cuban refugees were registered at the Cuban Refugee Center in Miami, Florida[29]. Many of these refugees had no formal military training and did not

28. Dobbs, Michael. One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War. p. 122.
29 Thomas, John F. "Cuban Refugees in the United States." International Migration Review 1, no. 2 (1967): 46. doi:10.2307/3002808.

know what to look for to detect significant military activities. In the month of September, 1962 alone, CIA debriefers interviewed 882 refugees, most arriving on the daily Pan American Airlines flight that flew from Havana to Miami.[30] The sheer volume of individuals to debrief provided analysts a flood of intelligence reporting. This flood of information proved to be a significant resource drain. Before 1962, only four analysts staffed the Miami debriefing station. It was only on 15 March 1962 that an expanded station opened, which would be capable of handling up to 150 interrogations per day. Before this, the lack of debriefers likely resulted in missing vital information relevant to Cuba.

Writing about debriefing procedures in 1963, a CIA analyst observed that even standardized questionnaires did not exist, and consequently interrogators had to spend considerable amounts of time performing multiple rewrites and clarifications, and resolving duplicated data entries before the report could be sent to analysts at CIA headquarters.[31]

Further, another CIA interrogator, also writing in 1963, observed that one of the major limitations of intelligence collection in Cuba was that analysts and interrogators were kept separate. As such, when interrogation reports reached analysts, any follow-on questions would be delayed until the interrogator or case officer working that defector could ask the question. In fact, the first joint debriefings did not take place until spring of

30 Dobbs, p.122.
31 Englejohn, Earl D. "For a Standard Defector Questionnaire." Studies in Intelligence 7, no. Summer (1963): 53-55. Accessed September 29, 2016. https://catalog.archives.gov/id/7283510.

1963, further delaying the proper exploitation of on-the-ground intelligence coming from Cuba.[32]

The interrogation guide issued to assist in interrogations in February, 1962, attests to just how much data individual analysts were attempting to sift through to make sense of events on the ground in Cuba. Comprising over 120 pages of questions, the Army interrogators performing initial refugee screening were required to ask about topics ranging from political developments, economic growth, militia development, infrastructure construction, and security force dispositions. Of all these questions, only two pertained to missile deployments. Worse, those questions were so general that they applied to any missile system, from short-range artillery rockets to surface-to-air missile sites.[33]

The US government also lacked the ability to manage the volume of information that would have come with a US military attack on Cuba or a preemptive Soviet attack on the United States. Once US forces were alerted to take part in a potential attack on Cuba, scores of US units began to flow to assembly areas within Cuba. The overall commander of the new invasion joint task was General Hamilton H. Howze, the commanding officer of the XVIII Airborne Corps. The selection of General Howze came from the pre-existing plan for an invasion of Cuba, OPLAN 316-62, which specified that the commander of the XVIII Airborne Corps was to become the joint task force commander. General Howze, however, had been sent by President Kennedy to command Army and

32 Layton, B.E.. "The Joint Debriefing of a Cuban." Studies in Intelligence 7, no. Summer (1963): 57-61. Accessed September 29, 2016. https://www.cia.gov/library/readingroom/docs/DOC_0000608373.pdf.
33 US Department of the Army. Interrogation Guide for Cuba. Washington, DC: Department of the Army, 1962.

National Guard forces assigned restore order in Mississippi after race riots broke out due to the desegregation of the University of Mississippi.[34]

In order to facilitate the establishment of staffs required to handle the flow of information coming in through military channels while also not tipping off either the press or Soviet intelligence that an operation was underway, it was necessary to relieve General Howze as commander of the XVIII Airborne Corps and place him in command of a new organization. Operations in Mississippi also complicated the Joint Chiefs of Staff's attempt to track the situation. The Joint War Room (JWR) in the Pentagon was in use monitoring the operation in Mississippi; the Joint Chiefs of Staff and their staff officers had to split the facilities and their communication systems, further complicating the flow of information.[35]

As the *ad-hoc* force preparing for operations in Cuba began to assemble, shortages in available staff officers became acute. Officers were borrowed from existing headquarters from across their respective services. These officers had never worked with each other before, and no established procedures existed. Air Force targeting officers, essential for targeting during air operations, were in particularly short supply. These officers worked 15-hour shifts seven days per week.[36]

Such shortages were only made worse by a lack of proper intelligence processing equipment. Photo reconnaissance machinery, in particular, was scarce. Such scarcity

34 Pardoe, Blaine Lee. The Fires of October: The Planned US Invasion of Cuba during the Missile Crisis of 1962. Stroud, England: Fonthill, 2013 p. 115.
35 Pardoe, p. 116.
36 Pardoe, p. 156.

made tracking Soviet movements for targeting purposes difficult and was only made worse by the massive influx of intelligence information arriving on an hourly basis[37].

Given the (fortunate) fact that the contemplated US military operation never took place, it is hard to fully project how effective information flows during the operation would have gone. However, several historical reference points provide useful insights: Since the conclusion of the Second World War, twenty-five percent of all military occupational specialties (MOS) categories within the Army were dedicated to combat troops. The rest of these MOS were dedicated to supporting functions, to include communications, staff work, intelligence, and command and control operations. By 1963, shortly after the Cuban Missile Crisis, this percentage had fallen to 14 percent.[38] This growth in non-combat MOS was to support the increasing automation and complexity required in managing military operations as more advanced systems, particularly communication systems, entered into service. By 1963, the message traffic needed to control US formations was twenty times larger than that of 1945.[39] The growth of communications systems is also reflected in the growth of communication sources during the Vietnam War. At the division level alone, radio communications jumped from eight channels during the Korean War to thirty-two channels in 1963.[40] One-quarter of MOS were dedicated to communications-related functions.[41] At the national level, the amount of information flowing into the intelligence community through technical means was also extensive. The Cunningham Report, a 1966 CIA Inspector General Report,

37 Pardoe, p. 157.
38 Creveld, Martin Van. Command in War. Cambridge, MA: Harvard University Press, 1985. p. 235.
39 Ibid.
40 Creveld, p. 238.
41 Creveld, p. 239.

concluded that the flow of information from collection assets was overwhelming intelligence analysts. "[W]e have come to realize that [analysts] are not the driving force behind the flow of information. Rather, the real push comes from the collectors themselves, particularly the operations of large, indiscriminating technical collection systems."[42] Simply put, both management and analysts were simply unable to keep pace with the rapid influx of information.[43]

Sandwiched between WW II and Vietnam, both of which experienced the formidable collection and data management challenges described above, one finds the Cuban Missile Crisis. The vast amount of reporting continued to challenge CIA analysts after Soviet missile forces were detected in October. A key assignment for intelligence analysts was to determine if nuclear warheads were present in Cuba, and if so, the number and location of those warheads. The main intelligence source for this information was imagery intelligence, both from high-altitude U2 spy-planes as well as low-level RF-8 Crusaders or RF-101 Voodoos.[44]

- Aerial reconnaissance detected the presence of Soviet nuclear warhead transport vans on 23 October. These vans were easily identifiable, both due to the large doors at the rear of the van and the prominent air vents to the cargo compartment's front. Aerial reconnaissance then detected specialized crane vehicles on 25 October at another facility. These cranes are specially designed for safely loading and unloading the hefty nuclear warheads from the transport vehicles. The two together are key for the maintenance and handling of nuclear warheads.[45]
- Additional American surveillance assets determined that the cargo ship Aleksandrovsk, which had arrived in Cuba, had departed the Soviet Union from a nuclear submarine base located in the Kola Peninsula. No civilian

42 US Congress, Select Committee on Governmental Operations, Foreign and Military Intelligence, S. Rept. 94-755, 94th Congress, 2nd Session, 1976, p. 346.
43 Bracken, Paul J. The Command and Control of Nuclear Forces. New Haven: Yale University Press, 1983. p. 32.
44 Pardoe, p. 161.
45 Dobbs, p. 174.

> cargo vessel had been observed visiting this port, and the facility was known as a major nuclear warhead storage depot[46].

These three pieces of intelligence were crucial for determining that nuclear warheads were present in Cuba. Yet CIA analysts did not combine the two photos, as well as the information about the Aleksandrovsk, until January 1963, a full three months after the crisis. Further, analysts only made this discovery because overhead surveillance had detected the warhead vans as Cuban and Soviet stevedores loaded the Aleksandrovsk during the Soviet withdrawal in November 1962[47].

Additionally, the Soviet Union had also moved two tactical nuclear delivery systems into Cuba. The first of these was the Luna, a short-range artillery rocket capable of carrying a 2-kiloton nuclear warhead out to a range of 25 miles[48]. The other was the FKR, an early cruise missile. This system was capable of carrying a 14-kiloton warhead. Soviet forces brought eighty of these warheads to Cuba[49]. These weapons were intended to attack the US facility at Guantanamo Bay, located in eastern Cuba. Yet, despite US intelligence tracking the movement of these weapons, it was not assessed that they would be used in a nuclear role[50]. In fact, US intelligence remained ignorant of the presence of the nuclear warheads for these systems until the 1990s.[51]

Had the Cuban Missile Crisis escalated, American planners would have needed to gauge the effectiveness of their operations against Soviet targets. After all, if the intent of a limited war is to inflict sufficient damage to an enemy, it would be necessary to

46 Dobbs, p. 175.
47 Ibid.
48 Dobbs, p. 158.
49 Dobbs, p. 179.
50 Pardoe, p. 168.
51 Dobbs, p. 179.

identify targets of reasonable value. For example, if a decision maker wished to inflict damage onto industrial targets to compel an adversary to surrender, then it would be necessary to understand which industrial targets were important to that adversary and which industrial targets were comparatively unimportant. A tank factory in Nizhny Tagil is not of the same importance as a shoe factory outside of Omsk.

Such assessments, however, require massive effort. For the NSA and its forerunners, the cornerstone of economic analysis was the traffic that was available to it via civilian radio links. Because it was unencrypted, it was easy to both collect and translate. Analysts then attempted to piece together details about the state of the Soviet economy[52].

> Working from clues as tenuous as a list of Gosbank account numbers that analysts were able to link to Soviet defense industries, [the NSA] issued reports identifying centers of munitions production, assessing the capacity of the Soviet transportation system, estimating the output of vehicle assembly and engine plants, and compiling basic production statistics for steel, chemicals, oil, and electrical power.[53]

But since this radio traffic required the monitoring of all civilian communications within the Soviet Union, the amount of information was voluminous. This analysis was able to exploit approximately only 0.3 percent of all intercepted messages.[54] This statistic demonstrates two things: the sheer volume of information that analysts had to exploit on a daily basis, and how much human effort must be expended to analyze the information needed to identify key trends and locate critical targets.

52 Budiansky, Stephen. Code Warriors: NSA's Codebreakers and the Secret Intelligence War against the Soviet Union. New York: Alfred A. Knopf, 2016. p. 110.
53 Budiansky, p. 114.
54 Budiansky, p. 115.

Information Denial and Deception

The mission of analysts was made additionally difficult due to the elaborate denial and deception measures taken by Soviet planners in preparing for the movement into Cuba.

The operation name selected by the Soviet General Staff, "ANADYR," is indicative of the efforts taken to obscure the nature of the movement should it have been compromised. The Anadyr is a river that empties into the Bering Sea at the extreme east of Russia. The intent behind this was to create the impression that the troops and missiles moving to Cuba, if compromised by an intelligence leak, would appear to be moving to Russia's Pacific Coast. To further the deception, the Soviet General Staff provided the units with snow equipment such as skis, heavy clothing, and sleds. Such clothing was suited to the arctic conditions in the Soviet Union's east.[55]

Loading equipment onto ships for transport to Cuba was also the subject of extensive denial and deception measures. Individuals from the ministry responsible for cargo vessels were not authorized to know what operation was underway. They were neither permitted to know the ships contents nor their destination. To plan the loads for individual ships, an official from the Soviet Merchant Marine only knew the weight and dimensions of each piece of equipment. Upon receiving this information, that official then planned the individual loads.[56]

During equipment loading, the individual troops assigned to a given transport were locked down at the port upon arrival and forbidden from communicating with the

55 Gribkov, A. I., William Y. Smith, and Alfred Friendly. Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis. Chicago: Edition Q, 1994 p.14.
56 Gribkov, p. 24.

outside world. Couriers hand-delivered all orders and ships were loaded only during periods of darkness. Once an individual ship was ready to leave port, its captain was ordered to proceed to a point in the open ocean, at which point he would be allowed to open a set of sealed orders that ordered the ship to Cuba.[57]

Disciplined security efforts continued during the journey. Equipment was stacked on the deck so as to make the ships appear to be carrying agricultural or construction equipment. Larger pieces of equipment were hidden by erecting false superstructures and flooring on the vessel to obscure the cargo. Hidden defensive armaments were installed in such a way as to ensure that they could be used by the ship and its occupants should they come under attack during the journey. Sensitive equipment was placed into lined containers that were resistant to thermal imaging.[58] Soviet soldiers were required to remain below decks during the voyage except at night, and even then, they were only allowed onto the deck for short periods of time. This rule was enforced in spite of the heat and the lack of any climate controls below. To ensure that they were not detected upon arrival and identified as combat troops, soldiers were issued civilian clothing to wear. The intent behind this was to give the soldiers the appearance of being civilian technicians dispatched to help develop Cuba's economy.

Upon arrival in Cuba, the denial and deception campaign continued. The unloading of the cargo vessels took place under tight security. Unloading of the heavy equipment and missiles occurred during periods of darkness to prevent their discovery. Equipment, whenever possible, remained crated. Convoys carrying the cargo also took place during periods of darkness.

57 Gribkov, p. 34.
58 Gribkov, p. 35.

Such denial and deception operations were largely successful. The CIA, reporting on the buildup, assessed on 20 August that while their sources indicated that there was a growing presence of Soviet advisors, "there is no evidence of organized Soviet military units, as such, being included". Though reports coming from Cuba indicated the unloading of sophisticated electronics, the CIA assessed that the cargo was either "increased technical assistance to Cuban industry and agriculture and/or the Cuban Armed Forces" or the "possible establishment of Soviet COMINT-ELINT facilities targeted against Canaveral and other important US installations."[59]

Additional collection sources, such as signals intelligence (SIGINT), were denied not just by the precautions taken by Operation ANADYR, but also by Soviet communications security protocol. From the Second World War to 1948, US signals intelligence had been able to intercept and decrypt large amounts of Soviet government communications traffic due to poor wartime communications measures. On Monday, 1 November 1948, The Soviet Union changed all of its communications security protocols, to include changing codes, encryption devices, and operational procedures. Known as "Black Monday" within the NSA, the net effect of this change was to deprive the US SIGINT enterprise of all SIGINT sources.[60]

The change in communications security across the Soviet Union had significant implications for the US SIGINT enterprise. Without access to these communications, the NSA was forced to rely other sources of SIGINT. The NSA was still able to comb through the Soviet Union's internal civilian radio links, which were not subject to the

59 US Central Intelligence Agency. Director Central Intelligence. Memorandum on Cuba, August 20 1962. By John A. McCone.
60 Budiansky, p. 110.

same security requirements. Though this intelligence offered answers for some intelligence questions (such as the state of the Soviet economy), it was not helpful in building the robust intelligence warning that would have been useful during the Cuban Missile Crisis.[61]

Collection Error

Error too can result in faulty information reaching decision makers. Human actors from intelligence analysts all the way to the national decision makers themselves can mistake mundane information as ominous, or miss ominous information entirely. Technical failures can either produce false indications or cause analysts miss real ones.

During the Cuban Missile Crisis, the sudden arrival of nuclear-capable missiles in Cuba seriously complicated the ability of the intelligence community to provide tactical warning to the President. Previously, the main threat from Soviet Missiles had been an attack that crossed the Arctic Circle, moving down against the United States from the north. With the installation of missile systems inside Cuba, however, the United States found itself with significant gaps in radar coverage. Though radar systems might be able to pick up some indications of a launch, it would be impossible to do so with any accuracy until it was too late.[62]

What radar coverage did exist was itself prone to error. On 27 October, the tracking equipment installed at a radar tracking station in Moorestown, N.J. reported that an inbound ballistic missile from the Gulf of Mexico. The trajectory for that missile

61 Budiansky, p. 113.
62 Soviet Military Buildup in Cuba. October 21, 1962. CIA Report for Heads of State, Washington, D.C.

contact made it appear that its target was US invasion forces staged in Tampa, Florida. After a short amount of time, operators determined that a training program had been inadvertently run, creating the illusion of an incoming attack.[63]

The increasing of alert statuses also has the effect of making false alarms more likely due to the lack of familiarity with systems and rarely rehearsed processes. Compounding this lack of familiarity is the fact many of the service members involved likely had not worked with each other in any enduring capacity at all. At 1:00 a.m. on 26 October, a sentry guarding an air defense command center in Duluth, Minnesota detected what he believed to be an intruder attempting to scale the fence. Believing the facility to be an important-enough target to make an attack by Soviet saboteurs likely, the sentry fired several shots at the figure, and then triggered the bases intruder alarm.[64]

In responding to this alarm, the night staff at the Duluth command center ordered all interceptors under their command to "flush," meaning they would take off from their fields and await further instructions in the ground. One group of these interceptors, which were carrying nuclear-armed air-to-air missiles, was operating out of a temporary base at Volk Field. Due to the *ad hoc* nature of the field, the crews mistook the "flush" alarm for a "scramble" order. Due to the growing amount of ice and snow at Volk Field, the aircrews assumed that the scramble order was genuine, reasoning that they would not be asked to take off under such hazardous conditions for anything other than an imminent attack.[65]

63 Pardoe, p. 173.
64 Dobbs, 133.
65 Dobbs, p. 133.

These fighters were preparing to proceed down the runway before being stopped. The "intruder" in Duluth was later determined to have been most likely a hungry bear scaling the fence to scavenge for food.

Summary

Intelligence collection, like all human endeavors, is not perfect. It must be administered by human, using systems built by humans, and against other humans. As such, these processes are prone to mistakes. Mistakes of those seen in the illustrations above would not suddenly disappear in the case of a conflict perceived to be escalating toward even a limited nuclear dimension. During the Cuban Missile Crisis, information was voluminous. Such volume made missing certain key information possible. Such collection would have only increased should the situation have escalated to the use of either conventional or nuclear weapons.

As in all things surrounding human conflict, one's adversary gets a say in the how the proceedings develop. In the case of the Cuban Missile Crisis, extensive denial and deception techniques were used by the Soviet Union to reduce the amount of time US decision makers would have to react to their actions. Deception operations had long been a fixture in Soviet military operations dating back to the Russian Civil War and was a core part of Soviet operations during the Second World War.

Finally, the equipment used to collect intelligence were not perfect and could experience technical faults. Further, operators could use the equipment improperly. Such occurrences almost gave inaccurate warning that an attack was underway, potentially pressuring President Kennedy into escalating unnecessarily. It is also likely such errors would have persisted during an armed escalation.

It is in this way, then, that the fog of war influenced information management during the Cuban Missile Crisis. Had the crisis escalated to military conflict, President Kennedy would have attempted to use the information being presented to him, processed through his understanding of the situation, to determine which military actions to take to terminate the conflict on terms favorable to the United States and its interests. To achieve optimal results during this process, Kennedy would have required the most accurate information possible. Yet as we can see, the potential for collection failure would have denied much of that necessary information to Kennedy.

Many of these same issues remain today, which will be discussed in Chapter 5.

3. ANALYTIC BIAS

Analytic bias is the result of the information being collected being processed by the intelligence community in such a way as to present a false view of reality for decision makers. This can occur in two key ways:

1. *Barriers to perfect analytic tradecraft*, which results in intelligence information collected being misinterpreted or dismissed outright, most often due to preconceptions on the part of intelligence analysts.
2. *Bureaucratic interference* can influence how intelligence is presented to decision makers. This occurs when individuals within the government misconstrue intelligence analysis or even outright refuse to accept or analysis as it is presented. This can be because they are attempting to achieve a particular political objective or personal information to or out of personal bias. It could also be simply because they incorrectly believe the intelligence to be incorrect.

It is worth noting that while the term bias carries with it certain implications, bias does not by itself imply malign or nefarious intent. As the Aristotle observed, humans are by their very nature political animals. "Nature," he writes, "which makes nothing idly or without purpose, has equipped them with speech, which enables them to communicate moral concepts such as justice which are formative of the household and city-state."[66] As such, even when consciously attempting to strike a neutral position, humans often act with agendas without even consciously realizing it. This bias can simply be a matter of the intelligence community, as an institution, wanting to make their customers happy. Andrew Liepman, the former deputy director of the National Counterterroism Center, put it this way:

66 Aristotle, David Keyt, and Richard Robinson. Politics, books III and IV. Oxford: Clarendon Press, 2004. p. xvii

> In my job, my audience was pretty limited. You could say that I was producing (crafting) products for one guy, which was the President. It's really not as simple as that, we had the Congress and the cabinet, but essentially if we wrote something and the President thought it valuable "we win," and that all of our ratings go through the roof. And yet we had to be really careful. The President is a pretty alluring audience. You can get sucked into that, by the power of the White House, and you have to be really careful. We have a saying, "telling truth to power is our job." You don't want to tell the President what he *wants* to hear, you want to tell him what he *needs* to hear.[67]

The Cuban Missile Crisis shows many of these same dynamics at work. This analytic bias resulted in President Kennedy being presented with inaccurate information both during the lead-up to the Cuban Missile Crisis, as well as throughout that crisis' duration. As we will see, the results of that bias would have had significant impacts on the outcome of any escalation.

Barriers to Perfect Analytic Tradecraft

Even when reports from Cuba began to filter into the intelligence community, the collection and analysis process was compromised by both analytic failures on the part of the CIA as well as the persistent manipulation (and outright rejection) of intelligence by individual decision makers. The massive amount of reporting coming in from refugee sources permitted analysts to "cherry-pick" their data to push "whatever hypothesis was most fashionable at the time."[68] A National Intelligence Estimate, of 19 September 1962 assessed that the "establishment on Cuban soil of Soviet nuclear striking forces which

67 Liepman, Andrew, and Howard Gordon. "How Accurate Is TV's Portrayal of Terrorism?" Rand Corporation (audio blog), May 6, 2016. Accessed April 16, 2017. https://www.rand.org/multimedia/audio/2015/05/06/how-accurate-is-tvs-portrayal-of-terrorism.html.
68 Dobbs, p. 123.

could be used against the US would be incompatible with Soviet policy as we presently estimate it."[69]

CIA analysts made a series of assumptions about Soviet decision making that were unfounded. Those unfounded assumptions then affected the assessments made about Soviet intentions and actions in Cuba. A special national intelligence estimate from 12 September 1962, "The Military Buildup in Cuba," provides an insight into these assumptions. Arguing from the outset that the USSR valued Cuba primarily for its political value, the analysts argue that:

> ...the main purpose of the present military buildup in Cuba is to strengthen the Communist regime there against what the Cubans and the Soviets conceive to be a danger that the US may attempt by one means or another to overthrow it. The Soviets evidently hope to deter any such attempt by enhancing Castro's defensive capabilities and by threatening military retaliation. At the same time, they evidently realize that the deployment of an offensive military base in Cuba might provoke US military intervention and thus defeat their present purpose.[70]

Discussing the ongoing buildup, which by this point had already seen the delivery of ballistic missiles and warheads, CIA analysts mused that the placement of short-range surface-to-surface missiles may occur but was not yet happening. Arguing that there would be a military utility to the deployment of larger systems, the Soviet Union would not do so since "it would indicate a far greater willingness to increase the level of risk in US-Soviet relations than the USSR has displayed thus far".

When reports began to flow in that ballistic missiles were being delivered to Cuba, analysts dismissed the sightings as ordinary surface-to-air missiles. Other

69 US Central Intelligence Agency. Inspector General's Survey of the Cuban Operation and Associated Documents. Washington, DC: Central Intelligence Agency Inspector General, November 1962.
70 US Central Intelligence Agency. The Military Buildup in Cuba. 1962.

observers, to include those from other Western countries such as the United Kingdom, skeptically dismissed reports of missiles, commenting that such reports were "wildly improbable".[71] Further, despite the vast amount of data flowing in, there continued to be certain intelligence gaps created due to a lack of assets on the ground. Such gaps led to analysts having to make intuitive assumptions. In attempting to determine which military facilities were Soviet and which were Cuban, intelligence analysts often used sporting facilities. If a facility contained a baseball pitch, it was assumed to be Cuban, due to the popularity of the sport on the island. If a facility included a soccer pitch, it was believed to be Soviet, since analysts assumed Russians did not play baseball. Additionally, photo analysts attempted to determine what kinds of units were at a given site by staring at the gardens at each garrison, believing that Soviet units would try to recreate their regimental crests using different kinds of flowers.[72] While these assumptions seemed sound, Cubans did in fact play soccer. Additionally, flower arrangements could just as easily be the product of a local gardener's imagination.

As the United States increasingly leaned towards a military attack, analysts attempted to determine if nuclear warheads had arrived in Cuba and if so where those warheads were stored. If a military action were intended to destroy the Soviet military force in Cuba, finding those sites would be essential. This effort, however, was a failure, mainly due to preconceptions about how Soviet nuclear forces stored their nuclear weapons.

As early as 1960, the CIA had observed the construction of two concrete bunkers near the town of Bejucal in western Cuba. The bunkers were constructed to be "blast

71 Dobbs, p. 123.
72 Dobbs, p. 140.

resistant" and were secured by a single chain-link fence. As the crisis continued, U2 overflights of the facility were augmented by low-level flights by Navy reconnaissance aircraft, which served to provide more detailed photos of the complex, none of which showed any significant changes. Another facility, this one located in Managua, was also photographed. This facility too also had a single fence surrounding several bunkers similar to those at Bejucal[73].

CIA analysts, examining the photos, dismissed both these facilities as being possible storage facilities for nuclear warheads: "We were told to look out for multiple security fences, roadblocks, [and] extra layers of protection. We did not observe any of that" one CIA analyst observed later[74]. Instead, the CIA focused on a former sugar port at Punta Gerardo, near Havana. This facility had an all the visible signatures of a nuclear facility, including a large guard force and the highly-visible double-fence arrangements that were standard to Soviet nuclear storage sites inside Russia.

The CIA analysts were wrong. Bejucal and Managua, despite lacking the obvious hallmarks associated with Soviet nuclear warhead storage sites, were actually home to all the nuclear warheads in Cuba. Bejucal stored 36 nuclear warheads for the strategic rocket forces, while Managua stored all the tactical warheads allocated for repelling an American invasion. Punta Gerardo was a temporary storage location for missile fuel that lay in between the loading docks at Mariel and the missile sites at Guanjay[75].

Soviet forces, upon their arrival in Cuba, had struggled to find proper storage facilities for their warheads. Though CIA analysts assumed that the primary consideration

73 Dobbs, p. 174.
74 Dobbs, p. 176.
75 Dobbs, p. 176.

for a warhead storage facility was security, the main Soviet concern in Cuba was meeting the safety requirements for storing warheads and preserving operational secrecy. Colonel Sergei Romanov, principally in charge of the transport and care of all nuclear warheads assigned to the operation, had selected the site for three reasons:

First, the facility had an underground parking area that would allow for the loading and unloading of essential equipment away from the prying eyes of overhead reconnaissance aircraft. Second, the facility best met the physical requirements mandated for the storage of nuclear warheads. Warheads had to be stored in a facility that was at least one-thousand square feet, allowing enough space to store each warhead at least twenty inches away from any other warhead. Third, safety regulations also mandated strict climate conditions for nuclear warheads. The temperature in a storage facility could not exceed 68 degrees Fahrenheit, and the humidity could not exceed 70 percent. The facilities at Bejucal and Managua were small enough to allow Romanov to properly use what few climate control systems he could scavenge from the Cubans to keep the storage site at these conditions.[76]

Bureaucratic Interference

Once indications began to appear that Soviet missile deployments were underway, officials within the Kennedy Administration actively interfered with collection and analysis efforts. The CIA's failed Bay of Pigs invasion had left a poor taste in the mouth of many within the Administration, and that colored their responses to Cuban intelligence. John McCone was selected as CIA Director in 1961, a decision that made

76 Dobbs, p. 172.

more liberal officials within the Kennedy Administration suspicious. McCone was a Republican and had earned a reputation in previous postings as a strident anti-Communist, which many administration officials interpreted as coloring his perceptions.[77]

McCone believed that the installation of surface-to-air missiles within Cuba was a sure sign that ballistic missiles were soon to follow. Why install such advanced air defense systems, he reasoned, unless they had something correspondingly valuable to protect? Yet other analysts within the intelligence community, as well as Kennedy Administration officials, were quick to push back against this assessment. Within the CIA, the Director of the Board of Estimates, Sherman Kent, observed that his "intuitive case" flew in the face of estimates from the US Intelligence Board and the senior "Kremlinologists" who advised the administration.[78]

The Administration itself was equally resistant to McCone's warnings. On 10 September, upon finding out that McCone wanted to increase the number of U2 spy plane overflights, National Security Advisor McGeorge Bundy send a memorandum to the Committee on Overhead Reconnaissance (COMOR). In this memorandum, Bundy demanded to know if "there is anyone involved in the planning of these missions who might want to provoke an incident [with Cuba]". Bundy, who had been criticized for not being more active in opposing the Bay of Pigs Invasion, was seeking to ensure that no such incident would occur again.[79]

77 Barrett, David M., and Max Holland. Blind over Cuba. College Station: Texas A & M University Press, 2012.
78 Barrett, p. 5.
79 Barrett, p. 7.

As intelligence of a Soviet buildup began to mount, this reticence continued to exist among senior decision makers, informing the reception McCone's reports received. Secretary of State Dean Rusk, on 21 August, hosted a meeting that included Secretary of Defense McNamara, McGeorge Bundy, and members of the JCS. During this discussion, McCone began to list off the detected Soviet activities in Cuba. At this point, the CIA still believed that Soviet technicians were installing surface-to-air missile systems and intelligence collection equipment. Further, McCone focused on outlining the economic situation on the island, arguing that the Soviet Union instead sought to grow Cuba's economy in order to serve as a "model for all dissident groups in Latin America."

McCone, during this discussion, listed this information seemingly to galvanize the group into more decisive action. In particular, the reports led to McNamara's advocacy for increased intelligence collection, sabotage efforts, and exile group-led irregular warfare across Cuba to counteract Soviet assistance to the Castro regime, something McCone agreed too, arguing that previous efforts had not been sufficient.

Bundy and Rusk, however, pushed back against McCone's assessment again. According to both Bundy and Rusk, they assessed that there was a "very definite inter-relationship between Cuba and other trouble spots, such as Berlin." Dramatic action, in their mind, would lead to "similar actions by the Soviets with respect to our bases and numerous missile sites, particularly Turkey and southern Italy."[80]

This discussion demonstrates the internal fault lines within the national security leadership of the Kennedy Administration and offers insight into reasons for the reticence to react to the increase in intelligence reporting. Both Rusk and Bundy (claiming to

80 US Central Intelligence Agency. Director Central Intelligence. Discussion in Secretary Rusk's Office at 12 O'Clock, 21 August 1962.

represent the White House's view) were highly concerned that any overt action could trigger another Berlin Crisis. This concern colored their predispositions and offers another reason why intelligence was often not received favorably.

McCone's absence during September 1962 also shows this rivalry. Once McCone was absent, Bundy was able to push for far more limited activities in Cuba, directly undoing McCone's efforts. Having recently remarried in 1962 McCone opted to go on an extended honeymoon with his new wife. Before this, as demonstrated in earlier meetings, McCone was the most forceful advocate for increased intelligence collection in Cuba. In particular, McCone pushed for increased photo reconnaissance over Cuba to monitor the Soviet buildup. Upon leaving, McCone had to rely on Marshall S. Carter, the Deputy Director of Central Intelligence, to represent the CIA and its positions, during meetings with other officials.

McCone, though absent, was in communication with Carter via a series of telegrams. Carter, in these telegrams, details the ongoing Soviet activity and reports the information that he had shared with the rest of the national security principles. Not willing to be rushed, McCone noted that he would "remain [in France] as scheduled" and would return at the time originally planned. During this absence, and despite his desire to increase surveillance, U2 overflights were grounded until further notice, ostensibly to avoid a diplomatic incident.[81]

Upon his return, McCone resumed pushing for increased intelligence collection. Starting 4 October, McCone observed that the government had made no progress in Cuba. McCone "observed a lack of forward motion due principally to 'hesitancy' in

81 "Eyes Only McCone from Carter." Marshall S. Carter to John McCone. September 8, 1962.

government circles to engage in any activities which would involve attribution to the United States." Continuing, McCone argued that "more dynamic action was indicated, [and] that hesitancy about overflights must be reconsidered." After this exchange, the CIA was ordered to draw up plans for new U2 overflights.[82]

Exploring counterfactuals in history is a perilous task. With limited data, it is hard to determine with certainty the genuine viability of alternative courses of action. Hence, it is hard to assess whether U2 overflights would have continued if McCone had opted not to go on his extended honeymoon to France. Further, even if U2 flights had been authorized, it is also not clear if they would have detected missile activity. However, what these documents do is demonstrate just how contentious the decision to suspect U2 overflights proved to be within the CIA.

Particularly telling is the memorandum that details the meeting where McGeorge Bundy questioned if U2 missions were being planned to provoke an incident. A memorandum to McCone written on 1 March 1963, nearly 7 months after the meeting took place, captures this tension. The decision to suspend overflights was significant enough that McCone thought it important to reconstruct the conduct of the meeting from the memories of the participants half a year after the fact[83].

This contentious relationship between the CIA under McCone and other members of the Administration continued as the crisis continued to unfold. On 5 October, McCone met with McGeorge Bundy to discuss the subject of intelligence collection. McCone argued that "restricting U2 overflights had placed the United States Intelligence

82 US Central Intelligence Agency. Director of Central Intelligence. "Memorandum of MONGOOSE Meeting Held on Thursday, October 4, 1962" 1962.
83 US Central Intelligence Agency. Director Central Intelligence. By Lyman B. Kirkpatrick. 1963.

community in a position where it could not report with assurance the development of offensive capabilities in Cuba". After observing this, McCone argued that the Soviet Union would follow its buildup of defensive weapons with the installation of an offensive capability "including MRBMs." Bundy, on the other hand, pushed back against this. Arguing that "the Soviets would not go that far" and that if they did it would not appreciably alter the strategic balance between the United States and the Soviet Union; and that risking a military action over Cuba was "intolerable."[84]

As the Cuban Missile Crisis demonstrates, the challenge of information management during escalation control does not end after collecting the information. The analytic biases of the analysts can severely hinder accurate assessments. Further, the managers and senior officials who receive that information, manage its production, and pass it along to the decision makers, have great power in controlling the conduct of that analysis. Consequently, those decision makers may be forced to judge an adversary incorrectly or select the wrong course of action during escalation.

Summary

Ensuring that there is a flow of timely and accurate information to decision makers is not just a problem of collection. Once the gathered, the information must be analyzed, processed, and passed through a chain of bureaucratic way-stations before it arriving a decision maker for action. In the case of the Cuban Missile Crisis, one can observe those limits bedeviling the process throughout:

84 US Central Intelligence. Director Central Intelligence. Memorandum of Discussion with Mr. McGeorge Bundy, Friday, 5 October 1962, 5:15pm. By John McCone.

Analysts failed to apply proper analytical tradecraft to ensure the assessments they were providing to decision makers was, in fact, accurate. Worse, much of this assessment making was done during periods of relative calm. It is difficult to assess what effect placing analysts under prolonged pressure would have had on the quality of intelligence assessments, but it is hard to see that impact as being a positive one. Further, these assessments were not being made during an escalation. The Cuban Missile Crisis never became conventional military battle, let alone a nuclear one. These analysts would have faced a far more dynamic and uncertain environment once the fog of war descended over events.

Information flow is critical to decision making. Information, as the saying goes, is power. Yet that same power is essential for managers, policy makers, and executives throughout the bureaucracy. By controlling it, those middle managers have a great ability to influence events in a manner favorable for their preferred agendas. The documents from the Crisis and the interviews after make it clear that these people sought to serve their country to their best ability. But they served it with the unique personal and professional perspectives they brought from their place in the decision chain. Even if the agenda was well-intentioned, it was an agenda nonetheless; and during the lead up to the Cuban Missile Crisis, it was that well-intended infighting that allowed the situation to escalate far more extensively than intended.

Had an escalation control scenario taken place, these analytic failures would have provided Kennedy with inaccurate, incomplete, or misleading information, which in turn would have meant he was making decisions with that inaccurate information. As discussed in the previous chapters, the very process of escalation control relies on a

decision maker being able to make the right decision at the right time to achieve conflict termination with the outcome most favorable to his or her national interests. If the information presented to a decision maker is inaccurate, such successful conflict termination becomes far more difficult.

Take the example of a car traveling down the interstate in the right lane. As this car travels, it sees a slow-moving truck ahead, traveling in the same lane. Desiring to maintain his or her current speed, the driver opts to move into the left lane to pass. Not wanting to be cited for traveling in the left lane, that driver aims to change lanes at the last possible moment. To do so, the driver gauges his or her speed to ensure that the car does not ram into the back of the fast-approaching truck. Judging by the cars speed indicated on the odometer, and the assessed range to the truck, the driver judges that he or she needs to change lanes within ten seconds.

But what if the indicated speed in the speedometer is incorrect? What if instead of traveling at 60 miles-per-hour as indicated the car is, in reality, traveling at 80 or 90 miles-per-hour? Despite the driver deciding that, according to the data available to him or her at the time, should allow the car to pass safely, the car would instead ram into the back of the truck.

It is in this way, then, that analytic failures can cause decision makers, who are acting in ways that are seemingly tailor-made to bring about success, can experience substandard outcomes. This is true of statecraft in general and warfare in particular, and nuclear escalation control is not uniquely immune to such challenges. Chapter 5 will examine how these same challenges, which we can see during the Cuban Missile Crisis,

still have relevancy in contemporary information management, and thus contemporary nuclear escalation control.

4. VULNERABILITIES TO THE COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C4I) INFRASTRUCTURE

All the discussions of assessment systems during the Cuban Missile Crisis are built around the structure of an intelligence and communication enterprise that is similar to that which exists in peacetime conditions. Those conditions change dramatically during wartime conditions, when new interagency and military personnel augment existing headquarters and establish new ones. These organizations must learn how to function given these changed conditions. In addition to this, however, battlefield attrition has a dramatic effect on organizational effectiveness.

Three key categories of facilities critical for the intelligence enterprise are vulnerable to enemy attack during escalation control:

1. *Communications infrastructure*—all the facilities needed to transmit the collected information to analysts, and then pass the analysis to decision makers.
2. *Analysis centers*—those facilities needed for intelligence analysts to properly analyze both collected information on enemy forces as well as determine the status of the nation's military and civilian populations.
3. *Command facilities*—the locations essential for national decision makers to receive intelligence assessments, process them, and use that intelligence to determine necessary courses of action.

Communications Infrastructure

By 1962, the US Government had created several hardened command facilities with the intent of providing national leadership the ability to survive a nuclear attack. Leaving aside the survivability of these facilities themselves, without the capacity to receive new information from the outside world, and without a similar ability to transmit both instructions and requests for further information, such survival is essentially

negated. Yet the communications tools needed to maintain this connection were vulnerable to Soviet attack.

In 1962, regular terrestrial phone lines and radio links transmitted critical nuclear command and control information. Most radio transmitters were exposed above ground and were thus vulnerable to the blast, heat, and overpressure of a nuclear blast. Most civilian communications switchboards were also not hardened, and thus were also vulnerable to enemy attack. In short, even if analysis centers and command centers survived a nuclear exchange, there was no guarantee that they would be capable of communicating their findings and follow-on orders[85].

Before 1960, little coordination occurred between each military service to attempt to ensure interoperability between communication systems. Each service procured and deployed its own communications equipment, and in doing so not only created redundant capabilities but also often communicated via media that were totally incompatible with those of other services. It would not be until 12 May 1960 that the Office of the Secretary of Defense (OSD) would attempt to resolve this dysfunction by establishing the both the Defense Communications System (DCS) and the Defense Communications Agency (DCA)[86].

When the first DCA director, Rear Admiral William D. Irvin, began to take charge of the communication system, a massive communications infrastructure had sprung up to support each of the major services. The services owned or leased a combined 3.4 million voice channel-miles and 6.9 million teletype channel-miles. Each

85 Blair, Bruce G. The Logic of Accidental Nuclear War. Washington, D.C.: Brookings Institution, 1993 p. 139.
86 Krugler, David F. This Is Only a Test: How Washington, D.C. Prepared for Nuclear War. New York: Palgrave Macmillan, 2006. p. 9.

of these media passed a massive amount of information, with teletypes alone being responsible for 110 million messages a year[87].

One of the first significant challenges facing DCA would directly impact communications during the Cuban Missile Crisis. Despite the massive amount of traffic traveling across the various services communications networks, the DoD had no manual switching facilities to even begin to interconnect them[88]. By way of metaphor, each services' communications were like a series of train lines: Each of these lines carried trains that had to deliver passengers or cargo to stops that were only serviced by other services transit lines. Lacking manual switching stations meant that there was no way to transfer one of those trains to the other services lines. The first of these facilities became operational in the last month of 1962[89]. As such, the DCA had no way to tie together the disparate communications networks that comprised the DCS. Further, as the name implies, these manual switching stations were not automated; they required human intervention, dramatically delaying data transmission. Starting in 1962, the Army would begin to automate some of the communications lines leased from commercial vendors. However, automation would not truly be integrated into the DCS until 1964[90]. As such, not only were communications networks not properly linked, but each of the networks was run at the speed of human intervention, which would have significantly slowed the flow of the communications traffic essential for escalation control.

A previously classified 1966 study by the US Air Force summarized the vulnerability of this system: Even if the President had successfully evacuated to a

87 Krugler, p.10.
88 Krugler, p. 59.
89 Krugler, p. 59.
90 Krugler, p. 62.

hardened relocation site, "[w]idespread destruction of communications and command posts would have probably have cut these survivors off from contact with the fighting forces. . . and the nation's leaders would not have known the outcome of the battle for hours, perhaps days, after the last bomb had been dropped."[91]

Leaders within the Pentagon, both civilian and military experts understood this vulnerability. In 1960, the Weapons Systems Evaluation Group (WSEG) published a study it had performed on the survivability of the national command and control system. After arguing that "delivery systems and local weapons control capabilities could outlive the national political and military command structure,"[92] the report went on to state the following:

> All primary communication nodes for missile and bomber system control are vulnerable to direct enemy attack on terminal facilities, including wire systems for land-based missile and aircraft, HF systems for airborne aircraft, and VLP systems for POLARIS SSBNs. HF systems are susceptible to nuclear blackout effects. HF and VLF communications to forces deployed outside of CONUS (including SAC aircraft under Positive Control and SSBN's) are vulnerable to enemy jamming and interference of increasing effectiveness as forces are deployed closer to enemy targets[93].

After observing this, WSEG's report went on to point out that a "President could not be confident, based on operation experience of exercises, that the whole system would work perfectly."[94] Indeed, this system vulnerability was seen as completely antithetical to the imperative to maintain absolute control of the US nuclear arsenal. The problem was not just one of the President or another surviving official being able to

91 Krugler, p. 2.
92 Cremans, C. D., J. K. Moriarty, and J. Porturo. The Evolution of US Strategic Command and Control and Warning, 1945-1972. Arlington, Virginia: Institute for Defense Analyses, 1975. p 240.
93 Cremans, p 241. Italics in the original.
94 Creamans, p. 242.

communicate with the US nuclear force. The breakdown of communications also highlights the problem of determining who in the line of succession survived the attack, along with the possibility that a comparatively junior official in the line of succession could end up assuming control of the nuclear force over another senior official because that junior official happened to gain a reliable communications link first. As the report argues, "the possibility exists that the man to wield presidential authority in a dire emergency might in fact be selected by a single field grade military officer" who happens to answer the phone[95]. Such a determination makes no determination of the suitability of that official to take command, nor does it ensure that that official would be sufficiently aware of the situation to control nuclear forces effectively.

The Kennedy Administration recognized these flaws from its outset. Yet, due to the limitations of the appropriations cycle during the 1960s, the first fiscal year the DoD could begin rolling out significant changes was not in time for the Cuban Missile Crisis. As such, during the Cuban Missile Crisis, the communications infrastructure was inefficient, vulnerable, not properly administered; and the personnel running the system would likely have struggled to merely properly maintain situational awareness for whomever in the line of succession survived, let alone provide reliable links for that successor to the military forces.

Analysis Centers

During the Cuban Missile Crisis, many key intelligence facilities were in close proximity to the national capital, including:

95 Creamens, p. 244.

- The Central Intelligence Agency, Langley, Virginia
- The National Security Agency, Fort Meade, Maryland
- The Defense Intelligence Agency, Arlington Hall, Virginia

These three facilities were essential intelligence analysis centers. Despite the threat to Washington, D.C. they all remained within 20 miles of the capital. Such proximity is the result of political factors, both in Congress and within the executive branch, which left the US Government's analytical facilities exposed during the Cuban Missile Crisis. Starting in 1950, the US Government began a program of relocation, intended to move as many as 40,000 essential government agencies away from the District of Columbia and its outskirts to locations 50 miles away from the District. Relocated facilities could not be any closer than 10 miles from the capital[96].

Almost immediately, this process was met with opposition by both members of Congress and federal employees themselves. One US representative proposed protecting 40,000 "government bureaucrats" by simply eliminating 40,000 federal jobs. Another demanded to know how the President could propose to protect 40,000 civilian employees while US service members were fighting in Korea[97].

The government employees selected for relocation also balked. Many of these civil servants resented the idea of moving out from their comfortable lives in the District of Columbia to comparatively rural and less developed suburbs. One government consultant estimated that approximately half of the planned employees slated to move would resign or retire instead. As such, many of the essential government agencies

96 Krugler, p. 50.
97 Krugler, p. 73.

needed for wartime assessments of both domestic damage levels and of foreign intelligence remained in or around the District of Columbia[98].

The CIA was no different. Having operated since its inception out of approximately 40 Second World War-era temporary office buildings, by 1953 CIA Director Allen Dulles was anxious to build a new headquarters facility that could house all of the CIA's employees under one roof. However, Director Dulles also recognized and valued the access to national decision makers afforded by the CIA's centrally-located temporary housing. Consequently, Dulles hedged his bets. The new CIA Headquarters would be in Langley, Virginia, a mere seven miles from the center of the District of Columbia. Dulles chose Langley both because he had enjoyed attending cocktail parties at the estates located in the surrounding area while assigned to the Department of State in the 1920s and because the location afforded him a short commute to the White House. [99]

In his attempt to remain close to the capital, Dulles was successful. But consequently, the Central Intelligence Agency in October 1962 ended up with a facility designed to house nearly 10,000 intelligence analysts and support employees well within the blast radius of any nuclear weapon targeted on Washington, D.C[100].

The CIA was not the only analysis center that remained dangerously close to the capital. The NSA had been previously at Arlington Hall, Virginia, a short distance away from the Pentagon[101]. The NSA, recognizing the risk of nuclear attack, began to look for a location to house its new headquarters that would be safely distant from the capital. NSA officials considered a multitude of potential sites. These included facilities in

98 Krugler, p. 62.
99 Krugler, p. 103.
100 Krugler, p. 103.
101 Budiansky, p. 10.

Colorado, Wyoming, Texas, Alabama, Kentucky, and Ohio. More exotic solutions were also discussed, including a ship that remained on constant patrol out in the Atlantic Ocean[102].

NSA leadership eventually decided to build the new headquarters at Fort Knox, Kentucky. This plan immediately faced opposition for two key reasons. First, like the civilian employees of many other agencies, those working for the NSA opposed any move that would require relocating from the comfortable environs of the District of Columbia. The initial field survey published by the NSA to address some of the concerns NSA employees were already raising stated that "the region is neither a wilderness, nor undesirable...any normal Washingtonian can be as comfortable and happy in this area as any."[103]

Second, the NSA at the time of the move had a sizable African-American workforce, which had worked during World War II in support of Arlington Hall's efforts to break German codes. Initially, they had been brought on board to load tapes into computer terminals and to scan intercept reports for specific words. This nucleus of African American employees would continue to work at the NSA in increasingly high-ranking positions through the 1950s and beyond[104]. However, this minority workforce also helped prevent a move to Fort Knox. Any move to Fort Knox would mean these employees would have to live in Kentucky—at the time a segregated "Jim Crow" state. A survey party attempted to paper over this objection as well, noting that segregation "is accomplished without noticeable friction as an accepted principle of long-established

102 "Finding a Home for the AFSA 1949-1952." Cryptolog, April 1985, 1-2.
103 Budiansky, p. 178.
104 Budansky, p. 118-119.

social order…[segregation] appears to be no problem for either the whites or the [African Americans] native to the area", even if it would require "adjustments" on the part of NSA's minority employees[105].Needless to say, these two factors resulted in extreme discontent on the part of the NSA's employees.

Given that these employees had very rare skills that were difficult to locate, these objections soon resulted in the NSA's being directed to build its new headquarters in Fort Meade, Maryland in February, 1952. The new headquarters would be completed in 1957[106]. Though Fort Meade was still relatively close to Washington, and even closer proximity to Baltimore, security considerations took a back seat to workforce considerations. Thus, the NSA headquarters was actually out of the damage radius of a Soviet warhead, though a follow-on attack or an errant missile could have easily destroyed the above-ground structure.

The DIA, only recently established at the time of the Cuban Missile Crisis, occupied the buildings vacated by the NSA upon its move to Fort Meade[107]. Though small, the DIA would provide vital intelligence during the Cuban Missile Crisis. Arlington Hall sits approximately 2.5 miles away from the Pentagon.

All of the agencies responsible for human intelligence and all source analysis were all located within the likely blast ring of a Soviet nuclear attack. Due to political and workforce considerations, the three key agencies necessary to provide the timely and accurate intelligence required to support escalation control would likely be destroyed early on after during the outbreak of hostilities.

---

105 Budansky, p. 178-179.
106 Budansky, p. 179.
107 "Defense Intelligence Agency." History. Accessed November 16, 2016. http://www.dia.mil/About/History/.

In 1962, however, an even more fundamental problem prevented these intelligence agencies from passing intelligence information to decision makers: In the event of escalation into actual conflict, President Kennedy and other leaders would have most likely moved to hardened command facilities to increase the likelihood that they would survive a Soviet nuclear attack. However, it was not until 16 October 1962 that Secretary of Defense McNamara would direct the military to properly integrate these civilian analysts into communications planning[108], and it would not be until 15 July 1963 that employees from these agencies would become a part of national command posts on a full-time basis[109].

A final challenge that reduced the effectiveness of proper analysis centers was the prearranged procedures between the DoD and these individual intelligence agencies. In the wake of the Cuban Missile Crisis, President Kennedy complained about the watch officers from these organizations who "sit and wait to be told-to be requested to make a recommendation". Intelligence agencies had watch officers providing some information, but they did not readily offer that information to decision makers unless they were directed to provide it[110].

In February 1963, the Anzoategui Affair further highlighted this problem. The MV Anzoategui was a Venezuelan-flagged freighter that was hijacked by Communist revolutionaries in Venezuela and steered toward Cuba[111]. Throughout the event, Kennedy was again frustrated at the lack of forthrightness from his intelligence analysts. Writing Director McCone after the event later that month McNamara indicated that both he and

108 Krugler, p. 18.
109 Krugler, p. 27.
110 Krugler, p. 42-43.
111 "Destroyers Close in on Seized Ship." The Chicago Tribune, February 15, 1963.

McCone had "agreed to have members of [DoDs] staff get together [with CIA's staff] and work out detailed procedures to effect better and closer coordination of emergency actions requiring quick reaction."[112]

In short, during the Cuban Missile Crisis the analytical centers essential to informing President Kennedy should the crisis have escalated into a conventional or nuclear conflict were vulnerable to Soviet nuclear attack. Further, these centers were not properly tied into the national military communications networks and did not have habitual working relationships with the command centers in which the President and his advisors would work.

The DoD also understood this vulnerability at the time of the Cuban Missile Crisis. In reflecting on the vulnerabilities that plagued the US Government as it entered the 1960, the WSEG wrote that "installations, such as damage assessment centers, whose capabilities are needed by command in the period after the initial strikes would be less certain of destruction in the initial attacks if they were not collocated with important primary targets that an enemy must include in his counterforce attacks."[113]

Yet this was not the case. In the event of an escalation control scenario, the analysis centers remained in large and above-ground facilities close to the Soviet Union's most likely target. These centers also lacked properly established and formal working relationships necessary for passing critical information. Finally, analytical centers also lacked physical representation at the (notionally) survivable relocation sites where President Kennedy or his successor would have sheltered during an attack. In short, if

112 "Anzoategui Affair." Robert S. McNamara and Roswell L. Gilpatric to Director John McCone. February 27, 1963. Office of the Secretary of Defense, Washington, DC.
113 Cremans, p. 240.

escalation control requires the flow of timely and accurate information to decision makers, the US intelligence community was not postured to do so in 1962.

Command Facilities

Broadly speaking, command facilities have the following key tasks, which take place both in peacetime and in crisis:

- Situation Monitoring. Command centers, as a matter of course, "must monitor strategic intelligence, both from classified means and from open sources, for indicators"[114] that an attack or strategically significant event is underway. Though the actual analysis and production portion for this intelligence support occur at analysis centers, command centers are a major consumer of those reports. Further, as a conflict escalates, the personnel assigned to a command center may have to begin performing their own analyses as individual analysis centers are forced offline due to enemy action or other post-attack disruptions.
- Tactical Warning and Attack Assessment (TW/AA). Closely linked but distinct from situation monitoring, command centers must verify if an attack is underway. If an attack were determined to be in progress, command centers must also determine its strength, composition, and probable targets. While analytical centers, at least at the outset, perform strategic and operational warning, it is the command centers that are responsible for generating tactical warning.[115]
- Decision Making. Command facilities must provide decision makers—in this case President Kennedy—with the ability to receive input from analysis centers, digest that analysis, and confer with the key advisers such as the JCS and other cabinet-level officials.
- Force Management. Facilitating situation awareness is an essential function of command nodes. This awareness must be not just of the enemy situation but also of the disposition of friendly forces. Such knowledge creates a "common operating picture" (COP) that decision makers and military commanders can use to determine what military assets (bombers, ICBMs, missile submarines, etc.) are available during escalation. If that escalation takes place post-attack, command centers determine which forces survived the attack and what capabilities they still possess. For example, an ICBM site might survive an

114 US Library of Congress. Congressional Research Service. Nuclear Command and Control: Current Programs and Issues. By Robert D. Critchlow. 5-6.
115 Critchlow, pp. 5-6.

initial attack during escalation but remain unavailable to attack targets until repaired.[116]

- Force Direction. Escalation control requires the measured employment of forces, both conventional and nuclear, against an adversary. Within a nuclear context, it is essential to such measured employment to use "positive control" and "negative control." Positive control "describes those elements that assure instructions to launch nuclear weapons reach the forces and will be carried out." Negative control, in contrast, consists of "controls designed to prevent the unauthorized use of nuclear weapons." Command facilities, then, facilitate escalation control by ensuring unity of command.

In 1962, the US government maintained the following major command centers:

- White House Situation Room - White House, Washington, D.C.
- Joint War Room - Pentagon, Washington, D.C.[117]
- Mount Weather - Blue Ridge Mountains, Virginia[118]
- Strategic Air Command - Offutt Air Force Base (AFB), Omaha, Nebraska[119]
- Raven Rock Mountain Complex - Blue Ridge Summit, Pennsylvania[120]
- North American Air Defense Command (NORAD) - Cheyenne Mountain, Colorado Springs, Colorado[121]
- National Emergency Airborne Command Post (NEACP)- headquartered at Andrews Air Force Base, Maryland[122]

In addition to these facilities, there were several alternate facilities, located at Barksdale AFB, Louisiana; Bunker Hill AFB, Indiana (later named Grissom Air Force Base): Westover AFB. Massachusetts, and March AFB, California[123]. These facilities

116 Carter, p. 138.
117 Sturm, Thomas A. The Air Force and The Worldwide Military Command and Control System. Washington, DC: USAF Historical Division Liaison Office, 1966. p.4.
118 Sturm, p. 5.
119 Sturm, p. 8.
120 Sturm, p. 5.
121 George, Alice L. Awaiting Armageddon: How Americans Faced the Cuban Missile Crisis. Chapel Hill: University of North Carolina Press, 2003. p. 70.
122 Sturm, p. 9.
123 Hopkins, J. C., and Sheldon A. Goldberg. The Development of Strategic Air Command, 1946-1986 (the Fortieth Anniversary History). Offutt Air Force Base, Neb.: Office of the Historian, Headquarters Strategic Air Command, 1986, p 115.

could replicate some of the facilities that existed at Offutt AFB in the event that enemy attack neutralized or destroyed Offutt AFB.

Additional support squadrons were located at four additional sites:

- Mountain Home AFB, Idaho
- Lincoln AFB, Nebraska
- Lockbourne AFB, Ohio (now Rickenbacker Air National Guard Base)
- Plattsburgh AFB, New York.

These four squadrons could operate smaller airborne command posts flying in EB-47L aircraft. Such aircraft had extremely limited capabilities but served as a further command-and-control backup. For the purposes of the questions at hand related to the Cuban Missile Crisis, we will examine three of the most likely facilities where decision-makers would have taken shelter: The White House Situation Room, Mount Weather, the Joint War Room, and Raven Rock Mountain Complex.

As part of the government's relocation plans, provisions were made to move President Kennedy and his cabinet to a secure location in the event of an attack. The first location, mostly intended to provide some protection in the case of a surprise attack before an increase of alert status, was the White House Situation Room, located in a bunker directly underneath the West Wing[124]. In the event of a Soviet attack that occurred before the decision to disperse the government, President Kennedy and approximately 50 other officials were to shelter in this facility, sealed behind 13 separate blast doors[125].

124 George, p. 70.
125 Krugler, p. 72.

However, it was highly unlikely President Kennedy would have survived an attack if he was sheltering in the White House's bunker. Still, the DoD created a contingency plan to recover him post-attack. The plan assumed that a combination of the White House's design and the likely location of a nuclear attack made evacuating this bunker in a post-attack environment challenging since rubble and debris would obstruct the shelter's egress routes. As such, a specialty rescue team, OUTPOST MISSION, was assembled at Olmstead Air Force Base in Pennsylvania and was comprised of both helicopter pilots and rescue crews. This team would fly to the White House, remove rubble and cut through damaged blast doors using acetylene torches, and evacuate the survivors to a more secure relocation facility buried deeper into the earth[126].

This bunker was located at Mount Weather, Virginia, referred to at the time as HIGHPOINT. It was capable of sheltering 200 personnel from the White House and elsewhere to continue to both lead the country and command and control the military during a nuclear crisis. The facility was self-sufficient, maintaining its own power and water generation, and had a variety of communication systems to connect the President to the outside world. That same communications infrastructure was designed to tie President Kennedy into the major broadcast networks should he want to address the nation[127].

Another command post, this one intended to support the Secretary of Defense and the Joint Chiefs of Staff, was the National Military Command Center (NMCC) was the primary day-to-day location for military command and control. The NMCC that was operating during the Cuban Missile Crisis was a product of the decisions made during the changing strategic landscape of the 1950s. Initially, the Pentagon had no central

126 Dobbs, p. 105.
127 George, p. 71.

command and control facility. The JCS had identified the need for a central command post as early as May 1948, but planning moved slowly. The study recommended the establishment of more hardened facilities, but construction moved slowly.[128]

The outbreak of the Korean War in 25 June 1950, however, accelerated the process. In an attempt to keep track of all messages flowing in from Korea and Japan, JCS officials converted an Air Force briefing room into an emergency command center.[129] This emergency facility would soon become the Air Force Command Post (AFCP), capable of communicating with Air Force units across the globe. In July 1955, the AFCP was designated as also serving as the national command post. Construction of the underground Raven Rock Military Complex as an alternate location had begun in 1951. However, it was assumed any attack on the Pentagon or Washington would come from Soviet bombers flying over the North Pole; thus, it was assumed that their slow flight time would give personnel at the AFCP time to evacuate to Raven Rock by ground or air[130]. By August 1959, the JCS had finally established the Joint War Room (JWC) also within the Pentagon, with plans to facilitate evacuation to Raven Rock during crisis.[131]

This development process, however, underscores the slowness with which the JCS responded to the challenge of Soviet nuclear attack. The JCS established their first command facility in haste at the outbreak of the Korean War. As time went on and the Pentagon became vulnerable, the JCS struggled even to establish their command facility. Even once established, it took even further time to recognize that such a vulnerable

128 Cremans, p. 116.
129 Creamans, p.118.
130 Sturm, p. 4.
131 Sturm, p 5.

facility would not have sufficient time to evacuate. Thus, there is every indication that the JWR could very well have been destroyed in an escalation-related attack during the Cuban Missile Crisis before relocating its staff to Raven Rock. Accordingly, the JWR was expanded in capability and renamed as the NMCC on 1 October 1962[132].Raven Rock Mountain Complex, or Site R, was designated as the "Alternate Joint Command Center" (AJCC), intended to serve as a backup facility for the Pentagon's NMCC. By the time of the Cuban Missile Crisis, Site R was not in full-time operation. A small cadre of personnel assigned to the facility on temporary duty would maintain the AJCC and keep the site in a "warm standby". In the event of a crisis that appeared severe enough to threaten the destruction of the NMCC, personnel would be flown to the AJCC from the NMCC at the Pentagon via helicopter, an approximately 30-minute-long flight. They could also travel to the AJCC by ground, an almost 50-mile drive.[133]

Each of these facilities, however, were vulnerable to a nuclear attack by the Soviet Union. "Should even a few weapons all on the central high command, the results to our retaliatory capabilities could be catastrophic" since "no other target system can offer equal potential returns from so few weapons."[134] An analysis within the WSEG report detailed that a Soviet strike would only require 6-10 warheads to effectively target and destroy the White House, the JWG, Raven Rock, and Mount Weather. The variance in the numbers was purely a function of weapon accuracy: the more accurate the Soviet missile system was, the fewer the number of warheads needed to destroy a target successfully. "Both the President and the [Secretary of Defense] and [Joint Chiefs of

132 Sturm, p. 18.
133 Sturm, p. 6.
134 Cremans, p. 296.

Staff] levels of command are presently subject to operational incapacitation by the same events", the report concluded[135].

Continuity of Government

A further limiting factor affected the utility of each of these three critical site categories. The staffing of personnel at these facilities was not guaranteed, further reducing the potential utility of these facilities due to staff shortages. Confusion and transportation difficulties could have prevented even the small number of personnel at these relocation sites from arriving. Other personnel may simply have abandoned their post. The Supreme Court offers a clear example of what could have happened. Plans for the evacuation of Washington D.C. directed that the Supreme Court would shelter with President Kennedy at Mount Weather. As the Cuban Missile Crisis unfolded, Chief Justice Earl Warren was approached by Federal emergency planners and asked which Supreme Court employees should be provided with evacuation passes. These employees would be evacuated to relocation facilities. Chief Justice Warren declared that every employee down to the elevator operators was "essential". Upon discovering that no provisions existed to evacuate his spouse, Chief Justice Warren declared that he would not evacuate to Mount Weather as planned[136]. Not only is the available space for relocation limited, but the people required to man those spaces may not report when ordered. This concern for loved ones does not merely affect those who refuse evacuation. Provisions existed within Mount Weather to forcibly prevent occupants from leaving in

135 Cremans, p. 243.
136 Krugler, p. 178.

an attempt to determine if their loved ones in the District of Columbia survived the attack[137].

Summary

President Kennedy, or any of his successors, would have faced dramatic practical limits on the ability to direct the affairs of government throughout the Cuban Missile Crisis. Those practical limits would have likely only gotten worse if the most likely target inside the Continental United States—specifically the Washington, D.C. area—had been struck with nuclear weapons.

The doctrine of "Flexible Response" was in its infancy, and the tools required to manage it had not evolved. But even in 1962, the proliferation of nuclear delivery systems by the Soviet Union demonstrated that those same problems that plagued the Cuban Missile Crisis were likely to continue. The ability to strike targets within the United States made previously invulnerable analytical infrastructure, communications systems, and command and control sites highly vulnerable. Though over the intervening decades the United States would seek to construct many more of these sites, this infrastructure would remain inherently vulnerable.

The intelligence analysis infrastructure was especially vulnerable. Given the requirement to maintain large workforces, the impracticality of hardening their facilities to withstand nuclear attack, and the limited space in already costly relocation sites, these capabilities would have likely found themselves knocked out early during any nuclear attack in, or even around, the National Capitol Region.

137 Ibid., p. 180.

In Chapter 5, the modern day vulnerability of this same analytic infrastructure will be examined to determine if the same challenges remain in a contemporary setting.

5. CONTEMPORARY APPLICATIONS

The Cuban Missile Crisis provides a wealth of examples of some of the practical hurdles that escalation control could likely face in an escalating conflict involving the employment or potential employment of nuclear weapons. Though the United States and the Soviet Union avoided entering into a nuclear conflict, the Cold War experience still highlights practical problems, which could severely complicate the theoretical constructs that underpin escalation control. These practical problems fall into three broad categories, which mirror the categories already examined in the case of the Cuban Missile Crisis.

Because half a century of history has elapsed since the 1962 Cuban Missile Crisis and the intelligence community, military, and other relevant sectors of the United States Government have had five decades in which to internalize the lessons of that crisis, it may be easy to dismiss a study of escalation control in the Cuban Missile Crisis as overly idiosyncratic. Such a dismissal, however, would be incorrect. Though much has changed, fundamental problems still stand to complicate the neat theory that underpins escalation control. By examining more recent history, one can see these same categories of problems that existed in 1962 continue to exist today. Worse, many of these problems are more pronounced today than they were in 1962.

The information management that decision makers require for is both fragile and vulnerable to disruption. Information can be missed, manipulated, or misinterpreted. The infrastructure needed to process that information is also finite and highly sensitive to battle damage, the flaws that can corrupt the flow of the information required for effective decision making can be divided into three broad areas:

1. Intelligence collected and forwarded to a decision maker can miss important developments, either due to gaps in intelligence collection or due to an unmanageably large amount of available information. This can be called c*ollection failure*.
2. Information can be misinterpreted, either to inadvertent analytical errors, technical failure, or deliberate manipulation in the service of internal agendas. These three causes are collectively referred to as *analytic bias.*
3. The physical infrastructure required for information collection is sensitive to battle damage. This sensitivity is referred to as the *vulnerability of C4I infrastructure.* This section will examine each of these three limitations and how each of these still exists in a modern context.

Collection Failure

As was discussed in an earlier chapter, there are three key sources of collection failure. First, is *information volume*, namely that the information collected was so voluminous as to overwhelm analysts. Second, is *denial and deception,* or actions by an adversary to obscure much of the signs that a significant movement was underway. Third is, *collection error*, which can result from the equipment needed for intelligence collection malfunctioning, due to either mechanical failure or misuse by its operators.

Information volume. As stated in the Cunningham Report, the "[information] push comes from the collectors themselves, particularly the operations of large, indiscriminating technical collection systems."[138] Since the Cuban Missile Crisis, the ability for the intelligence community to collect information has grown dramatically. This growth in available information has kept pace with similar data growth in the private sector. Writing on the subject of data collection in 2008 the Defense Science Board, the Department of Defense's science and technology advisory body observed: "the number of images and signal intercepts are well beyond the capacity of the existing analyst

138 US Congress, Select Committee on Governmental Operations, Foreign and Military Intelligence, S. Rept. 94-755, 94th Congress, 2nd Session, 1976, p. 346.

community, so there are huge backlogs for translators and image interpreters, and much of the collected data are never reviewed….decision makers and intelligence analysts [also] have difficulty knowing what information is available."[139] Further, it found that "too often sensor integration occurs only when multiple sensors have coincidentally (accidentally) collected complementary data, and the results of that collection were serendipitously discovered to provide a benefit.[140]

The amount of data coming into the US intelligence community is enormous and continues to grow. The Rand Corporation, tasked to study the problem of data growth in the Navy's intelligence collection apparatus, found that:

> To understand how big "big data" is, think about the volume of information contained in the Library of Congress, one of the world's largest libraries in terms of shelf space and number of books. All of the information in the Library of Congress could be digitized into 200 terabytes, or 200 trillion bytes. Then consider the fact that the Navy currently collects the equivalent of a Library of Congress' worth of data almost every other day.[141]

Such information volume has already resulted in the intelligence community failing to provide timely warning to US decision makers. In 2008, the Pakistan-based terrorist group Lashkar-e-Taiba was planning a major, spectacular attack in Mumbai—India's most populous city. The attack involved nine gunmen attacking six crowded and prominent targets throughout the city with small arms and explosive devices[142]. Such a

139 Intelligence Science Board, Integrating Sensor-Collected Intelligence, Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, November 2008 p. 3.
140 Defense Science Board, p. 41.
141 Porche, Issac R., III, Bradley Wilson, Eric-Elizabeth Johnson, Shane Tierney, and Evan Saltzman. Data Flood: Helping the Navy Address the Rising Tide of Sensor. Santa Monica: Rand Corporation, 2014.
142 Mumbai Massacre. PBS Secrets. November 25, 2009. Accessed November 16, 2016. http://www.pbs.org/wnet/secrets/mumbai-massacre-watch-the-full-episode/536/.

terrorist attack is of significant interest to US officials. Pakistan and India are both nuclear powers who have fought multiple wars since the partition of India in 1947. According to reporting in the New York Times, the US intelligence community had collected large amounts of data, including communications between the attack planners, their preparation activities, and even much of their schedule. And while some information was identified, exploited, and shared, much more was missed in the sea of available data. The result was that the attack was able to take place without the US intelligence community being able to provide proper warning.[143]

The resulting fallout surrounding the attack resulted in Indian troops moving to the border with Pakistan to force Pakistan to provide more assistance in curtailing cross-border terrorism[144]. Such a movement could have potentially caused an escalation between two nuclear powers, a crisis which would have directly involved the US Government.

The rise of smartphones and social media accounts has also created new opportunities for intelligence collection. Open source researchers have used social media postings to track military deployments, even clandestine ones, with increasing success. Two excellent case studies exist, both involving the tracking of Russian forces. The first involves the undeclared involvement of regular Russian troops in eastern Ukraine. The

143 Glanz, James, Sebastian Rotella, and David Sanger. "In 2008 Mumbai Attacks, Piles of Spy Data, but an Uncompleted Puzzle." The New York Times, December 21, 2014. Accessed November 16, 2016. http://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html?_r=0.

144 "Pak Might Soon Move Troops from Border with India - Times of India." The Times of India. Accessed November 17, 2016. http://timesofindia.indiatimes.com/india/Pak-might-soon-move-troops-from-border-with-India/articleshow/4660681.cms.

second involves tracking the deployment of nuclear-capable short-range ballistic missiles being deployed to the Russian exclave of Kaliningrad, located on the Baltic Coast.

I. On 11 March 2015, researchers working for the website Bellingcat, which describes itself as "by and for citizen journalists," published a study that demonstrated conclusive evidence that Russian Ground Forces units had traveled into eastern Ukraine, undeclared, and participated in combat operations during the Battle of Debaltseve on 19 February 2015. Cued onto their possible participation by limited reports coming from Moscow purporting to be from a wounded Russian soldier, Bellingcat researchers scanned VK, a Russian social media service, for photos that would prove that his unit (the 5th Tank Brigade), was in Ukraine. Despite removing the unit identification markings from their tanks and fighting vehicles, Bellingcat researchers could use distinctive landmarks (such a train station platforms, mountains, and other unique architecture) to track the unit's movement. As such, Bellingcat could follow the group from its home station in Buryatia, Siberian District to training facilities further west, and eventually into Ukraine. The photos then confirmed that the 5th Tank Brigade was fighting around Debaltseve. One set of information demonstrated the value of intelligence gained from social media. Soldiers in the 5th Tank Brigade kept two Siberian Husky puppies as mascots. Using the photos, the journalists could track these dogs and their distinctive fur patterns, then geolocate where the photo was taken based on surrounding geographic landmarks[145]. These photos were freely available to any analyst with a laptop and an internet connection.

145 Toler, Aric. "How These Adorable Puppies Exposed Russian Involvement in Ukraine - Bellingcat." Bellingcat. March 13, 2015. Accessed November 27, 2016. https://www.bellingcat.com/news/uk-and-europe/2015/03/11/vreditel-sobaka/.

II. In this case study, researchers employed at the Middlebury Institute for International Studies at Monterey, California, also used social media. Also, making use of VK, these researchers used photos taken of conscripts assigned to a unit equipped with 9K720 "Iskander" SRBMs (NATO designation SS-26 STONE). Wanting to verify their movements to and from Kaliningrad, these researchers began to track the photos that a conscript assigned to the unit uploaded onto his VK profile. Of value was a unique item that the unit carried while on maneuvers and one that appeared in many of the photos. Like many conscript militaries, the Russian army has a tradition of hazing in their individual units. Called *dedovshchina*, which translates literally to the "Rule of the Grandfathers," this tradition involves newer conscripts enduring abuse from the conscripts that are nearing the end of their service. Though this hazing frequently involves physical abuse, in the SS-26 unit being tracked, this hazing consisted of conscripts carrying around a distinctive suitcase filled with a sizable number of sex toys. By tracking these conscripts and their suitcase he was forced to carry, researchers were able to confirm deployments of the SS-26 unit to Kaliningrad, as well as some exercise locations.

Researchers were able to ensure that this suitcase was not some another similar-looking piece of luggage, because the older conscripts required that the bag's couriers inventory the sex toys at every location they deployed to as if the bag's contents were accountable items. This research also yielded several insights into the unit's discipline and morale: Conscripts at this nuclear unit were growing cannabis plants at their barracks[146].

146 Lewis, Jeffrey. "Iskander, INF and Kaliningrad." Arms Control Wonk. Accessed November 27, 2016. http://www.armscontrolwonk.com/archive/1202123/iskander-inf-and-kaliningrad/.

These two case studies would appear, at least on the surface, to paint a valuable new intelligence collection tool; indeed, they show a way to leverage the ubiquitous nature of smartphones and the modern propensity to post photos and personal information on the internet. But this tendency cuts both ways. The number of photos uploaded yearly will exceed 1.3 trillion in 2017[147]. One researcher estimated in 2014 that approximately 1.8 billion photos are uploaded onto social media each day[148]. This mass of data only adds to the amount of material analysts must search through on a daily basis. As such, collection failure due to an excess of information is likely to continue, as the surplus of information available to analysts will grow at an exponential rate over time.

Information Denial and Deception. Denial and deception, particularly by Russia, has continued to be a significant constraint to the providing of proper intelligence warning to decision makers. The Russian seizure and annexation of the Crimean Peninsula demonstrate the challenges faced in providing strategic warning for contemporary leaders. In 2014 mass protests forced Ukraine's pro-Russian government out of power. These protests, known as the Euromaidan Revolution, deposed then-President Viktor Yanukovych and brought a new, pro-western Ukrainian government into power. In response, Russia seized the Crimean Peninsula, which housed the Russian Navy's most significant Black Sea naval facilities[149].

147 Hayman, Stephen. "Photos, Photos Everywhere." The New York Times, July 23, 2015. Accessed November 27, 2016. http://www.nytimes.com/2015/07/23/arts/international/photos-photos-everywhere.html?_r=0.

148 Edwards, Jim. "PLANET SELFIE: We're Now Posting A Staggering 1.8 Billion Photos Every Day." Business Insider. May 28, 2014. Accessed November 27, 2016. http://www.businessinsider.com/were-now-posting-a-staggering-18-billion-photos-to-social-media-every-day-2014-5.

149 Treisman, Daniel. "Why Putin Took Crimea." Foreign Affairs, May/June 2016.

Russia did not seize the Crimean Peninsula through overt military action. Instead, groups of armed Soldiers, lacking proper national or unit identification, began appearing across the Crimean Peninsula. These “Little Green Men” as they were referred to in western media quickly seized control of government buildings, Ukrainian military bases, and other key infrastructure across Crimea. Referred to by the Russian media as "self-defense militias," these groups claimed to be spontaneous uprisings of angry residents who claimed to be defending themselves against a supposedly fascist government that had taken power in Kiev[150]. These groups then began to support rebel groups that had arisen in Ukraine's ethnically Russian Donetsk and Luhansk regions[151].The non-attributional nature of these fighters delayed the United States and other NATO powers from being able to identify these units as Russian. By the time the United States and NATO were willing to publicly agree that the Little Green Men were, in fact, Russian troops, Crimea was under the control of Russian forces[152].

These tactics followed an emerging Russian unconventional warfare technique called the “Gerasimov Doctrine,” named after the Russian Chief of the General Staff during the Ukraine Crisis. Gerasimov detailed many of the same tactics used in Ukraine in an article he published in *Voyenno-Promyshlennyy Kurier* (VPK) (*Military-Industrial Courier*), entitled “The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations.” Though

150 "Little Green Men:" A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014. Fort Bragg, NC: US Special Operations Command, 2015. p. 32.
151 “Little Green Men” p. 42.
152 Goure, Dan. "U.S. Experience In Iraq Can Teach NATO How To Hunt Russia's “Little Green Men”." The National Interest. September 9, 2016. Accessed November 17, 2016. http://nationalinterest.org/blog/the-buzz/us-experience-iraq-can-teach-nato-how-hunt-russias-“little-17637.

Gerasimov himself cautions that every conflict is different and, as such, no one-size-fits-all approach is possible, Gerasimov argues that "indirect and asymmetric methods" are required to counter supposed western interventions that take place under the guise of Ukrainian-style "color revolutions."[153] Scholars such as Michael Kofman have researched this concept and has raised doubts if such tactics constitute a formal doctrine. Many armies, he argues, use similar tactics. Just because an entire Russian unit takes off their identifying patches, he argues, does not mean that they have suddenly become a special hybrid unit. But regardless if Gerasimov's ideas have been adopted as formal doctrine, the discussion surrounding them identify the challenge covert military action causes in NATO Alliance decision making.[154]NATO circles fear the use of these tactics in the Baltic States of Latvia, Lithuania, and Estonia. All three of these countries have ethnically Russian populations as Ukraine does. Further, such an effort to seize terrain by similar covert means would allow Russia to both subvert NATO and create a land-bridge to Kaliningrad, a Russian exclave on the Baltic Coast[155]. Should such an effort occur, US collection could be slow to confirm the effort is being Russian-led until the only methods remaining to the United States is a conventional conflict which risks a nuclear escalation with Russia's nuclear forces.

Collection failure. Collection error remains a significant potential vulnerability during future escalation control scenarios. Given that discussions of the characteristics of

153 Bartles, Charles K. "Getting Gerasimov Right." Military Review, January 1, 2016.
154 Kofman, Michael. "Russian Hybrid Warfare and Other Dark Arts." War on the Rocks. March 11, 2016. Accessed December 11, 2016. http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.
155 Person, Robert. "6 Reasons Not to Worry about Russia Invading the Baltics." The Washington Post, November 12, 2015. Accessed November 17, 2016. https://www.washingtonpost.com/news/monkey-cage/wp/2015/11/12/6-reasons-not-to-worry-about-russia-invading-the-baltics/.

contemporary collection systems could compromise sources and methods, much of the information surrounding system effectiveness remains classified and thus largely unavailable. However, there are two current collection assets that have publicly available data detailing system shortcomings: the JLENS and DCGS-A.

The Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS) was designed to detect incoming cruise missiles and low-flying aircraft. JLENS is an aerostat or a tethered lighter-than-air balloon, which aims to provide persistent top-down surveillance for upwards of 30 days at a time. In addition to providing early warning of an incoming enemy cruise missile system, JLENS was also designed to provide the fire control information needed for air defense sites and interceptors to engage and destroy the missile before it reached its target[156]. The proliferation of foreign cruise missile systems designed by Russia, Iran, and the People's Republic of China prompted this system. Cruise missiles, due to their low thermal signature, small size, and low flight altitude, are exceedingly difficult to detect with conventional ground-based radars or satellite[157].

The JLENS program, however, was beset with serious issues from its outset. JLENS was unable to provide 30 days of continuous coverage as intended, requiring frequent idle periods due to technical failure. The system proved especially vulnerable to weather, a problem that doomed one JLENS deployed at Aberdeen Proving Ground, Maryland's Edgewood Area. High winds on 29 October 2015 caused the JLENS to break

156 "How a $2.7 Billion Air-defense System Became a 'zombie' Program." The Los Angeles Times, September 24, 2015. Accessed November 16, 2016. http://graphics.latimes.com/missile-defense-jlens/.
157 Lewis, Jeffrey. "Cruise Missile Proliferation." Arms Control Wonk. Accessed November 16, 2016. http://www.armscontrolwonk.com/archive/206749/cruise-missile-proliferation/.

free of its tether and drift over 240km before crashing in rural Pennsylvania[158]. This failure was due to a depleted battery that rendered the auto-deflate feature on the JLENS inoperable[159].

Worse, the JLENS also had digital communications issues. Auditors found that the JLENS's fire control systems were incapable of differentiating between friendly and enemy targets. Those same systems struggled to maintain communications with the overall national air defense network. JLENS also failed in real world scenarios to detect the very systems against which it was designed to defend. Auditors discovered that the JLENS "had certain features incorporated into its software intended to deal with the very high target densities that exist. However, the design approach chosen to deal with this problem resulted in certain target sets being excluded by the software algorithms associated with the surveillance radar. This could result in some high-priority radar targets not being processed and tracked."[160] On 15 April 2015, a postal worker was able to fly over the capital in a low-flying rotary wing aircraft, despite JLENS being specifically designed to detect objects flying in that flight profile[161].

158 Stewart, Phil, and Yeganeh Torbati. "Runaway Military Blimp Wreaks Havoc in US." Sydney Morning Herald, October 29, 2015. Accessed November 16, 2016. http://www.smh.com.au/world/runaway-military-blimp-loose-over-us-20151028-gklaeq.html.
159 Atherton, Kelsey. "The Army's Runaway Blimp Escaped Due To...Dead Batteries." Popular Science, February 16, 2016. Accessed November 16, 2016. http://www.popsci.com/this-one-cool-trick-could-save-billion-dollar-blimps.
160 US Department of Defense. Operation Test and Evaluation Command. Director, Operational Test and Evaluation FY 2015 Annual Report. By J. Michael Gilmore. 21.
161 "How a $2.7 Billion Air-defense System Became a 'Zombie' Program." The Los Angeles Times, September 24, 2015. Accessed November 16, 2016. http://graphics.latimes.com/missile-defense-jlens/.

JLENS remains in development, and is still intended for fielding to defend the National Capital Region as of this writing.[162]. However, the failings already demonstrated by this system demonstrate the enduring challenge of collection error in the contemporary environment, one which has real implication for future escalation control scenarios. An unreliable warning system like JLENS could cause decision makers to opt to escalate due to a concern that an attack could go undetected and thus prevent them from being able to issue commands to US forces.

Another example of collection failure is the Department of Defense's Distributed Common Ground System-Army, or "DCGS-A." This system, as described by the Department of the Army, is an "intelligence program that enables operational visualization, situational awareness, current and future operations."[163] In short, DCGS-A is intended as a multi-service intelligence processing system. It is designed to take collection data, combine it with existing data that is stored on central servers, and "fuse" that information into products that can be used to better understand the operational environment. "DCGS-A provides Commanders the ability to track and task battle-space sensors and receive intelligence information from multiple sources, and will facilitate 'Seeing' and 'Knowing' on the battlefield."[164]

DCGS-A has demonstrated significant problems in accomplishing this mission, however. The system, as it was fielded, was met with persistent criticisms from its users. A report from November 2013 commented that DCGS-A was "unstable, slow, not

162 Sterk, Richard. "JLENS Will Be Produced, but Not in Numbers Once Expected." Forecast International, October 10, 2016. Accessed November 16, 2016. http://blog.forecastinternational.com/wordpress/jlens-will-be-produced-but-not-in-numbers-once-expected/.
163 "About DCGS-A." DCGS-A. Accessed April 17, 2017. https://dcgsa.army.mil/about/.
164 Ibid

friendly and a major hindrance to operations," with units complaining that DCGS-A upgrades would delete all data saved on the systems. Even worse, these same persistent problems would result in DCGS-A not working for 5 calendar days every month due to repair and maintenance requirements[165].

These problems continued throughout the systems rollout. In one 2014 incident, units operating DCGS-A observed that the system continued to be unreliable. In one case, 10 hours of targeting analysis necessary for an attack was deleted permanently due to a system malfunction that was no fault of the operators. The system also struggled to connect to the necessary databases required to function, failed to search for information accurately, and prevented users from being able to navigate between reports effectively.[166] In short, DCGS-A was failing to properly perform its function analyzing collection data.

On 3 October 2015, Army Special Forces operating inside Kunduz, Afghanistan requested an airstrike against what they believed to be a Taliban position close to their position. An AC-130 destroyed the compound, firing over 200 rounds against the target, which turned out to be not a Taliban position but rather a hospital run by Doctors Without Borders. The ensuing investigation indicated that the AC-130 did not have the database that listed hospitals uploaded onto its computers.[167] In later investigations, it was

165 US Department of Defense. Headquarters, International Security Assistance Force Joint command. Training Requirements to Maintain Proficiency on Distributed Common Ground System-Army (DCGS-A). By Christopher Ballard.
166 Scarborough, Rowan. "Problems with Army's battlefield intel system unresolved after two years." The Washington Times. May 01, 2014. Accessed April 17, 2017. http://www.washingtontimes.com/news/2014/may/1/problems-with-armys-battlefield-intel-system-unres/.
167 Rosenberg, Matthew. "Pentagon Details Chain of Errors in Strike on Afghan Hospital." The New York Times. April 29, 2016. Accessed April 17, 2017.

determined that DCGS-A was not operational during the period of the strike. One of the roles of DCGS-A was to cross-reference intelligence collection feeds and combine them with databases of known hospital locations. As such, the AC-130 when departing for its mission did not have the information it needed because DCGS-A was offline.[168]

One counterargument to these examples is that both JLENS and DCGS-A are new, complex, and relatively immature systems that are currently undergoing extensive research and development. There are any number of systems in the Department of Defense that go through lengthy and problem-filled development cycles before having long and valuable service lives. This is undeniably true. However, during the time it takes to develop these systems into useful and reliable platforms, those same systems still result in collection errors. As the Kunduz strike example demonstrates, those development hurdles can have significant consequences, and though systems like DCGS-A may eventually become useful and reliable systems, decision makers and the intelligence community still must contend with their problems until those systems reach maturity.

Analytic Bias

As was discussed in Chapter 2, analytic bias can occur in three key ways. First, *poor analytic tradecraft* results in intelligence information collected being misinterpreted or dismissed outright, most often due to preconceptions on the part of intelligence analysts. Second, *bureaucratic interference* can influence the presentation of information to decision makers, occurring when individuals within the government misconstrue

https://www.nytimes.com/2016/04/30/world/asia/afghanistan-doctors-without-borders-hospital-strike.html.

168 http://www.c4isrnet.com/story/military/tech/2015/10/21/lawmaker-alleges-key-army-dcgs-system-down-during-hospital-airstrike/74347222/

intelligence analysis or even outright refuse to accept it as presented, so as to either serve a particular political objective or personal bias, or simply because they are unable to accept the report's finding due to their own preconceptions. Third, *insufficient aggregation* of intelligence can present decision makers situational awareness that is insufficiently nuanced. Such a lack of nuance results from overly granular reports given in parallel that can fail to provide decision makers with the proper understanding that could have been achieved by combining those reports into a more holistic assessment.

In the time between the Cuban Missile Crisis and the present day, these intelligence community has undertaken numerous efforts to improve its analytic performance. One example of this is the Team B effort. Desiring a "competitive estimate" to determine if CIA assessments of Soviet doctrine were accurate, Team B was an effort to bring in outside analysts to review CIA intelligence. Releasing their report in 1976, Team B argued that indeed the CIA had been too dovish in its assessments of the Soviet Union.

Team B, however, had its issues. To quote a later CIA history examining Team B's effectiveness:

> In retrospect, and with the Team B report and records now largely declassified, it is possible to see that virtually all of Team B's criticisms of the NIE proved to be wrong. On several important specific points it wrongly criticized and "corrected" the official estimates, always in the direction of enlarging the impression of danger and threat. For example, the range of the *Backfire* medium bomber was considerably overestimated, and the number of *Backfires* the Soviet Union would acquire by 1984 was overestimated by more than 100 percent (estimating 500 when the real figure was 235). … It regarded as ominous, rather than reassuring, that no intelligence information had been acquired on Soviet development of a nonacoustic antisubmarine warfare capability, again raising concerns over a looming threat that did not arise.[169]

169 Gartoff, Raymond. "Chapter V." Center for the Study of intelligence. June 28, 2008. Accessed April 17, 2017. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-

Team B, though it had its flaws, showed an interest in ensuring that the intelligence community remained objective in its analysis. In the area of strategic warning alone, the Central Intelligence Agency undertook five such studies from 1995-1999 alone[170]. Yet in spite of this, analytic failure continues to be an issue within the intelligence community. While the intelligence community at large attempts to improve its analytic tradecraft, it is a discipline that must operate at times with limited information. As such, just as analytic failure bedeviled the proper flow of information to decision makers during the planning for potential military escalation in Cuba, due both to the personal bias of policymakers, analysts, and to faulty assumptions, intelligence is still open to errors in analytical thinking, and the flow and use of that intelligence is vulnerable to misuse by interested parties attempting to advance specific agendas.

Three cases in recent years demonstrate enduring analytic bias. The first is faulty assumptions underlying intelligence that helped lead to the 2003 Iraq War. The second is a dispute between Ambassador John Bolton and intelligence analysts within the State Department's intelligence division, over the former's claims that Cuba maintained an active offensive biological weapons program. The third example is that of Ana Montes and the 1996 Brothers to the Rescue incident, in which her management of interactions between government officials and unofficial diplomatic messengers from Cuba resulted

publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/article05.html.

170 Davis, Jack. "Improving CIA Analytic Performance: Strategic Warning." Center for Intelligence Analysis. January 03, 2012. Accessed April 17, 2017. https://www.cia.gov/library/kent-center-occasional-papers/vol1no1.htm.

in the Clinton Administration finding its available options to resolve a crisis being limited from that crisis' outset.

I. Poor analytic tradecraft. Perhaps the best known incident in recent years of faulty assumptions leading to inaccurate intelligence reporting used by decision makers was the 2002 National Intelligence Estimate (NIE), produced in December of 2002 during the lead-up to the Iraq War. That particular NIE asserted that Iraq "has continued its weapons of mass destruction program in defiance of United Nations resolutions and restrictions. Baghdad has chemical and biological weapons as well as missiles with ranges exceeding United Nations restrictions; if left unchecked, it will likely have a nuclear weapon during this decade."[171]

Intelligence analysts, while preparing this report, used several key assumptions into their analysis, assumptions which later proved to be faulty. These assumptions resulted in inaccurate assessments of the scope of Iraq's weapons of mass destruction program. First, intelligence analysts assumed that since they had failed to correctly capture the scale of Saddam Hussein's weapons of mass destruction programs before the 1991 Gulf War due to the regime's denial and deception programs, any absence of evidence must be the result of similar deception efforts.[172] Second, intelligence analysts assumed that previous assessments were accurate, and then built on those assessments to produce future reports. Earlier reports had indicated that Saddam Hussein had a major weapons of mass destruction program and so new reporting did the same. Once that initial faulty reporting made it into the assessment, it created the appearance that the

171 US Central Intelligence Agency. Director of Central Intelligence. Iraq's Continuing Programs for Weapons of Mass Destruction. Washington, DC, 2002.
172 Immerman, Richard H. "Intelligence and the Iraq and Afghanistan Wars." Political Science Quarterly 131, no. 3 (2016): 477-501. doi:10.1002/polq.12489.

analysis was more comprehensive than it was in reality.[173] Finally, analysts assumed that Saddam Hussein's regime had a coherent plan for developing weapons of mass destruction. The regime had acquired chemical weapons during the Iran-Iraq War, it had continued to produce them during the Gulf War, and after the Gulf War, it appeared to be continuing with the chemical weapons program. Consequently, analysts assumed that Saddam Hussein had a coherent plan centered on acquiring weapons of mass destruction, when in fact Hussein had no such intentions.[174]

One counterargument to this was that Saddam Hussein himself encouraged the perception that Iraq maintained a chemical weapons stockpile. If the state in question is signaling that it maintains a WMD program, how can analysts be expected to judge otherwise. The problem with this counterargument, however, is that state deception programs are a common issue faced by intelligence agencies. As discussed in the Cuban Missile Crisis example, states will often attempt to conceal their intentions from the eyes of intelligence agencies with deliberate deception programs. Indeed, the best deception programs are those that present an image to an adversary that an adversary expects to see. Consequently, proper analytic tradecraft would have solved this problem.

In this way, then, one can see how even in contemporary times, and even after numerous attempts to improve analytic tradecraft, how faulty assumptions still can severely warp intelligence assessments and consequently alter a decision maker's perception of a potential adversary. Further, one also can see how decision maker bias can also make the transmittal of accurate information more difficult.

---

173 Jervis, Robert. Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War. Ithaca: Cornell University Press, 2010. p. 130.
174 Jervis, p. 131.

II. Bureaucratic interference. In May of 2002, Undersecretary of State for Arms Control and International Security Affairs John Bolton announced that Cuba was maintaining an active offensive biological weapons program. “The United States believes that Cuba has at least a limited offensive biological warfare research and development effort," Bolton announced, continuing that Cuba had "provided dual-use biotechnology to other rogue states.”[175] In response to this, Bush Administration officials announced that the United States would tighten sanctions against Cuba.[176]

Soon after this announcement, however, other officials within the Bush Administration began to walk back this statement. When interviewed at a meeting of NATO leaders being held in Iceland, then Secretary of State Colin Powell stated that “we do believe Cuba has a biological offensive research capability...we didn't say it actually had some weapons, but it has the capacity and capability to conduct such research.” National Security Advisor Condoleezza Rice clarified further, stating “"you can't show someone a biotech lab and be assured they're not creating weapons of mass destruction. That's not how biotech weapons work. And they're actually very easy to conceal and you need multiple measures to make certain biotech weapons aren't being developed and transferred.”"[177]

In April 2005, nearly three years later, Ambassador Bolton was nominated to become the US Ambassador to the United Nations. During his nomination hearings, it

175 Miller, Judith. "Washington Accuses Cuba Of Germ-Warfare Research." The New York Times, May 7, 2002. Accessed October 16, 2016.
176 Marquis, Christopher. The New York Times, May 15, 2002. Accessed October 16, 2016. http://www.nytimes.com/2002/05/15/world/bush-plans-to-tighten-sanctions-on-cuba-not-ease-them.html.
177 Gonzales, David. "Carter and Powell Cast Doubt on Bioarms in Cuba." The New York Times, May 14, 2002. Accessed October 16, 2016.

was alleged by Christian Westermann and Carl Ford Jr, both from the State Department's Intelligence and Research Division, had testified that Bolton attempted to pressure them into changing their intelligence assessments to paint what they viewed was a grimmer picture of Cuba's potential biological weapons program. Ford, during testimony to Congress, asserted that after Westermann had refused to change Cuban intelligence for Bolton, the Ambassador called Westermann into his office and "reamed him a new one."[178]

After this incident, Powell opted to visit Intelligence and Research and inform the staff there that they were to continue "speak truth to power" in their intelligence assessments. Ford, commenting on the incident in Congress, remarked that "There are a lot of screamers that work in government. But you don't pull somebody so low down the bureaucracy that they are completely defenseless. It's an 800-pound gorilla devouring a banana."[179]

A counterargument to this example is that Bolton, while defending himself, asserted that he had felt the intelligence assessments on Cuba being produced by Intelligence and Research (INR) were "too cautious." Because he thought they were too cautious, and because the threat a biological weapons program would pose, Bolton felt that assessment an assessment that identified Cuba as a state maintaining an offensive biological weapons program was necessary despite the information having lower than normal confidence levels.

178 Weisman, Steven R. "Ex-Official Says Nominee Bullied Analyst on Arms." The New York Times. April 13, 2005. Accessed October 16, 2016. http://www.nytimes.com/2005/04/13/world/exofficial-says-nominee-bullied-analyst-on-arms.html.
179 Ibid.

The problem with this argument is that it still shows how elements within the bureaucracy are altering an intelligence product to one particular point of view or another. The purpose of this example is not to cast judgment on either of the participants. Rather, it is to show that both Bolton and INR cannot both be right. The first option is that Cuba actually has a biological weapons program, and that INR has been creating inaccurate reports that say the opposite. The second option is that Bolton was incorrect, and that Cuba does not have an offensive biological weapons program. In this telling, it is Bolton who is attempting to pass along inaccurate intelligence that can influence decision makers.

Again, this does not imply any malign intend on the part of either party. Different individuals and organizations view the same sets of information differently. But only one individual group can be right. Further, both offices could be seen to have agendas. In the case of INR, their pushback against a more substantive intelligence assessment could be seen as an attempt to maintain a degree of independence, or an attempt to impose a more robust standard for intelligence assessments. In the case of Bolton, on the other hand, either Bolton is attempting to push the administration to take a more hardline position on Cuba despite objections within the administration (as evidenced by the immediate pushback from both the national security advisor and the secretary of state), or an attempt to impose his own standards on INR's intelligence review process.

Another example of distortion case of Ana Montes, a Defense Intelligence Agency (DIA) arrested in September 2001 for spying on behalf of the Cubans is instructive of how a sufficiently high-placed analyst can seriously influence how national decision makers operate during escalation control. Montes was recruited by Cuban

intelligence in 1984 while an employee of the US Justice Department, and upon being recruited applied and was accepted by the DIA as an analyst.[180] At the time of her arrest, Montes was considered to be one of the government's best Cuba analysts,[181] earning her the nickname within the intelligence community as the "Queen of Cuba."[182]

On 24 February 1996, Cuban fighter aircraft shot down two private planes flown over international waters by Brothers to the Rescue, an aid organization that frequently overflew Cuba to drop anti-Castro leaflets.[183] After the shoot down occurred, retired Admiral Eugene Carroll came forward publicly to claim that while on a visit to Cuba sponsored by the Center for Defense Information, a left-leaning defense think-tank, representatives from the Cuban government had warned him in advance that the Cuban Air Force might shoot down these aircraft should they continue to operate, and stated that he passed those warnings to government officials.[184]

The result was a public relations crisis for the Clinton Administration.[185] Rather than public attention being focused on Cuba's involvement in shooting down of two civilian aircraft over international water, the focus was instead on why the Clinton

---

180 Popkin, Jim. "Ana Montes Did Much Harm Spying for Cuba. Chances Are, You Haven't Heard of Her." The Washington Post, April 21, 2013. Accessed 2016. http://www.washingtonpost.com/sf/feature/wp/2013/04/18/ana-montes-did-much-harm-spying-for-cuba-chances-are-you-havent-heard-of-her/.

181 Lattel, Brian. "New Revelations about Cuban Spy Ana Montes." Miami Herald, August 2, 2014. Accessed October 16, 2016. http://www.miamiherald.com/opinion/issues-ideas/article1978099.html.

182 "Most Damaging US Spy You've Never Heard of." CNN. Accessed October 16, 2016. http://www.cnn.com/2016/07/06/us/declassified-ana-montes-american-spy-profile/.

183 Nieves, Gail Epstein. "Basulto Testifies on Role as Anti-Castro Operative." The Miami Herald, March 13, 2001. Accessed October 16, 2016. http://www.latinamericanstudies.org/exile/basulto-testifies.htm.

184 Rohter, Larry. "Cuba's 2 Steps Back." The New York Times, February 29, 1996. Accessed October 16, 2016. http://www.nytimes.com/1996/02/29/world/cuba-s-2-steps-back.html.

185 Rohter, Larry. "Cuba Blames U.S. in Downing of Planes." The New York Times, February 27, 1996. Accessed October 16, 2016.

Administration had failed to put a stop to the flights after being told by Cuba that they were prepared to take action.[186] Carroll's comment managed, therefore, to badly set back the Clinton Administration's crisis management.

Yet for some within the DIA, looking back at the incident in hindsight, the timing seemed too neat to be entirely coincidental. Just one day before the shoot down, Cuban officials had managed to meet with Carroll, a source known to be critical of US policy towards Cuba. The meeting in question had been organized by than Ana Montes, who had specially arranged the meeting dates.[187] In this respect, then, Montes had arranged for Carroll to meet with the Cuban representatives in just enough time to receive a warning and pass it along to representatives from the State Department, but without enough time for those representatives to actually prevent the flights from happening.

A counterargument to this example is that Montes could have been unaware of the planned attack by the Cuban Air Force, or that the Cuban government could have ordered the strike without the intent of using the tour group to tie the Clinton Administration's hands. While these arguments do have some logic, the weight of evidence points to the fact that Cuba had likely chosen the timeline to ensure that there would be insufficient warning. The delegation was informed that standing orders existed to shoot down any further BTTR flights violating Cuban Air Space.[188] Yet Cuban Intelligence had successfully penetrated the BTTR organization, and as such knew of that organization's

186 "The Cuban Shootdown." The New York Times, February 27, 1996. Accessed October 16, 2016. http://www.nytimes.com/1996/02/27/opinion/the-cuban-shootdown.html.
187 Carmichael, Scott W. True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy. Annapolis, Maryland: Naval Institute Press, 2007. p. 6.
188 LeoGrande, William M., and Peter Kornbluh. Back channel to Cuba: the hidden history of negotiations between Washington and Havana. Chapel Hill: The University of North Carolina Press, 2015.

planned flight schedule.[189] With that information, paired with the standing order to shoot down any BTTR planes, Cuba would have likely known the time they were giving those representatives was insufficient to prevent the planned flight.

Given the thaw in relations between the United States and Cuba is relatively recent, and given the fact that Cuba's government has been slow to relax its security restrictions, it will likely be some time until additional information about this incident will be revealed, this case study shows another potential way that individuals operating inside the US government could influence events, consciously or otherwise.

Vulnerable C4I Infrastructure

As previously mentioned, there are three key categories of facilities critical for the intelligence enterprise are vulnerable to enemy attack during on control. First, *collection infrastructure* are all the facilities needed to properly collect intelligence for decision makers. This includes the platforms collecting intelligence themselves, such as reconnaissance aircraft or listening stations. Second, *analysis centers* are those facilities needed for intelligence analysts to accurately analyze both collected information on enemy forces as well as determine the status of the nation's military and civilian populations. Third, *command facilities* are the locations essential for national decision makers to receive intelligence assessments, process them, and use that intelligence to determine necessary courses of action.

189 Roig-Franzia, Manuel. "Cubans Jailed in U.S. as Spies Are Hailed at Home as Heroes." The Washington Post. June 03, 2006. Accessed April 17, 2017. http://www.washingtonpost.com/wp-dyn/content/article/2006/06/02/AR2006060201780.html.

Communications infrastructure. In the wake of the Cuban Missile Crisis, the United States Government invested significant resources in efforts to improve the DoD's communications infrastructure, recognizing that such communications provided invaluable command and control of US forces. Government officials also recognized the importance of facilitating necessary communications between decision makers and their advisors. Working to adapt US command and control infrastructure in an "evolutionary" manner, the DoD and the DCA opted to eliminate redundant communications infrastructure and expand the systems that showed the most promise.[190] Such steps included expanding airborne command and control platforms, as well as developing improved links to US embassies and diplomatic outposts in South America and Europe, so as to provide the President the ability to consult with US officials located there[191].

As part of this effort, the DoD began to place a greater emphasis on the automation of communications. In 1964, Rand Corporation's Paul Baran began to write about the need for a communication network that ensures communications resiliency through the use of "hot potato routing" through a distributed communications network,[192].he writes, "[e]tremely survivable networks can be built using a moderately low redundancy of connectivity level. Redundancy levels on the order of only three permit withstanding extremely heaving level attacks with negligible additional loss to communications….[T]he redundancy level required to survive even very heavy attacks is not great -- on the order of only three or four times that of [baseline]."[193] This logical

190 Sturm, p. 14.
191 Sturm, p. 28.
192 "Paul Baran and the Origins of the Internet." Rand Corporation. Accessed November 26, 2016. http://www.rand.org/about/history/baran.html.
193 Baran, Paul. On Distributed Communications. Santa Monica, CA: Rand, 1964. p. 6.

framework, combined with advances in computer processing power, provided the basis both for the modern internet as well as more advanced command and control systems. In 1969, ARPANet, employing "network redundancy" to compensate for potential outages[194]. Digital communications technology would allow for the development of modern communications networks.

The current incarnation of the DCA is the Defense Information Systems Agency, or (DISA), based at Fort Meade, Maryland. DISA maintains and improves the current nuclear command and control system, the Minimum Essential Emergency Communications Network (MEECN). According to DISA, "MEECN is a highly survivable communications capability which transmits Nuclear Command and Control (NC2) messages and establishes crisis conferences with the President, Vice President, Secretary of Defense, and the Chairman of the Joint Chiefs of Staff to the commanders of the [Combatant Commands] and to deployed nuclear forces." MEECN is composed of "C3 assets that provide connectivity from the President to the Secretary of Defense through the National Military Command System."[195] MEECN is primarily intended to allow the President to exercise command and control of nuclear forces. It is designed to support the transmission of orders by the President in a robust enough fashion to survive a nuclear attack. While MEECN mitigates many of the problems associated with transmitting nuclear orders to the force that existed in 1962, it is not intended to support intelligence collection and the collaboration of US intelligence agencies, nor can it

194 Jacobsen, Annie. The Pentagon's Brain. New York, NY: Little, Brown and Company, 2016. p. 245.
195 US Defense Information Systems Agency. Comptroller. Operation and Maintenance, Defense-Wide Fiscal Year (FY) 2017 President's Budget. Fort Meade, Maryland: DISA, 2016. 204.

provide robust communications between the President and advisors at sites which lack MEECN-connections. For example, MEECN does not connect the President to all members of the cabinet.

Additionally, much of the nuclear command and control infrastructure is becoming increasingly dated. The Strategic Automated Command and Control System, which “"coordinates the operational functions of the United States' nuclear forces, such as intercontinental ballistic missiles, nuclear bombers, and tanker support aircraft" currently runs on a mainframe computer which dates back to the 1970s.[196] Pentagon spokeswoman Lieutenant Colonel Valerie Henderson, commenting on the current state of the nuclear command and control infrastructure to NPR, observed that Modernization across the entire Nuclear Command, Control, and Communications (NC3) enterprise remains ongoing."[197] This is because much of that infrastructure is extremely outdated.

An example of this modernization is the development of new nuclear command and control facilities to better manage NC3 systems. The US Air Force has begun standing up new facilities which are intended to better “provide the technical support to help keep the systems running, maintained and modernized.”[198] Additionally, the DoD is also seeking to field newer, more advanced communication systems that provide more resilient communications. An example of this is the advanced extremely high frequency

196 Rep. No. GAO-16-468 (2016). "Federal Agencies Need to Address Aging Legacy Systems."
197 Kennedy, Merrit. "Report: U.S. Nuclear System Relies On Outdated Technology Such As Floppy Disks." NPR. May 26, 2016. Accessed April 11, 2017. http://www.npr.org/sections/thetwo-way/2016/05/26/479588478/report-u-s-nuclear-system-relies-on-outdated-technology-such-as-floppy-disks.
198 Crawford, Sarah. "Air Force Nuclear Command Center at BAFB will employ 236." Shreveporttimes.com. April 04, 2017. Accessed April 12, 2017. http://www.shreveporttimes.com/story/news/2017/04/03/air-force-nuclear-command-center-activated-barksdale-employ-236/99996698/.

(AEHF) communications system, which is intended to maintain communication with deployed nuclear forces[199]. These systems are intended to be deployed within the next decade.[200]

Even so, however, this C4I infrastructure remains vulnerable to attack. Orbiting collection satellites and their downlink stations, in particular, are susceptible to attack by a growing number of state actors, to include Russia and China. Development of orbital weapons by both the United States and Russia (then the Soviet Union) began in the 1970s and has continued today. These weapons would allow either of these two potential adversaries the ability to destroy US intelligence collection satellites as well as US communication satellites[201]. Such weapons could also target commercial satellites. Approximately 80 to 90 percent of US military communications, to include the communication of critical intelligence information, occurs across civilian satellites. An adversary would not necessarily have to destroy one of these satellites. The option also exists to jam them to prevent their reliably transmitting their traffic.[202]

The growth of precision munitions has made targeting vulnerable facilities such as satellite downlink stations, control nodes, and data processing facilities vulnerable to attack. China and Russia both have dramatically expanded their land-attack cruise

199 US Air Force, Air Force Space Command. December 2016. Accessed April 12, 2017. http://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/249024/advanced-extremely-high-frequency-system/.
200 Grossman, Elaine. "Reviving Cold War Doomsday Devices Could Patch America's Broken Nuclear Controls." War Is Boring. February 22, 2017. Accessed April 12, 2017. http://warisboring.com/reviving-cold-war-doomsday-devices-could-patch-americas-broken-nuclear-controls/#.y3lxmv7wb.
201 Finch, James B. "Bringing Crisis Stability Down to Earth." Joint Forces Quarterly, January 2015.
202 Wilgenbush, Ronald C., and Alan Heisig. "Command and Control Vulnerabilities to Communications Jamming." Joint Forces Quarterly, April 2013.

missile (LACM) capabilities, which could allow the targeting of such facilities. China, for instance, has expanded its LACM arsenal to include land-, sea- (both surface and subsurface), and air-launched missiles. Russia too has done so, going so far as to mount these missiles in shipping containers to make detecting their launcher far more difficult[203].

Cyber warfare such as hacking and denial-of-service attacks have emerged as another means to disrupt vital collection communications. Over the summer of 2015, the communications networks of the JCS were compromised by Russian hackers. This compromise resulted in their communications being disabled for approximately two weeks[204]. Similar hacking attacks against both the Department of State and White House email networks have also taken place. China too has continued to launch hacking attacks against US government systems. One such cyber-attack targeted approximately 60 separate networks simultaneously. Such attacks allow the attacker to obscure their identity, further complicating efforts to combat those attacks.

A counterargument to this is that steps are being taken to protect against cyber-intrusions and cyber-attacks. In recognition of this threat, the Pentagon in 2016 proposed increasing cyber defense spending to approximately $900 million USD[205]. A emphasis has been placed on the surety of the nuclear command and control system. Since the US Air Force has announced that newer missile systems will demonstrate “some level of

203 Gormley, Dennis M., Andrew S. Erickson, and Jingdong Yuan. "A Potent Vector: Assessing Chinese Cruise Missile Developments." Joint Forces Quarterly, September 2015.
204 Harris, Shane. The Daily Beast. Accessed November 17, 2016. http://www.thedailybeast.com/articles/2015/07/18/russian-hackers-target-the-pentagon.html.
205 Gertz, Bill. "China Continuing Cyber Attacks on U.S. Networks." Washington Free Beacon. Accessed November 17, 2016. http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/.

connectivity to the rest of the warfighting system,"[206] a great deal of acquisitions and research is focused on procuring defenses to limit the effectiveness of cyber-attacks. The Defense Advanced Research Projects Agency (DARPA) has been developing "blockchains," currently used to secure virtual currencies such as Bitcoin, Equinox, and DogeCoin. This technology essentially acts as an "immutable ledger" that reports if any given information traveling on the network has been accessed and/or modified[207].

That said, however, blockchains only allow the DoD to determine if somebody has accessed or modified data. It doesn't prevent that person from doing so in the first place. In effect, a blockchain acts like a closed-circuit television (CCTV) security system in a bank. By using that system, security could determine if somebody has broken into the bank and document what, if anything, that person stole. It does not, however, prevent that burglar from breaking into the bank in the first place. If an adversary disables an essential computer network during a crisis, attribution is only part of the problem. Though decision makers will know who is responsible, they'll also still need to make use of that communications network which is now unavailable.

Why is this so? To return to the bank example, while it's useful that the bank can identify that a burglar forced his or her way into the bank, if the bank was relying on the money said burglar stole to operate that next business day then there are additional issues with which the CCTV did not help. It is for this reason, then, that nuclear strategist Paul

206 Tucker, Patrick. "Hacking Into Future Nuclear Weapons: The US Military's Next Worry." Defense One. December 29, 2016. Accessed April 12, 2017. http://www.defenseone.com/technology/2016/12/hacking-future-nuclear-weapons-us-militarys-next-worry/134237/?oref=search_command and control.
207 Wong, Joon Ian. "Bitcoin-Style Security May Soon Guard US Nukes and Satellites." Defense One. October 11, 2016. Accessed April 12, 2017. http://www.defenseone.com/technology/2016/10/bitcoin-style-security-may-soon-guard-us-nukes-and-satellites/132235/?oref=search_command and control.

Bracken remarks that "[t]he intersection of cyberwar and nuclear deterrence has enormous and widely overlooked implications for stability."[208]

Each of these methods could significantly disrupt communications linkages required for the passing of collected information for exploitation by intelligence analysts. Such a disruption would complicate the ability of the intelligence community and the US military to pass critical information to US decision makers, having a potentially destabilizing impact on escalation control. Worse, these methods of attack are likely as part of anti-access/area denial (A2/AD) efforts to defeat US forces in conventional combat. In short, the very weapons an adversary can use to prevail in a conventional conflict could very much degrade the ability of the US to control a nuclear escalation scenario.

Analysis centers. Today, the intelligence community remains mostly concentrated around Washington, D.C. Those facilities are as follows.

- The Central Intelligence Agency, Langley, Virginia
- The National Security Agency, Fort Meade, Maryland
- The Defense Intelligence Agency, Joint Base Anacostia-Bolling, D.C.
- National Geospatial-Intelligence Agency, Fort Belvoir, Virginia
- Director of National Intelligence, McClean, Virginia

Both the CIA and NSA remain in their previous locations. The DIA has moved to Joint Base Anacostia-Bolling just inside the District of Columbia. At this site, DIA is now closer to the Pentagon and the center of the District of Columbia than it was at

208 Bracken, Paul. "The Intersection of Cyber and Nuclear War." RealClearDefense. January 17, 2017. Accessed April 12, 2017. http://www.realcleardefense.com/articles/2017/01/17/the_intersection_of_cyber_and_nuclear_war_110646.html

Arlington Hall, Virginia. In the interim, two additional agencies essential to escalation control have since built headquarters near Washington. The first is the National Geospatial-Intelligence Agency (NGA), responsible for the analysis of overhead photography for the intelligence community, to include satellite photography. The second is the Director of National Intelligence (DNI), who serves as the President's primary intelligence advisor and oversees the work of the intelligence community.

In short, as more members of the intelligence community have merged since 1962, either as new organizations or the consolidation of pre-existing ones, they have remained clustered around the capital. The government has effectively abandoned dispersal as a method of protecting high-value targets[209].

From a practical standpoint, abandoning such efforts made sound financial sense. With the number of Soviet missiles growing, and with their accuracy improving to the point where the number of warheads required to destroy a target dropped, it was realized that few such facilities would survive attack. Further, starting in 1963, the individual intelligence agencies started building more clearly-defined liaison relationships with both the hardened and mobile command facilities needed to advise the President or the President's designated successor.

The lack of survivable facilities for the analysis agencies, combined with their proximity to Washington, D.C. still means that the vast analytic enterprise required to support a President as they attempt to decide the best course of action to take in an escalation control scenario remains. The continuing vulnerability of these facilities was demonstrated during the September 11th attacks in 2001.

209 Krugler, p. 183.

During the September 11th (9/11) attacks, the United States intelligence community found itself operating out of extremely vulnerable facilities. The consequences of such a vulnerability dramatically impacted the ability of the intelligence community to respond to the crisis. The attack struck the north and south World Trade Center Towers at 8:46 am and 9:03 am EST respectively. The Pentagon was hit by a third aircraft at approximately 09:45 am EST[210]. Due to ongoing confusion about the number of planes and targets involved, there were serious concerns that a follow-on attack was likely.

At CIA headquarters, the agency's senior leadership opted to meet to discuss ongoing events at 9:50 am EST. Of particular concern was information provided by Ramzi Yousef, which indicated that the CIA Headquarters as a potential target during the planning of the first World Trade Center Bombings in 1993. Within a few minutes of the attack starting, the decision was made to evacuate CIA headquarters.[211] After making this decision, only a small cadre of senior managers inside the CIA remained behind to perform intelligence analysis and advise President George W. Bush, which they did at 3:30 pm. Though such a communication took place, most of the Agency's personnel were unavailable due to the evacuation.

A similar situation occurred at the DIA. The attack on the Pentagon resulted in the deaths of several DIA employees. As part of the response to this attack, and due to similar concerns as those of the CIA, the majority of DIA employees evacuated from DIA headquarters. Though some senior staff remained behind, the majority of analysts

210 9/11 Report p. 1.
211 Brennan, John O. "Remarks as Prepared for Delivery by Central Intelligence Agency Director John O. Brennan at the 9/11 Memorial Museum in New York City." Speech, 9/11 Memorial Museum, New York, September 26, 2016.

and support staff at DIA were unable to work until intelligence agencies determined that no further attacks were imminent.[212]

This same vulnerability was also evidenced further in the future. Over Christmas, 2003, US intelligence officials believed that an increase of terrorist communications meant that an attack on the US, possibly with nuclear weapons, was imminent. Accordingly, US government officials began to prepare for the possibility that a nuclear attack on Washington could damage or destroy key government facilities[213]. At the NSA, such a fear led then-Director Michael Hayden to contact his counterpart, Government Communications Headquarters (GCHQ) Director David Pepper, to discuss his concerns. After the conversation, Hayden observed that while NSA satellite locations could pick up much of the slack should Fort Meade be damaged or destroyed, much of the important analysis and management would be lost. As such, in the event of such an attack, Hayden told Pepper that he would transfer control of the NSA's collection apparatus to GCHQ until such a time as the Agency could reconstitute elsewhere[214].

Each of these examples demonstrates how vulnerable the large, above-ground infrastructure are to even conventional attack. A nuclear attack could have equally dramatic consequences, disabling these facilities during a nuclear escalation scenario and depriving national decision makers of critical intelligence.

---

212 "This Day in History: Sept. 11, 2001." Defense Intelligence Agency. 2015. Accessed November 15, 2016. http://www.dia.mil/News/Articles/Article/616903/this-day-in-history-sept-11-2001/.
213 Harris, Shane. The Daily Beast. Accessed November 16, 2016. http://www.thedailybeast.com/articles/2016/09/10/the-time-u-s-spies-thought-al-qaeda-was-ready-to-nuke-d-c.html.
214 Ibid.

Command Facilities. Many national command and facilities remain vulnerable today as they did during the Cuban Missile Crisis.

Fearing that Soviet attacks would threaten the survival of the President, the government built 75 Presidential Emergency Facilities (PAFs) through the 1970s. Intended to provide the President or a designated successor a safe location to shelter during Crisis, the government funded construction of these facilities out of money allocated for the effort hidden within the US Army's budget and directed construction of these facilities through the White House Military Office (WHMO). These facilities consisted of a small shelter to house the President and the President's entourage, and a communications suite designed to allow the President to communicate with the outside world.[215] These facilities were augmented by the mobile command centers that had begun to enter operation in 1962. The President or a designated successor could travel in either the National Airborne Command post (NEACP), or travel via ground in a convoy of trucks known as the Ground Mobile Command Facility (GMCF).

Despite all this, the day-to-day command facilities that afford decision makers the greatest capacity for command and control remain at fixed sites and also remain vulnerable. And the attacks on 9/11 also provide a case study involving the National Military Command Center (NMCC) that demonstrates this fact. At 9:37 EST, American Flight 77[216] crashed into the Pentagon's western side. The aircraft traveled through the first floor of the building and penetrated the building's E- and D-Rings (the outermost and second outermost rings), with the remains of the aircraft stopping just short of C-

215 Krugler, p.184.
216 PBS. Accessed November 17, 2016. http://www.pbs.org/program/911-inside-pentagon/.

Ring[217]. The impact of Flight 77 immediately started fires throughout the Pentagon complex. Though the NMCC was located under the other side of the Pentagon, the building's interconnected support systems such as air processing, temperature control, and power were connected to the same system. As the fires continued to burn in the western side, these systems began to fail within the NMCC. Had there not been significant intervention from the Pentagon's support staff, the NMCC would have been forced offline[218].

Continuity of Government. Continuity of government also remains a challenge for the US Government. In the wake of 9/11, a renewed emphasis was placed on continuity-of-government exercises to prepare for potential attacks on the national capital. In the weeks following the attacks, essential personnel remained at offsite locations such as Site R for several weeks until the determination was made that no further attacks were likely.[219] In the ensuing decade, the Federal Government ran many continuity-of-government exercises. These exercises, however, demonstrated that there were still serious flaws in government readiness. One study by the Government Accountability Office audited continuity-of-government exercises by different federal agencies. They found deficiencies in these preparations, including an inability to validate that continuity-of-government sites would even have the necessary infrastructure, such as power, to function. It also found that much of the preparation for continuity-of-government remained on paper and was not fully exercised with the rigor needed in a

217 Condon-Rall, Mary Ellen. Attack on the Pentagon: The Medical Response to 9/11. Fort Detrick, Maryland: Borden Institute, 2011. p 4.
218 PBS. Accessed November 17, 2016. http://www.pbs.org/program/911-inside-pentagon/.
219 Krugler, p. 185.

nuclear environment[220]. Another Government Accountability Office study determined that the Defense Department remained unready to provide support to continuity-of-government and civil response activities that would be essential to continue government operations[221].

Summary

In discussions of escalation control, an enormous amount of attention is paid to the survivability of nuclear forces, of civil targets, and of key strategic resources. Part of this is likely a legacy of the earliest nuclear weapons. In a world of massive retaliation, the need for nuanced assessments realistically extended no further than assessing what targets required re-attack. As nuclear strategy has evolved, so too has the need to provide timely, accurate, unbiased, and persistent intelligence updates.

In the modern era, decision makers have inherited an information management enterprise that retains many of the shortcomings of previous generations. Bias still enters the system. Denial and deception remain an issue. Information volume has grown exponentially every year since 1962, without a corresponding growth in tools to manage that growth. Worse, the more capable near-peer nuclear forces become, the few techniques available to protect the assets required to make such assessments have further declined in utility.

220 Rep. No. GAO-08-185 (2007).
"Selected Agencies Tested Various Capabilities during 2006 Governmentwide Exercise."
221 Rep. No. GAO-13-763 (2013).
"Actions Are Needed to Improve DOD's Planning for a Complex Catastrophe."

In short, the dynamics from the Cuban Missile Crisis remain in place. The practical limits remain, thus potentially depriving decision makers with the information they need. And without that, escalation control becomes much harder to manage.

5. CONCLUSION

Nuclear escalation control, as a concept, attempts to avert a total and uncontrolled nuclear exchange. To do so, it relies on a decision maker choosing limited targeting options based on the situation that could compel an adversary to accept conflict termination terms that are favorable to that decision maker's national interests.

Such decision making, however, requires accurate information, in order to determine how much damage an adversary has taken, as well as to determine the damage his or her own forces. Yet the fog of war is as much a part of nuclear escalation control as it is conventional conflict. The information that a decision maker receives will often be incomplete, can be inaccurate, and can degrade as the conflict continues.

As we have seen, information management during the Cuban Missile Crisis was extremely challenging and deeply flawed, due to three principle shortcomings: collection failures, analytic bias, and vulnerabilities to the command, control, communications, and intelligence (C4I) infrastructure. These challenges all would have contributed to the "fog" President Kennedy would have been forced to peer through to determine which best course of action to take to terminate the conflict on favorable terms.

Failures in collection, driven by the sheer volume of information, robust denial and deception efforts by an adversary, or technical error on the part of any number of collection platforms can all result in incomplete or inaccurate information being processed by the intelligence community. An intelligence community cannot exploit information that it cannot see, and poor information provided to the intelligence community will in turn result in poor intelligence.

The intelligence community, then, would have processed that information. However, this analytical process was itself vulnerable to analytic bias. Poor analytic tradecraft and bureaucratic interference both distorted the information being provided to President Kennedy. Even if collection efforts had been perfect, this analytic bias would have likely resulted in distorted information being presented to Kennedy, as it was at numerous points before and during the crisis.

Finally, the command, control, communications, and intelligence infrastructure necessary for this collection, analysis, and transmission to Kennedy, as well as the infrastructure needed to transmit Kennedy's instructions once he decided to act, were extremely vulnerable to enemy attack. The communications infrastructure, the analytic facilities, and the command facilities were both finite in number and vulnerable to even a few nuclear weapons.

But even over the intervening decades, these issues persist. In examining numerous contemporary (or near contemporary) case studies, we can see how the same issues bedevil information management today. In particular, the vulnerability of continuity-of-government in the face of nuclear attack, persists. The institutional and bureaucratic pressures that prevented proper dispersal have not disappeared; indeed, the number of intelligence agencies headquartered in Washington D.C. has only grown. Ironically, this construction may result in dispersal simply because there are no more facilities left available in or around the District of Columbia.

An example of this would be the US Army's Cyber Operations Center, in Augusta, Georgia. However, given the number of nuclear delivery systems and warheads available to a near-peer adversary, this dispersal concept is likely obsolete. These

agencies could create more hardened facilities, but cost precludes building these facilities in a quantity or quality that is likely to serve the number and accuracy of modern nuclear delivery systems. Further, the growth in near-peer conventional precision strike systems means those adversaries could accomplish the same thing without crossing the nuclear threshold and may do so under the guise of conventional warfighting.

We must remain cognizant of these problems today for this very reason. Forecasting the future is a fraught process. As we have seen, such a process is inherently vulnerable to any number of analytic failures and biases. That said, perfect collection systems, a bias-free analytic process, and totally invulnerable C4I facilities all seem outside the realm of possibility.

Escalation control, at its core, is built around human decision making, yet the fog of war, omnipresent throughout history, will not suddenly disappear. But without accurate information to use while making that decision, national leaders cannot expect to make the best decision possible. And when it comes to nuclear escalation, such suboptimal decisions can have cataclysmic costs.

REFERENCES

"About DCGS-A." DCGS-A. Accessed April 17, 2017. https://dcgsa.army.mil/about/.

Aristotle, David Keyt, and Richard Robinson. Politics, books III and IV. Oxford: Clarendon Press, 2004.

Atherton, Kelsey. "The Army's Runaway Blimp Escaped Due To...Dead Batteries." *Popular Science*, February 16, 2016. Accessed November 16, 2016. http://www.popsci.com/this-one-cool-trick-could-save-billion-dollar-blimps.

Baran, Paul. *On Distributed Communications*. Santa Monica, CA: Rand, 1964.

Barrett, David M., and Max Holland. *Blind over Cuba*. College Station: Texas A & M University Press, 2012.

Bartles, Charles K. "Getting Gerasimov Right." *Military Review*, January 1, 2016.

Blair, Bruce G. *The Logic of Accidental Nuclear War*. Washington, D.C.: Brookings Institution, 1993.

Bolger, Daniel P. "Maneuver Warfare Reconsidered," in Maneuver Warfare Anthology ed. Richard D. Hooker, Jr. (CA: Presidio Press, 1993).

Bracken, Paul J. *The Command and Control of Nuclear Forces*. New Haven: Yale University Press, 1983.

---------- "The Intersection of Cyber and Nuclear War." RealClearDefense. January 17, 2017. Accessed April 12, 2017 http://www.realcleardefense.com/articles/2017/01/17/the_intersection_of_cyber_and_nuclear_war_110646.html.

Brennan, John O. "Remarks as Prepared for Delivery by Central Intelligence Agency Director John O. Brennan at the 9/11 Memorial Museum in New York City." Speech, 9/11 Memorial Museum, New York, September 26, 2016.

Budiansky, Stephen. *Code Warriors: NSA's Codebreakers and the Secret Intelligence War against the Soviet Union*. New York: Alfred A. Knopf, 2016.

Burr, William. The Nixon Administration, the SIOP, and the Search for Limited Nuclear Options, 1969-1974. November 23, 2005. Accessed April 17, 2017. http://nsarchive.gwu.edu/NSAEBB/NSAEBB173/.

Carmichael, Scott W. *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy*. Annapolis, Maryland: Naval Institute Press, 2007.

Carter, Ashton B., John D. Steinbruner, and Charles A. Zraket. *Managing Nuclear Operations*. Washington, D.C.: Brookings Institution, 1987.

Condon-Rall, Mary Ellen. *Attack on the Pentagon: The Medical Response to 9/11*. Fort Detrick, Maryland: Borden Institute, 2011.

Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. Boston: Little, Brown, 2002.

Crawford, Sarah. "Air Force Nuclear Command Center at BAFB will employ 236." Shreveporttimes.com. April 04, 2017. Accessed April 12, 2017. http://www.shreveporttimes.com/story/news/2017/04/03/air-force-nuclear-command-center-activated-barksdale-employ-236/99996698/.

Creveld, Martin Van. *Command in War*. Cambridge, MA: Harvard University Press, 1985.

CNN. "Most Damaging US Spy You've Never Heard of." Accessed October 16, 2016. http://www.cnn.com/2016/07/06/us/declassified-ana-montes-american-spy-profile/.

Chicago Tribune. "Destroyers Close in on Seized Ship." February 15, 1963.

Cremans, C. D., J. K. Moriarty, and J. Porturo. *The Evolution of US Strategic Command and Control and Warning, 1945-1972*. Arlington, Virginia: Institute for Defense Analyses, 1975.

Cooper, Jeffrey R. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*. Washington, DC.: Center for the Study of Intelligence, 2005.

Dobbs, Michael. *One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War*.

Dodge, Michela, and John Venable. "Why the United States Needs an LRSO Capability." Why the United States Needs an LRSO Capability. June 17, 2016. Accessed November 30, 2016. http://www.heritage.org/research/reports/2016/06/why-the-united-states-needs-an-lrso-capability.

Ducharme, Douglas R. "Measuring Strategic Deterrence: A Wargaming Approach." *Joint Forces Quarterly*, July 2016.

Edwards, Jim. "PLANET SELFIE: We're Now Posting A Staggering 1.8 Billion Photos Every Day." Business Insider. May 28, 2014. Accessed November 27, 2016. http://www.businessinsider.com/were-now-posting-a-staggering-18-billion-photos-to-social-media-every-day-2014-5.

Englejohn, Earl D. "For a Standard Defector Questionnaire." *Studies in Intelligence* 7, no. Summer (1963): 53-55. Accessed September 29, 2016. https://catalog.archives.gov/id/7283510.

Finch, James B. "Bringing Crisis Stability Down to Earth." *Joint Forces Quarterly*, January 2015.

George, Alice L. *Awaiting Armageddon: How Americans Faced the Cuban Missile Crisis*. Chapel Hill: University of North Carolina Press, 2003.

Garthoff, Raymond L. *Detente and confrontation: American-Soviet relations from Nixon to Reagan*. Washington, D.C.: Brookings Institution, 1994.

Gertz, Bill. "China Continuing Cyber Attacks on U.S. Networks." Washington Free Beacon. Accessed November 17, 2016. http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/.

Glanz, James, Sebastian Rotella, and David Sanger. "In 2008 Mumbai Attacks, Piles of Spy Data, but an Uncompleted Puzzle." *The New York Times*, December 21, 2014. Accessed November 16, 2016. http://www.nytimes.com/2014/12/22/world/asia/in-2008-mumbai-attacks-piles-of-spy-data-but-an-uncompleted-puzzle.html?_r=0.

Gleichauf, Justin F. "A Listening Post in Miami." *Studies in Intelligence* 44, no. 5 (2001): 49-53. Accessed September 29, 2016. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter_spring01/article06.pdf.

Gonzales, David. "Carter and Powell Cast Doubt on Bioarms in Cuba." *The New York Times*, May 14, 2002. Accessed October 16, 2016.

Gormley, Dennis M., Andrew S. Erickson, and Jingdong Yuan. "A Potent Vector: Assessing Chinese Cruise Missile Developments." *Joint Forces Quarterly*, September 2015.

Goure, Dan. "U.S. Experience in Iraq Can Teach NATO How To Hunt Russia's "Little Green Men"." The National Interest. September 9, 2016. Accessed November 17, 2016. http://nationalinterest.org/blog/the-buzz/us-experience-iraq-can-teach-nato-how-hunt-russias-"little-17637.

Gribkov, A. I., William Y. Smith, and Alfred Friendly. *Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis*. Chicago: Edition Q, 1994.

Grossman, Elaine. "Reviving Cold War Doomsday Devices Could Patch America's Broken Nuclear Controls." War Is Boring. February 22, 2017. Accessed April 12, 2017. http://warisboring.com/reviving-cold-war-doomsday-devices-could-patch-americas-broken-nuclear-controls/#.y3lxmv7wb.

Harris, Shane. The Daily Beast. Accessed November 16, 2016. http://www.thedailybeast.com/articles/2016/09/10/the-time-u-s-spies-thought-al-qaeda-was-ready-to-nuke-d-c.html.

--------. The Daily Beast. Accessed November 17, 2016. http://www.thedailybeast.com/articles/2015/07/18/russian-hackers-target-the-pentagon.html.

Hayman, Stephen. "Photos, Photos Everywhere." *The New York Times*, July 23, 2015. Accessed November 27, 2016. http://www.nytimes.com/2015/07/23/arts/international/photos-photos-everywhere.html?_r=0.

Hopkins, J. C., and Sheldon A. Goldberg. *The Development of Strategic Air Command, 1946-1986 (the Fortieth Anniversary History)*. Offutt Air Force Base, Neb.: Office of the Historian, Headquarters Strategic Air Command, 1986.

Houghton, Vince, and Nate Jones. "Able Archer 83: An Interview with Nate Jones · SpyCast." Spycast. November 15, 2016. Accessed November 28, 2016. https://www.spymuseum.org/multimedia/spycast/episode/able-archer-83-an-interview-with-nate-jones/.

Immerman, Richard H. "Intelligence and the Iraq and Afghanistan Wars." *Political Science Quarterly* 131, no. 3 (2016): 477-501. doi:10.1002/polq.12489.

Jacobsen, Annie. *The Pentagon's Brain*. New York, NY: Little, Brown and Company, 2016.

Jehl, Douglas. "Senate Panel Is Set to Vote On Bolton Nomination Today." *The New York Times*, May 12, 2005. Accessed October 16, 2016. http://www.nytimes.com/2005/05/12/politics/senate-panel-is-set-to-vote-onbolton-nomination-today.html.

Jervis, Robert. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*. Ithaca: Cornell University Press, 2010.

Kaplan, Fred M. The wizards of Armageddon. Stanford, CA: Stanford University Press, 1991.

Kennedy, Merrit. "Report: U.S. Nuclear System Relies On Outdated Technology Such As Floppy Disks." NPR. May 26, 2016. Accessed April 11, 2017. http://www.npr.org/sections/thetwo-way/2016/05/26/479588478/report-u-s-nuclear-system-relies-on-outdated-technology-such-as-floppy-disks.

Kiesling, Eugina C. ""On War: Without the Fog"." Military Review, Sept. & Oct. 2001.

Kofman, Michael. "Russian Hybrid Warfare and Other Dark Arts." War on the Rocks. March 11, 2016. Accessed December 11, 2016. http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/.

Krugler, David F. *This Is Only a Test: How Washington, D.C. Prepared for Nuclear War*. New York: Palgrave Macmillan, 2006.

Lattel, Brian. "New Revelations about Cuban Spy Ana Montes." *Miami Herald*, August 2, 2014. Accessed October 16, 2016. http://www.miamiherald.com/opinion/issues-ideas/article1978099.html.

Layton, B.E.. "The Joint Debriefing of a Cuban." *Studies in Intelligence* 7, no. Summer (1963): 57-61. Accessed September 29, 2016. https://www.cia.gov/library/readingroom/docs/DOC_0000608373.pdf.

Lewis, Jeffrey. "Cruise Missile Proliferation." Arms Control Wonk. Accessed November 16, 2016. http://www.armscontrolwonk.com/archive/206749/cruise-missile-proliferation/.

----------. "Iskander, INF and Kaliningrad." Arms Control Wonk. Accessed November 27, 2016.

http://www.armscontrolwonk.com/archive/1202123/iskander-inf-and-kaliningrad/.

Lind, William S. *Maneuver Warfare Handbook*. Boulder, CO: Westview Press, 1985.

Liepman, Andrew, and Howard Gordon. "How Accurate Is TV's Portrayal of Terrorism?" Rand Corporation (audio blog), May 6, 2016. Accessed April 16, 2017. https://www.rand.org/multimedia/audio/2015/05/06/how-accurate-is-tvs-portrayal-of-terrorism.html.

Marquis, Christopher. "Bush Plans to Tighten Sanctions on Cuba, Not Ease Them.' *The New York Times*, May 15, 2002. Accessed October 16, 2016. http://www.nytimes.com/2002/05/15/world/bush-plans-to-tighten-sanctions-on-cuba-not-ease-them.html.

McCarthy, Mary. "The National Warning System: Striving for an Elusive Goal," Defense Intelligence Journal 3 (1994).

Morgan, Forrest E. *Dangerous Thresholds: Managing Escalation in the 21st Century*. Santa Monica, CA: RAND Project Air Force, 2008.

Miller, Judith. "Washington Accuses Cuba Of Germ-Warfare Research." *The New York Times*, May 7, 2002. Accessed October 16, 2016.

New York Times. "The Cuban Shootdown." *The New York Times*, February 27, 1996. Accessed October 16, 2016. http://www.nytimes.com/1996/02/27/opinion/the-cuban-shootdown.html.

Nieves, Gail Epstein. "Basulto Testifies on Role as Anti-Castro Operative." *The Miami Herald*, March 13, 2001. Accessed October 16, 2016. http://www.latinamericanstudies.org/exile/basulto-testifies.htm.

Pardoe, Blaine Lee. The fires of October: the planned US invasion of Cuba during the missile crisis of 1962. Stroud, England: Fonthill, 2013.

PBS. 9-11: Inside the Pentagon. Accessed November 17, 2016. http://www.pbs.org/program/911-inside-pentagon/.

---- *Mumbai Massacre*. PBS Secrets. November 25, 2009. Accessed November 16, 2016. http://www.pbs.org/wnet/secrets/mumbai-massacre-watch-the-full-episode/536/.

Person, Robert. "6 Reasons Not to Worry about Russia Invading the Baltics." *The Washington Post*, November 12, 2015. Accessed November 17, 2016.

https://www.washingtonpost.com/news/monkey-cage/wp/2015/11/12/6-reasons-not-to-worry-about-russia-invading-the-baltics/.

Polk, Robert B. "A Critique of the Boyd Theory: Is It Applicable to the Army." M.A. thesis, School of Advanced Military Studies, 1999.

Popkin, Jim. "Ana Montes Did Much Harm Spying for Cuba. Chances Are, You Haven't Heard of Her." *The Washington Post*, April 21, 2013. Accessed 2016.

Porche, Issac R., III, Bradley Wilson, Eric-Elizabeth Johnson, Shane Tierney, and Evan Saltzman. *Data Flood: Helping the Navy Address the Rising Tide of Sensor*. Santa Monica: Rand Corporation, 2014.

Rand Corporation. "Paul Baran and the Origins of the Internet." Accessed November 26, 2016. http://www.rand.org/about/history/baran.html.

Read, Thornton, and Klaus Knorr. *Limited Strategic War*. New York: Published for the Center of International Studies, Princeton University, by Praeger, 1962.

Rohter, Larry. "Cuba Blames U.S. in Downing of Planes." *The New York Times*, February 27, 1996. Accessed October 16, 2016.

---------"Cuba's 2 Steps Back." *The New York Times*, February 29, 1996. Accessed October 16, 2016. http://www.nytimes.com/1996/02/29/world/cuba-s-2-steps-back.html.

Scarborough, Rowan. *"Problems with Army's battlefield intel system unresolved after two years."* The Washington Times. May 01, 2014. Accessed April 17, 2017. http://www.washingtontimes.com/news/2014/may/1/problems-with-armys-battlefield-intel-system-unres/.

Setear, J. K. Simulating the Fog of War. Santa Monica: Rand Corporation, 1989.

Sterk, Richard. "JLENS Will Be Produced, but Not in Numbers Once Expected." *Forecast International*, October 10, 2016. Accessed November 16, 2016. http://blog.forecastinternational.com/wordpress/jlens-will-be-produced-but-not-in-numbers-once-expected/.

Stewart, Phil, and Yeganeh Torbati. "Runaway Military Blimp Wreaks Havoc in US." *Sydney Morning Herald*, October 29, 2015. Accessed November 16, 2016. http://www.smh.com.au/world/runaway-military-blimp-loose-over-us-20151028-gklaeq.html.

Sturm, Thomas A. *The Air Force and The Worldwide Military Command and Control System*. Washington, DC: USAF Historical Division Liaison Office, 1966.

Taylor, Maxwell D. *The Uncertain Trumpet*. New York: Harper, 1960.

Thomas, John F. "Cuban Refugees in the United States." *International Migration Review* 1, no. 2 (1967): 46. doi:10.2307/3002808.

Times of India. Pak Might Soon Move Troops from Border with India" Accessed November 17, 2016. http://timesofindia.indiatimes.com/india/Pak-might-soon-move-troops-from-border-with-India/articleshow/4660681.cms.

Toler, Aric. "How These Adorable Puppies Exposed Russian Involvement in Ukraine - Bellingcat." Bellingcat. March 13, 2015. Accessed November 27, 2016. https://www.bellingcat.com/news/uk-and-europe/2015/03/11/vreditel-sobaka/.

Treisman, Daniel. "Why Putin Took Crimea." *Foreign Affairs*, May/June 2016.

Tucker, Patrick. "Hacking Into Future Nuclear Weapons: The US Military's Next Worry." Defense One. December 29, 2016. Accessed April 12, 2017. http://www.defenseone.com/technology/2016/12/hacking-future-nuclear-weapons-us-militarys-next-worry/134237/?oref=search_command and control.

US Air Force, Air Force Space Command. December 2016. Accessed April 12, 2017. http://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/249024/advanced-extremely-high-frequency-system/.

US Central Intelligence Agency. Director of Central Intelligence. *Iraq's Continuing Programs for Weapons of Mass Destruction*. Washington, DC, 2002.

-------- *Discussion in Secretary Rusk's Office at 12 O'Clock, 21 August 1962*.

--------"Eyes Only McCone from Carter." Marshall S. Carter to John McCone. September 8, 1962.

---------Director Central Intelligence. *Memorandum on Cuba, August 20 1962*. By John A. McCone.

---------*Memorandum of Discussion with Mr. McGeorge Bundy, Friday, 5 October 1962, 5:15pm*. By John McCone.

--------- *Memorandum by Lyman B. Kirkpatrick.* 1963.

----------*"Memorandum of MONGOOSE Meeting Held on Thursday, October 4, 1962"* 1962.

---------*Soviet Military Buildup in Cuba.* October 21, 1962. CIA Report for Heads of State, Washington, D.C.

US Central Intelligence Agency. Inspector General's Office. *Inspector General's Survey of the Cuban Operation and Associated Documents*. Washington, DC: Central Intelligence Agency Inspector General, November 1962.

US Congress, Select Committee on Governmental Operations, *Foreign and Military Intelligence,* S. Rept. 94-755, 94th Congress, 2nd Session, 1976.

US Defense Information Systems Agency. Comptroller. *Operation and Maintenance, Defense-Wide Fiscal Year (FY) 2017 President's Budget*. Fort Meade, Maryland: DISA, 2016.

US Department of the Air Force. Curtis E. LeMay Center for Doctrine Development. *Practical Design: The Coercion Continuum*. 2012.

US Department of the Army. *Interrogation Guide for Cuba*. Washington, DC: Department of the Army, 1962.

US Department of Defense. Headquarters, International Security Assistance Force Joint command. Training Requirements to Maintain Proficiency on Distributed Common Ground System-Army (DCGS-A). By Christopher Ballard.

US Department of Defense. Intelligence Science Board, "Integrating Sensor-Collected Intelligence," Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, November 2008.

----------. Office of the Secretary of Defense. "Anzoategui Affair." Robert S. McNamara and Roswell L. Gilpatric to Director John McCone. February 27, 1963. Office of the Secretary of Defense, Washington, DC.

----------. Office of the Secretary of Defense. "Nuclear Weapons Employment Policy." 10 April 1974. Washington, D.C.

---------"Department of Defense 101." Accessed November 21, 2016. http://www.defense.gov/About-DoD/DoD-101.

----------. Operation Test and Evaluation Command. Director, Operational Test and Evaluation FY 2015 Annual Report. By J. Michael Gilmore.

US Defense Intelligence Agency. “History.” Accessed November 16, 2016. http://www.dia.mil/About/History/.

---------"This Day in History: Sept. 11, 2001." 2015. Accessed November 15, 2016. http://www.dia.mil/News/Articles/Article/616903/this-day-in-history-sept-11-2001/.

US Federal Emergency Management Agency. *Recovery from Nuclear Attack, and Research and Action Programs to Enhance Recovery Prospects* (1979).

US Government Accountability Office. Rep. No. GAO-08-185 (2007). "Selected Agencies Tested Various Capabilities during 2006 Governmentwide Exercise."

---------Rep. No. GAO-13-763 (2013). "Actions Are Needed to Improve DOD's Planning for a Complex Catastrophe."

---------Rep. No. GAO-16-468 (2016). " Federal Agencies Need to Address Aging Legacy Systems."

US Library of Congress. Congressional Research Service. *Nuclear Command and Control: Current Programs and Issues*. By Robert D. Critchlow. 5-6.

US National Security Agency. Finding a Home for the AFSA 1949-1952." *Cryptolog*, April 1985, 1-2.

US National Security Council. “Notes on NSC Meeting 14 February 1969.” Washington, D.C.

US Special Operations Command. *"Little Green Men:" A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*. 2015.

US White House. Office of the National Security Advisor. Memorandum for the President “Nuclear Policy.” Henry A. Kissinger. January 7, 1974. Office of the President, Washington, D.C.

Von Clausewitz, Carl, Michael Howard, and Peter Paret. On war. Norwalk, CT: Easton Press, 1991.

Weisman, Steven R. "Ex-Official Says Nominee Bullied Analyst on Arms." *The New York Times*. April 13, 2005. Accessed October 16, 2016. http://www.nytimes.com/2005/04/13/world/exofficial-says-nominee-bullied-analyst-on-arms.html.

Wilgenbush, Ronald C., and Alan Heisig. "Command and Control Vulnerabilities to Communications Jamming." *Joint Forces Quarterly*, April 2013.

Willman, David. "How a $2.7 Billion Air-defense System Became a 'Zombie' Program." *The Los Angeles Times*, September 24, 2015. Accessed November 16, 2016. http://graphics.latimes.com/missile-defense-jlens/.

Wong, Joon Ian. "Bitcoin-Style Security May Soon Guard US Nukes and Satellites." Defense One. October 11, 2016. Accessed April 12, 2017. http://www.defenseone.com/technology/2016/10/bitcoin-style-security-may-soon-guard-us-nukes-and-satellites/132235/?oref=search_command and control.

Zuckerman, Edward. *The Day after World War III*. New York: Viking Press, 1984.